

Our Humanity Exposed

Predictive Modelling in a Legal Context

Stanley Greenstein

Academic dissertation for the Degree of Doctor of Laws in Law and Information Technology at Stockholm University to be publicly defended on Thursday 1 June 2017 at 10.00 in De Geersalen, Geovetenskapens hus, Svante Arrhenius väg 14.

Abstract

This thesis examines predictive modelling from the legal perspective. Predictive modelling is a technology based on applied statistics, mathematics, machine learning and artificial intelligence that uses algorithms to analyse big data collections, and identify patterns that are invisible to human beings. The accumulated knowledge is incorporated into computer models, which are then used to identify and predict human activity in new circumstances, allowing for the manipulation of human behaviour.

Predictive models use big data to represent people. Big data is a term used to describe the large amounts of data produced in the digital environment. It is growing rapidly due mainly to the fact that individuals are spending an increasing portion of their lives within the on-line environment, spurred by the internet and social media. As individuals make use of the on-line environment, they part with information about themselves. This information may concern their actions but may also reveal their personality traits.

Predictive modelling is a powerful tool, which private companies are increasingly using to identify business risks and opportunities. They are incorporated into on-line commercial decision-making systems, determining, among other things, the music people listen to, the news feeds they receive, the content people see and whether they will be granted credit. This results in a number of potential harms to the individual, especially in relation to personal autonomy.

This thesis examines the harms resulting from predictive modelling, some of which are recognized by traditional law. Using the European legal context as a point of departure, this study ascertains to what extent legal regimes address the use of predictive models and the threats to personal autonomy. In particular, it analyses Article 8 of the European Convention on Human Rights (ECHR) and the forthcoming General Data Protection Regulation (GDPR) adopted by the European Union (EU). Considering the shortcomings of traditional legal instruments, a strategy entitled 'empowerment' is suggested. It comprises components of a legal and technical nature, aimed at levelling the playing field between companies and individuals in the commercial setting. Is there a way to strengthen humanity as predictive modelling continues to develop?

Keywords: *predictive modelling, predictive analytics, profiling, big data, algorithm, surveillance, privacy, autonomy, identity, digital identity, data privacy, human rights, data protection, European Convention on Human Rights, Data Protection Directive, General Data Protection Regulation (GDPR), empowerment.*

Stockholm 2017

<http://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-141657>

ISBN 978-91-7649-748-7
ISBN 978-91-7649-749-4



Department of Law

Stockholm University, 106 91 Stockholm

OUR HUMANITY EXPOSED
Predictive Modelling in a Legal Context

Stanley Greenstein



Our Humanity Exposed

Predictive Modelling in a Legal Context

Stanley Greenstein

©Stanley Greenstein, Stockholm University 2017

ISBN printed 978-91-7649-748-7

ISBN PDF 978-91-7649-749-4

Cover image: Simon Dobrzynski and Indra Jungkvist

Photo of the author: Staffan Westerlund

Printed by Universitetservice US-AB, Stockholm 2017

Distributor: Department of Law, Stockholm University

To my family - Anna, Levi,
Nomie and Jonah.

Acknowledgements

I have heard that writing a thesis is like running a marathon. Having run two marathons I feel that I am in a position to comment. There are similarities in that both are long, they require lots of training and endurance and they both have many ups and downs. However, there are some major differences. A marathon has race officials to show the way, the finish line is clearly demarcated and it is not a team effort. This is definitely not the case when writing a thesis.

I would therefore like to take this opportunity to thank my thesis team. I would like to start by extending my appreciation to my supervisor, Peter Wahlgren (Professor in Law and Information Technology), who provided the legal perspective and who was always available to discuss both legal and technical developments. A big thank you also to my deputy supervisor Jussi Karlgren (Adjunct Professor in Language Technology), who provided the technical perspective and who was able to explain the intricate complexities of technical phenomena in an understandable manner. Thank you both also for translating this thesis into Swedish. During the second to last year of writing, the three of us would meet regularly to discuss what I had written and plan the way forward. These meetings were insightful in that I experienced what it is like to review a text with a lawyer on one side and a computer scientist on the other. It was motivating, it was informative, it was frustrating but most of all it was fun! Thank you!

I would also like to express my gratitude to Cecilia Magnusson Sjöberg (Professor in Law and Information Technology). Thank you for your patience over the years for all those occasions I barged into your office without warning in order to get advice on one matter or another. Most of all thank you for giving me the freedom and space during these past six months so that I could focus entirely on completing this thesis. I am fully aware that this could not have been easy considering your responsibilities for making sure that all lecturing and examination duties were covered.

I would like to thank Peter Seipel (Professor Emeritus in Law and Information Technology), who took an interest in my project early on and, as a

pioneer in the field of legal informatics, made the path easier for the rest of us, in this the most interesting and relevant field of law. A special thank you also to my present colleagues at the Swedish Law and Informatics Research Institute (IRI): Liane Colonna, Maeve Dion, Mårten Edenroth, Ängla Eklund, Alexandra Sackemark, Madeleine Sandberg and Christine Storr. Thank you for making sure that the daily existence as a doctoral student was not as lonely as it sometimes is made out to be.

A special thank you also to Mark Klamberg for taking on the role of ‘opponent’ at my final seminar, for providing me with all the feedback and constructive criticism, especially within the area of international law and for taking the time to address all my follow-up queries.

This thesis would not have been possible without the support of the Faculty of Law, Stockholm University. After receiving the opportunity to embark on doctoral studies, the Faculty of Law allowed me to pursue my doctoral studies within my appointment as an Adjunkt, in effect financing this project. Many thanks also to the Stiftelsen av den 28 oktober 1982 for the generous yearly book grant, allowing me to purchase the necessary reading material.

Many thanks must also be given to a number of individuals at the Faculty of Law, Stockholm University. First, my appreciation to Åsa Hellstadius, for providing suggestions regarding the structuring of this thesis, for assisting me with the thesis template and most of all for reassuring me that the time was ripe to proceed with the opposition of this thesis. Also, considering that this thesis delved into areas of law that I am not a specialist in, I would like to thank Helene Andersson, Antonina Bakardjieva-Engelbrekt, Claes Granmar, Jaan Paju, Martin Ratcovich, Pål Wrangé, Torben Spaak and Mauro Zamboni. In addition, many thanks to Bengt Baeckmark, Laura Carlson, Jonas Ekfeldt, Ulf Färjare, Agita Akule Larsson, Lydia Lundstedt, Grant McWilliams, Dan Olsson, Panagiotis Papapetrou, Christina Ramberg, Ida Söderberg Tah, Stafan Westerlund and Roger Persson-Österman. You have all helped me in some way or another and at some point in time. You have all been generous with your time, support and words of encouragement. Thank you!

A special thank you also to Lee Bygrave of the Senter for rettsinformatikk, Department of Private Law, Oslo University. We would meet at the annual Nordic Conference on Law and IT where you would always show an interest in my progress, offer valuable insights and most importantly not hold back as far as providing words of encouragement was concerned. Tusen takk!

In addition, the cover of this thesis would be blank were it not for the creative efforts of Simon Dobrzynski and Indra Jungkvist. Thank you both for all

the time spent on enhancing the graphic impression of this thesis. A huge thank you also to Laura Chadwick, who on extremely short notice agreed to proof read my thesis, providing valuable input and improving the overall impression of the text markedly. Your assistance with this thesis was invaluable! All mistakes in this text should be attributed to changes made by me after it was proof read. I would also like to thank the staff of the Stockholm University library for helping with the production of this thesis.

On a more personal note, I would like to thank my in-laws, Kalle and Eva-Lii, for making life a lot easier in many respects since I moved to Sweden. Many thanks also to Indra and Simon for the warmth you have both shown over the years. Finally, a special thank you to my wife and soulmate Anna, for the love and companionship over the years. You have always been positive about this project even when faced with a partner that has on occasion been 'a little less positive'. Thank you for polishing the cover texts and Swedish translation – when it comes to working with text, you are in a class of your own. Thank you also for bearing the major load of family life during the run up to the completion of this thesis. Finally, I would probably not have survived this excruciating process were it not for my children Levi, Nomie and Jonah. Your mere existence has constantly put things into perspective and reminded me that this is just a thesis, nothing more!

Stockholm, 24th April 2017.

Stanley Greenstein

Contents

1	Introduction	21
1.1	Problem Identification.....	22
1.2	Overall Objectives	26
1.3	Research Questions.....	29
1.4	Method and Material	30
1.5	Definitions.....	41
1.6	Perspectives	48
1.7	Scope and Delimitation	52
1.8	Previous Research	55
1.9	Positive Aspects of Predictive Modelling.....	61
1.10	The Dangers Associated with Predictive Modelling	64
1.11	Structural Overview.....	68
2	'The Black Box'.....	69
2.1	Introductory Remarks.....	69
2.2	The Predictive Modelling Process Outlined.....	70
2.3	The Development of Technology	74
2.3.1	The Features of Data.....	74
2.3.2	'Big Data'	75
2.3.3	The Sources of Big Data	79
2.3.3.1	Trace Data.....	80
2.3.3.2	Sensor Data	82
2.3.3.3	Data from Inferences	85
2.3.3.4	Clickstream Data.....	86
2.3.3.5	Surveillance Data	87
2.3.3.6	Social Engineering.....	88
2.3.3.7	Insight Data	89
2.3.4	Big Data on the Rise.....	90
2.3.5	Big Data Offshoots.....	93
2.3.6	Theory Driven versus Data Driven Approaches.....	94
2.3.6.1	Databases and the Theory Driven Approach.....	94

2.3.6.2	Databases and a Data Driven Approach	95
2.3.7	Knowledge Representation.....	96
2.4	From Profiling to Predictive Modelling	97
2.4.1.1	Profiling	97
2.4.1.2	Profiling versus Predictive Modelling	100
2.4.1.3	Predictive Analytics and the Predictive Model.....	102
2.4.1.4	Building a Predictive Model	105
2.4.1.5	Notable Considerations of Control.....	105
2.4.1.6	Predictive Modelling Applied.....	112
2.4.1.6.1	The Social Media	113
2.4.1.6.2	Computational Linguistics.....	114
2.4.1.6.3	Target.....	116
2.4.1.6.4	Hewlett-Packard	118
2.5	Influencing Human Behaviour.....	118
2.6	Summary and Conclusions	122
3	A Theoretical Background.....	125
3.1	Introductory Remarks.....	125
3.2	Surveillance and Social Change.....	126
3.3	A Context for Surveillance	130
3.3.1	Panopticism.....	131
3.3.2	Orwell and Nineteen Eighty-Four.....	134
3.3.3	Kafka and The Trial	135
3.3.4	The Panspectron	136
3.3.5	The Superpanopticon	137
3.3.6	The Surveillant Assemblage.....	139
3.3.7	The Commercial Dimension	141
3.3.8	The Minority Report.....	143
3.3.9	Concluding Remarks.....	144
3.4	Autonomy and Identity.....	147
3.4.1	A Philosophical Background	147
3.4.2	Autonomy.....	152
3.4.2.1	Autonomy Defined	153
3.4.2.2	The Value of Autonomy.....	156
3.4.2.3	Autonomy and Democracy	159
3.4.2.4	Autonomy and the Law	161
3.4.2.5	Autonomy and Technology.....	162
3.4.3	Concluding Remarks.....	164

3.4.4	Identity	168
3.4.4.1	Defining Identity.....	170
3.4.4.2	Abstract Models of Identity	171
3.4.4.2.1	The 'I', the 'Implicit Me' and the 'Explicit Me'	171
3.4.4.2.2	Identity as Three Tiers	172
3.4.4.2.3	Identity and Philosophy	172
3.4.4.2.4	Identity and Psychology.....	173
3.4.4.3	A Common Denominator	173
3.4.4.4	The 'Digital Identity' versus the 'True Identity'	175
3.4.5	Concluding Remarks.....	178
3.5	Summary and Conclusions	181
4	Predictive Modelling and the Potential Harms	183
4.1	Introductory Remarks.....	183
4.2	Privacy.....	184
4.2.1	Privacy in General.....	185
4.2.1.1	Traditional Approaches to Conceptualizing Privacy.....	187
4.2.1.2	Alternative Approaches to Privacy	190
4.2.1.2.1	A Privacy Taxonomy	190
4.2.1.2.2	Contextual Integrity.....	191
4.2.2	Remarks	193
4.3	Reputation	194
4.3.1	Reputation and the Law.....	197
4.3.2	Reputation in the Era of the Internet.....	198
4.3.2.1	Netflix.....	200
4.3.2.2	You Are What You Drive.....	201
4.3.2.3	Creditworthiness in China	202
4.3.3	Remarks	203
4.4	Discrimination	204
4.4.1	On a European Level.....	206
4.4.2	The Context of Price Discrimination	208
4.4.3	Discrimination on a Technical Level	211
4.4.4	Remarks	212
4.5	Self-Censorship.....	213
4.5.1	Remarks	216
4.6	Deindividualization	218
4.6.1	Remarks	220
4.7	Loss of Agency.....	221

4.7.1	Agency and Law	222
4.7.2	Remarks	225
4.8	Stereotyping	226
4.8.1	The Computer Assisted Passenger Pre-screening System ..	228
4.8.2	Stereotyping and the Law	229
4.8.3	Remarks	230
4.9	Manipulation	231
4.9.1	Unfair Commercial Practices Directive	234
4.9.2	Remarks	235
4.10	Lost Human Dignity	235
4.10.1	Human Dignity and Law	238
4.10.2	American Constitutional Law	239
4.10.3	European Patent Law	240
4.10.4	Remarks	241
4.11	Lost Human Identity	241
4.11.1	The Narrative Identity	242
4.11.2	The Database Discourse	243
4.11.3	Accompanying Themes	245
4.11.4	Remarks	247
4.12	Summary and Conclusions	248
5	The Data Privacy Legal Regime	249
5.1	Introductory Remarks	249
5.2	Two Actors within the European Legal Space	250
5.2.1	The Council of Europe (CoE)	250
5.2.2	The European Union (EU)	251
5.2.3	The Council of Europe and European Union Regulatory Interplay	253
5.3	Data Privacy	258
5.3.1	The Symbiosis Between Data Protection and Privacy	259
5.3.2	The Tension Between Council of Europe and European Union	263
5.4	International Law	264
5.4.1	Human Rights Law	265
5.4.2	Human Rights Protection at the Global Level	266
5.4.2.1	The Universal Declaration of Human Rights	267
5.4.2.2	International Covenant on Civil and Political Rights (ICCPR)	268

5.4.2.3	Customary International Law.....	269
5.4.3	Human Rights Protection at the Regional Level.....	270
5.4.3.1	European Convention on Human Rights.....	270
5.4.3.2	The European Court of Human Rights (ECtHR).....	271
5.4.3.3	Human Rights and Autonomy.....	273
5.4.3.4	The Protection of Private and Family Life in Article 8 ECHR	274
5.4.3.5	The Horizontal Effect.....	279
5.4.3.6	Case Law on the Right to Private Life.....	280
5.4.3.6.1	Autonomy.....	281
5.4.3.6.2	A Reasonable Expectation of Privacy.....	285
5.4.3.6.3	Data Protection.....	288
5.4.3.6.4	Access to Information.....	290
5.4.3.6.5	Collection of Personal Information.....	291
5.4.3.6.6	Mass Surveillance.....	294
5.4.4	Data Protection.....	295
5.4.4.1	The Development of Data Protection.....	297
5.4.4.1.1	Alan Westin.....	298
5.4.4.1.2	The Fair Credit Reporting Act.....	300
5.4.4.1.3	The HEW Committee.....	301
5.4.4.2	A Legal Framework.....	303
5.4.4.2.1	OECD Guidelines.....	303
5.4.4.2.2	Council of Europe Convention 108.....	306
5.4.4.3	The Data Protection Directive.....	307
5.4.4.3.1	Data Protection and Autonomy.....	309
5.4.4.3.2	The Principles of Data Protection.....	310
5.4.4.3.3	Articles 12(a) and 15 of the Data Protection Directive	313
5.4.4.4	The General Data Protection Regulation.....	316
5.4.4.4.1	Addressing Predictive Modelling.....	316
5.4.4.4.2	Article 22 General Data Protection Regulation.....	318
5.4.4.5	Court of Justice of the European Union and Mass Surveillance.....	320
5.5	Preliminary Analysis.....	322
5.5.1	Human Rights Analysis.....	323
5.5.2	Data Protection Analysis.....	325
5.6	Summary and Conclusions.....	336

6	A Strategy of Empowerment.....	339
6.1	Introductory Remarks.....	339
6.2	Empowerment Revisited.....	341
6.3	Theoretical Considerations.....	344
6.4	The Components of Empowerment.....	348
6.4.1	Knowledge.....	349
6.4.1.1	Background.....	350
6.4.1.2	A New Type of Knowledge.....	353
6.4.1.3	Data Protection and Knowledge.....	356
6.4.1.4	Remarks.....	358
6.4.2	Accountability.....	360
6.4.2.1	The Development of a Principle.....	361
6.4.2.2	The General Data Protection Regulation.....	363
6.4.2.3	Constituting Accountability.....	365
6.4.2.4	Transparency as an Element of Accountability.....	366
6.4.2.5	Remarks.....	369
6.4.3	A Duty of Care.....	370
6.4.3.1	Background.....	371
6.4.3.2	Status-Based versus Fact-Based Fiduciary Relationships..	373
6.4.3.3	Hedley Byrne.....	374
6.4.3.4	Remarks.....	376
6.4.4	A Right of Access.....	377
6.4.4.1	A Right to Know.....	378
6.4.4.2	The s3418 United States Senate Bill.....	379
6.4.4.3	The Right to Know Act.....	383
6.4.4.4	Remarks.....	384
6.4.5	Participation in the Legislative Process.....	386
6.4.5.1	Crowdsourcing Legislation.....	386
6.4.5.2	Crowdsourcing the Legislative Process.....	387
6.4.5.3	Other Societal Initiatives.....	389
6.4.5.4	Remarks.....	390
6.4.6	An Independent Supervisory Authority.....	392
6.4.6.1	The European Court of Human Rights Case Law.....	392
6.4.6.2	Remarks.....	395
6.4.7	Collective Redress.....	396
6.4.7.1	Development.....	396
6.4.7.2	The European Union.....	398

6.4.7.3	The Principles of Collective Redress	402
6.4.7.4	In the Context of Consent	404
6.4.7.5	Remarks.....	405
6.4.8	Soft Law.....	406
6.4.8.1	Background	406
6.4.8.2	The Solution.....	408
6.4.8.3	The Scope of the Guidelines.....	409
6.4.8.4	Remarks.....	410
6.4.9	Technology.....	411
6.4.9.1	Cases in Point	412
6.4.9.2	The Notion of Resistance	413
6.4.9.3	Embedding Legal Rules in Technology	415
6.4.9.3.1	Privacy by Design.....	416
6.4.9.3.2	Coding Accountability	419
6.4.9.3.3	Incorporating Interpretability	421
6.4.9.3.4	Blockchain Technology	422
6.4.9.4	Remarks.....	424
6.5	The 'Washington, D.C. Example' Revisited	425
6.6	Summary and Conclusions	427
7	Conclusion	431
7.1	Introduction.....	431
7.2	Summary of Findings.....	432
7.3	General Opinions	435
7.3.1	The European Legal Terrain.....	435
7.3.2	Relevance of Human Rights.....	437
7.3.3	Relevance of the Data Protection Framework	438
7.3.4	Technology.....	441
7.3.5	The Law	443
7.4	Looking Ahead.....	445
7.4.1	Future Research.....	445
7.4.2	General Observations.....	446
7.5	Final Thoughts.....	448
	Swedish Summary	451
	Table of Cases.....	453
	European Court of Human Rights (ECtHR)	453
	Court of Justice of the European Union (CJEU)	454

United States.....	455
Canada	455
United Kingdom	455
Netherlands	455
Table of Statutes, Conventions and Preparatory Works.....	456
European Union	456
Council of Europe	457
United Nations.....	458
OECD	458
United States.....	459
United Kingdom	459
Germany	460
Sweden.....	460
Australia	460
European Commission	461
Article 29 Working Party Documents	463
Other.....	463
Bibliography.....	465
Books.....	465
Journals and Articles.....	472
Electronic Sources and web pages.....	484

Abbreviations

AI	Artificial Intelligence
AmI	Ambient Intelligence
API	Application Programming Interface
CJEU	Court of Justice of the European Union
CoE	Council of Europe
DPD	Data Protection Directive
DDD	Data-Driven decision-making
EU Charter	Charter of Fundamental Rights of the European Union
GDPR	General Data Protection Regulation
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic, Social and Cultural Rights
IoT	Internet of Things
IP	Internet Protocol
ICT	Information and Communication Technology
ISP	Internet Service Provider
KDD	Knowledge Discovery in Databases
NSA	National Security Agency (US)
OECD	Organization for Economic Co-Operation and Development
PTS	Swedish Post and Telecom Authority
RFID	Radio Frequency Identity
TEU	Treaty of the European Union
TEFU	Treaty on the Functioning of the European Union
TTP	Trusted Third Party
UDHR	Universal Declaration of Human Rights
UDID	Unique Device Identifier
UN	United Nations
US	United States

1 Introduction

This is a thesis about technology and the law. The realization of the technology-centric society, with mobile technologies at the forefront of this development, has made the on-line environment accessible to the masses. Due to the popularity of the applications that can be utilized from within this environment, their ease of use, and the convenience associated with them, people are spending a large part of their lives in this environment. Whereas previously one could refer to the ‘on-line world’ and ‘off-line world’, this distinction is becoming blurred, as these two spheres continue to merge. The hyper-connectivity characterising present day society is being spurred on by the use of the digital media, such as the internet and more specifically the social media, which are increasingly being used not only for everyday means of communication and commercial purposes, but also as an instrument by means of which people are publically documenting their lives. There are many advantages associated with this on-line environment. The huge amounts of data being produced every second and contributing to the notion ‘big data’ hold great potential for humanity, with the phrase ‘data-driven innovation’ frequently used in commercial and technological settings. New technologies are being developed to exploit big data in order to extract previously inaccessible knowledge from it.

While the advantages to be gained from the exploitation by new technologies of big data are undisputed, their use also entails the exposure of individuals and society to risks and vulnerabilities, which multiply as the reliance on digital technologies increases. In addition, these new technologies are being incorporated into decision-making systems, which are increasingly relied on to make unsupervised decisions about humans and facilitate social control. The risks and vulnerabilities associated with this technology also increase as these technologies and systems become ambient and automated. Ultimately, this state of affairs requires a consideration as to what kind of society is desired, and how great a degree of human agency people are willing to acquiesce

to technology, in return for the benefits that it brings. Taking this argumentation one step further, and as society's reliance on decision-making systems increases, a concern is whether, in the near future, humans will even be in a position to have a say in the nature of the fabric of society, human agency having slowly been eroded as digital outputs determine the basis for social steering.

The more data modern decision-making systems can use to base their predictions on, the more accurate their predictions. Consequently, actors using these technologies have acquired an insatiable thirst for data. This in turn has resulted in a society characterised by surveillance. This surveillance is made possible by the architecture of the digital environment, which is essentially made up of computer hardware and code, and which allows for the tracking of a person's every move as they make their way through this coded space. Individuals' movements, ideas, preferences, habits, personality traits and opinions are monitored, recorded and stored for an infinite period of time, to be used at a later stage for some purpose that was not anticipated at the time of collection.

Humanity is presently faced with the challenge of addressing the hazards associated with relying too heavily on the outputs from decision-making systems without taking into account the pitfalls. The extent to which a positive outcome can be achieved will depend on the extent to which the relationship between law, technology and society can be exploited. It is within this context that predictive modelling forms the object of this legal examination.

1.1 Problem Identification

The catalyst of this thesis is the challenges posed by the increased reliance on digital decision-making systems, which incorporate predictive models. It is a common theme within the field of legal informatics that technology brings with it both advantages and disadvantages. This is no different as far as predictive modelling is concerned, which can be described as the incorporation of machine learning algorithms into models, which learn from historical data and have the ability to apply this novel insight on new data. The following is a formal definition of the predictive model:

A predictive model captures the relationships between predictor data and behaviour, and is the output from the predictive analytics process. Once a model has been created, it can be used to make new predictions about people (or other entities) whose behaviour is unknown.¹

At the core of this technology is statistics, mathematics, machine learning and artificial intelligence, a main component being the mathematical algorithm, which is, '[a] process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer'.² The algorithm examines data and finds correlations or links between those data. The unique aspect is that these correlations are invisible to human beings who do not have access to the required technology. From these correlations algorithms 'learn' not only to identify human behavioural preferences but also predict them.

The notion of modelling the future has become a reality. For example, an attempt to model everything is being led by the Swiss Federal Institute of Technology, where the FutureICT Project is building a single model that will be fed almost all available data in the world and will potentially be able to predict anything. The heart of the project is the Living Earth Simulator, a huge predictive model that will model economies, governments, cultural trends, epidemics, agriculture and technological developments by employing algorithms, and ultimately have insight into the future.³

Just as predictive models are being used to predict the weather, earthquakes and volcanic eruptions, so too can they be used to predict human behaviour. This is not particularly difficult considering that human beings are creatures of habit. It is estimated that habit accounts for forty-five percent of the choices humans make every day.⁴ The thrust, therefore, of predictive modelling is that

1 Finlay, Steven, *Predictive Analytics, Data Mining, and Big Data: Myths, Misconceptions and Methods*, Palgrave Macmillan, 2014, at p. 215.

2 English Oxford Living Dictionaries, *Algorithm*, available at <https://en.oxforddictionaries.com/definition/algorithm> (last accessed on 2017-03-19).

3 Weinberger, David, *The Machine That Would Predict the Future*, Scientific American, December 2011 at p. 32.

4 Neal, David T., Wood, Wendy and Quinn, Jeffrey M., *Habits- A Repeat Performance*, Current Directions in Psychological Science, August 2006, Vol. 15 no. 4, pp 198-202, at p. 198, available at <http://cdp.sagepub.com/content/15/4/198.abstract> (last accessed on 2016-11-25), see also Chi, Kelly Rae, *Why are Habits So Hard to Break?*, DukeToday, available at <https://today.duke.edu/2016/01/habits> (last accessed on 2016-11-25).

the greater the extent to which a human action has been repeated in the past, the greater the probability will be that it will occur in the future. It is on this premise that algorithms, using machine-learning techniques, search data and identify examples of human actions, acquiring the ability to assess the probability of these actions re-occurring in the future.

Predictive models determine a considerable amount of human interaction with the digital environment: they determine the content that an individual sees or does not see, they determine what an individual listens to, they determine who an individual will meet, they determine whether an individual will be considered for a job or not, they determine whether an individual is a credit risk, they determine whether an individual is a security risk and they determine the health status of a person, to mention but a few applications. Ultimately, predictive models make decisions about humans.

The power emanating from the access to predictive models increases as the knowledge they identify is combined with the behavioural sciences, which provide even greater insight into human behaviour. It has been stated that, '[w]e live in an age of psychology and behavioural economics – the behavioural sciences'.⁵ Consequently, with this insight into human behaviour, comes power, as the ability to identify human behaviour brings with it the ability to influence and alter human behaviour. Subsequently, people are susceptible to being manipulated into making choices that they otherwise may not have made, this manipulation taking place covertly, in turn threatening personal autonomy and the notion of the individual as an autonomous agent.

Many actors within society are utilizing predictive modelling, for example, governments, public authorities, law enforcement, the health care sector and most notably, private commercial actors.⁶ Sunstein remarks:

For-profit companies are using behavioural research every day. They want to learn how people think and to use that learning to make money. Charitable organizations consult behavioural scientists to find out how they might attract donors and increase donations. For their part, public officials are increasingly turning to the behavioural sciences to promote their goals. They are influencing people in multiple ways in order to reduce poverty, to increase employment,

5 Sunstein, Cass R., *The Ethics of Influence: Government in the Age of Behavioural Science*, Cambridge University Press, 2016, at p 1.

6 The term 'commercial actor' is used for the most part throughout this thesis. It refers to private companies or corporations, these terms used interchangeably.

to clean the air, to improve health, to encourage people to vote, and to increase safety on the highways. What are the ethical constraints on their actions?⁷

Witten and Frank highlight the connection between predictive modelling and business:

A scientist's job ... is to make sense of data, to discover the patterns that govern how the physical world works and encapsulate them in theories that can be used for predicting what will happen in new situations. The entrepreneur's job is to identify opportunities, that is patterns in behaviour that can be turned into a profitable business, and exploit them.⁸

This thesis focuses on the use of predictive models by commercial actors, which are constantly required to make strategic commercial decisions, a substantial part of this process requiring the identification of various forms of risk.⁹ For a commercial actor, a research and development project can entail a risk, taking on a new marketing strategy can be a risk or entering into a contract can entail a risk. However, people's behaviour in relation to that commercial actor can also be a risk. For example, an existing customer about to leave for a competitor is a risk or a potential customer can become a risk should he or she result in unnecessary and unexpected costs. The ability to predict and therefore pre-empt these risks places the commercial actor in a powerful position. Here, reference is made to the concept of 'nudge', discussed in the next chapter, which Thaler and Sunstein use to describe the manner in which the actions of individuals can be modified using subliminal techniques which are seemingly insignificant yet which can have a substantial effect on behaviour.¹⁰

7 Sunstein, *The Ethics of Influence*, above n. 5, at p 1.

8 Witten, Ian H. and Frank, Eibe, *Data Mining: Practical Machine Learning Tools and Techniques*, Elsevier, 2005, at p. 4.

9 In search of a definition of 'risk' many alternatives exist. For example, The Society for Risk Analysis (SRA) defines it as, 'the potential for realization of unwanted, adverse consequences to human life, health, property, or the environment', in Wahlgren, Peter, *Legal Risk Analysis: A Proactive Legal Method*, Jure, 2013 at p. 20.

10 Thaler, Richard and Sunstein, Cass R., *Nudge: Improving Decisions about Health, Wealth and Happiness*, Penguin Books, 2008. The concepts of Thaler and Sunstein are described further in Chapter 2. It should also be noted that the notion of 'nudging' can have both positive and negative connotations.

For all the benefits associated with predictive modelling, there are a number of potential harms that can negatively affect the individuals upon whom these models operate. There is little public awareness of this practice, and when knowledge of its existence is publicised, it results in a feeling of uncertainty, insecurity and a loss of control on the part of individuals, who are the target of this powerful technology. However, the harms resulting from predictive modelling are not only emotional. Predictive modelling can result in harms that are concrete in nature and with a varying degree of recognition in the law. This thesis investigates these potential harms in the context of a specifically chosen legal framework from within the European legal space, in order to determine to what extent they are addressed. In doing so, it examines alternative mechanisms that could potentially improve the situation of the individual in the face of the use of predictive models. The main challenge, therefore, is how to level the playing field between commercial actor and individual in the commercial setting.

1.2 Overall Objectives

This thesis has a number of aims. The first aim is to create a societal awareness of the existence of predictive modelling. While this aim may seem simplistic and trivial in nature, it is deemed a necessary step towards protecting society from the associated dangers. It is also as a result of increased societal awareness that greater demands can be placed on those developing the technology as well as those operating it, to bring about positive change.

The second aim of this thesis is to identify and make an inventory of the risks and vulnerabilities associated with the use of predictive modelling. Studies have shown that both internationally and nationally, there is a limited appreciation for the effects of technologies such as predictive modelling.¹¹ It is in pursuing this aim that the potential harms resulting from the use of predictive modelling techniques are explored. An inventory of these harms is compiled by studying the vast amount of reading material on the topic, both within law but also within other disciplines, such as information communication

11 Swedish Government Official Reports, SOU 2016:41, *Hur står det till med den personliga integriteten? – en kartläggning av Integritetskommittén*, Delbetänkande av Integritetskommittén, Stockholm 2016, at p. 52.

technology, sociology, psychology, the behavioural sciences and surveillance studies.

The third aim of this thesis is to examine if, and to what extent, traditional law addresses the potential harms resulting from predictive modelling as well as whether, and to what extent, predictive modelling itself is regulated. This is achieved by examining the degree to which the European data privacy legal framework addresses personal autonomy and predictive modelling.¹²

The fourth aim of this thesis is to provide an alternative strategy to minimize the risks and vulnerabilities connected to predictive modelling and address the potential harms. In this regard the strategy of empowerment is introduced. It comprises various components that possess either a traditional legal character, have a soft law character, are technical in nature or are neutral in nature.¹³ It is within this regulatory mechanism that traditional law retains its role as a regulatory instrument, but where soft law, technology and other components are suggested as a complement. The strategy of empowerment also highlights the role of traditional law as an indirect regulatory instrument.

The fifth aim of this thesis is to demonstrate the complexities that a solution must take into consideration, in that there are multiple interests at stake. For example, the interests of the individual may clash with those of society-at-large. An illustration of this is provided by considering taxation systems, where predictive models assist the tax authorities in identifying tax evasion. The excessive empowerment of individuals in this context, for example in the form of providing knowledge concerning tax evasion detection capabilities, while empowering individuals, would also allow them to strategically bypass the system in order to evade detection, a phenomenon referred to as ‘gaming’ a system.¹⁴ This may be beneficial from the tax evader’s point of view (individual), but is harmful from the societal perspective, as the services provided

12 This thesis does not promote the European legal framework of data privacy as the only, or even most suitable, framework for addressing the harms associated with this technology. For example, predictive models or like technologies, could very well be effectively addressed by other legal frameworks, be they international or national, or other legal spheres, for example, consumer protection, labour law, competition law or contract law, to mention but a few.

13 In this context, the label ‘neutral’ refers to the fact that a component does not fall under one of the other labels (traditional law, soft law or technology). For example, the access to knowledge is one such component.

14 Kroll, Joshua A., Huey, Joanna, Barocas, Solon, Felten, Edward W., Reidenberg, Joel R., Robinson, David G., and Yu, Harlan, *Accountable Algorithms*, Vol. 165, Issue 3,

by the state in order to maximise general welfare would decline in the face of a decreased revenue from taxation. The same applies to the private sector. For example, it is in the interests of society-at-large to have a strong and stable financial sector that instils confidence in that society and increases general prosperity, for example by attracting external investment, something from which all members of that society benefit. These financial institutions rely on predictive models to identify risks, such as fraud. Empowering individuals by providing them with unfettered insight into the technology underlying these predictive models, would provide them with the know-how to bypass the systems that identify risk and would endanger not only the stability of these financial institutions but also put the economic well-being of the entire society at risk. Another example is health care practices, where predictive modelling technology could potentially erode an individual's privacy and autonomy while at the same time be beneficial from the societal perspective, as the ability to cure illnesses would increase.¹⁵ This aim therefore concerns the issue of where to draw the line and where the perimeters of empowerment should lie. The individual requires empowering in order to be able to establish that the decisions taken about him or her by algorithms are correct and fair and preserve personal autonomy, while at the same time the business models of companies rely on this technology. Therefore, it is important to realize that while the focus of this thesis is the commercial actor versus individual relationship, there are a number of simultaneous and mutually dependent interests that are constantly influencing each other. Consequently, while focussing on the commercial relationship between company and individual, the influence of the state on this relationship cannot be totally ignored.

The general goal of this thesis, therefore, can be described as the examination of the challenges associated with designing an environment that allows for the use of technology in the pursuit of innovation, while simultaneously

University of Pennsylvania Law Review, p. 633, 2017, available at: http://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3 (last accessed on 2017-04-13), at p. 639.

15 For an in-depth discussion on the notion of the balancing of interests with reference to a practical example from the Swedish context, see Lind, Anna-Sara, *LifeGene – a Closed Case?* in Lind, Anna-Sara, Reichel, Jane and Österdahl, Inger (eds.), *Information and Law in Transition – Freedom of Speech, the Internet, Privacy and Democracy in the 21st Century*, Liber, 2015, at p. 339.

addressing the risks and vulnerabilities resulting from the use of these increasingly invasive technologies to make decisions about humans.

1.3 Research Questions

This thesis has the technological phenomenon of predictive modelling as its point of departure. It examines the risks and vulnerabilities associated with this particular technology, making an inventory of the potential harms to individuals, which are connected in that a characteristic they share is the manner in which personal autonomy is negatively influenced. Thereafter, the European data privacy legal regime is examined in order to ascertain if and to what extent existing regulations address the notion of autonomy and the phenomenon of predictive modelling. Working on the hypothesis that generally, traditional law alone can be an inadequate mechanism with which to address the potential harms associated with complex technologies, the main aim of this thesis is to suggest a general regulatory strategy, made up of traditional legal components, non-traditional legal components, technological components and neutral components that promote the protection and development of personal autonomy and regulate predictive modelling. This regulatory strategy is called ‘empowerment’ and addresses a perceived governance gap. Consequently, the following questions are set:

1. What is predictive modelling and how does it work?
2. What are the potential harms associated with the use of predictive modelling?
3. To what extent does predictive modelling diminish personal autonomy and restrict its development?
4. To what extent does the European data privacy legal framework address personal autonomy and predictive modelling, thereby diminishing the potential harms?
5. Working on the hypothesis that traditional law alone can generally be an instrument that is inadequate in protecting people against the risks and vulnerabilities posed by modern complex technologies, what reg-

ulative strategy best protects personal autonomy in the face of the increased use of predictive modelling techniques in the commercial setting?

Therefore, the main research question of this thesis is the following:

Notwithstanding the positive applications of predictive modelling, to what extent can the strategy of empowerment protect the individual against the potential harms to personal autonomy resulting from the increased use of predictive models by private commercial actors?

1.4 Method and Material

This thesis is a study of the relationship between law and information communication technology, this field of law traditionally referred to as ‘legal informatics’. In pursuing its aims, this thesis utilizes three legal methodologies. The predominant methodology applied is that of proactive law. This, in turn, is complimented with the limited application of the traditional legal method, also referred to as the doctrinal research method, as well as with the legal method of making comparisons.

Legal informatics is a branch of legal science, and is interdisciplinary in nature in that it complements the traditional legal perspective, characterised by the text-oriented analysis of valid law, with perspectives from the field of informatics.¹⁶ It encapsulates a two-way perspective, the notion referring not only to the manner in which information communication technology (ICT) affects society but also the manner in which society impacts on technology, for example, by studying the extent to which social choices, preferences and tradition affect technology, this interaction between law and ICT being described as, ‘the interaction between “rules” and “tools”’.¹⁷ In this sense, legal

16 Seipel, Peter, *IT Law in the Framework of Legal Informatics*, in Wahlgren, Peter (ed.), *IT Law, Scandinavian Studies in Law, Volume 47*, Stockholm Institute for Scandinavian Law, 2004, at p. 32.

17 Seipel, Peter, *Legal Informatics Broad and Narrow*, in Magnusson Sjöberg, Cecilia, (ed.), *Legal Management of Information Systems: Incorporating Law in e-solutions*,

informatics focuses on the interplay, interaction and mutual dependencies between the law and IT.¹⁸ An aspect of this interplay is best illuminated by means of the example, where a new technology may create possibilities to improve the application of a right, for example the right to access information, while an existing regulation may prohibit this same right, considering it harmful or risky.¹⁹

The methodology of proactive law is prescribed by Seipel, who considers it, ‘one of the pillars of legal informatics’.²⁰ Taking into account the technical nature of the problem at hand and the multidisciplinary nature a possible solution requires, the proactive law method, ‘supplies a language ... for problem formulation, analyses, theory building etc. in a fragmented environment’.²¹ This is relevant to the extent that this thesis does not remain within the strict confines of the traditional sources of law, but extends its examination to technological developments as well as the influence of research in other disciplines, for example, the behavioural sciences. Seipel also refers to ‘nutshell descriptions’ of proactive law:

To be proactive means not to be reactive, proactive law means using legal and ‘technical’ strategies in a constructive and mutually supporting way, proactive law is a tool to develop the information society according to specific blueprints and proactive law is a strategy for risk management.²²

Proactive law is a methodology whereby, instead of addressing problems after they have occurred (‘curative’ law), they are avoided or prevented before they

Studentlitteratur, 2005, at p. 25. It should be noted that the more modern term ‘information communication technology (ICT) is used in this text, replacing the term ‘information technology’ (IT), used in the above cited work.

18 Seipel, *IT Law in the Framework of Legal Informatics*, above n. 16, at p. 32.

19 Seipel, *Legal Informatics Broad and Narrow*, above n. 17, at p. 26.

20 Seipel, Peter, *Nordic School of Proactive Law Conference, June 2005 Closing Comments*, in Wahlgren, Peter (ed.), *A Proactive Approach*, *Scandinavian Studies in Law* Volume 49, 2006, at p. 362.

21 *Ibid*, at p. 359.

22 *Ibid*, at p. 360.

can occur.²³ The metaphor of the lighthouse is used, describing a coastal building with a flashing light the purpose of which is to warn seafarers of dangers hidden in the dark.²⁴ An additional way of conceptualizing proactive law is as a ‘perspective’ or ‘world view’, an advantage with this being that it negates the view that it is something totally novel and a threat to ‘traditional law.’²⁵ The notion of perspective is also important from the point of view that, ‘[e]ven small changes of perspective can make us see things differently and in a new way’.²⁶ An important basis for the acceptance of proactive law as a methodology is derived from the manner in which one views the function of law. In this regard, a useful starting point is to identify legal systems as dynamic and to view, ‘... law as a conceptual system subject to change and law as a system intended to produce as well as to accommodate changes in social structures’.²⁷ In his treatment of proactive law, Seipel refers to the field of ‘legal futurology’ as an important element of what he describes as ‘computing law’, where traditional legal research, such as comparative law, is complimented with a ‘prognostication of developments in the legal system and with future-oriented policy issues’.²⁸ Two well-known concepts within the context of the study of the law are ‘lex lata’ (‘valid law’) or the law as it is and ‘lex ferenda’ (‘desired law’), namely the law as it ought to be.²⁹ In this regard reference is made to the discussion surrounding the creation of a third category of compartmentalization of the law, namely ‘lex ponderanda’, meaning ‘probing law’ or ‘speculating law’, it also being described as ‘a speculative, critical analysis of the law’.³⁰ The emphasis on the concept of ‘lex ponderanda’ is fitting in the con-

23 Ibid.

24 Ibid.

25 Ibid.

26 Ibid, at p. 359

27 Ibid, at p. 362.

28 Ibid.

29 These concepts are alternatively referred to as ‘de lege lata’ and ‘de lege ferenda’.

30 Seipel, Peter (ed.), *Law and Information Technology: Swedish Views*, Swedish Government Official Reports, SOU 2002:112, Information and Communication Technology Commission Report, Stockholm, 2002, inside of the back cover. See also Seipel, Peter, *Nordic School of Proactive Law Conference*, above n. 20, at p. 362. During deliberations of the Swedish Government’s Information and Communication Technology Commission, the idea of creating the new term ‘lex ponderanda’ was considered.

text of this thesis, where in the face of the harms caused by predictive modelling, it provides a speculative, critical analysis of the law, alternatively referred to as a legal policy analysis. It is also important to note that the proactive legal method, in applying a speculative analysis of the law, is not without limits as to what can be argued. In other words, its speculative characteristic is constrained by boundaries. Proactive law is viewed merely as providing a new perspective to traditional law.³¹ It is therefore in this regard that traditional law assists with boundary identification as far as the speculative nature of proactive law is concerned. A final attribute characterising proactive law is its flexibility, which makes it amenable to being combined with other legal methodologies.

This thesis also utilizes legal doctrine or the traditional ‘legal method’ to a limited extent and confined mainly to Chapter 5. Legal doctrine, also referred to as legal dogmatics, consists of professional legal writings whose task it is to systematize and interpret valid law.³² It aims at acquiring a, ‘coherent picture of the law ... presenting the law as a network of principles, rules, meta-rules, and exceptions, at different levels of abstraction, connected by support relations’, this achieved not only by means of description and logic, but also by including evaluative or normative steps.³³ Referring to it as the ‘legal method’, focuses on its utility in solving legal problems, being that method taught to law students, providing them with the competence to use tools such as interpretive arguments, modalities of decision, conflict-solving maxims, the principle of legality and the rule of lenity.³⁴ Associated with the traditional

However, this became controversial due to the fact that the question of who undertakes to be proactive is a politically sensitive question, as the issue of who speculates about the future is closely associated with whose description of the future should guide regulatory work. This situation was complicated by the fact that the ICT Commission was an advisory body to the Swedish Government, its examination requiring consideration of the work of other government bodies and lawmaking committees. Here Seipel provides a reminder of the fact that the proactive method in relation to lawmaking is not a simple matter as it opens up for a power play and the conflicting of different initiatives by different actors (see, Seipel, Peter, *Law and Information Technology: Swedish Views*, pp. 362-363, note 9).

- 31 Seipel, Peter, *Nordic School of Proactive Law* Conference, above n. 20, at p. 360.
- 32 Peczenik, Alexander, *A Theory of Legal Doctrine*, Ratio Juris, Vol. 14, No. 1, March 2001, at p. 75.
- 33 Ibid, p. 79.
- 34 Spaak, Torben, *Guidance and Constraint: The Action-Guiding Capacity of Theories of Legal Reasoning*, Iustus Förlag, 2007, at p. 12, footnote 5.

legal method are four main interpretive arguments, namely, textual arguments (literal meaning of the provision), systemic arguments (giving a statute the meaning that is most in line with the surrounding body of law), intentionalist arguments (the intention of the legislature is decisive) and teleological arguments (judging on the purpose of the statute), these approaches dictating what is relevant when interpreting statutes.³⁵ It is in this context that the role of law has been discussed, with emphasis placed on the question of how legal systems ought to decide cases and the manner in which the institutions of a legal system ought to arrive at their decisions.³⁶ Wasserstrom identifies two possible alternatives:

... that a court should be realistic in rendering a verdict, that the content of sociological inquiries and the methodology of the sociologists ought to be utilized by the judiciary and the legislature in the performance of their functions, or that a judge should be pragmatic in the adjudication of the cases that come before him.³⁷

A different manner of describing these two alternatives is that the first is a 'rationalistic or deductive decision procedure', whereas other alternatives reject this 'logical' decision procedure.³⁸ In this vein, Spaak notes that the legal method concerns the 'process of justification', whereby the judge is guided and constrained when justifying a decision, and is opposed to the 'process of discovery', which can be described as a more creative process.³⁹

This thesis also makes a limited use of comparisons as a methodology. The making of comparisons concerns how one solves concrete legal problems by examining the relevant sources of law, the relative weight to be assigned these sources of law, rules of interpretation as well as other norms relating to legal argumentation.⁴⁰ There are also a number of ways in which one can make

35 Ibid, at p. 43.

36 Wasserstrom, Richard, A., *The Judicial Decision: Toward a Theory of Legal Justification*, Stanford University Press, 1961.

37 Ibid, at p. 3.

38 Ibid at p. 5. In his study, Wasserstrom refers to three alternative methods of arriving at decisions, namely, the 'procedure of precedent', the 'procedure of equality' and the 'two-level procedure of justification'.

39 Spaak, above n. 34, at p. 43.

40 Asp, Petter, *Om relationalistik metod eller spridda anteckningar i jämförande rättsvetenskap*, in *Konsten att rättsvetenskap - den tysta kunskapen i juridisk forskning*,

comparisons. On the one hand, one can look backwards in time and investigate how the legal situation was in the past and consequently compare this with the present.⁴¹ While this thesis is not a comparative work in the traditional sense, it does nevertheless compare different notions and concepts in different legal systems and jurisdictions. Asp, referring to the benefits of making use of comparison as a method, states that one can look forward and compare this with the present, thereby comparing the law as it is ('de lege lata') with the law as it could be ('de lege ferenda'), with reform being desired if the situation could be improved with the law as it should be.⁴²

The choice of these three complementary methodologies addresses some fundamental themes presented by Svantesson as recurring within the context of research within the area of internet technology but that are also of relevance in relation to legal informatics: first, law always encounters difficulties in keeping pace with technology, second, practitioners have difficulty understanding technology, third, the phenomenon of globalisation results in our thinking being directed towards the bigger picture and not limited to our immediate surroundings and fourth, the internet is characterised by dramatic growth instilling a fear for the risks involved with its use, an attribute that can be transposed to technology in general.⁴³ For example, this thesis references legislative attempts in the US as a source of inspiration to support certain arguments. It also takes into account, in comparing aspects of different legal systems, that the basis of these legal systems may be different. However, there is a certain value in comparing how different legal systems treat similar notions and concepts. In addition, in looking to other legal systems for inspiration or for the sake of making analogies, it should be noted that these specific legal systems were chosen for pragmatic reasons and precisely because they incorporate certain specific notions. For example, the concept of fiduciary duty is examined briefly. This notion exists mainly in common law legal systems and therefore the Canadian and English legal systems were referenced in this regard.

Asp, Petter och Nuotio, Kimmo (red.), Iustus, 2004, at p 47, as translated by the author from the original in Swedish.

41 Ibid, at p. 53.

42 Ibid, at p. 54.

43 Svantesson, Dan Jerker B., *A Legal Method for Solving Issues of Internet Regulation*, International Journal of Law and Information Technology, Vol. 19, No. 3, Oxford University Press, 2011, at p. 244-245.

While the proactive legal method is flexible in its combination with other methods, it is at odds with the theory of legal doctrine to the extent that the reference to 'lex ponderanda' takes its application outside of the boundaries established by the theory of legal doctrine, which essentially is confined to the central sources of law. However, the utilization of these two opposing methodologies, together with the method of comparison, is not only legitimate, but also makes for a more exciting and realistic thesis.

This thesis begins by focusing on the technology of predictive modelling. To this end, knowledge concerning the technical aspects of predictive modelling is attained from reading both technical and legal material on the topic as well as from consulting academics within the realm of computer science. Predictive modelling requires volumes of data. This has led to the unprecedented monitoring of individuals as they traverse the digital environment. With this in mind, a theoretical context is provided for this unrivalled surveillance of society, outlining the reasons for this development. Thereafter a short examination of the notion of autonomy is made, anticipating that the main risk from predictive technology is its potential harm to personal autonomy, necessitating a subsequent examination of the notion of identity, these two concepts being closely related.

Next, this thesis investigates the negative effects of predictive modelling on individuals within society, making an inventory of the potential harms. The basis for establishing such an inventory is the assumption that with many modern technological developments and applications, while there are advantages, there are usually accompanying disadvantages. Some of the harms referred to in the inventory have a stronger connection to current traditional law while others have a weaker one, these harms 'potential' to the extent that they may not occur in every instance of predictive modelling. Here the method of comparisons is used, for example, where the disciplines of philosophy and psychology are referred to and in which such harms are also studied. Finally, it is important to stress that the inventory provided is not intended to be exhaustive and is open to additional harms. Nevertheless, in its current form it represents the nature of the potential harms that predictive modelling could give rise to.

Having inventoried the potential harms associated with predictive modelling, a notion identified as uniting them is that of personal autonomy. Therefore, the conclusion is drawn that in order to protect individuals from the above harms, individual personal autonomy requires bolstering. It is for this reason that an examination is made of how the law addresses autonomy and predictive modelling, the rationale being that a robust protection of autonomy

is necessary in order to prevent the realization of the potential harms of predictive modelling.

Next, in assessing the extent to which existing traditional regulatory structures address the potential harms to autonomy and the risks and vulnerabilities associated with predictive modelling, the European data privacy legal framework is examined. In other words, an examination of the law is made in order to ascertain whether and to what extent the notions of autonomy and predictive modelling are addressed. The data privacy legal framework is chosen based on the assumption that, considering its tradition of attempting to regulate technology, more specifically, personal data, it would be that sphere of law best suited to addressing the problems arising from predictive modelling. In addition, prior knowledge of the fact that profiling, a notion argued to be closely related to predictive modelling, is addressed by this legal framework is a compelling argument for its examination. Similarly, the European perspective is chosen as it is within this jurisdiction that data privacy has developed most in addition to the fact that the data privacy legal instruments comprising this legal framework have had a significant influence on data privacy regulation worldwide.

Arguably, ‘data privacy’ is a nomenclature that has as its objective the amalgamation of the sub-concepts of ‘privacy’ and ‘data protection’. Privacy is an internationally recognized concept and in this thesis is represented by Article 8 of the European Convention on Human Rights (ECHR) as developed by the Council of Europe (CoE). Human rights law, a sub-category of international law, is placed in context by means of a study of the main international human rights instruments as well as the application by the European Court of Human Rights (ECtHR) of Article 8 ECHR. This is done to the extent that the judgements from the ECtHR are illustrative of arguments made and it is not the intention that these judgements be regarded as precedent. A study of international law is made, providing a brief background regarding its development, its legal instruments and the normative legal status that these have in relation to each other. Thereafter, the focus shifts to a narrower aspect of international law, namely human rights law, which includes rules adopted at the global or universal level as well as at the regional level. International human rights law is examined by canvassing the United Nations Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the International Covenant on Economic, Social and Cultural Rights

(ICESCR) and customary international law.⁴⁴ Included in regional human rights law is the European Convention on Human Rights (ECHR) and judgments from the European Court of Human Rights (ECtHR).⁴⁵ The chapter then turns to the European legal regime concerning data protection. The historical development of data protection is illustrated by means of brief references to the Organization for Economic Cooperation and Development Guidelines (OECD Guidelines) and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108) (Convention 108). The main sources comprising the study of the data protection regime are the Data Protection Directive 95/46/EC ('DPD')⁴⁶, the General Data Protection Regulation 2016/679 ('GDPR')⁴⁷, the Charter of Fundamental Rights of the European Union ('EU Charter') and judgments from the Court of Justice of the European Union (CJEU).

It is also necessary to be aware that instruments are referred to that, taking into account their status within the legal normative hierarchy, cannot be considered binding law in the strict sense of the word. For example, within the context of data protection, a body that is of relevance is the European Commission's Article 29 Data Protection Working Party. This body was set up in connection with the establishment of the DPD and is composed of a representative of the data protection authorities from each EU country, as well as

44 The ICESCR is mentioned to the extent that it is part of the International Bill of Rights, while its material applicability to this thesis is limited.

45 It is argued that the content of the ECHR and ICCPR are relatively similar. Considering this, the ECHR is the main focus of this study for the reasons highlighted above.

46 Directive 95/46 of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995.

47 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016. At the time of the conclusion of this thesis, the DPD is the legal instrument of the European Union data protection framework that is applicable law. However, on the 15th of December 2015 it became public knowledge that the final text of the proposed GDPR had been negotiated by the European Parliament and Council. Thereafter, since publication of the GDPR in the official journal of the EU, the GDPR will be coming into effect on the 25th of May, 2018. Consequently, it was decided to focus both on the DPD as applicable law but also on the GDPR as forthcoming law. In this regard, cognizance should be taken of the fact that the GDPR is not applicable law at the time of the finalization of this thesis but will be treated as such for the purposes of completeness.

representatives of other EU institutions and the Commission. It provides opinions, working documents and letters, and makes recommendations within the area of data protection on a European level.⁴⁸ In making references to the Article 29 Data Protection Working Party, it is necessary to highlight that it is not a legislative body and the normative weight of its recommendations and other material must be seen in this context. Nor does the material it produces reflect the opinion of the European Commission. Another example is the reference to guiding principles, for example, the Guiding Principles on Business and Human Rights, which do not have the status of a binding legal document, yet do have a regulatory function from the soft law perspective. It is in this regard that reference is made to soft law as a regulatory tool.

Empowerment is the name given to a regulative strategy suggested in this thesis, which amounts to the compilation of an inventory of potential mechanisms available in order to address the harms associated with predictive modelling and with the function of protecting autonomy. This inventory is not exhaustive and serves as an illustration of the types of mechanisms that could be utilized to regulate a problem resulting from technology. Here a mention of the role of law is necessary. The assumption made is that traditional law alone cannot effectively regulate a technology such as predictive modelling. This argument is supported by an interim Swedish Government Official Report, entitled ‘What is the Privacy Situation?’, which analyses the attempts on a national level to implement traditional legal means of data protection, and wherein it is stated that, ‘[i]n our final report we intend to investigate the steps that could be taken to counteract the risks that we have identified. Here, methods other than legislation may be relevant, such as industry agreements or proactive measures on the part of the supervisory authorities’.⁴⁹ This statement supports the notion that tools other than traditional law must be resorted to when regulating technology. As evidence of the ineffectiveness of traditional law alone, the Report refers to statistics concerning the national sanction system within the area of data protection, more specifically the lack thereof:

48 European Commission, *Article 29 Working Party*, available at http://ec.europa.eu/justice/data-protection/article-29/index_en.htm (last accessed on 2016-05-30).

49 Swedish Government Official Reports, SOU 2016:41, *Hur står det till med den personliga integriteten? – en kartläggning av Integritetskommittén*, above n. 11, at p. 117.

Very few cases reach the courts in any case. For example, in the period 2012–2015 we have found only five disputes that came before the district courts in which the case involved damages under the Personal Data Act. The situation in criminal law is no different. In 2014 in Sweden as a whole, a decision was reached in a total of only four cases of breach of the Personal Data Act (by a judicial ruling, imposition of a penalty or decision not to prosecute).⁵⁰

Some mechanisms included in the strategy of empowerment can be considered to be of a traditional legal nature. In such cases, traditional law directly addresses the central problems posed by predictive modelling. Other mechanisms, besides traditional law, may also regulate the problem. One such example is that of technology. This, however, does not eliminate the role of traditional law, but merely changes its function, as even the technical solutions themselves require traditional legal regulation. In such situations, traditional law indirectly addresses the problem. This is best illustrated utilizing an example, namely that of hate speech in the on-line environment. The effectiveness of traditional law in combatting hate speech must be questioned, considering the fact that it has not been eradicated. An alternative potential solution is technical in nature and entails the development of an algorithm to parse the digital environment, removing all speech that is hateful in character. This is a regulatory mechanism using technology that would be more effective than traditional law. However, the legality of the algorithm should be questioned, for neglecting to take important constitutional legal norms and principles into account, such as freedom of expression. Consequently, should such an algorithm be resorted to, traditional law would still be required to regulate the algorithm (technology), ensuring that legal norms and principles are adhered to even in so far as the technical solutions are concerned. In such circumstances, the regulatory nature of the law is indirect.

Prins, referring to technologies of profiling, states that, ‘[t]he commodification of our identities and behaviour does not need a property rights debate with respect to individual and isolated personal data; it requires a debate on the role of law in providing the necessary instruments to know and to control the way in which our identities are made’.⁵¹ It is at this juncture that the role of the law can be considered. It is often the case that law is not the only remedy

50 Ibid, at p. 125.

51 Prins, J. E. J., *The Propertization of Personal Data and Identities*, Electronic Journal of Comparative Law, Vol. 8(3), October 2004, at p. 7, available at <http://www.ejcl.org/83/abs83-1.html> (last accessed on 2016-04-26).

for developments considered undesirable consequences resulting from technological advances. For example, public outcry in reaction to the undesirable effects of certain technologies has remedied the harm in such instances by resulting in the withdrawal of the technology.⁵² Ethics may have a role to play, while soft law approaches, morals and maybe even religion are also relevant. In this regard, mention is made of Lessig's model of regulation, where the interaction between what he refers to as the 'constraints' of 'code', 'market', 'architecture' and 'norms' regulate problems.⁵³

A final aspect worth noting is that law itself has the objective of empowering, something that should not be overlooked in examining a general strategy of empowerment. Law-making has a number of functions: it ensures stability in society while at the same time allowing for flexibility, it secures foreseeability, it protects individuals and groups, it provides security and it solves conflicts, to mention but a few.⁵⁴ In this regard, law can also be seen as a mechanism of empowerment, especially where individuals or groups are identified as being in a position of weakness or disadvantage in relation to more powerful actors or where the excessive concentration of power in a limited number of commercial entities is prevented, for example in the case of monopolies.⁵⁵

1.5 Definitions

This thesis refers specifically to the technology of predictive modelling. It is argued that there is an inherent difficulty in placing labels on specific technologies as different actors potentially label the same phenomenon differently. For example, two related concepts are 'predictive analytics' and 'predictive modelling'. While the former refers to the entire process of predicting human behaviour using a variety of technical solutions, the latter is accepted as being

52 Paul, Ian, *Girls Around Me App Voluntarily Pulled After Privacy Backlash*, PC World, available at http://www.pcworld.com/article/252996/girls_around_me_app_voluntarily_pulled_after_privacy_backlash.html (last accessed on 2016-01-12).

53 Lessig, L., *Code 2.0*, Basic Books, 2006, at p. 123.

54 Wahlgren, Peter, *Lagstiftning: rationalitet teknik och möjligheter*, Jure, 2014, at pp. 35-46.

55 *Ibid*, at p. 40.

a specific part of that process. In other words, it is narrower in that it refers to a certain technical mechanism used in order to pre-empt behaviour. Predictive analytics represents multiple methods for predicting human behaviour and may not necessarily use models. For the purposes of this thesis, the use of predictive models is focused upon, being a practical implementation of predictive analytics.

Another term that requires clarification is that of ‘profiling’. Profiling is used differently depending on context. The term is used to describe a certain technology but its meaning has also changed over time. The pastime of profiling is argued to be as old as life itself, the example given that it is used by organisms that are required to profile in order to survive in their environment, being required to anticipate risk and opportunity.⁵⁶ Profiling has also been associated with discrimination, where people, based on their having a certain physical appearance, are treated disadvantageously.⁵⁷ The notion of profiling, also, has changed over time and while it previously was used to describe the scientific possibility of grouping data in order to gain insight into that data, it seems that from the meaning that has been given to profiling more recently, it is used more in line with the notion of predictive analytics. For example, according to the GDPR:

‘profiling’ means any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.⁵⁸

Profiling is best described in terms of a spectrum. At one end are basic practices of profiling, where a limited number of basic attributes are utilized to form a simple and general image of a person, for example with a specific purpose in mind such as attaining a picture of a person’s financial position. At the

56 Hildebrandt, Mireille, *Defining Profiling: A New Type of Knowledge*, in Hildebrandt, Mireille and Gutwirth, Serge (eds.), *Profiling the European Citizen*, Springer, 2008, at p. 272.

57 Merriam-Webster Dictionary, *Profiling*, available at <https://www.merriam-webster.com/dictionary/profiling> (last accessed on 2017-01-24).

58 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, above n. 47.

other end of this spectrum are the more advanced forms of profiling, where deep personality analyses of individuals are created, predicting the behaviour of these individuals as well as influencing these people's future behaviour. It is this latter notion of profiling that is reflected by the term predictive modelling. This interchangeable use of the term profiling should be taken into account when examining the texts of scholars, as their reference to profiling may be referring to profiling in its simpler meaning or it may be referring to that notion of profiling that corresponds more closely to predictive modelling.

Mention must also be made of the concept of big data, which refers to the large amounts of different types of data making up and stored in the digital environment. The term big data, from the semantic perspective, is unsatisfactory as it creates the impression that the only unique characteristic of big data is that there is a lot of it, and that it is size alone that defines the difficulties in handling it. The critics of the use of this concept state that it can itself be misleading and is not really descriptive of the meaning that it is attempting to convey. For example, Hildebrandt argues that the concept big data is misleading as what it actually concerns is modelling.⁵⁹ In addition, the misleading use of the concept to a certain extent lies with the use of the term 'big', which detracts from other characteristics that the data may have, for example, the fact that it is fluid in nature and also comprises varying types of data. In other words, it creates the impression that the data is in some way static and permanent. As will be addressed hereunder, the notion of storing data is becoming archaic and some modern technological processes utilize data in a different manner. Certainly, big data involves a lot of data, however, it is not necessarily the amount of data that characterises its uniqueness, but rather its fluid and streaming nature. Another issues involves the identification of the border between data and big data, especially considering that the concept is relative to a commercial actor's size, where a dataset will be perceived as big data by a small commercial actor but not by a large one, as well as the fact that new technologies are being created constantly that render big data more manageable.⁶⁰ Finally, a problem with the term big data is its insinuation that more is better. A criticism of this point of view is that one should distinguish between data that is actually useful and that which is not, something that has led to the

59 Hildebrandt, M., *Slaves to Big Data. Or Are We?*, IDP. REVISTA DE INTERNET, DERECHO Y POLÍTICA, Issue 17, October 2013, at p. 28, available at http://works.bepress.com/mireille_hildebrandt/52 (last accessed on 2017-04-14).

60 Finlay, above n. 1, at p. 14.

coining of the term ‘smart data’, which is used to counter the notion that bigger is better.⁶¹ However, in characterizing big data, what is important is that besides there being large volumes of it, it is also being created rapidly and exists in various forms, which can complicate its analysis. It is in this regard that an appropriate term for big data is that of ‘noise’. In technical terms, noise is ‘anything that distorts or destroys the communication process’.⁶² In terms of data, more specifically big data, it refers to the fact that the useful data is hidden by the volumes of useless data, the challenge being to find the useful data in all the messy data.⁶³ A counter argument, however, is that the notion that more data is not necessarily better may not be totally true when it comes to seeing ‘the big picture’. What is meant here is that the bigger the data set, the more correlations that can be identified between the data, enabling those who have access to more data to see the bigger picture, as compared to those who see just individual data points. The term big data is in need of replacement, however, this remains difficult as it has become a well-known ‘buzz word’, it is a notion that is fashionable and most importantly, it is a notion that is most generally recognized by people who do not have a technical background. Consequently, the term is retained for pedagogic reasons, with the proviso that it is in need of replacement.

It is also necessary to address the concept ‘digital environment’. The digital environment is constituted by digital and networked technologies, represented

61 Rossi, Ben, *Is big data dead? The rise of smart data*, Information Age, available at <http://www.information-age.com/technology/information-management/123458486/big-data-dead-rise-smart-data#> (last accessed on 2016-08-16).

62 Lundblad, Nicklas, *Privacy in the Noise Society*, in Wahlgren, Peter (ed.), *IT Law, Scandinavian Studies in Law*, Vol. 47, Stockholm Institute for Scandinavian Law, 2004, at p. 359. Here Lundblad summarizes Shannon, C, *A Mathematical Theory of Communication*, The Bell System Technical Journal, Vol. 27, p. 379-423, 623-656, July, October, 1948.

63 In this regard reference is made to the term ‘exformation’ coined by Tor Nørretranders. Exformation refers to the action where information is explicitly sorted away or weeded out, yet in correspondence for example, it is concretely referred to despite the fact that it has been weeded out. In other words, it refers to the situation where, considering that one has to deal with lots of information, some of the information is weeded out in a factual correspondence while the same information remains in the senders consciousness and is explicitly referred to. Nørretranders, Tor, *Märk världen: En bok om vetenskap och intuition*, Bonnier Alba, translation by Wahlén, January, 1991, at pp. 132-137.

mainly by the internet, together with accompanying applications and platforms, such as the social media. The term digital environment includes the 'on-line' environment, the term 'digital environment' being preferred as it covers processes taking place in digital environments that are not necessarily connected to the internet. For example, a database with captured data can produce a predictive model without it ever having been connected to the internet.

Associated with the notion of the digital environment is the 'digital identity'. The digital identity is an identity created from big data using the tools of predictive analytics and predictive modelling. It is subsequently imposed on the human being that it represents. The human being has little influence over the creation of the digital identity, which is used as a proxy, replacing the real life individual in his or her interactions with commercial actors. Opposing the digital identity is the 'true identity', which is the subjective identity of a human being. In other words, it is the way in which a person sees him or herself, alternatively, the way in which he or she wishes to be portrayed. It is the identity that a person wishes to make public, possibly differing from one context to another. It is a true identity to the extent that it is that identity with which a person associates in a specific context. There are challenges labelling the notion of identity, considering that it is a notion that is fluid, dynamic, subjective and constantly in a flux. One could have used previously coined concepts such as the 'digital persona'⁶⁴, 'data image'⁶⁵, 'data double'⁶⁶ or 'digital dossier'⁶⁷ as others have done, to describe the portrayal of the individual in the digital environment. The concept 'digital footprint' is also used.⁶⁸ However, the word 'identity' better describes the richness of this digital image, its nuanced nature and its function of replacing a person's true identity. Referring to a 'true' identity is bound to be controversial, as the truth is a subjective matter and alleging that something is 'true' opens up to the question of 'whose truth'? However,

64 Clarke, Roger, *The Digital Persona and its Application to Data Surveillance*, The Information Society, Vol. 10, Issue 2, 1994, at pp. 77-92 in Lyon, David, *Surveillance Studies: An Overview*, Polity Press, 2007, at p. 87.

65 Lyon, David, *The Electronic Eye: The Rise of Surveillance Society*, Polity press, 1994 in Lyon, *Surveillance Studies: An Overview*, above n. 64, at p. 87.

66 Haggerty, Kevin D. and Ericson, Richard V., *The Surveillant Assemblage*, British Journal of Sociology, Vol. 51 Issue 4, 2000, at pp. 605-622 in Lyon, *Surveillance Studies: An Overview*, above n. 64, at p. 87.

67 Solove, Daniel, *The Digital Person*, New York University Press, 2004, at p. 1.

68 Internet Society, *Your Digital Footprint Matters*, available at <https://www.internetsociety.org/your-digital-footprint-matters> (last accessed on 2017-03-23).

semantically the word ‘true’ best captures the nature of that type of identity wishing to be portrayed and is of pedagogic relevance.

The concepts IT (information technology) and ICT (information communication technology) are used. Where possible, the more modern concept of ICT is referred to, highlighting the fact that technologies of communication are playing an increasingly important role in technological development. However, in some of the literature, the term IT is used. Where authors refer to IT, this is for the most part left unchanged in order to maintain the originality and integrity of these texts.

This thesis uses the term ‘data privacy’ to a certain extent, yet retains the clear distinction between ‘privacy’ and ‘data protection’. This is done in order to be able to apply different legal frameworks to the research questions.⁶⁹ The term ‘data privacy’ is commonly used to incorporate the sub-terms ‘privacy’ and ‘data protection’ and in effect functions as an umbrella term. It is therefore used as an initial step to delineate the legal research parameters of this thesis, and is indicative of the close and interrelated connection between data protection and privacy. Notwithstanding this, a clear distinction is maintained between ‘data protection’ and ‘privacy’. This is useful in applying the differing legal regimes of the CoE and EU and reflects the distinction that is maintained between these two notions on an EU Constitutional level, where the EU Charter treats them as two separate rights.

Two concepts that to a certain degree define each other and that are used extensively throughout this thesis are on the one hand ‘soft law’ and on the other hand ‘traditional law’, alternatively referred to as ‘black letter law’ or ‘hard law’. Starting with soft law, while it has no universal definition, it can be defined in terms of its characteristics.⁷⁰ In the field of international law, soft law is argued to have three main characteristics: first, it is not binding, second, it consists of general norms or principles, which are open-textured and

69 For a more detailed analysis of the semantics surrounding these terms and the effects thereof, reference is made to Bygrave, Lee, *Privacy Protection in a Global Context*, in Wahlgren, Peter (ed.), *IT Law, Scandinavian Studies in Law, Volume 47*, Stockholm Institute for Scandinavian Law, 2004, at p. 319, Bygrave, Lee, *Privacy and Data Protection in an International Perspective*, in Wahlgren, Peter (ed.), *ICT Legal Issues, Scandinavian Studies in Law, Volume 56*, Stockholm Institute for Scandinavian Law, 2010, at p. 165 and Bygrave, Lee, A., *Data Privacy Law: An International Perspective*, Oxford University Press, 2014, at p. 23.

70 Van der Sluijs, Jessika, *Soft Law – an International Concept in a National Context*, in Wahlgren, Peter (ed.), *Soft Law, Scandinavian Studies in Law, Volume 58*, Stockholm Institute for Scandinavian Law, 2013, at p. 287.

general in their content and wording and third, it is not enforceable through binding dispute resolution.⁷¹ This can be seen in relation to traditional law or hard law, which is binding and based on rules that incorporate specific commitments.⁷² The characteristic nature of soft law is demonstrated by two additional concepts, namely, ‘legal soft law’ and ‘non-legal soft law’. Legal soft law is comprised of non-binding or voluntary codes of conduct as accepted by international and regional organisations. In other words, it is made up of binding regulations with a vague content and with no concrete obligations being conferred.⁷³ Non-legal soft law is described as statements by individuals, which promote general principles.⁷⁴ Put another way, it provides advice and guidelines, sometimes including the ethical dimension, yet remains outside the traditional development of the law.⁷⁵ In this thesis, the term ‘traditional law’ is used to refer to that body of law, which is formally recognized as hard law and which usually finds expression in the written form, from where the notion ‘black letter law’ is derived. The term ‘soft law’ is used to represent that body of law falling outside of traditional law, yet which has a regulatory function, alternatively referred to as ‘non-traditional law’.

This thesis also refers to the notion of prediction. The general meaning of the word is, ‘say or estimate that (a specified thing) will happen in the future or will be a consequence of something’.⁷⁶ Within data science, it means, ‘to estimate an unknown value. This value could be something in the future ... but it could also be something in the present or the past’.⁷⁷

71 Boyle, A. E., *Some Reflections on the Relationship of Treaties and Soft Law*, International and Comparative Law Quarterly, Vol. 48, 1999, at pp. 901-902.

72 Ibid.

73 Van der Sluijs, above n. 70, at p. 286.

74 Chinkin, C. M., *The Challenge of Soft Law: Development and Change in International Law*, International and Comparative Law Quarterly, Vol. 38, 1989, at p. 851.

75 Van der Sluijs, above n. 70, at p. 286.

76 English Oxford Living Dictionaries, *Predict*, available at <https://en.oxforddictionaries.com/definition/predict> (last accessed on 2017-01-27).

77 Provost, Foster and Fawcett, Tom, *Data Science for Business: What you Need to Know About Data Mining and Data-Analytic Thinking*, O’Reilly Media, 2013, at p. 45.

1.6 Perspectives

The main perspective through which this thesis studies the potential harms associated with predictive modelling is that of the individual. In other words, in the commercial relationship between private commercial actor and individual, it is the perspective of the individual that takes precedence, where the individual is the object of decisions arrived at using predictive modelling. It highlights how this technology puts companies that possess the resources to employ the predictive technology and make visible the previously invisible knowledge within big data, at a distinct advantage. It is a relationship characterised by a power imbalance, where the knowledge available to companies far outweighs that of the individual.

A number of issues concretises this perspective. First, what to do when ‘the computer says “no”!’ In other words, as more decision-making systems are resorted to, using algorithms and predictive models, the insight of human beings into these decision-making processes is diminished. Of increased concern is that even those entities using these decision-making systems have limited insight into the grounds for the decision or output. In this context, the term ‘data-driven decision-making’ (DDD) is referred to, described as the process of basing decisions on the analysis of data as opposed to intuition or gut feel.⁷⁸ The applications of predictive models are endless: they determine the music people listen to (Spotify)⁷⁹, the news feeds they receive (Facebook)⁸⁰, the pictures they see (Instagram)⁸¹, the perfect partner (dating sites)⁸², the job search

78 Ibid, at p. 5.

79 Quartz, *The magic that makes Spotify’s Discover Weekly playlists so damn good*, available at <http://qz.com/571007/the-magic-that-makes-spotifys-discover-weekly-playlists-so-damn-good/> (last accessed on 2016-10-20).

80 Oremus, Will, *Who Controls Your Facebook Feed?*, available at http://www.slate.com/articles/technology/cover_story/2016/01/how_facebook_news_feed_algorithm_works.html (last accessed on 2016-10-20).

81 Hunt, Elle, *New algorithm-driven Instagram feed rolled out to the dismay of users*, available at <https://www.theguardian.com/technology/2016/jun/07/new-algorithm-driven-instagram-feed-rolled-out-to-the-dismay-of-users> (last accessed on 2016-10-20).

82 Bridle, James, The Guardian, *The algorithm method: how internet dating became everyone’s route to a perfect love match*, available at <https://www.theguardian.com/life-andstyle/2014/feb/09/match-charmony-algorithm-internet-dating> (last accessed on 2016-10-20).

(job recruitment agencies)⁸³, the diagnosis of disease⁸⁴ and whether they will be granted a loan (credit agencies). More and more decisions within society are being taken by computers and applications that have at their core complex predictive algorithms and predictive models. These are ambient, working undetected in the background, and autonomic, in that they can have a certain degree of independence in making decisions about human behaviour. The complexities of the technology and its widespread application are decreasing the possibility for humans to gain insight into these systems-based automatic decisions. The result is the potential for these decision-making processes to be viewed with increased scepticism. Also relevant is the imbalance of power in the above relationship, where companies have the financial resources required to purchase predictive technologies and gain access to big data. There is a margin of leeway for exceptions, where individuals have the ability to utilize predictive technologies, however these remain the exception. Also relevant is that the institutions using predictive modelling are central to the functioning of society and that the decisions being taken by predictive models are not of an inconsequential nature. Banks, insurance companies, credit institutions, employment agencies and public authorities are using this technology and it can determine whether a job is offered, a loan granted, insurance is obtained or a state benefit granted. The areas of application are increasing, with predictive modelling algorithms defining the nature and scope of a human being's interaction with the digital environment.

Irrespective of the outcome of a predictive modelling process, the actual process is fraught with dangers to the individual, who can be negatively influenced. Individuals are constantly being scrutinized: what they buy, what they don't buy, what they click on, what they don't click on, the digital route they took when they bought goods or services, the length of time the mouse cursor hovered over a certain link on-line before they clicked on it (or did not click on it), etcetera. The vulnerabilities to the individual are exacerbated because there is a general lack of awareness of predictive modelling. Even where there is an awareness of its existence, a danger is the attempt on the part of the

83 Lam, Bourree, *For More Workplace Diversity, Should Algorithms Make Hiring Decisions?*, available at <http://www.theatlantic.com/business/archive/2015/06/algorithm-hiring-diversity-HR/396374/> (last accessed on 2016-10-20).

84 TMF, *Can an Algorithm Diagnose Better than a Doctor*, available at <http://medicalfuturist.com/can-an-algorithm-diagnose-better-than-a-doctor/> (last accessed on 2016-10-20).

individual either to alter his or her behaviour in the face of this surveillance (in order to be seen in a more favourable light) or refrain from a certain behaviour completely. A further consequence of predictive modelling is the likelihood that the individual enters a comfort zone that he or she finds no reason to leave. An example is an on-line news site that is aligned with and skewed to a reader's political convictions. The site is comforting to the reader in that it reinforces his or her political convictions and belief system, and creates the impression that there is a wide consensus on this political view, reinforcing that view no matter how skewed it is in reality. There is a value in people being confronted with ideas or images that they do not necessarily agree with even if these are disliked, in that it promotes identity-building. It is in this light that tailored content negatively influences personal autonomy.

The second perspective taken is that of the group to the extent that groups are made up of individuals. This can occur as it is in the nature of this technology to place individuals into groups or categories, where they assume the characteristics of the group. These groups can potentially be discriminated against as a group, or the individuals, as members of that group, run the risk of being harmed. It is also noteworthy that the individual's interests may not necessarily be the same as a group interest or may even conflict with the group's interests. The group perspective, however, remains peripheral in relation to that of the individual.

A third perspective that is also theorized upon, is that of the circumstances and interests of the commercial actor performing the predictive modelling. While also a peripheral perspective, it is represented by the contemplation over the advantages and disadvantages that predictive modelling and a consequential empowerment strategy may have on a company's commercial development. For example, there may be situations where companies have access to large depositories of data, yet are afraid to use these data for fear of scaring off clients or potential clients. It is envisaged that resorting to an empowerment strategy would instil confidence in the commercial actor on the part of the individual, a consequence being the possibility for commercial actors to take advantage of untapped resources.

A fourth and final perspective taken into account is that of the state's interests in the relationship between the commercial actor and individual. As mentioned above, while state surveillance is not the focus of this study, it cannot be ignored that a state's surveillance policy may include commercial targets, the main aims being economic gain and the acquiring of control information on individuals. To this extent, states exert a degree of influence over

the commercial actor versus individual relationship.⁸⁵ Confining the focus of this thesis only to the relationship between commercial entity and individual is done with the awareness that this perspective is artificial in the sense that the three-way relationship as depicted by Figure 1 is difficult to separate.⁸⁶ An illustration of this is the law that was recently voted through the US Congress allowing Internet Service providers (ISP's) to sell the Web browsing and app usage data of their clients on to advertisers and other entities.⁸⁷

85 In this regard and for an in-depth investigation of the abilities of and reasons for the NSA's surveillance objectives in the US, see Greenwald, Glenn, *No Place to Hide*, Picador, 2014. Solove also refers to three types of information flow: first, between the databases of corporations, second, from the Government public record system to private corporations, and third, from the private sector to Government, in Solove, *The Digital Person*, above n. 67, at p. 3. See also pp. 168-175 for a description of the information flow between private companies and Government.

86 For an example of the relationship between private companies and authoritarian regimes, see Black, Edwin, *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation*, Crown Books, 2001.

87 Sundberg, Sam, *Trumps nya lag öppnar för helt ny nivå av propaganda*, Svenska Dagbladet, available at <https://www.svd.se/trumps-nya-lag-oppnar-for-helt-ny-niva-av-propaganda> (last accessed on 2017-03-30). See also Fung, Brian, *What to Expect Now That Internet Providers Can Collect and Sell Your Web Browser History*, The Washington Post, available at https://www.washingtonpost.com/news/the-switch/wp/2017/03/29/what-to-expect-now-that-internet-providers-can-collect-and-sell-your-web-browser-history/?hpid=hp_hp-more-top-stories_switch-inter-net606m%3Ahomepage%2Fstory&utm_term=.d8cc4a3b6a81 (last accessed on 2017-03-30).

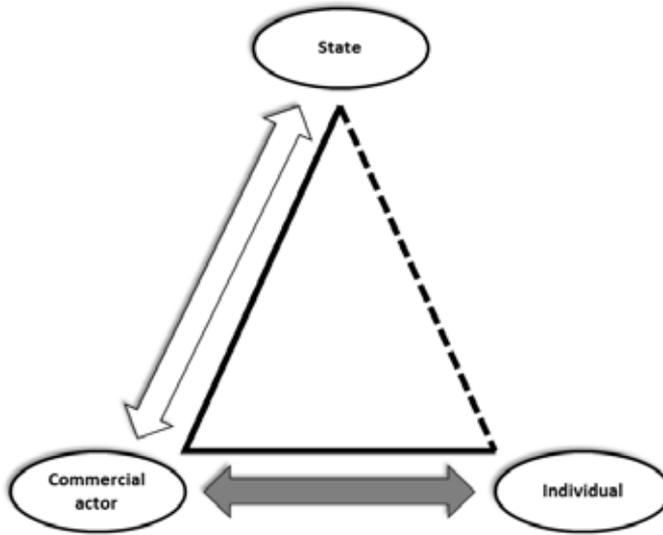


Figure 1 represents the main relationship of this study, namely that between the commercial actor and individual, as represented by the dark horizontal arrow. What this figure represents is the manner in which the relationship between commercial actor and individual is influenced by the state, where the state's interaction with commercial actors indirectly influences individuals. As a result it is difficult to study the relationship between commercial actor and individual in isolation. This study does not examine the direct relationship between state and individual as represented by the broken line. For example, instances of state surveillance on individuals by law enforcement are not covered.

1.7 Scope and Delimitation

The main focus of this thesis is the use by companies of predictive modelling techniques in order to regulate their relationships with clients or potential clients. It does not examine the use of predictive modelling by the state on its citizens, for example, in as far as it is used by public authorities or law enforcement agencies. In this regard, two reservations are necessary.

First, references are made to instances where the state does utilize predictive modelling for various purposes, however, these references are provided to the extent that they highlight the cooperation between the state and companies or for the purposes of illustrating the power of technologies such as predictive modelling in specific contexts. As a result, questions surrounding an individual's right to access his or her profile held by a public authority and

used as a basis for an administrative decision, will not be canvased. Also, reference is made to certain principles that have their origin in administrative law, for example, the principle of the right to access public information. This is done for the purposes of illustrating a point or providing argumentation.

Second, and as mentioned above, it is impossible to examine the relationship between commercial actor and individual without involving the state. Even where the relationship between state and individual is hidden, the state still either exerts control over the individual via its relationship with companies or uses companies as a mechanism through which information on individuals is collected. It is in this context that, while the main focus is the relationship between commercial actor and individual, the role of the state cannot be completely ignored and will be illuminated to the extent that it is relevant.

A further delimitation, closely linked to the first, is that this thesis does not directly examine the use of predictive modelling by the security apparatus. However, these instances will be addressed to the extent that they are relevant in the context of the relationship between commercial actor and individual. Many countries' law enforcement departments, security sections and even military have acquired predictive modelling capabilities. This has been done in order to combat crime, detect terrorist activity and identify internal as well as external security threats. However, included in the above list is also commercial espionage, in which case the involvement by the security apparatus becomes relevant.

In examining the phenomenon of predictive modelling, it is recognized that the preoccupation with a specific technology is done with caution and with a realization of the inherent danger associated with focussing on one single technological phenomenon. Taking into account the speed with which technology develops, it is important to emphasise the speed with which a technology can also become redundant, only to be replaced by another, more effective technology. Nevertheless, a superficial investigation of predictive modelling is carried out in order to ascertain its effects on human beings and therefore society. Consequently, in examining predictive modelling, the emphasis is not so much on the minute details of the technology itself, but focuses rather on the effects that this technology has on human beings.

This thesis focuses on the legal framework of data privacy in order to examine whether the technological phenomenon of predictive modelling, and consequently its effects on personal autonomy, is satisfactorily addressed. It is submitted that this is not a study of data privacy in its entirety. Data privacy

is utilized in order to highlight the difficulties that can be encountered in attempting to regulate a technological phenomenon using only traditional law. In fact, the reach of the phenomenon of predictive modelling is such that it essentially affects all areas of law. For example, anti-discrimination law, jurisprudence, consumer protection, contract law and even labour law are just some of the areas of law that are triggered by this phenomenon. Each of the above areas of law could be applied and potentially regulate predictive modelling just as effectively as data privacy. Consequently, where reference is made to data privacy, the intention is not to bind a potential solution to the harms of predictive modelling, to any particular area of law.

This thesis takes up the issue of identity and more specifically the fact that a person can have multiple identities depending on the context that he or she is operating in. For example, a person may portray a different identity at home as opposed to the identity portrayed at work. It is also accepted that many people give expression to their identity through avatars that are used in Massively Multiplayer Online (MMO) games. Here a player may identify strongly with his or her on-line character or avatar, which in itself is an expression of identity. However, where the issue of identity is raised in this thesis, it excludes the examination of the role of avatars in the formation of an individual's identity.

A suggested solution to the challenges associated with predictive modelling is the creation of a proprietary right in data, which would force commercial actors to pay for the use of personal data and thereby provide the individual with a form of control. While reference may be made to this notion, this issue remains outside of the boundaries of this thesis.⁸⁸

The main focus of this thesis is the European legal space. More specifically, it examines the European data privacy regulatory framework. Two qualifications are required in this regard. First, considering the international nature of the technological phenomenon studied, references are made to international developments, both technical as well as legal. Second, references are made to national regulatory regimes and the sources of law that are relevant to that system. For example, traditional laws, preparatory works and even technical developments from Sweden are consulted. This is done in order to obtain inspiration and identify trends, and is intended to function as a source of material to the extent that it reinforces an argument being made.

88 For an analysis on this issue, reference is made to Purtova, Nadezhda, *Property Rights in Personal Data: A European Perspective*, Wolters Kluwer Law and Business, 2012.

An observation concerning the scope of this thesis is that the sphere of legal informatics is extremely broad and that so many aspects are potentially relevant. For example, the subject matter of this thesis could be studied from a purely cybernetic perspective or a purely behavioural sciences perspective could be taken. It is with this in mind that it was necessary to establish limits as far as the content of this thesis is concerned.

Finally, it is not the intention that this thesis will provide an ultimate solution. Rather, the intention with this thesis is to provide a general orientation in relation to the subject of predictive modelling that can form the basis for future studies.

1.8 Previous Research

The research ambit of this thesis is wide and as a consequence, attempting to identify all previous research on the topic is futile, considering that many scholars from multiple disciplines have touched on this topic in some manner and at some point in time. To mention only a handful of scholars would be disrespectful to those who are not mentioned but whom also have contributed.

Instead, while reflecting on previous research done in relation to the phenomenon of predictive modelling, a point in need of stressing is that the mechanics of predictive modelling, in other words its basis in operational terms, are not that novel and have existed for some time. Essentially, the methodology that lies at the heart of predictive modelling is the practical application of statistics and mathematics to data. In order to make sense of and even predict social behaviour, the main aim is the acquisition of insight into behavioural phenomena based on a quantitative measure to assist in a decision-making process and facilitate social steering. An inherent element of this process is the operationalization of the quantitative basis of analysis. In other words, where data is used, the categorization and labelling of that data can affect the outcome of the statistical analysis.

The methodology of gaining insight by means of empirical data is not new to the behavioural sciences and can be found in disciplines such as economics, criminology, sociology and even the law. Within the legal sphere, a term reflecting the above methodology is ‘jurimetrics’, which was coined by

Loevinger, who described it as, ‘the scientific investigation of legal problems’.⁸⁹ He argued that the law, like any other mechanism of social control, must start employing the methods used to attain knowledge in other fields, criticising the area of legal jurisprudence, which he argued was based on, ‘speculation, supposition and superstition ... concerned with meaningless questions ... and, after more than two thousand years, [...] has not yet offered a useful answer to any question or a workable technique for attacking any problem’.⁹⁰ It is in this context that Loevinger distinguished jurisprudence from jurimetrics in a number of ways. First, the problems of jurisprudence are meaningless in that they can be discussed but never decided, whereas problems within jurimetrics can be investigated and solved, with an answer being provided. Second, if one were to argue that a problem within jurisprudence was solved, for example by the provision of an authoritative argument, this would have no practical implications whereas answers attained within jurimetrics significantly affect individuals. Third, compared to jurisprudence, which is static in nature and allows only for one authoritative answer, jurimetrics is dynamic in that it allows for multiple answers as knowledge grows and where the questions themselves change as knowledge increases.⁹¹

Seeking another definition of ‘jurimetrics’ one can turn to the work of De Mulder et al.:

Jurimetrics is concerned with the empirical study of the law in the widest sense, not only the meaning but also the form and the pragmatic aspects of the law ... Jurimetric research uses a model building approach ... an attempt is made to express the theory in mathematical and statistical models. This usually entails quantification, often unavoidable because of the necessity of calculating probability. It is essential to select the best possible model for describing, explaining and predicting human behaviour.⁹²

89 Loevinger, Lee, *Jurimetrics the Next Step Forward*, Minnesota Law Review, Vol. 33, No. 5, April 1949, p. 455, at p. 483.

90 Ibid.

91 Ibid, at p. 489.

92 De Mulder, Richard V., Van Noortwijk, Kees and Kleve, Pieter, *Knowledge Management for Lawyers: A New School Approach in Vem reglerar informationsamhället?* Greenstein, Stanley (ed.), Nordisk Årsbok i rättsinformatik 2006-2008, Jure, 2010, at p. 216.

Put another way, De Mulder describes it as, “the empirical legal science” that should be concerned with the world of experience’, equating it with Loevinger’s argument that it was closely related to other terms that had a similar meaning, such as ‘biometrics’ and ‘econometrics’, the scientific approach of economic phenomena.⁹³

Generally, jurimetrics contains the following aspects: first, there is an empirical study of legal phenomena, second, with the aid of mathematical models and third, based on methodological individualism or rationality.⁹⁴ A legal phenomena can be a legal document, for example, the mathematical model is usually based on statistics, while methodological individualism is a theory to describe, explain and predict human behaviour.⁹⁵ In many circumstances the manner in which a person acted is judged against a standard of how a regular person would have reacted under those same circumstances. For example, within law, the ‘reasonable man’ or ‘reasonable person’ test is often utilized in criminal law. This standard is described as, ‘a fictional person with an ordinary degree of reason, prudence, care, foresight, or intelligence whose conduct, conclusion, or expectation in relation to a particular circumstance or fact is used as an objective standard by which to measure or determine something (as the existence of negligence)’.⁹⁶ Within jurimetrics, a standard of the individual is taken from modern economic theory, known as the ‘homo economicus’ or REMO (resourceful, evaluating, maximizing person) against which processes are studied.⁹⁷ Just as the ‘reasonable person’ standard is used within law, the standard of the ‘economic man’ is the fictional standard against which people are judged within jurimetrics.

A Swedish example from the 1970’s shows how jurimetrics can be applied in practice, for example, to the area of family law and how attempts were made to apply the methodology of quantifying a body of legal text and assessing it

93 De Mulder, Richard, Van Noortwijk, Kees and Combrink-Kuiters, Lia, *Jurimetrics Please!*, in Paliwala, Abdul (ed.), *A History of Legal Informatics*, LEFIS Series 9, Prensas Universitarias de Zaragoza, 2010, at p. 147, see also Loevinger, above n. 89, at p. 483, footnote 77.

94 Ibid, at p. 150.

95 Ibid.

96 Merriam-Webster Dictionary, *Reasonable person*, available at <https://www.merriam-webster.com/legal/reasonable%20person> (last accessed on 2017-01-18).

97 De Mulder, Van Noortwijk, and Combrink-Kuiters, above n. 93, at p. 151.

with statistical methods and with the help of information technology.⁹⁸ The Swedish legal scholar Saldeen produced a book entitled *Divorce Damages: A Study in the Field of Sociology of Law and Jurimetrics*, which was based on his prior thesis and which examined a rule commencing damages in divorce matters according to the Marriage Code of 1920. The jurimetrics work examined how this rule was interpreted and what importance it had in practice, by subjecting it to a quantitative analysis and using what was at that time called an ‘automotive data processing technique’. In studying the relationship between various factors and the ensuing damages awarded, one hypothesis in the research tested the extent to which a work that existed at the time, which summarised decisions of the higher courts and that was relied on by the courts as guidelines, was actually used by lower courts in their decisions. The jurimetrics study revealed that the lower courts did not follow this work as extensively as one would have assumed, but rather placed a greater emphasis on the factors of each individual case.⁹⁹ Another finding of the study showed that statistical analysis, for example multiple regression analysis, could be utilized in identifying which factor, of many, was most relevant when determining damages.¹⁰⁰ Since the introduction of jurimetrics, it has undergone swings in its popularity and while it may not receive the attention that it once did, the principles of jurimetrics are still being applied, especially within the area of knowledge management and legal advice systems.¹⁰¹

Criminology is another discipline that utilises a statistical and quantitative analysis of data in order to develop a basis for decision-making and eventually social steering. An example here is the Swedish National Council for Crime Prevention (Brå), a public authority under the Ministry of Justice.¹⁰² The main aim of Brå is to collect statistics concerning crime, which in turn form the basis for decisions relating to crime prevention taken by the judicial system, Parliament and Government.¹⁰³ In other words, by evaluating criminal activity

98 Saldeen, Åke, *Divorce Damages: A Study in the Field of Sociology of Law and Jurimetrics (Skadestånd vid äktenskapsskilnad: En rättssociologisk och jurimetrisk studie)*, Almqvist and Wiksell, 1973, summary in English at p. 267.

99 Ibid.

100 Ibid, at p. 279.

101 De Mulder, Van Noortwijk, and Kleve, above n. 92, at p. 216.

102 BRÅ, The Swedish National Council for Crime Prevention, available at <http://www.bra.se/bra/bra-in-english/home.html> (last accessed on 2017-01-18).

103 Ibid.

through statistical application, resources can be funnelled in a certain direction. One can also make reference to academic publications that connect the law with statistical analysis.¹⁰⁴ Another example on the EU level is Eurostat, the statistical office of the EU. It provides statistics for politicians to base their policies on as well as in order to provide an accurate picture of society.¹⁰⁵

Finally, another relevant term that can be associated with this study of predictive modelling is that of ‘cybernetics’, which originates from the Greek word ‘to steer’ and is defined as, ‘the scientific study of how people, animals, and machines control and communicate information’.¹⁰⁶ This term was coined by Wiener and incorporated into the title of a book he wrote, called *Cybernetics: Or Control and Communication in the Animal and the Machine*.¹⁰⁷ A description of the relevance of cybernetics is that it, ‘connects control (actions taken in hope of achieving goals) with communication (connection and information flow between the actor and the environment)’, in effect stating that the ability to control something requires communication.¹⁰⁸ The title of Wiener’s book thus suggests that both animals and machines operate according to the principles of cybernetics and as a result that both living and non-living entities can have a purpose.¹⁰⁹ Pangaro, in explaining cybernetics, states that:

Cybernetics is about steering and reaching a goal and that all interactive and intelligent systems have the property of a self-correcting loop whereby, in relation to the goal, they are repeatedly trying, acting, and seeing the difference

104 Finkelstein, Michael O. and Levin, Bruce, *Statistics for Lawyers*, Springer-Verlag, 1990.

105 Eurostat, *Overview*, available at <http://ec.europa.eu/eurostat/about/overview> (last accessed on 2017-03-30).

106 Merriam-Webster Dictionary, *Cybernetics*, available at <https://www.merriam-webster.com/dictionary/cybernetics> (last accessed on 2017-01-19).

107 Wiener, Norbert, *Cybernetics: Or Control and Communication in the Animal and the Machine*, (Hermann & Cie) & Camb. Mass. (MIT Press), 1948.

108 Pangaro, Paul, “*Getting Started*” *Guide to Cybernetics*, available at <http://www.pangaro.com/definition-cybernetics.html> (last accessed on 2017-01-19).

109 Ibid.

and changing, and without the loop of constantly acting, sensing and comparing to a goal, a system cannot be considered intelligent. Cybernetics describes systems that have goals, be they social, technical or biological.¹¹⁰

Broadly speaking, cybernetics is a principle that has broad application and has at its core the notions of steering and feedback control combined with automatic correction. The feedback notion is described as, ‘a self-correcting device which enables a machine to regulate its operation by adapting the drift of its own deviations’.¹¹¹ Latil, describing the feedback mechanism as, ‘the secret of universal order’, provides a formal definition: ‘[a] feedback system is a “retroactive coupling” which, within certain limits, will protect the effect from the variations of its factors’.¹¹² The cybernetics feedback loop coupled with electronic circuits allowed for immense industrial progress. An industrial application of a feedback system is illustrated by the example of the production of sheet metal on a rolling-mill. The difficulty with this process lies in achieving sheet metal of a uniform thickness as at least seven factors can affect the outcome of this process: the metal sheet, the distance between rolls, the thickness of the metal, temperature and traction on the sheet as it is rolled backwards and forwards, speed of the rolls, malleability and ductility. The traditional manner of approaching this problem was to attempt to calculate and set all the variables in advance. However, adjusting one variable automatically influences the other variables and considering the time required to implement this change, all the variables would have changed anyway by that time. To solve the problem, a feeler gauge was used to measure the finished product and then send an electronic signal to just one of the variables, that is the last variable affecting the thickness of the steel as it came out of the rolls (the cybernetic feedback loop). The rolls, being the last variable, could indirectly compensate for adjustments to inaccuracies with all the other variables. This revolutionary working method has two distinct characteristics: first, there was

110 This citation is a paraphrased account of what cybernetics entails, based on an interview available on the internet and conducted with Pangaro, Paul, entitled *What is Cybernetics?*, available at <https://vimeo.com/41776276> (last accessed on 2017-01-19).

111 De Latil, Pierre, *Thinking by Machine: A Study of Cybernetics*, Houghton Mifflin Company Boston, 1957, (translated by Golla, Y. M.), at p. 51.

112 *Ibid*, at p. 60.

no concern regarding the cause of a problem, it was just fixed and second, even unforeseen variables could be addressed.¹¹³

Therefore, taking into account the above notions, while the amounts of available data have increased and the technological tools available for seeking knowledge from this data have developed, the fundamental processes of predictive modelling are not novel. The operation of predictive modelling in essence relies on a well-established tradition of the quantitative analysis of data and the accompanying applied statistical manipulation of that data. Predictive modelling is rather similar to this tradition: it involves observing human behaviour, quantifying it to allow for the application of statistical and mathematical analytical techniques, building statistical models for describing, explaining and predicting human behaviour and finally, attaining a scientific basis for embarking on a strategy of social control.

Finally, reference is made to Wendell Holmes who stated that, '[f]or the rational study of the law the black-letter man may be the man of the present, but the man of the future is the man of statistics and the master of economics'.¹¹⁴

All in all, the main message being portrayed here is that while technology advances rapidly and developments sometimes seem novel, it is important to bear in mind that the underlying ideas may not necessarily be as novel as would seem on the surface, giving legitimacy to the proverb that, 'there is nothing new under the sun'.

1.9 Positive Aspects of Predictive Modelling

In order to avoid a far too dystopian picture of predictive modelling, some positive aspects are illuminate here. First, from the economic perspective, the increased availability of data, together with the technical means to exploit it, is valuable, and even necessary, for the economic development of society in general. Some examples mentioned by the OECD are the effectivization of the

113 Ibid, at pp. 56-58.

114 Holmes Jr., Oliver Wendell, *The Path of the Law*, 10 Harvard Law Review, 1897, Project Gutenberg, 2006, available at <https://www.gutenberg.org/files/2373/2373-h/2373-h.htm> (last accessed on 2017-03-30).

manufacturing industry, the more effective use of labour, the ability to tailor services and the more effective use of energy resources by implementing ‘smart’ solutions.¹¹⁵ The EU too has identified the benefits to be gained from data, stating that, ‘[d]ata has become the essential resource for economic growth, job creation and societal progress. Data analysis facilitates better decision-making, innovation and the prediction of future events’.¹¹⁶ Within the health industry, the use of technology based on data and modelling practices is helping medical practitioners diagnose and treat illnesses.¹¹⁷ Siegel outlines predictive modelling incentives by private companies and public authorities that are of benefit to society, both from an economic perspective but also from the perspective of the individual.¹¹⁸ For example, models assess the risks associated with surgery, models predict influenza trends (Google flu trends), models predict breast cancer, sepsis, HIV progression and the effect of medical drugs and models identify the risks for babies born prematurely.¹¹⁹

Delving a little deeper into the treatment of prematurely born babies, a venture between IBM, the University of Ontario Institute of Technology and Canadian Hospital will allow for the use of software developed by IBM to increase the chance of survival of these babies. By monitoring various biomedical information with the use of sensors, doctors will be provided with information to help them make better decisions concerning treatment, where the

115 OECD, *Data-Driven Innovation for Growth and Well-being*, available at <http://www.oecd.org/sti/ieconomy/data-driven-innovation.htm> (last accessed on 2017-01-18).

116 European Commission, *Public Consultation on Building the European Data Economy*, available at <https://ec.europa.eu/digital-single-market/en/news/public-consultation-building-european-data-economy> (last accessed on 2017-03-30). See also European Commission, *Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*, {COM(2017) final}, Brussels, 10.1.2017, SWD(2017) 2 final, available at <https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy> (last accessed on 2017-03-30).

117 Memorial Sloan Kettering Cancer Center, *Memorial Sloan Kettering Trains IBM Watson to Help Doctors Make Better Cancer Treatment Choices*, available at <https://www.mskcc.org/blog/msk-trains-ibm-watson-help-doctors-make-better-treatment-choices> (last accessed on 2017-01-18) and TMF, *Can an Algorithm Diagnose Better than a Doctor*, available at <http://medicalfuturist.com/can-an-algorithm-diagnose-better-than-a-doctor/> (last accessed on 2016-10-20).

118 Siegel, Eric, *Predictive Analytics – The Power to Predict Who Will Click, Buy, Lie or Die*, John Wiley & Sons, 2013, at pp. 265-289.

119 Ibid, at p. 274.

model will be able to notify of a change in a baby's medical condition up to twenty-four hours in advance by analysing the physiological data.¹²⁰

Predictive modelling also improves the experience of the consumers of services in the digital environment. For example, people prefer receiving advertising that is more relevant as opposed to unrelated advertising, tailored digital services more accurately reflect the tastes of the consumer and the use of predictive models by public authorities benefits society as a whole. Predictive modelling can be used to reduce crime, to fight terrorism and be used to increase the welfare of the state in general, for example by making sure that the economy is strong and that taxes are collected, allowing for society to prosper.

Initiatives at airports using predictive models are also not only solving congestion problems, but also reducing emissions from planes, thereby resulting in gains in relation to the environment. For example, predictive models are being used at Heathrow airport to predict the best order of take-off for the planes. This system then allows air traffic control to determine with more precision, when planes should push back from their gates, thereby reducing the amount of time that they stand idle with their engines running.¹²¹

Another positive aspect with predictive modelling is the manner in which this technology can be beneficial to the individual in respect of identity building. Considering technological developments, it can be argued that the ability for people to express themselves using multiple identities has never been greater. To a large degree, mainly the negative influences of predictive models on identity are illustrated throughout this thesis. However, it must be borne in mind that many of the on-line applications that individuals use in order to create multiple differing identities, use predictive modelling technology too. It is in this regard that both the pros and cons associated with technology must be viewed.

However, considering the advantages, one should not become blind to the challenges that technologies such as predictive modelling pose.

120 IBM, *First-of-a-Kind Technology to Help Doctors Care for Premature Babies*, available at <https://www-03.ibm.com/press/us/en/pressrelease/24694.wss> (last accessed on 2017-01-18) in Siegel, above n. 118, at p. 60.

121 Institute for Aerospace Technology, *IAT Academic discusses airport scheduling at Heathrow on BBC series*, available at <https://www.nottingham.ac.uk/aero-space/news/iat-academic-discusses-airport-scheduling-at-heathrow-on-bbc-series.aspx> (last accessed on 2017-02-27).

1.10 The Dangers Associated with Predictive Modelling

Despite the advantages associated with predictive modelling, there are some inherent dangers that require attention. In order to illustrate the risks associated with predictive modelling, three examples are briefly described.

The first example is a real-life reference to what will hereinafter be referred to as the ‘Washington, DC example’. It depicts not only the risks associated with predictive models in this specific instance, but is illustrative of the risks associated with the use of predictive models in general. This scenario is relevant for the themes that it invokes, addressed throughout this thesis.¹²²

In 2007 the mayor of Washington, DC wanted to increase the performance of school children in the area. Acting upon the theory that the students’ bad results were the result of bad teachers, the newly hired school chancellor for Washington, DC embarked on a plan to rid the district of the bad teachers by implementing a teacher assessment tool called IMPACT. The system utilized a ‘value-added’ method that used mathematical formulas to determine how much value a teacher had added to what a student had learnt.¹²³ As a result of the system, 206 teachers (the bottom 2 percent identified by the system) were fired. One of the victims of IMPACT was a 5th grade teacher SW. As a teacher she was receiving excellent reviews from the school principal and parents alike. However, she received a poor IMPACT assessment for teaching maths

122 O’Neil Cathy, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Crown, 2016, at pp. 3-11. This real-life example is portrayed by O’Neil who uses the term ‘Weapons of Math Destruction’ (WMD) to describe models based on mathematics and that are predictive in nature. The above scenario was also investigated in Turque, Bill, ‘Creative ... motivating’ and fired, *The Washington Post*, March 6, 2012, available at https://www.washingtonpost.com/local/education/creative--motivating-and-fired/2012/02/04/gIQAwzZpvR_story.html?utm_term=.c00363531ed5 (last accessed on 2017-02-27), Strauss, Valerie, *Firing of D.C. teacher reveals flaws in value-added evaluation*, March 7, 2012, available at https://www.washingtonpost.com/blogs/answer-sheet/post/firing-of-dc-teacher-reveals-flaws-in-value-added-evaluation/2012/03/07/gIQAtmlGxR_blog.html?utm_term=.6e40150898f2 (last accessed on 2017-02-27) and Gillum, Jack and Bello, Marisol, *When standardized test scores soared in D. C., were the gains real?* USA Today, March 30, 2011, available at http://usatoday30.usatoday.com/news/education/2011-03-28-1Aschooltest-ing28_CV_N.htm (last accessed on 2017-02-27).

123 Strauss, Valerie, *Firing of D.C. teacher reveals flaws in value-added evaluation*, above n. 122.

and language, as generated by the algorithm used by the IMPACT model. Despite SW's positive reviews by principal and parents, the attitude of the authorities was that the data did not lie and was objective, and she was one of the 206 teachers consequently fired. The company behind the development of IMPACT had been given the task of trying to model the progress of the students in the district and then to calculate how much of their advance or decline could be attributed to their teachers. The problem to be solved was complex in nature due to the abundance of factors that could shape the outcome, for example, the personal circumstances of the students. This model exhibited some initial flaws: first, there were many factors that could result in a student doing better/worse from one school year to the next, making this a complex situation, second, basing a test on only about 30 student assessments was statistically unsound and third, having a feedback loop is useful in teaching a model where it went wrong, something that IMPACT lacked. To add insult to injury, the predictive model used was complex and was for all intents and purposes, a 'black box', with teachers who questioned the system unable to receive an explanation regarding how it worked. Two further anomalies present themselves. First, SW noticed that the level of proficiency of the students leaving 4th grade was stated to be high but that they had dropped considerably by the time they started SW's 5th grade class. Second, the media that started to investigate this event found that the actual tests of the students showed a large degree of erasure, up to seventy percent, a sign that there may have been cheating.¹²⁴ Considering that teachers received a monetary incentive for their students outperforming other students coupled with the fact that their own jobs were on the line, being under the constant scrutiny of the IMPACT model, a plausible finding suggested that 4th grade teachers were in fact altering the tests of their students in order to portray themselves in a better light. This resulted in the appearance that SW's students had become worse during the 5th grade, while in actual fact they had started the school year with an inflated level of proficiency, making SW look bad. O'Neil, using the term 'weapons of math destruction' (WMD), depicts one of the main dangers with predictive models:

But you cannot appeal to a WMD. That's part of their fearsome power. They do not listen. They do not bend. They're deaf not only to charm, threats and cajoling but also to logic – even when there is good reason to question the data

124 Gillum and Bello, above n. 122.

that feeds their conclusions. Yes, if it becomes clear that automated systems are screwing up on an embarrassing and systematic basis, programmers will go back and tweak the algorithm. But for the most part, the programs deliver unflinching verdicts, and the human beings employing them can only shrug, as if to say, “Hey, what can you do?”.¹²⁵

SW was fortunate in that her former principal and parents vouched for her and she found a new job. However, this scenario demonstrates the hidden dangers associated with the wide-spread use of predictive modelling. The technology is a ‘black box’, where few understand its complex mathematical nature, if they are even aware of its existence. It also represents the faith in data and the accompanying refusal to entertain suggestions that technology can get it wrong. It portrays the utter helplessness of the individual who is the victim of an unjust decision. A final dimension is cited by O’Neil in describing WMD’s:

They tend to punish the poor. This is, in part, because they are engineered to evaluate large numbers of people. They specialize in bulk, and they’re cheap. That’s part of their appeal. The wealthy, by contrast, often benefit from personal input. A white-shoe law firm or an exclusive prep school will lean far more on recommendations and face-to-face interviews than will a fast-food chain or a cash-stripped urban school district.¹²⁶

The second example refers to research in China, where predictive models are being used to identify criminals based on facial features.¹²⁷ The researchers alledge that after feeding 1856 images of real people into a computer, they were able to identify some structural features that separated criminals from non-criminals. They state that, ‘we find some discriminating structural fea-

125 O’Neil, above n. 122, at p. 10.

126 Ibid, at p. 8.

127 Wu, Xiaolin and Xi, Zhang, *Automated Inference on Criminality using Face Images*, 2016, available at <https://arxiv.org/abs/1611.04135> and <https://arxiv.org/pdf/1611.04135.pdf> (last accessed on 2017-03-21). See also Biddle, Sam, *Troubling Study Says Artificial Intelligence Can Predict Who Will Be Criminals Based on Facial Features*, *The Intercept*, 18 November 2016, available at <https://the-intercept.com/2016/11/18/troubling-study-says-artificial-intelligence-can-predict-who-will-be-criminals-based-on-facial-features/> (last accessed on 2017-03-22).

tures for predicting criminality, such as lip curvature, eye inner corner distance, and the so-called nose-mouth angle'.¹²⁸ The researchers also state the following:

Unlike a human examiner/judge, a computer vision algorithm or classifier has absolutely no subjective baggages, having no emotions, no biases whatsoever due to past experience, race, religion, political doctrine, gender, age, etc., no mental fatigue, no preconditioning of a bad sleep or meal. The automated inference on criminality eliminates the variable of meta-accuracy (the competence of the human judge/examiner) all together. Besides the advantage of objectivity, sophisticated algorithms based on machine learning may discover very delicate and elusive nuances in facial characteristics and structures that correlate to innate personal traits and yet hide below the cognitive threshold of most untrained nonexperts. This is at least a distinct theoretical possibility.¹²⁹

The degree to which such a predictive model can be abused is infinite.

The third example also illustrates the degree to which technologies, such as predictive modelling, are using facial recognition 'black boxes' to determine personality traits. The company called Faception uses machine learning techniques to determine an individual's personality using facial recognition techniques. The sources of the data are live and recorded video streams, pictures and databases, with some of the labels used to describe an individual's personality being 'extrovert', 'hi IQ', 'brand promoter' and 'terrorist'.¹³⁰ The technology is based on theory from the social and life sciences, which states that personalities are affected by genes and that a person's face is a reflection of their DNA, the developers basing this technology on the identification of five genes that influence the shape of a person's face.¹³¹ In the commercial sector, this technology can be used to identify a type of shopper: 'an early adopter', 'a compulsive buyer' or 'an adventurous type'.¹³²

Many of the dystopic themes and potential harms associated with predictive modelling highlighted by the above examples are addressed throughout this thesis.

128 Ibid.

129 Ibid.

130 Faception, available at <http://www.faception.com/our-technology> (last accessed on 2017-03-22).

131 Ibid, see also <http://www.faception.com/about-us> (last accessed on 2017-03-22).

132 Ibid, see also <http://www.faception.com/copy-of-financial-services> (last accessed on 2017-03-22).

1.11 Structural Overview

This thesis begins by describing the characteristics of the technological phenomenon of predictive modelling in Chapter 2. Entitled ‘The Black Box’, it sketches the historical development of certain technologies that are considered relevant for an understanding of the origins of the predictive modelling process. In doing so, it also makes reference to changing trends in technological developments. Chapter 3 provides a theoretical context to predictive modelling and the associated surveillance that it encourages. First, it explains why technological developments, such as the phenomenon of predictive modelling, have become popular. Technologies are seldom developed in a vacuum and do not invent themselves. There is usually a socio-technological dimension surrounding these developments. Predictive modelling is closely associated with surveillance, which is examined further in this chapter. Also, the notions of autonomy and identity are examined. Autonomy is delved into due to it being a central notion and common denominator in relation to the harms of predictive modelling. Identity is also examined to the extent that it is reliant on autonomy for its development as well as due to the fact that it is a central instrument by means of which human beings are judged in the digital environment. Chapter 4 comprises an inventory of the potential harms associated with predictive modelling. Some of these harms have a stronger association with the law, while others have a weaker one. While it is stressed that this list is by no means exhaustive, it does provide an inventory of the types of potential harms that can arise with the use of predictive modelling. Chapter 5 provides a legal framework in order to ascertain the extent to which autonomy and predictive modelling are addressed by traditional law. To this end, the legal realm of the European data privacy regime is utilized. Chapter 6 introduces a strategy, comprising various mechanisms, that can be used to bolster personal autonomy. This strategy is referred to as ‘empowerment’. Working from the hypothesis that traditional law alone seldom provides an adequate response to the risks associated with new technologies, empowerment is introduced as a complement to traditional law. In this regard, a number of components of the strategy of empowerment are laid out. Finally, Chapter 7 provides some concluding remarks and suggestions going forward.

2 ‘The Black Box’

2.1 Introductory Remarks

The ability to monitor the actions of individuals and their social interactions in the digital environment has increased markedly. This process has been made possible by modern digital networking technologies that constitute the on-line environment, represented by the internet and used by individuals for their every-day communication and social needs. This environment is increasingly being used by people to document their lives. Private companies and states also rely on the monitoring of this space. Companies do so to acquire information about their clients or potential clients for business reasons, in the face of increased commercial competition and where the increased mobility of people has weakened traditional commercial relationships.

A ‘black box’ is a popular metaphor for describing something, the characteristics of which are difficult to grasp. This is especially relevant regarding predictive modelling, an advanced technology used to assist with decision-making and extracting knowledge from data. While the manner in which this technology behaves is known, its inner workings are not, utilizing algorithms based on mathematics, statistics, machine learning and artificial intelligence techniques, which makes it particularly inaccessible for the common person. Predictive modelling is a ‘black box’ for a number of reasons. Most individuals either have no knowledge of their existence or if they do, they do not understand how they work or the implications of their use. Even in cases where the technology is comprehensible, it may still require a certain amount of research in order to grasp its operation or the effects on people. Also, even where the risks are illuminated, they may not be persuasive, as convenience of use in many situations trumps concerns over privacy in situations where time and attention is scarce. This complexity regarding technology affects not only the

individual that is the target of the technology but also the user of the technology. The challenge is exacerbated by the fact that the technology inside the ‘black box’ may have been developed by a person or company that is unrelated to where the technology is being applied. In addition, the technology that is represented is dynamic and in a constant flux. Tools presently being used to construct predictive models may become outdated overnight, only to be replaced by new, improved and more effective technology. It is impossible for individuals to keep abreast of this technological development. The inputs into the technology are also changing. With the increase in digitalization and with the new technologies not only consuming data but also creating new data, the amount of data points being produced is increasing dramatically. For example, in order to challenge a decision taken by an algorithm encapsulated in a decision-making software, it is required firstly that the algorithm is understood but also that an exact record of the data set provided to the algorithm is recorded, as changing the data set with one data point can affect the entire result produced by the algorithm, especially taking into account the iterative nature of the predictive process.

2.2 The Predictive Modelling Process Outlined

The following is intended as a preliminary general overview of the different stages in the predictive modelling process as outlined in this thesis, providing a preview of this process. This overview is depicted in Figure 2 below, which provides a visual explanation of the stages in the predictive modelling process. The technical concepts used in the figure are addressed in more detail throughout the chapter.

The Predictive Modelling Process

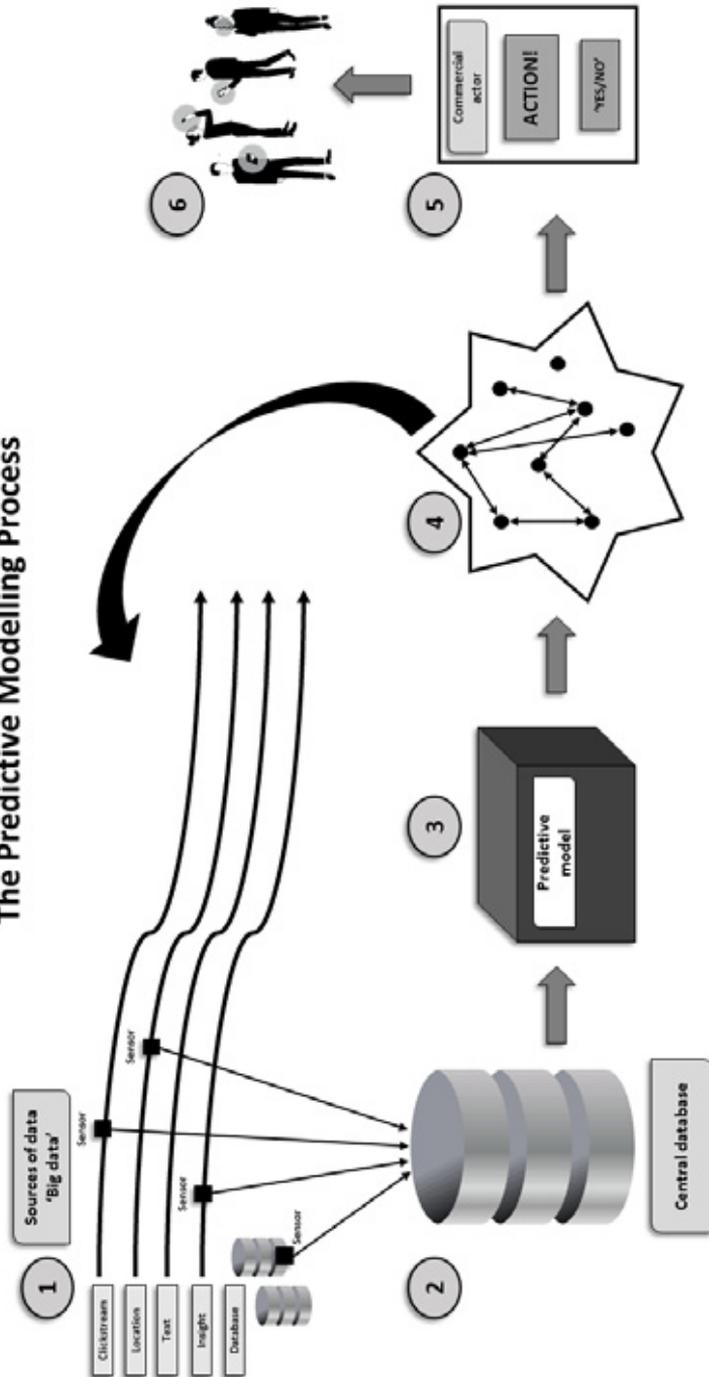


Figure 2 representing the six stages in the predictive modelling process.

Stage 1 of the predictive modelling process begins with the identification of the different sources of data and the various forms that these data can take. Here an important distinction is between the streams of live data that are ‘flowing out there in the digital environment’ and those data that have been stored in a more structured manner. Representing the streams of fluid data in figure 2 are ‘clickstream’ data, ‘location’ data, ‘text’ (for example, within the social media) and ‘insight’ data. These different types of data combined are represented by the term big data. Representing the data of a more static and structured nature are the data stored in databases. The various sources of data used in Figure 2 are only examples and in reality, many more types of data sources potentially exist. The squares represent sensors or filters that collect the various streams of data as well as the static data in databases. These sensors can take various forms, for example, a thermometer measuring temperature or an application monitoring the chat within the social media.¹³³ It is important to note that already at this stage, a decision has been made about what streams of live and structured data are to be monitored and which are not. In addition, an awareness is required concerning which data, from the monitored streams of data, are to be retained and stored. For example, having monitored a group of people with red hats, will data be stored concerning the fact that people with red hats were identified or will the data only refer to the fact that people with hats were identified, the fact that the hats were red potentially being irrelevant for the specific purpose of the data identification?

Stage 2 is characterized by the collection of these data into one central data collection point, for example, a central database. Again, here a number of options arise. First, the actual data analysed by the sensors may not require storing, but only the inferences or knowledge gained from these data (or a combination thereof). For example, having compiled a meteorological analysis of the weather, the raw data from all the weather stations forming the basis of that prediction need not be stored, the insight from these data, wherein the

133 The concept ‘sensor’ can be studied on many levels. Sensors can be viewed in terms of mechanical devices or on a more abstract level, where people are viewed as sensors. In this regard, reference is made to Seipel who describes ‘sensation’ as one of five elements making up ICT. The other four elements are ‘automation’, ‘information’, ‘communication’ and ‘integration’. It is in this context that Seipel emphasizes that humans sense not only with their brains, but also with their tools. Seipel, Peter, *Law and ICT. A Whole and its Parts*, in Seipel, Peter (ed.), Swedish Government Official Reports, SOU 2002:112, *Law and Information Technology: Swedish Views*, above n. 30, at p. 23.

value lies, having been incorporated into a model forecasting the weather. Data of a more structured nature may also be stored in the central database by combining it with other databases.

Stage 3 involves the development of a predictive model, which can be described as a 'black box'. Many terms can be used to describe this 'black box'. Here the term predictive model is used, although the terms machine learning and artificial intelligence are also relevant. This predictive model contains the 'machinery' that processes the data that has been stored in the central data collection point and which is fed into the predictive model in the form of an input. The predictive model, using different machine learning techniques, proceeds to analyse the input data, finding correlations between these data as well as knowledge that is invisible to human beings. One can argue that the 'black box' has taken over a human function that was previously performed by the expert consultant. Traditionally, a human being would analyse data from a specific industry and then provide expert advice to commercial actors on how to proceed on matters of a commercial nature. The difference now, however, is that while one could ask the human expert consultant for the reasons as to why certain advice was provided, this option is more limited in the age of the 'black box'.

Stage 4 takes the form of an output from the predictive model in the form of a representation of the knowledge that the predictive model discovered in the data supplied from the central data collection point (database). Here, the black dots represent individual data points and the arrows, the correlation between these data points. For example, two people may be connected by means of correlating two data points each belonging to one of these people. It may also identify a pattern in the data associated with a person that is indicative of a certain anticipated behaviour. It may identify a personality trait, it may identify personal preferences, it may reveal religious beliefs, it may reveal health information, it may reveal a person's political views or it may reveal which person has the most influence in a certain network. The arrow at stage 4, which points to stage 1, represents the fact whereby the information represented at this stage itself becomes part of big data, represented at stage 1. In other words, this 'new' information will potentially also be taken into account in future cycles or iterations of the predictive modelling process.

Stage 5 involves a commercial actor (or public authority) taking action based on the data representation. In other words, an entity, for example a private company or public authority, will make a decision for action based upon the knowledge as represented by the predictive model. This may take the form

of a ‘yes’ or ‘no’ decision. A bank may be required to decide whether to grant a loan to a prospective client or a public authority may be required to decide if a certain person qualifies for a benefit or not.

Stage 6 represents the individuals who are the target of the decisions taken by private or public entities and who either receive a positive outcome or must deal with the negative consequences of the predictive modelling process.

2.3 The Development of Technology

The increased use of predictive modelling has occurred for three main reasons. First, it is in the nature of technology and science to progress, and little can get in the way of this inherent characteristic of technology. Second, the increased mobility of people in a globalized world has resulted in a change in societal relationships between private companies and their clients, which has necessitated the increased reliance on technology.¹³⁴ Third, a number of developments within the digital environment have been a catalyst for the practical application of certain technologies that were previously of only a theoretical nature.

2.3.1 The Features of Data

Recent years have seen the proliferation of the availability of data. This growth has occurred in conjunction with the popularity of the internet as a sphere for commerce, communication purposes and social activities. As the insight into what purposes this data can be used for has deepened, so too has the demand for access to data increased, leading to the development of applications that not only rely on data, but actively produce new data. The result is that a lot of data has been created and a popular term used these days is that of ‘big data’. However, this label is misleading as these days it is not only the amount or size of the data that is at issue, but also its nature. This next section

134 This development is dealt with in more detail in Chapter 3 below.

examines the evolution of big data, the techniques used to extract knowledge from big data and provides insight into its changing nature.

2.3.2 ‘Big Data’

The term ‘big data’ is related to the use of concepts such as machine learning, algorithms and predictive modelling. The notion big data received public exposure in the an article entitled, ‘The End of Theory: The Data Deluge Makes the Scientific Method Obsolete’, using the phrase ‘biggest computing cluster’.¹³⁵ Since then the term big data has become common and not only its size has received attention, but also its nature:

Big data is an umbrella term. It encompasses everything from digital data to health data (including your DNA and genome) to the data collected from years and years of paperwork issued and filed by the government. And that’s just what it officially covers.¹³⁶

While there are no official or legal definitions of what big data actually is, there have been various attempts to describe it. These definitions help in capturing its nature and essence. One such definition is provided by boyd and Crawford, who describe it as:

[a] cultural, technological, and scholarly phenomenon that rests on the interplay of: technology (maximizing computation power and algorithmic accuracy to gather, analyse, link, and compare large data sets), analysis (drawing on large data sets to identify patterns in order to make economic, social, technical, and legal claims) and mythology (the widespread belief that large data sets offer a higher form of intelligence and knowledge that can generate insights that were previously impossible, with the aura of truth, objectivity, and accuracy).¹³⁷

135 Anderson, Chris, *The End of Theory: The Data Deluge Makes the Scientific Method Obsolete*, Wired, available at <https://www.wired.com/2008/06/pb-theory/> (last accessed on 2017-04-05).

136 Maycotte, Higinio, *The Evolution of Big Data, And Where We’re Headed*, Wired, available at <https://www.wired.com/insights/2014/03/evolution-big-data-headed/> (last accessed on 2017-04-05).

137 boyd, danah and Crawford, Kate, *Critical Questions for Big Data*, Information, Communication and Society, Vol. 15, Issue 5, 2012, at pp. 662-679.

Another term relevant in this context is the ‘data set’:

[a] collection of data ... collated from one or more separate sources and held in a single file ... The major difference between a database and a dataset is that a dataset is usually a single file/table and is intended for a single specific purpose, whereas a database is a more strategic collection of data that may be distributed across many different tables/files.¹³⁸

Yet another way of describing big data is in relation to its sheer size, referring to datasets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyse it.¹³⁹ An alternative reference is the ‘three V’s’, which relates to the words ‘volume’, ‘variety’ and ‘velocity’, where, ‘big data is high volume, high velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision-making’.¹⁴⁰ It has also been defined in relation to ‘volume’, ‘velocity’, ‘variety’, ‘veracity’, ‘validity’ and ‘volatility’.¹⁴¹ The data comprising big data can take the form of pictures, videos, sound or print, including both content data and meta data.¹⁴² It is the rate at which the data changes, which of course can result in problems with using the data, for example, for analytical purposes. One way of perceiving big data is as a philosophy concerning how to deal with data, where the main pillars of this philosophy are, ‘seek’, ‘store’, ‘analyse’ and ‘act’, and where the main principle of the philosophy is to take a holistic view of data and to do the best with what data is available to you.¹⁴³ One definition of big data focuses on the analytical tools used in conjunction with it, it being stated that, ‘... the main issues do

138 Finlay, above n. 1, at p. 211.

139 McKinsey Global Institute, *Big Data: The Next Frontier for Innovation, Competition and Productivity*, June 2011, referred to in Edvardsson, Tobias and Frydinger, David, Molntjänster – Juridik, Affär och säkerhet, Norstedts Juridik, 2013 at p. 195.

140 Gartner IT Glossary, *Big data*, available at <http://www.gartner.com/it-glossary/big-data> (last accessed on 2017-03-01).

141 This set of characteristics describing big data was put forward by Karlgren, Jussi at a conference organized by Stiftelsen för rättsinformation held on the 10th of November, 2015. More information can be found at <https://rattsinfo.se/> (last accessed on 2017-04-14).

142 These concepts are dealt with more extensively in section 2.3.3.1.

143 Finlay, above n. 1, at p. 14. The trend from storing data to merely using the insight to be gained from it and then discarding it is reflected upon hereunder.

not only concern the volume, velocity, and variety of processed data, but also the analysis of the data using software to extract new and predictive knowledge for decision-making purposes regarding individuals and groups'.¹⁴⁴ Another definition states that it is, '[a] paradigm for enabling the collection, storage, management, analysis and visualization, potentially under real-time constraints, of extensive datasets with heterogeneous characteristics'.¹⁴⁵ It is argued that an effective manner by which to describe the nature of big data is by the use of the word 'streaming', referring to its fluid nature and differentiating it from data of a more structured nature found in databases. The above characteristics of big data are accurately depicted by the following passage:

... and I say, hey stop, where is that database, it is not on the net, it isn't on the big net is it? Yes, it is on the big net, he says, but I hate the net, because the net is water ... because on the net everything flows, on the net the flow is free, freer than all other places together, it changes all the time, it is like an information flock of birds, it constantly changes direction, but not elegantly and at the same time, like a flock of birds, the image was miserable, forget it, but the direction changes, and you cannot step down into the same net twice, because it only exists for the moment and the next moment it will be something else, and I hate everything that is something else the next moment and I don't want to have anything to do with it ...¹⁴⁶

Big data can be characterised by a lack of structure, which distinguishes it from other forms of structured data, such as business intelligence. Within this lack of structure, correlations and patterns are sought.¹⁴⁷ Explaining the concept 'correlation', '[t]wo variables are said to be correlated if a change in one

144 Council of Europe, Consultative Committee of the Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, *Guidelines on the Protection of Individuals With Regard to the Processing of Personal Data in a World of Big Data*, Strasbourg, 23 January, 2017, at p. 2.

145 International Telecommunication Union, *Big Data – Cloud Computing Based Requirements and Capabilities*, Recommendation Y.3600, available at <http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12584&lang=en> (last accessed on 2017-03-30), at p. 2.

146 Loe, Erlend, *Facta om Finland* (Facts about Finland), Oslo, Cappelen, 2001, at p. 137 as translated and referred to in Seipel, Peter, Law and Information Technology Swedish Views, above n. 30, at p. 88.

147 Edvardsson, above n. 139, at p. 194.

occurs in tandem to a change in another ... Not to be confused with causation'.¹⁴⁸ Mayer-Schönberger and Cukier describe big data as, 'things one can do on a large scale that cannot be done on a smaller scale, to extract new insights or create new forms of value, in ways that change markets, organizations, the relationship between citizens and governments, and more'.¹⁴⁹

An interesting aspect associated with data in general, but that is also relevant in the context of big data, is the manner in which it is viewed. Data generally and as a result also big data are assumed to be totally objective by those relying on it. It is a collection of one's and zero's, either 'on' or 'off', purely digital and as a result one hundred percent 'true'. In other words, the data and accompanying sciences are always correct and provide a true reflection of reality. However, this view of big data is not shared by all. Hildebrandt points out that the term 'raw data', which is often used to describe the data comprising big data, is not as objective as it would seem and as it is made out to be, the reason being that human activity, which she refers to as 'the flux of life', can be translated into data in a number of ways.¹⁵⁰ Data is not necessarily objective and neither are the technologies that utilize it. All systems that in some way use data are built by someone who has an objective with that system or who has been given the task of building a system that has a certain functionality.

The potential associated with big data analysis should not be underestimated. This in turn has led to the use of the term 'data-driven society', where the abundance of big data and the decreased costs associated with collecting, storing and analysing it, is viewed as a key element to innovation within society and a driving force for economies, the production of products, the welfare of people and the increasingly efficient exploitation of energy resources.¹⁵¹

148 Finlay, above n. 1, at p. 210.

149 Mayer-Schönberger, Viktor and Cukier, Kenneth, *Big Data: A Revolution That Will Transform How We Live, Work and Think*, Mifflin Harcourt Publishing Company, 2013, at p. 6.

150 Hildebrandt, *Slaves to Big Data. Or Are We?*, above n. 59, at p. 32.

151 OECD, *Data-Driven Innovation*, 6 October 2015, available at <http://www.oecd.org/sti/data-driven-innovation-9789264229358-en.htm> (last accessed on 2016-09-09).

2.3.3 The Sources of Big Data

The data points making up big data originate from multiple sources of data. An important consideration is that computers consistently produce data, in other words, data is a by-product of computing in that computers document everything they do.¹⁵² In addition to this, individual's upload lots of data to the on-line environment. It could be data that the individual him or herself has uploaded to the digital environment, or that is uploaded by others yet which concern the individual. It could comprise trace data that the individual has left behind while navigating the digital environment, such as surfing the internet, or it could come from previously created digital profiles of the individual, be they full or partial. There are a multitude of sources that are increasing constantly.¹⁵³

A phenomenon that is connected to the rise of big data is what Mayer-Schönberger and Cukier refer to as 'datafication', described as the process of 'the taking of a phenomenon and putting it in to a quantified format so that it can be tabulated and analysed'.¹⁵⁴ Put another way, it is 'the process of trans-

152 Schneier, Bruce, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, Norton, 2015.

153 Providing a historical background to the development of big data, reference is made to the Swedish National Data Service (Svensk Nationell Datatjänst, SND), in the Swedish context, web site available at <https://snd.gu.se/sv> (last accessed on 2017-03-31). SND was previously referred to as the Swedish Social Science Data Service (Svensk Samhällsvetenskaplig Datatjänst), which in 1981 started to make an inventory of data from within the social sciences with the view of creating a central Swedish academic data archive that would potentially include all data from the research community (Svensk Samhällsvetenskaplig Datatjänst, SSD, *Svenska Databaser I*, Svensk Samhällsvetenskaplig Datatjänst, 1982). The main aim of SND is to facilitate the collection of, access to and safe storage of research data and related metadata in order that it can be re-used in the future. Reference in turn is made to the Consortium of European Social Science Data Archives (Cessda), established in 1976 as an umbrella organization for all the European national data archives, web site available at <https://cessda.net> (last accessed on 2017-03-31). Currently 15 European countries are members of Cessda. The mandate of Cessda includes the provision of data services to the social sciences and it also coordinates the national European data service providers. It coordinates the development of standards, protocols and best practices for the preservation and dissemination of data and associated digital objects. The vision of Cessda is to provide a full scale sustainable research infrastructure to the research community.

154 Mayer-Schönberger and Cukier, above n. 149, at p. 6.

lating the flux of life into discrete, machine-readable, measurable and manipulable bits and bytes'.¹⁵⁵ This includes the transfer of analogue data to the digital format. Not only are large amounts of digital information being collected, stored and analysed, but the nature of big data is influenced by the novel technical methods being developed in order to measure activities associated with human life. For example, people's posteriors are being measured and insight into identification via weight distribution is being used to prevent car theft and enhance road safety, the distribution of weight being an indicator that a person has fallen asleep behind the steering wheel of a car.¹⁵⁶

This collection and storage of data need not be done with the view of attaining immediate gains. Data may be collected and stored on the understanding that it will have value, if not in the immediate present, then in the future. It is only after attempts to gain knowledge or insight from data, that it can be established whether the data is of any use. In other words, the knowledge or insight being sought is only identified as such once located. The different sources of data collection are telling in that it reveals the extent to which surveillance is optimised in order to obtain this data.

2.3.3.1 Trace Data

One type of data associated with the digital environment is 'trace data', which is data, the creation of which, is made possible primarily due to the architecture of the internet and nature of digital technologies in general. An example is the digital photograph, where besides the actual image, large amounts of meta data are created by the camera. The meta data describes the picture, providing data such as when it was taken, where it was taken and what time it was taken.¹⁵⁷ Trace data created as a result of an action is alternatively referred to as 'meta data', which is defined as 'data about data' and describes data that

155 Hildebrandt, *Slaves to Big Data. Or Are We?*, above n. 59, at p. 31.

156 Mayer-Schönberger and Cukier, above n. 149, at p. 77.

157 Bylund, Markus, *Datadriven digitalisering – översikt och strukturering*, in Temarapport 2016:1 från Digitaliseringskommissionen (N2012:04), *Det datadrivna samhället*, Stockholm, 2014, at p. 40.

has the function of describing other data, typically of a content nature.¹⁵⁸ Computer code enables tracing in the digital environment, something that Lessig asserts is coupled with a conscientious choice on the part of the producers and owners of the code, who build traceability into the code of the applications that make up the internet.¹⁵⁹ In other words, trace data are those data created from actions and communications, of an active or passive nature, in the digital environment that can be traced back to an individual.¹⁶⁰ Trace data, as distinguished from the content of communications, can be revealing and of a sensitive nature. The fact that a communication took place and between whom is just as important as the content. For example, a telephone call from a person to a suicide help line in itself allows for certain inferences to be drawn.

Two forms of social network analysis are ‘ego-centric’ and ‘network centric’, the former involving a focus on the individual and an examination of his or her surrounding network with the aim of understanding him or her, whereas the latter focuses on the actual network and connections, in order to identify someone who exerts influence in a certain network.¹⁶¹ People with the same values and ideals usually associate with each other. Identifying one person enables the identification of like-minded people, who could, for example, be interested in similar products.

Therefore, the trace data that individuals leave behind them as they make their way through the digital environment are becoming important from the commercial perspective, especially where commercial actors want to learn more about how their customers think and why they act in a certain manner. Until the 2000’s, predictive analytics was based largely upon capturing peoples’ actual transactions in order to get information about them. The trend, however, has moved to analysing ‘the spaces between our transactions and the paths that led us to the decisions that we made’.¹⁶² In other words, analysing the steps that an individual took before purchasing a certain product can reveal

158 Eriksson, Bengt, *Maintaining Informtion Quality – Experiences from the Swedish Parliament- Sveriges Riksdag*, in Magnusson Sjöberg, Cecilia (ed.), *Legal Management of Information Systems: Incorporating Law in e-Solutions*, Studentlitteratur, 2005, at p. 240.

159 Lessig, above n. 53, at p. 91.

160 Whatis.com, *Digital Footprint*, available at <http://whatis.techtarget.com/definition/digital-footprint> (last accessed on 2017-03-16).

161 Finlay, above n. 1, at p. 189.

162 Ibid, at p. 1.

information concerning why he or she purchased one product over another. This can be more beneficial than knowing merely that an individual purchased a certain product. In this regard, the term ‘path to purchase’ has become popular within the marketing sector.¹⁶³

2.3.3.2 Sensor Data

As technology progresses, an increasing number of gadgets are being equipped with sensors, the ‘smart phone’ being a prime example. A sensor is described as, ‘a device which detects or measures a physical property and records, indicates, or otherwise responds to it.’¹⁶⁴ Cars are also fixed with sensors that record how people drive, health devices monitor individuals and report on their health status, fitness apparel monitor exercise rates and report back on exercise activity, such as calories consumed, sensors record the weather, sensors record traffic flows and devices within the home contain sensors that produce environmental data. These mechanical devices produce environmental measurements, report on the physiological status of individuals and relay location data, an application of which could entail personalized advertising at a fixed geographical point and at a certain point in time.¹⁶⁵ Trace data can be sensitive to the extent that it can show that an individual was at a certain location when a political meeting took place or it can show that two individuals were in the same vicinity at the same time.

Using historical location data, predictive models are able to predict where an individual will be in the future. For example, Nokia recorded the smart phone data of a group of users over a one-and-a-half-year period, releasing it to the scientific community as part of the Nokia Challenge. One project based on this data was able to predict the movements of people in Lausanne, Switzerland. It used telephone numbers, Global Positioning System (GPS) data, texting history and call history and was able to predict within a 24-hour period

163 KPMG, *The Path to Purchase Journey*, available at <https://home.kpmg.com/xx/en/home/insights/2017/01/the-path-to-purchase-journey.html> (last accessed on 2017-03-19).

164 English Oxford Living Dictionaries, *Sensor*, available at <https://en.oxforddictionaries.com/definition/sensor> (last accessed on 2017-03-19).

165 Gartner, IT Glossary, *Location-based Services*, available at <http://www.gartner.com/it-glossary/lbs-location-based-services/> (last accessed on 2017-01-26).

where individuals were heading to within a 20 square meter radius.¹⁶⁶ The algorithm designed for this purpose was more effective if it could process the data of a person's friends in the social media as well. Without this data, the algorithm could only make this prediction to within a 1000 square meter radius.¹⁶⁷ This highlights the value of network data within the social networks and the utility of being able to monitor an individual through his or her connections.

The 'Internet of Things' (IoT), is a phenomenon whereby devices are being equipped with sensors that have the ability to connect to the internet and envisages a future scenario where all devices connected to the internet will be able to communicate not only with humans but also with each other. It is predicted that by the year 2020 there will be 26 billion devices connected to the internet.¹⁶⁸ Ashton, who is attributed with coining the concept IoT refers to the savings, in terms of material as well as in monetary value, derived from the ability, 'to track and count everything'.¹⁶⁹

The IoT is a precursor to the creation of what is generally referred to as 'Ambient Intelligence' (AmI), which is essentially an electronic environment, made up of electronic devices connected to each other, that is sensitive and responsive to the presence of people and that assists them in carrying out certain tasks with the help of information and intelligence in the network itself.¹⁷⁰ AmI is characterised by two notions, namely, that the devices that operate within this environment are 'smart' (they interact with each other and without human involvement, in order to make decisions that are most beneficial for the person that they act on behalf of) and also that they operate everywhere

166 For a more precise description of GPS and how it works, see the website of Garmin, available at <http://www8.garmin.com/aboutGPS/> (last accessed on 2017-01-26).

167 Olson, Parmy, *Algorithm Aims to Predict Crime By Tracking Mobile Phones*, Forbes Tech, available at <http://www.forbes.com/sites/parmyolson/2012/08/06/algorithm-aims-to-predict-crime-by-tracking-mobile-phones/> (last accessed on 2015-05-06).

168 Morgan, Jacob, *A Simple Explanation of 'The Internet of Things'*, Forbes, available at <http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/> (last accessed on 2017-03-16).

169 Techopedia, *Internet of Things (IoT)*, available at <http://www.techopedia.com/definition/28247/internet-of-things-iot> (last accessed on 2017-03-16).

170 Ibid.

and also in the background, without being noticed (and hence are ambient).¹⁷¹ The distinction is made between ‘dumb’ and ‘smart’ devices, and where people previously physically manipulated ‘dumb’ devices, they now co-exist with the ‘smart’ ones, with which they exist in an, ‘unconscious, presumed symbiosis’, simply fading into the background.¹⁷² Yet another reference to AmI defines its key elements, namely: embedded (many network devices integrated into the environment); context-aware (these devices can recognize you and your situational context); personalized (they can be tailored towards your needs); adaptive (they may change in response to you) and anticipatory (they can anticipate your desires without conscious mediation).¹⁷³

Many of the electronic devices that contain sensors are designed to record and relay data concerning the health activities of the wearer of these devices. For example, the Nike Fuel Band¹⁷⁴ records steps taken in the day, calories burned and minutes asleep, iBGStar¹⁷⁵ (an iPhone add on) monitors blood glucose levels and Scanadu Scout¹⁷⁶ measures temperature, heart rate and haemoglobin levels and other vital physiological data just by placing this apparatus on one’s forehead.¹⁷⁷ There are also other everyday tools, such as watches, that include GPS sensors that track the route run by its users but that can also provide important data about the health of its user and that can be uploaded onto the internet. For example, a producer of sports watches has logged over 6 billion kilometres of movement by its users. This can provide

171 Brenner, Susan W., *Law in an Era of “Smart” Technology*, Oxford Scholarship Online, 2007 at p. 5, available at <http://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780195333480.001.0001/acprof-9780195333480-chapter-1> (last accessed on 2016-09-07).

172 Ibid.

173 Aarts, Emile, and Marzano, Stefano, (eds.), *The New Everyday. Views on Ambient Intelligence*, 2003, at p. 14.

174 For more information, see Nike at https://secure-nikeplus.nike.com/plus/what_is_fuel/ (last accessed on 2017-01-26).

175 For more information, see Myster, at <http://www.mystarsanofi.com/web/products/glucometers/ibgstar> (last accessed on 2017-01-26).

176 For more information, see Scandau, at <https://www.scanadu.com/blog/a-week-in-the-life-of-a-young-medical-consumer-company> (last accessed on 2017-01-26).

177 Peppet, Scott, R., *Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security and Consent*, Texas Law Review, Vol. 93, Issue 85, p. 87, 2014, at p. 88.

useful information about its users, for example, relating to health issues.¹⁷⁸ A technology usually mentioned in the IoT discourse, is that of the RFID (Radio Frequency Identity) tag. It is a small microchip with a built-in radio antenna, the smallest being 0.4 millimetres.¹⁷⁹ RFID sensors can be placed in any article purchased, where a tracking function can track the goods throughout the production chain, from manufacturer to purchaser. The contentious issue regarding RFID chips is that this technology can be used in order to track individuals. Another technology that requires mention is the ‘cookie’, a small text file that a web site visited places on your computer and that can reveal information about a user’s internet surfing habits. While having uses for marketers, there are risks with regard to privacy, which has resulted in this technology being regulated by the law.¹⁸⁰

It is within this context that the term ‘ubiquitous computing’ is relevant. Its potential is described in the following manner:

Ubiquitous computing will create a context-aware environment in which, by means of the coordinated use of databases, sensors, micro-devices and software agents, numerous systems can scan our environment for data and serve us with particular information, based on certain notions about what is appropriate for us as unique individual persons given the particulars of daily life and context.¹⁸¹

2.3.3.3 Data from Inferences

In addition to data provided by a person, technology allows for data to be inferred from other data. For example, a street name and city can be used to infer a postal code. Where data cannot be inferred, a suitable indicator highlighting that the data is missing is sometimes provided, since blank spaces in a database

178 Bylund, Markus, *Personlig integritet på nätet*, Fores, 2013, at p. 46.

179 Kumagai, Jean, Cherry, Steven, *Sensors and Sensibility*, IEEE Spectrum, available at <http://spectrum.ieee.org/computing/networks/sensors-and-sensibility> (last accessed on 2017-03-16).

180 The Swedish Post and Telecom Authority (PTS), *Q&A About Cookies*, available at <http://www.pts.se/en-GB/Industry/Regulations/Legislation/Electronic-Communications-Act/FAQ-about-cookies/> (last accessed on 2015-11-24).

181 Prins, above n 51, at p. 7.

are undesirable.¹⁸² The data inferred is not verified data, which can be problematic, not having been collected from an original source. This ability to infer data is part of the ‘knowledge discovery in databases’ (KDD) process developed by Fayad et al.¹⁸³ KDD is defined as the, ‘... nontrivial process of identifying valid, novel, potentially useful, and ultimately understandable patterns in data’.¹⁸⁴ The third stage of the KDD process, after selecting a target domain and data set, is cleaning the data, an important aspect of this process the decision of a strategy for dealing with missing data fields.¹⁸⁵ This inference process is also referred to as ‘missing value imputation’, where algorithms, faced with missing values infer an appropriate value.¹⁸⁶ The process of making inferences is not new and is accepted as being an integral part of the profiling process, as identified by Gandy in his work on the profiling of consumers.¹⁸⁷ It is also relevant in circumstances where algorithms are confronted with novel circumstances with which they have not been trained to deal.

2.3.3.4 Clickstream Data

So-called ‘clickstream data’ is data that is attained from the trail a person leaves as he or she navigates websites on the internet. It provides information on what part of a web page a user clicked on, for how long a web page was visited or what part of a web page was not clicked, which also says something about the user. For example, Amazon stores information not only about what book a customer purchased, but also what books the customer clicked on but

182 Bari, Anasse, Chaouchi, Mohamed and Jung, Tommy, *Predictive Analytics for Dummies*, John Wiley and Sons Inc., New York, 2014.

183 Fayyad, Usama, Piatetsky-Shapiro, Gregory and Smythe, Padhraic, *From Data Mining to Knowledge Discovery in Databases*, in American Association for Artificial Intelligence, Fall, 1996 at p. 37, available at <http://www.kdnuggets.com/gpspubs/aimag-kdd-overview-1996-Fayyad.pdf> (last accessed on 2016-09-08).

184 Ibid.

185 Ibid.

186 Custers, Bart and Calders, Toon, *What is Data Mining and How Does it Work?*, in Custers, Bart et al. (eds.), *Discrimination and Privacy in the Information Society – Data Mining and Profiling in Large Databases*, Springer, 2013, at p. 39.

187 Gandy, Oscar H., Jr., *The Panoptic Sort: A Political Economy of Personal Information*, Westview Press, 1993, at p. 16.

then did not purchase.¹⁸⁸ Even how long the user's cursor hovered over a part of a web page can provide insight into the personality of the customer. Click-stream data is particularly powerful as it can measure attention span, due to the interactive nature of the internet.¹⁸⁹ Clicking on a 'like' button can also reveal a person's preferences. Clicking Facebook's 'like' button, for example, can reveal information such as gender, race, political allegiance and even whether the user was a divorced parent.¹⁹⁰

2.3.3.5 Surveillance Data

Surveillance data is defined by its composition, comprising trace data but even other data, for example, data that a person has uploaded him or herself. Lessig describes 'digital surveillance' as, 'the process by which some form of human activity is analysed by a computer according to some specified rule'.¹⁹¹ This practice is not limited to the digital environment, as technologies monitor peoples' actions off-line and then store this data in a digital format. The data relating to the observation of people can potentially be stored forever, which can be disadvantageous and gives rise to the saying that, '[r]ight or wrong, the Internet is a cruel historian'.¹⁹²

As Lessig mentions, private or public monitoring in the digital age has the effect that it can be increased considerably without the individual having any knowledge of this fact.¹⁹³ And in situations where the architecture is not suitable for monitoring individuals, it can be easily re-written. For example, web browsers were not constructed to remember internet searches. They follow the instruction to connect to a certain resource and display the supplied content supplied by the web server. However, in many situations, it is desirable that web browsers have some form of 'memory'. To this end the HTTP (Hypertext

188 Solove, *The Digital Person*, above n. 67, at p. 24.

189 Ibid.

190 Andersson, Katarina, *Vad säger våra digitala fotspar?*, Aftonbladet, 7 April 2016, available at <http://www.aftonbladet.se/partnerstudio/digitalalivet/article22525851.ab> (last accessed on 2017-03-16).

191 Lessig, above n. 53, at p. 209.

192 Solove, Daniel J., *The Future of Reputation – Gossip, Rumor, and Privacy on the Internet*, Yale University Press, 2007, at p. 11.

193 Lessig, above n. 53, at p. 23.

Transfer Protocol) cookie was developed in order for web servers to keep track of the computers that visited them.¹⁹⁴ In order to monitor surfing habits, many companies employ the use of cookies. Even the Safari browser, which by default blocks cookies and thus prevents monitoring, on one occasion happened to have a loophole whereby the default mechanism was by-passed by tricking Safari into believing that it was submitting a web-based form, consequently by-passing the system.¹⁹⁵

The surveillance of a person may be initiated by the individual him or herself. In this regard the concept 'little data' has been coined to describe data that individuals have attained through self-monitoring, an example being where a person records his or her own purchasing habits or consumption levels.¹⁹⁶ Bonchek refers to the power of combining both big data and little data. Provided that an individual has insight into his or her own consumption habits, these could be compared with general consumption habits in order to ascertain how that individual's consumption habits differ from that of other users. He argues that this relationship gives a greater sense of control and transparency, thereby providing individuals with a greater incentive to part with their data.¹⁹⁷

2.3.3.6 Social Engineering

Various techniques are utilized to induce individuals to give up their data. Within the KDD process, the collection of data is recognized as a separate step in the process. Step one in the KDD process requires the identification and collection of relevant information in relation to the purpose for collection. The data collection stage, as seen in the context of the entire predictive modelling process, is not trivial in that there may be various techniques used already at this early stage that are unwarranted in that the circumstances under which people are forced to part with their personal data cannot be considered fair.

194 Bylund, *Personlig integritet på nätet*, above n. 178, at p. 57.

195 Angwin, Julian and Valentino-Devries, Jennifer, *Google's iPhone Tracking*, Wall Street Journal, 17 February, 2012, available at <http://online.wsj.com/news/articles/SB10001424052970204880404577225380456599176> (last accessed on 2014-10-01, article subsequently available only to subscribers).

196 Bonchek, Mark, HBR Blog Network, *Little Data Makes Big Data More Powerful*, 3 May 2013, available at <http://blogs.hbr.org/2013/05/little-data-makes-big-data-more/> (last accessed on 2017-03-16).

197 Ibid.

One method of enticing individuals to part with their personal information is to ensure that they receive no service if personal details are not provided. In addition, the information usually required by commercial actors far exceeds that which is required in order to provide the service. In this regard, the most effective tool for getting customers to agree to the collection of excessive data is the lengthy Terms of Service Agreement.¹⁹⁸ Excessively underhand means of attaining this objective involves creating the illusion that the individual has ‘won’ something or is getting something for ‘free’, where in actual fact the individual involved has been tricked into signing a contract.¹⁹⁹

2.3.3.7 Insight Data

Data referred to here as ‘insight data’ are data that are not necessarily connected to or associated with a specific individual or group and where the value lies in their generality as opposed to individual-specific data. It provides insight into societal trends as opposed to the actions of individuals, the value lying in the ability to pinpoint what the masses are thinking, how they are feeling and what their opinions are. Insight into general emotion conditions can have practical consequences. One research project made the connection between mood and behaviour. Gilbert and Karahalios found a connection between emotion and stock market prices. The emotion studied was that of anxiety, or fear, termed the ‘Anxiety Index’, where they witnessed the correlation between the increase in anxiety and the pressure to send the prices of shares on the stock market (S&P 500) down. The researchers examined 20 million posts on the blogging site called LiveJournal,²⁰⁰ which had the functionality of allowing a blogger to label posts, and selected those that were labelled with a specific mood, for example, ‘anxious’, ‘worried’, ‘nervous’ and ‘fearful’.²⁰¹ This research highlighted the applicability of insight data. Using models, the

198 Lundberg, Johanna, *Användarvillkoren som ingen läser*, Stiftelsen för internetinfrastruktur, .SE:s Internetguide nr 35 at p. 8.

199 Ibid, at p. 27.

200 Livejournal, available at <http://www.livejournal.com/> (last accessed on 2017-03-01).

201 Gilbert, Eric and Karahalios, Karrie, *Widespread Worry and the Stock Market*, Association for The Advancement of Artificial Intelligence, available at <https://www.aaai.org/ocs/index.php/ICWSM/ICWSM10/paper/viewFile/1513/1833> (last accessed 2015-05-05).

researchers were able to establish the link between insight data relating to mood and the movement of share prices on the stock market. Once again, it was not the mood of individuals that provided this insight into the movement of the stock market, rather it was the collective mood of the masses within the social media. Even the UN has embarked on an initiative called ‘Global Pulse’, which scans the digital trails that people leave behind in order to attain insight into certain activities that can be associated with humanitarian assistance. It also examines sentiment in the social media to the extent that it ‘reveal insights on changes in human well-being, real-time trends on population behaviour or perceptions related to sustainable development issues’.²⁰² Facebook too is interested in gauging the emotions of people as well as gaining insight into the social dynamics expressed in groups. By analysing key words and gaining insight into the emotions of people, it boasts the ability to capture ‘gross national happiness’.²⁰³

2.3.4 Big Data on the Rise

Having discussed some of the sources of big data, there are a number of reasons as to why its size is constantly on the increase. First, is a cost issue. For decades, the hardware required to produce data and also store data has become cheaper. With a decrease in the costs associated with the technology of producing and storing data, its availability can easily increase. Also, as the value of these data becomes more apparent, so too is hardware designed in order to more easily store the large amounts of available data.²⁰⁴ In this context, reference is often made to Moore’s Law, which was an observation made in 1965 by Moore in relation to computing hardware where the amount of transistors that can be fitted onto an integrated circuit doubles every two years.²⁰⁵ As

202 United Nations Global Pulse, available at <http://www.unglobalpulse.org/about-new> (last accessed on 2015-05-07).

203 Simonite, Tom, *What Facebook Knows*, MIT Technology Review, available at <http://www.technologyreview.com/featuredstory/428150/what-facebook-knows/> (last accessed on 2015-05-13).

204 Hardy, Quentin, *Big Data Done Cheap*, The New York Times, available at http://bits.blogs.nytimes.com/2013/03/04/big-data-done-cheap/?_r=0 (last accessed on 2017-04-14).

205 Moore’s Law, available at <http://www.moorelaw.org/> (last accessed on 2017-03-21).

more transistors are fitted onto a smaller space, processing power increases and the end user of technology receives access to computing power at a lower cost. Moore argued that computing power would increase and costs decrease at an exponential rate.²⁰⁶ Second, individuals are spending more time than ever in the digital environment. This unprecedented extent to which people spend time in this digital sphere has been referred to as ‘hyper-connectivity’, being fuelled by the mobility of modern technology.²⁰⁷ This in turn has resulted in the view that the internet has come to play such an important role in the individual’s daily existence that access to it be seen as a human right.²⁰⁸ Third, much of the data resulting in big data is leaked data. A study by Krishnamurthy and Wills showed how users increasingly leaked data from the mobile versions of the social media to the regular versions of these networks. This was due to mobile devices relying on two factors that are not an issue with regular social networks sites, namely that of ‘presence’ and ‘location’ and where the ability to ‘check-in’ can reveal telling data. Other factors were the use of an API (Application Programming Interface) to connect these two variations of social network sites as well as the functionality of the applications, an example being the mobile social network Foursquare,²⁰⁹ which passes on latitude and longitude information to Google maps, which is then able to present a person’s current location. Finally, certain technologies leak information by default, for example, many devices have a UDID (Unique Device Identifier), which can

206 Intel, available at <http://www.intel.com/content/www/us/en/silicon-innovations/moores-law-technology.html> (last accessed on 2015-05-07).

207 Foresight, *Future Identities - Changing Identities in the UK: the Next 10 Years*, Government Office for Science, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/273968/13-524-future-identities-changing-identities-summary.pdf (last accessed on 2014-09-30), at p. 4.

208 Kravets, David, Wired, *U.N. Report Declares Internet Access a Human Right*, available at <http://www.wired.com/2011/06/internet-a-human-right/> (last accessed on 2017-04-14).

209 Foursquare is a mobile online social network that allows real time ‘check-in’ and location sharing with others. Foursquare, available at <https://foursquare.com/about> (last accessed on 2017-03-01).

be tracked by third parties.²¹⁰ The increase in user participation on the internet, characterised by user-generated content, is also a contributing factor.²¹¹

A particularly important explanation for the rise of big data is probably their utility for the commercial sector. Data have become a valued commodity due to their newfound utility, described by Siegel:

Data always speaks. It is because everything is connected to everything else ... your purchases relate to your shopping history, online behaviour and preferred payment method, and to the actions of your social contacts. Data reveals how to predict consumer behaviour from these elements. Your health relates to your life choices and environment, and therefore data captures connections predictive of health based on type of neighbourhood and household characteristics, your job satisfaction relates to your salary, evaluations and promotions, and data mirrors this reality ... it always has a story to tell.²¹²

In addition, there is the notion of power. Data is easy and cheap to collect and store but it is also the very thing that gives power. Siegel once again states that, '[t]he more data, the more power. The more powerful the data, the more sensitive'.²¹³ Some companies, such as Acxiom and ChoicePoint, have been established upon the business model of the collection and re-sale of raw data.²¹⁴ Sobel also provides insight, stating that, '[o]nce information exists, it's virtually impossible to limit its use. You have all this great data lying around, and sooner or later, somebody will say, "What else can I do with it?"'²¹⁵ The above is an important observation. It highlights the fact that one really does not know when the value in the data that is merely lying around,

210 Krishnamurthy, Balachander and Wills, Craig E., *Privacy Leakage in Mobile Online Social Networks*, Proceedings of the 3rd Conference on Online Social Networks, 2010, at p. 8.

211 OECD Report, *Participative Web: User-created Content*, STI/ICCP/IE(2006)7/FINAL, 12th April 2007 at page 4 available at <http://www.oecd.org/sti/38393115.pdf> (last accessed on 2015-01-01).

212 Siegel, above n. 118, at p. 79.

213 Ibid, at p. 39.

214 Kumagai, Jean and Cherry, Steven, *Sensors and Sensibility*, available at <http://spec-trum.ieee.org/computing/networks/sensors-and-sensibility> (last accessed on 2015-05-13).

215 Ibid.

will appear. The prevailing sentiment in relation to data, especially in the commercial sector, is the more the better and its value is perceived as substantial, leading to comments that ‘data is the new oil’.²¹⁶

2.3.5 Big Data Offshoots

As the notion big data evolves, terms have come to the fore that can be described as ‘offshoots’. Higinio refers to three offshoots of big data, namely, ‘smart data’, ‘identity data’ and ‘people data’. Smart data can be understood by referring to smart data platforms, where big data is stored in compartments and where one can visualize the data according to business needs. What differentiates big data from smart data is that big data usually requires a professional to seek correlations between the data points.²¹⁷ Smart data replaces the professional with a system. Also, a smart data platform can customize the visualisation of the data depending on a specific need. Identity data essentially refers to the story about a person’s identity that data points combined with other data may tell, and can be based on factors such as what a person wrote in the social media or how he or she navigated a website. Finally, people data refers to the data concerning an entity’s audience. For example their likes and dislikes and what their preferences are in order that their experiences on-line can be customized.²¹⁸

The above references to the offshoots of big data illustrate the difficulty not only with defining big data but also with attempting to describe its characteristics. What is certain is that the data comprising the digital environment is growing and that its features are continuously evolving.

216 Rotella, Perry, *Is Data the New Oil?*, Forbes, available at <http://www.forbes.com/sites/perryrotella/2012/04/02/is-data-the-new-oil/> (last accessed on 2015-05-22), Moss, Simon, *Big Data: New Oil or Snake Oil?*, Wired, available at <http://www.wired.com/2014/10/big-data-new-oil-or-snake-oil/> (last accessed on 2015-05-22).

217 Maycotte, above n. 136.

218 Ibid.

2.3.6 Theory Driven versus Data Driven Approaches

The increase in the availability of data has had two main consequences for technology. First, it has changed the way data is analysed. Previously, the data held in databases could be analysed by humans. However, as the databases grew, this became impossible, resulting in the creation of data mining techniques in the 1980's, which had the function of automatically finding the correlation between these data.²¹⁹ A simple definition of 'data mining' is that it is '[t]he analysis of large and complex data sets'.²²⁰ Second is the coming to the fore of a trend whereby less emphasis was placed on the collection and storage of as much data as possible in databases, but rather a greater emphasis was placed on the creation of technologies designed to capture the value and knowledge held by dispersed and unstructured data, and not only confined to databases. Once the knowledge is acquired from these constellations of data, there is no reason to store the data any longer, since the value is in the knowledge acquired rather than the actual data. This trend away from databases is highlighted in some applications. For example, 'SnapChat', a photo and messaging application that allows for the sharing of photos and videos, allows content to be viewed only for a limited amount of time before it is discarded.²²¹ Databases and database technologies are by no means relics of the past, however, the trend is towards the realization of the ephemeral nature of data with the emphasis on the knowledge that it carries.

2.3.6.1 Databases and the Theory Driven Approach

During the 1970's companies and public authorities began using databases in order to increase productivity, these institutions being the only ones that could afford the hardware upon which to run these databases. It was soon realized that these databases contained lots of useful data and they started to be analysed in what can today be described as a relatively simple fashion in order to learn from the data. These techniques are referred to as 'traditional' methods

219 Finlay, above n. 1, at p. 2.

220 Ibid.

221 Pocket-Lint, *What's the Point of Snapchat and How Does it Work*, available at <http://www.pocket-lint.com/news/131313-what-s-the-point-of-snapchat-and-how-does-it-work> (last accessed on 2015-11-25).

of database analysis. They were traditional in that they used methods common with regular statistical analysis in order to ascertain and extract information and ultimately knowledge from the data. The technological process began with a hypothesis, which would then be tested against the data to examine whether it could be proven true. This is known as a ‘top-down’ or ‘theory-driven’ approach. This type of database analysis can be effective if one wants to prove or establish something or find out the reason for an event. It is especially effective if one takes the initial database and breaks it down into smaller databases.²²²

The problem with the traditional approach, as mentioned above, was that databases became too large in size in order to effectively handle such queries. Also, it did not accommodate the desire of those who wanted to dig deeper into the data and find new connections that could not be seen or detected by traditional statistical analysis, something that increased commercial competition required.

2.3.6.2 Databases and a Data Driven Approach

The era of big data ushered in a different technique for analysing data. The availability of big data and the creation of data mining tools necessary to analyse and extract knowledge from it, allowed for a new explorative approach. By running data mining tools against big data, in some cases spanning multiple physical databases, a hypothesis was created by the data mining tool, which hypothesis could then be tested against the data. This new approach to data analysis is referred to as a ‘bottom-up’ or ‘data driven’ approach. Instead of inventing a hypothesis to be tested against the data, the data is randomly analysed for connections and correlations between the data. In other words, what was sought were the patterns in the data. The correlations were novel in that humans would never have thought of making such connections and it was only by utilizing tools from within the spheres of machine learning and artificial intelligence, that one was able to extract this knowledge.²²³

222 Custers, Bart, *Data Dilemmas in the Information Society: Introduction and Overview*, in Custers, Bart et al. (eds.), *Discrimination and Privacy in the Information Society – Data Mining and Profiling in Large Databases*, Springer, 2013, at p. 9.

223 Ibid.

Depending on the circumstances, the data driven approach may encompass a larger degree of human activity or it may be completely automatic, providing real time insight. What is of importance in this respect is that this process does not answer the question ‘why?’. In other words, it does not provide a causal link between the data.²²⁴ It just establishes that a link is present and then it is up to humans to make assumptions as to why there is a link or relationship. A hypothetical example, is where the data driven research detects that people who drive an orange car have a higher risk of being involved in an accident. This correlation cannot be explained without human interpretation and it is almost impossible to provide a reason for this occurrence. This process of pattern search is described by Zarsky who states that, ‘data mining provides users with the answers to the questions they did not know to ask’.²²⁵ The fact that no answer to the question ‘why?’ is available, is irrelevant. All that is important is the ‘that!’.

2.3.7 Knowledge Representation

A notion that requires attention is that of knowledge representation. Having examined the nature of big data and its various sources, it is important to acknowledge the influence of the notion of knowledge representation.

A fundamental issue is that not all the data points comprising big data are required automatically. Besides being technically challenging to achieve, this issue recognizes the fact that already at the collection stage, a choice as to what data to include in a collection of data, is required. The data that are used will depend on the purpose for analysing these data. For example, a collection of data concerning certain specified individuals may be required. Just exactly what data will be accessed concerning these individuals will depend on whether we are interested in their location, whether we are interested in their communications or whether we are interested in their purchases? Therefore, the purpose associated with a collection of data will correspond with the manner in which that data is represented. Referring to Figure 2 above, one can

224 It is acknowledged that the theory driven approach may not necessarily provide a causal link between the data either.

225 Zarsky, Tal Z., ‘*Mine Your Own Business!*’: *Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion*, Yale Journal of Law and Technology, 2002-2003, at p. 6.

argue that already at stage 2, a representation of data is occurring. Some of the sources of big data are accessed and recorded in the central database, while others are not. Already here a representation of data occurs. This, in turn, will also affect the representation of data that takes place later at stage 4.

A useful analogy is that of the individual using his or her human senses in order to access and record information from a physical context, the major part of the data processed, discarded almost immediately. For example, a person may look into a room full of people in order to determine how many people are present. He or she will acquire lots of different types of data (information) by using his or her senses: how many people there are in the room, what they are wearing (some will be wearing suits and some will be dressed more casually, some will have black shoes and some will have brown shoes), what languages they are speaking, who is speaking to whom and the different perfumes they may be using, etcetera. This mass of data is analogous to the notion of big data, where there is a large variation in the different types of both static as well as streaming or live data. The purpose is only to determine the number of people in the room and consequently the data concerning clothing, language and perfume will be discarded, the only relevant data being the number of people present in the room. In other words, only the data concerning the number of people in the room need be represented in relation to the initial goal.

2.4 From Profiling to Predictive Modelling

The terms ‘profiling’ and ‘predictive modelling’ are challenging in that any attempts to define the boundaries between different technologies are bound to be artificial and contested. With this in mind, the following section examines the development from profiling to predictive modelling.

2.4.1.1 Profiling

Profiling, depending on the context, is nothing new and taken out of the digital context, can be said to be as old as humanity itself. In fact, it has been argued to be ‘as old as life on earth’, where, set in the biological context, organisms

are required to profile their environment in order to re-produce themselves.²²⁶ As Hildebrandt argues, the purpose of profiling is selection, where the ultimate goal is to include and exclude, whether it be objects or people, and that it is an inherent part of life, where quite simply information is taken in and processed in order to assess the next step.²²⁷ Therefore, profiling is important for human existence, where over time people are required to profile and adjust to their environment, be it physical or social.

A consequence of profiling is the act of placing persons into categories, something which is identified in disciplines such as sociology, where Lyon defines this categorization as ‘social sorting’ and as the process whereby, ‘populations are clustered in order to single out different groups for different kinds of treatment’.²²⁸ This corresponds with Hildebrandt’s notion that the aim with profiling is selection, a warning being that where selection exists, it impacts the lives of those it affects and is in need of justification.²²⁹ Related to the digital environment, Nissenbaum describes profiling as a form of discrimination and is a consequence of the collection, aggregation, mining and analysis of huge amounts of data, resulting in the potential for discrimination or differential treatment.²³⁰

Another repercussion of profiling and social sorting is a categorization process, where people are placed into categories and it may be a certain attribute connected with a person’s character that has resulted in the person being placed in a certain category. In this circumstance, it is no longer the person’s character that is all-important, but rather the category that he or she falls in to.²³¹ Lyon refers to the fact that social sorting has always occurred within society. Many cities may be divided by physical objects, for example train tracks, where one community is assigned a lower status in society, depending

226 Hildebrandt, Mireille, *Profiles and Correlatable Humans*, in Stehr, Nico and Weiler, Bernd (eds.), *Who Owns Knowledge?: Knowledge and the Law*, Transaction Publishers, 2008, at p. 272.

227 Ibid, at p. 269.

228 Lyon, *Surveillance Studies*, above n. 64, at p. 98.

229 Hildebrandt, *Profiles and Correlatable Humans*, above n. 226, at p. 270.

230 Nissenbaum, Helen, *Privacy in Context*, Stanford University Press, 2010.

231 Lyon, *Surveillance Studies*, above n. 64, at p. 101.

on which side of the tracks it is situated.²³² However, in the digital environment, social sorting is no longer determined by the physical attributes. It is determined by clustering data about people. The method is different, yet the outcome is the same: people are placed in categories, which results in a certain consequence. As Lyon points out, this phenomenon of social sorting leads to the creation of new social classes.²³³ Not only does it affect the social fabric of society, but it brings with it the ability to manipulate, Lessig too referring to the manipulation that may result from the process of profiling combined with targeted advertising, for example.²³⁴

Within the digital environment, profiling is equated with the collection, storage and analysis of data as well as the formation of groupings based on the correlations or patterns found in the data utilizing the data driven approach. Hildebrandt defines it in the following manner:

The process of 'discovering' correlations between data in databases that can be used to identify and represent a human or nonhuman subject (individual or group) and/or the application of profiles (sets of correlated data) to individuate and represent a subject or to identify a subject as a member of a group or category.²³⁵

Concepts such as clustering and classification are associated with the act of profiling. Within the area of machine learning there are a number of ways to categorize things. The difference between clustering and classification is that classification uses pre-defined classes while a part of the clustering process is the identification of classes or groups.²³⁶ Irrespective of the effectiveness of the technique used, what these two concepts facilitate is the process of grouping or categorizing and part of the process is to associate individuals with these categories.

There are a number of reasons why it is preferable to group people. Creating group profiles is more cost effective, it may be more effective to view the individual as part of a group than merely as an individual and the individual

232 Ibid, at p. 98.

233 Ibid, at p. 117.

234 Lessig, above n. 53, at p. 151.

235 Hildebrandt, Mireille, *Defining Profiling: A New Type of Knowledge?*, above n. 56, at p. 19.

236 Custers and Calders, above n. 186, at p.32.

alone may not possess any attributes that are of interest to the commercial actor. However, the individual as a member of a group may be more interesting as this group membership may divulge information about him or her that would have been difficult to obtain by individual assessment alone. It is within the group scenario that profiling is most unfair, with group profiles being applied to the individual even where he or she does not in reality possess the characteristics that the group profile portrays.²³⁷

2.4.1.2 Profiling versus Predictive Modelling

The concepts of ‘profiling’ and ‘predictive modelling’ bear similarities, yet there are differences. Profiling is concerned with categorizing data in order to gain insight from these categories of data, without necessarily labelling the groups or data as such. Predictive modelling, on the other hand, is more hands-on, in that examples of behaviour are identified (data is grouped), with labels assigned to these groups, the main aim to identify these groupings of data in the present or future. Predictive modelling, therefore, can be characterized as entailing greater human control and intervention.

The extent to which profiling can be compared to predictive modelling also depends on the meaning associated with profiling. Profiling can be seen in terms of a long spectrum, that is, its complexity can range from the simple to the very complex. At the complex side of this spectrum, profiling can resemble predictive modelling closely while at the other end of the spectrum, it does not.

These two concepts differ in other respects. First, they differ with regard to the time aspect. The act of profiling has its emphasis on the past and present time, whereas predictive modelling is more future orientated in that it not only looks for patterns in human behaviour, but also attempts to predict these patterns. Second, with profiling the main focus is the individual as part of a group in order to establish broader generalisations or classifications regarding groups or regarding individuals as members of a group, while predictive modelling is more individual orientated and while it does concern groups, and the

237 Hildebrandt, Mireille, *Who is Profiling Who? Invisible Visibility*, in Gutwirth, Serge, Poulet, Yves, De Hert, Paul, de Terwangne Cecile and Nouwt, Sjaak, (eds.), *Reinventing Data Protection?*, Springer Science and Media, 2009, at p. 243.

analysis of individual behaviour as part of a group, the main focus is the prediction of individual human behaviour in order that an entity be able to exert influence over that individual in respect to a specified goal. Third, profiling can be viewed as ‘defensive’ and predictive modelling as ‘offensive’.²³⁸ Gandy performs a thorough investigation of profiling, referring to ‘the panoptic sort’, describing it as a, ‘kind of high-tech, cybernetic triage through which individuals and groups of people are being sorted according to their presumed economic or political value’.²³⁹ The aim of the panoptic sort is to gain power, in this case power over consumers. It does this by means of profiling, where individuals are categorized and assigned to groups in order that commercial actors can communicate differently with the various groups and influence their choices (as consumers). Possibly, one of the main differences between predictive modelling and profiling is in fact expressed by Gandy, where he states that the panoptic sort, or profiling, is a defensive technology, operating through victimization and avoidance. This defensive notion is best described in his own words:

The panoptic sort is a screen that excludes a filter that blocks, a magnet that ignores fine wood in preference for base metals ... the sorting process works primarily by eliminating those who are too much, too little, too late ... too bad!’²⁴⁰

Using Gandy’s terminology then, predictive modelling can be viewed as offensive in nature. It not only sorts, but predicts and influences. It sorts based on past behaviour, but then identifies future behaviour, thereby establishing the capacity to influence this future behaviour. A fourth difference concerns the input data as well as the type of knowledge being sought from the actual process. Profiling uses the data stored in large databases in order to categorize people and place individuals in pre-defined groups. As described above, KDD, which is an essential element of profiling, in its name specifically mentions the technology of ‘databases’. Predictive modelling is associated with data in general, irrespective of its source or structure, be it from the social media,

238 This description of predictive modelling as defensive in nature is made within the commercial setting. The predictive modelling techniques used by law enforcement, for example, can be viewed as having a more offensive character.

239 Gandy, above n. 187, at p. 2.

240 Ibid, at p. 18.

blogosphere or any other digital source. While it does use databases, there are forms of predictive models that do not. It is not as concerned with the creation of groups, but rather with the extraction of insight and trends from data in general. In other words, profiling is more database orientated whereas it can be argued that predictive modelling, depending on its form, is not as reliant on the database structure.

2.4.1.3 Predictive Analytics and the Predictive Model

Two closely related concepts are ‘predictive analytics’ and ‘predictive modelling’. In simple terms, the former has a broader scope whereas the latter has a narrower scope. Predictive analytics is a term used to describe the use of data mining tools to predict human behaviour and is the practical application of data mining technology.²⁴¹ Predictive analytics was first used in the 1950’s in the US in the form of credit scoring mechanisms used by mail order companies to determine who they could give credit to, after which it became commonplace in the financial industry, assisting with the adjudication of applications for loans and credit.²⁴²

Predictive analytics is defined as, ‘technology that learns from experience (data) to predict the future behaviour of individuals in order to drive better decisions’.²⁴³ Of importance is that predictive analytics has at its centrum predicting behaviour, most notably of the individual. In other words, it analyses past behaviour and predicts future behaviour based on this past behaviour. The practical consequence is that it provides knowledge concerning how an individual should be treated in relation to a certain desired outcome. The main focus, therefore, of predictive analytics is that of future behaviour prediction. This view is supported by the Office of the Privacy Commissioner of Canada:

... it is important to acknowledge that predictive analytics is a process that is closely intertwined with previously known notions of data mining; however the inferences extend beyond retrospective pattern analysis to a result that is

241 Finlay, above n. 1, at p. 3.

242 Ibid, at p. 3.

243 Siegel, above n. 118, at p. 11.

more prospective and anticipatory ... predictive analytics is characterised by its ability or attempt to forecast, anticipate, or infer.²⁴⁴

Another definition provided for predictive analytics states that:

Predictive analytics is the branch of data mining concerned with forecasting probabilities. The technique uses variables that can be measured to predict the future behaviour of a person or other entity. Multiple predictors are combined into a predictive model. In predictive modelling, data is collected to create a statistical model, which is tweaked as additional data becomes available.²⁴⁵

A final definition of predictive analytics is that it is, '[t]he process of determining important relationships between items of data to aid in the prediction of future (or otherwise unknown) outcomes'.²⁴⁶ An inherent part of predictive analytics is the development of a model by means of which behaviour is predicted, this leading to the establishment of the term 'predictive modelling'.

Modelling as such is nothing new, although the instruments portraying models may have changed somewhat. For example, Philips modelled the UK economy using plumbing supplies and a windshield-wiper motor, the flow of coloured water representing the flow of income tax.²⁴⁷ The tools for modelling, however, have become more complicated, using mathematics, statistics, machine learning and even artificial intelligence to digitally simulate outcomes. However, the main function of the model remains the same, namely, to 'stipulate a set of relations among factors, feed in data, watch the outcome. If the predictions are off, that itself becomes valuable information that can be used to refine the model'.²⁴⁸ In the modern era, the predictive model has been described as:

244 Office of the Privacy Commissioner of Canada, *The Age of Predictive Analytics: From Patterns to Predictions*, Report Prepared by the Research Group of The Office of the Privacy Commissioner of Canada, August 2012.

245 Matlis, Jan, *Predictive Analytics*, Computer World, available at <http://www.computer-world.com/article/2554079/business-intelligence/predictive-analytics.html?page=2> (last accessed on 2015-05-11).

246 Finlay, above n. 1, at p. 215.

247 Weinberger, David, *The Machine That Would Predict the Future*, Scientific American, December 2011, at p. 34.

248 Ibid.

A mechanism that predicts a behaviour of an individual, such as click, buy, lie or die. It takes characteristics of the individual as input, and provides a predictive score as output. The higher the score, the more likely it is that the individual will exhibit the predicted behaviour.²⁴⁹

Predictive modelling is also described in the following manner:

A commonly used statistical technique to predict future behaviour. Predictive modelling solutions are a form of data mining technology that works by analysing historical and current data and generating a model to help predict future outcomes.²⁵⁰

Yet another definition of the predictive model states that:

A predictive model captures the relationships between predictor data and behaviour, and is the output from the predictive analytics process. Once a model has been created, it can be used to make new predictions about people (or other entities) whose behaviour is unknown'.²⁵¹

Predictive modelling is therefore the practical application of predictive analytics, where the insight gained from predictive analytics is embodied in a statistical model that can be applied to future scenarios. An additional aspect is that predictive modelling can operate in real time.²⁵²

The predictive model may present its outcome or decision (output) in the form of a score. It is a predetermined value on a pre-determined scale and may determine further action, for example, where an individual is identified as 'high risk' in relation to the behaviour that is being predicted.

An important part of the predictive modelling process, once the relevant factors in relation to a desired behaviour prediction have been identified, is to assign each variable a weight in relation to each other. This function is usually performed by the algorithm used to find the relevant factors. Predictive modelling has therefore been described as 'predictive mathematics', where one typically takes a large number of variables in relation to the target group, for

249 Siegel, above n. 118, at p. 26.

250 Gartner, IT Glossary, *Predictive Modelling*, available at <http://www.gartner.com/it-glossary/predictive-modeling> (last accessed on 2015-11-25).

251 Finlay, above n. 1, at p. 215.

252 Gartner, IT Glossary, *Predictive Modelling*, above n. 250.

example customers, and leverages them against one another in order to determine which variables are most effective in predicting a certain action.²⁵³

2.4.1.4 Building a Predictive Model

What is significant about the predictive modelling process is that historical data, once tapped into, has potential commercial value due mainly to the advent of modern computing techniques and statistical methods. These afford systems the ability to use patterns in historical data to forecast and predict future outcomes given current observed data on human behaviour or other states of the world. They use predictive algorithms, as developed by research in machine learning, knowledge discovery, data mining, and related fields, which can be used to identify patterns and regularities that overwhelm human information processing abilities, either because they process impracticably large sets of data or because the patterns need sophisticated models of dependencies to be detected. The identification of patterns in turn results in the creation of generalizations, alternatively referred to as rules, which form the basis for identifying future behaviour. In simple terms, data about past individual behaviour is used to predict future individual behaviour.

2.4.1.5 Notable Considerations of Control

There are a number of aspects that should be noted pertaining to the use of predictive models. First, an important notion is that of supervision. The degree of supervision will influence how the predictive model operates and its accuracy once it is put in place to decide novel situations. For example, a predictive model may be tested on test data before being employed on new situations. This may involve one iteration or it may involve many. In this sense, a degree of supervision has been exerted over the predictive model building process. One may even provide the predictive model with pre-determined examples to learn from and corresponding labels to identify in the test data (and eventually in novel situations). Already here a degree of supervision can be said to be

253 McCarthy, Erin, *Profiling Versus Modelling Versus Segmentation*, available at <http://www.sourcelink.com/blog/guest-author-series/2013/03/06/profiling-versus-modeling-versus-segmentation> (last accessed on 2015-11-24).

exerted.²⁵⁴ Another way of describing supervision is that the model is provided with an example and the outcome of that example, after which it is tested on test data, however, this time withholding the outcome information.²⁵⁵

In general terms, supervision occurs in cases where a predictive model is built using previously acquired data, that is structured, for example, in a database. This process refers to ‘fitting’ the predictive model to the data.²⁵⁶ It could be the historical data that a bank has saved concerning previous loans provided and the outcomes. The data may require cleaning, for example, where there are values missing. Where data is missing, it may need to be substituted, in addition to the fact that something can also be learned from the fact that a certain type of data is missing and the reason for this.²⁵⁷ Once cleaned, the data is typically divided into ‘training data’ and ‘test data’. Setting the test data aside, the training data should include primarily two types of data, namely, ‘predictor data’ (the data to be fed into the predictive model and used to make the prediction), also referred to as ‘predictor variables’ or ‘independent variables’ (examples being age, occupation, gender), and ‘behavioural data’ (the behavioural outcome to be predicted), also referred to as the ‘dependent variable’, ‘target variable’ or ‘modelling objective’ and which is a representation of the behaviour that one is trying to predict.²⁵⁸ The dependent variable is then represented by a label. Put simply, the historical data, structured in rows and columns, represents past examples and is assigned a label, representing the outcome associated with each particular example. The data fed into the predictive model can be well structured, two types of structuring

254 In the context of data mining, the supervised method is described as having a target. For example, ‘[c]an we find groups of customers who have particularly high likelihoods of cancelling their service soon after their contracts expire?’. Unsupervised methods have no target, and are represented by questions such as, ‘[d]o our customers naturally fall into different groups?’, Provost and Fawcett, above n. 77, at p. 24. The authors metaphorically note the correlation with supervised and unsupervised learning in the classroom, where the former is represented by a teacher providing students with examples accompanied with target information, while with the latter, the same examples are provided, however, without the target information, the students being required to draw their own conclusions regarding the connection between the examples.

255 Witten and Frank, above n. 8, at p. 43.

256 Provost, above n. 77, at p. 110.

257 Finlay, above n. 1, at p. 162.

258 Ibid, at p. 25.

being either ‘categorical’ (for example, ‘lawyer’, ‘divorcee’, ‘female’) or numeric (for example ‘age’, ‘income’).²⁵⁹ It is desirable that different types of behaviour are represented by the behavioural data in order that one can distinguish between the predictor variables that were present for each different type of behaviour.²⁶⁰ For example, data about who purchased a book and who did not would be two types of behavioural data. Another type is who defaulted on a loan and who did not. Predictive analytics has at its basis the understanding of the relationships between predictor data and behavioural data and both are required as part of the predictive process.²⁶¹ The historical data and labels are then embedded in a predictive model together with an algorithm, represented by the ‘black box’. The algorithm is assigned the task of accepting new examples and comparing them against those encapsulated in the model. If there is a new example that corresponds with an example in the model, then the algorithm knows what label to assign the new example, based on what it has learned from the historical data. After confirming that the model works as anticipated, by running it against the test data, the model is finally employed in a live situation, assigning labels to new examples or situations that it is required to adjudicate. Also relevant is that knowledge gained from the live operation of the predictive model can be looped back to the test phase data so as to improve the accuracy of the model. In this manner, predictive models can be said to be ‘self-learning’.

Predictive models may also be developed in situations where less supervision is exerted over the process. Here, data can be processed without pre-determined categories, in order to explore unexpected correlations. This process can be accomplished by running statistical algorithms and other machine learning techniques against the training data in order to discover patterns of correlation. These correlations need not be causal in nature – they simply exist and cannot necessarily be explained. The patterns are usually of a general nature and are inductive in nature. In other words, the data used to learn the labels does not exist in neatly structured rows and columns. Rather, they may exist in constellations of data that have no logical connection. It is these correlations that are hidden from human insight or calculation, making this knowledge inaccessible to those lacking access to the technology. In addition,

259 Ibid, at p. 181.

260 Ibid, at p. 25.

261 Ibid.

the use of a model that is more (or less) supervised, does not necessarily exclude the use of the other type and in practice a combination of these two model types could be used. For example, a model requiring less supervision may initially be used, with the knowledge acquired from it incorporated into a model that is more supervised, thus maintaining a degree of control.

An example of a less supervised technology is that of the ‘neural network’, which is described as, ‘an artificial-intelligence processing method within a computer that allows self-learning from experience’.²⁶² Neural networks employ an approach to machine learning that gains inspiration from biological evolution, alternatively described as ‘biologically motivated approaches to machine learning, inspired by ideas from neuroscience’.²⁶³ Therefore, the technology uses the human brain as a source of inspiration. Neural networks can arrive at conclusions from a complex and seemingly unrelated set of information.²⁶⁴ For example, instead of embedding pre-determined and structured examples from historical data into predictive models, this technology makes its own correlations between the data.²⁶⁵ The neural network comprises three kinds of layers, namely, the input layer (feeds data into the next layer), the hidden layer, which may be a stack or sequence of layers (creates predictors, hidden from the user) and the output layer (collects predictions made at the hidden layer and displays the result).²⁶⁶

Second, associated with the above notion of supervision is that of ‘overfitting’. Within the sphere of data science, the concepts of ‘overfitting’ and ‘generalization’ can be viewed as complementary notions.²⁶⁷ Broadly speaking, overfitting occurs when a predictive model, once operating live, is confronted with an example that is not covered by or incorporated in that model and therefore cannot deal with it. In other words, the algorithm operating in the model has not been trained to deal with exactly this scenario. The algorithm is consequently required to fit the example to one of the previously learnt ones,

262 Gartner IT Glossary, *Neural Net or Neural Network*, available at <http://www.gartner.com/it-glossary/neural-net-or-neural-network/> (last accessed on 2017-01-31).

263 Mitchell, Melanie, *An Introduction to Genetic Algorithms*, Massachusetts Institute of Technology, 1996, at p. 65.

264 Gartner IT Glossary, *Neural Net or Neural Network*, available at <http://www.gartner.com/it-glossary/neural-net-or-neural-network/> (last accessed on 2017-01-31).

265 Bari, Chaouchi, and Jung, above n. 182, at p. 134.

266 Ibid.

267 Provost and Fawcett, above n. 77, at p. 111.

which can lead to an incorrect label being attached to that example (or an incorrect output/decision). Put another way, the aim when constructing a predictive model is that it should apply to all examples that it is confronted with and not only to the training data set, which is why it is important for the model to generalize beyond the training set. Overfitting is defined as, ‘... the tendency ... to tailor models to the training data, at the expense of generalization to previously unseen data points’.²⁶⁸ Consequently, overfitting can be associated with model complexity and by decreasing complexity, the extent to which overfitting occurs can be controlled.²⁶⁹ It is argued that less supervised predictive models are more prone to overfitting mainly due to the fact that humans have less control over the functioning of the model. For example, neural networks are more prone to overfitting.²⁷⁰

Third, the predictive modelling process distinguishes between two types of predictive models, namely ‘interpretable’ and ‘non-interpretable’ predictive models.²⁷¹ The distinction between these two variations is important in that their type essentially determines the amount of insight one has into how a decision was reached. Returning to the notion of seeking patterns in data, the notion of representation, addressed above, becomes relevant:

There are two extremes for the expression of pattern ... The difference is whether or not the patterns that are mined are represented in terms of a structure that can be examined, reasoned about, and used to inform future decisions. Such patterns we call *structural* because they capture the decision structure in an explicit way. In other words, they help to explain something about the data.²⁷²

An example of a predictive model that is more interpretable is that of the decision tree. The characteristics of the decision tree are as follows: the population is broken down into smaller and smaller segments, the model is represented as a ‘tree diagram’ and the final score produced by the predictive model

268 Ibid, at p. 113.

269 Ibid, at p. 140.

270 Finlay, above n. 1, at p. 102.

271 The terms ‘interpretable’ and ‘non-interpretable’ have been provided by Papapetrou, Panagiotis, Associate Professor, Department of Computer and Systems Sciences, Stockholm University, in conversation dated the 25th January 2017.

272 Witten and Frank, above n. 8, at p. 5, use of italics in the original.

is determined by the properties of the end node into which an observation falls after having passed through the entire tree.²⁷³ The actual decision tree is usually created by an algorithm, which decides on the optimal manner to split a population.²⁷⁴ The nature of the decision tree is such that there are no weights given to the respective bits of data and all decisions are based on the logic for segmenting the population.²⁷⁵ Decision trees are easy to understand and also to explain to non-technical people.²⁷⁶ In other words, as an observation falls through the tree, the logic used to determine which branch of the tree to send it on to, is identifiable and explainable.

Fourth, the score or label assigned by some predictive models is just a probability or estimation and the prediction is by no means guaranteed to occur. In other words, the predictive model may not be one hundred percent correct in every case nor is it presumed to be so. In fact, the intention is not that it be one hundred percent correct. In many cases, it is adequate that the predictive model increases effectivity of the company by just a few percent in order for it to be a worthwhile commercial tool. A commercial actor using a predictive model can increase its profits by adjusting its effectivity marginally. Mayer-Schönberger and Cukier refer to a quote by Forrester, who stated that, ‘sometimes two plus two can equal 3.9, and that is good enough’, the main idea being that it is worthwhile to sacrifice a little accuracy in order to identify behaviour.²⁷⁷ For example, being assigned a score under that which is stipulated by the predictive model in no way means that a loan applicant will default on his or her loan. All it means is that the risk is larger, based on the correlations from the data, that the loan applicant will default on the loan. In fact, most applicants receiving a score lower than the cut off score stipulated by the model, if granted a loan would probably not default on it, just as many of those who are granted a loan in fact do default.

Fifth, a factor that is always relevant is that of human intervention, which may vary from case to case and depending on the model implemented. For example, supervised models are more open to human control as opposed to

273 Finlay, above n. 1, at p. 112.

274 Ibid.

275 Ibid, at p. 114.

276 Ibid.

277 Mayer-Schönberger and Cukier, above n. 149, at p. 35.

unsupervised models. Supervised models allow more easily for human intervention in determining the features or attributes considered relevant in arriving at a decision. In addition, the outcome of a supervised model is highly dependent on many operative decisions taken by humans during the model building process and even on the labels used and that were assigned by humans. For example, historical data may be used to identify features relevant in determining whether or not an email is SPAM or not. By designating something as ‘SPAM’, that is by designating it with that label, an active decision is made. This puts a certain value on that outcome being predicted, which can either be subjective or even have legal implications, as is the case with the notion of SPAM.²⁷⁸ The score provided by a model is indicative only. A score under the cut off required by the model can naturally always be overridden by a human decision. It is therefore an operative decision as to whether the model will be adhered to completely in all cases or if there will be human considerations.

Sixth, the predictive modelling process may take other rules into account. These are called ‘override rules’, which take into account considerations that must be adhered to over and above the mathematical result of the predictive model.²⁷⁹ Even if the model has identified all the attributes necessary, there may be other considerations that the commercial actor may wish or be required to take into account. It may be a business ideology that is relevant but it may also be the law that stipulates a consideration be taken into account, for example, the effect of dealing with minors. In business, it is common that there may be many override rules operating simultaneously. Some examples include never providing credit to people who were recently bankrupted, never granting credit to people under 18 and always declining a credit application from a person who has had a credit application declined within the previous 30 days, even if his or her credit situation has improved.²⁸⁰

Seventh, given that predictive models operate on the individual level, the decisions on how to treat people may differ from person to person. For example, hypothetically speaking, two people eligible for a benefit from the state,

278 SPAM is defined as, ‘irrelevant or unsolicited messages sent over the Internet, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc.’, English Oxford Living Dictionaries, *SPAM*, available at <https://en.oxforddictionaries.com/definition/spam> (last accessed on 2017-01-26).

279 Ibid, at p. 36.

280 Finlay, above n. 1, at pp. 36-37.

based on the output from a predictive model, could potentially receive different pay-outs depending on their personal circumstances as identified by the algorithm. In this regard, not only will the state be required to justify the different amounts to the individuals, but people may also be required to get used to the idea that this is a reality and for the benefit of society at large.²⁸¹ In other words, the use of predictive models may challenge people's ideas of fairness as well as traditional norms, such as the equal treatment for all citizens.

Finally, it must be acknowledged that the correlations between data identified by the algorithm, are usually invisible to human analysis. This is particularly relevant concerning less supervised models. In the words of Hildebrandt, the algorithms, 'render visible the invisible'.²⁸² The main issue here is that the individual, whose behaviour is predicted and influenced, does not have this same access to the knowledge extracted by the predictive model and thus the correlations remain invisible. In other words, individuals do not have access to the technologies that analyse big data and thereby lack access to the big picture in terms of the data points correlated with each other in order to extract this new knowledge. It is for this reason that this data is referred to as a new type of knowledge or 'knowledge data' and as a consequence can be sensitive in nature, providing insight into the personality of individuals and which must be handled with extreme care and responsibility.²⁸³

2.4.1.6 Predictive Modelling Applied

A greater number of uses for the insight from data are being identified. This has resulted in an increase in the varieties of applications that are being produced in order to gain this insight. It is in this context that popular applications, such as social networking sites, are being trawled in order to retrieve data that can be beneficial for predicting behaviour. This, in turn, has encouraged the development of analytical tools that are able to utilize the data available in the social media despite the fact that they may not be as structured as compared

281 Tamarapport 2016:1 från Digitaliseringskommissionen (N2012:04), above n. 157, at p. 22.

282 Hildebrandt, *Who is Profiling Who? Invisible Visibility*, above n. 237, at p. 241.

283 Hildebrandt, Mireille, *Profiling and the Identity of the European Citizen*, in Hildebrandt, Mireille and Gutwirth, Serge (eds.), *Profiling the European Citizen*, Springer, 2008, at p. 320.

to databases. The below section deals with the advent of the social media as a source of predictive modelling data and illustrates the challenges that it poses.

2.4.1.6.1 *The Social Media*

The social media are becoming a valuable source of data for predictive modelling due to their popularity. However, the data available in the social media is not as structured as in databases, which creates the necessity for new ways to gain value from it. Much of the data in the social media are in text format or in another format, such as pictures or sound. Analysing text requires techniques in order to convert the unstructured data into a more structured format. As far as text is concerned, there are two types of predictor variables, namely ‘within document predictors’ and ‘across document predictors’, the former linking words within a document to form an impression as to whether the sentiments expressed are positive or negative on the whole, the latter seeking links between different documents.²⁸⁴ Extracting meaning from text is achieved by creating predictor variables for each word from the text and a variable value to represent each predictor variable, the challenge posed by the availability of large amounts of text being solved, for example, by removing stop words, using techniques such as stemming and also by utilizing standardization techniques.²⁸⁵

When examining the social media, the main object of investigations is an individual’s network. This could be, for instance, his or her friends within a certain social network site. Of importance also is the objective associated with looking to the social media in order to learn from the data available there. Here, two perspectives are relevant, namely the ‘ego-centric’ perspective, where the goal of studying a person’s network is to find out more about the individual (for example, do they like a certain product) and the ‘network centric’ perspective, where the accompanying connections in the network are of central importance, (for example, which person in the network exerts the most influence over that network).²⁸⁶

284 Finlay, above n. 1, at p. 182.

285 Ibid, at pp. 182-183.

286 Ibid, at p. 190.

2.4.1.6.2 *Computational Linguistics*

Commercial text analytics software are readily available that are able to identify not only regular text but also diagnose opinion, based not only on the actual text but also on factors underlying the text, for example, the relationship between words and not necessarily the words themselves. This provides the capability to identify sentiment in the digital environment, for example, ‘worry’, ‘anger’, ‘disgust’ or ‘happiness’. One such computer-based programme has the capacity to identify the propensity for violence in addition to having the following characteristics: it is self-learning (it learns a language just as a human would), it is not language specific and it is not disrupted by the use of slang, unique expressions, synonyms, code words or even misspellings. These qualities are invaluable when scrutinizing text on-line.²⁸⁷ Of special importance here is the nature of the data that is scrutinized. It is not necessarily well structured, but rather unstructured in the form of blogs, the social media and web pages.

Another characteristic of this tool is its ability to extract information, and ultimately knowledge, not only from text at face value, but also by the manner in which the text is produced. For example, much can be learned about a person by examining the way that he or she writes and not solely by the actual words themselves. The way someone writes, in addition to conveying that person’s most inner thoughts, can divulge information concerning that person’s physical or physiological traits. For example, it may indicate a state of intoxication over a certain period of time, information which a prospective employer might want. Another example of this type of knowledge extraction is provided by research into Twitter usage during the flooding of the Red River Valley by the Red River that runs along the border between the US and Canada. This research showed how information can be extracted from Twitter feeds during emergency situations, such as natural disasters, that can be of benefit to emergency management. In this case, the authorities made public information about the disaster situation, which was then either supported, refuted or new representations distributed.²⁸⁸

287 For an example of the available technology and its applications, more information can be found at the site of Gavagai, available at <https://www.gavagai.se/solutions/> (last accessed on 2017-04-07).

288 Palen, Leysia, Starbird, Kate, Vieweg, Sarah and Hughes, Amanda, *Twitter-Based Information Distribution During the 2009 Red River Valley Flood Threat*, Bulletin of

A research project used predictive modelling to detect sarcasm on Twitter (where 5.9 million tweets were analysed), and Amazon (where 66 000 product evaluations were analysed).²⁸⁹ The importance of detecting sarcasm can be useful for different reasons. Concerning product evaluation, it can be useful in identifying what a clientele really thinks about a product. Law enforcement may also have an interest in discovering the real intentions of individuals, who may attempt to hide their intentions behind a certain language use.

Attempts have also been made to identify psychological illnesses by examining the use of language through the written medium. A competition advertised on Kaggle, in conjunction with the Online Privacy Foundation, resulted in a project that examined the social media using predictive methods in order to predict personality traits, where the anti-social traits of narcissism, Machiavellianism and psychopathy were identified from the use of language on Twitter. Once again, the value of the research was not in the determining of psychopathy in individuals, but rather concerning its prevalence amongst groups.²⁹⁰

The level at which predictive modelling is operating becomes apparent when examining technologies such as Content OneBox (COB), which is an application used by Google that places its users into ‘buckets’, after scanning every action performed by its users. In short it is a means of sorting its users into categories based on certain attributes, such as areas of interest. The possibility exists to create millions of buckets, each bucket being a grouping of

the American Society for Information Science and Technology, Vol. 36, No. 5, available at <https://pdfs.semanticscholar.org/29aa/e3480fb3b1563d83d600787487e7d8427535.pdf> (last accessed on 2017-03-31), at p. 13.

- 289 Davidov, Dmitry, Tsour, Oren and Rappoport, Ari, *Semi-Supervised Recognition of Sarcastic Sentences in Twitter and Amazon*, Proceedings of the Fourteenth Conference on Computational Natural Language Learning, pages 107–116, Uppsala, Sweden, 15-16 July 2010, Association for Computational Linguistics, available at <http://www.aclweb.org/anthology/W10-2914> (last accessed on 2017-03-17).
- 290 Sumner, Chris, Byers, Alison, Boochever, Rachel, Park, Gregory. J., *Predicting Dark Triad Personality Traits from Twitter Usage and a Linguistic Analysis of Tweets*, Proceeding, ICMLA '12 Proceedings of the 2012 11th International Conference on Machine Learning and Applications - Volume 02, Pages 386-393, available at https://www.onlineprivacyfoundation.org/research/_Sumner_Predicting_Dark_Triad_Traits_from_Twitter_Usage_V5.pdf (last accessed on 2015-05-06) and Solon, Olivia, *Study: Twitter analysis can be used to detect psychopathy*, Wired, available at <http://www.wired.co.uk/news/archive/2012-07/23/twitter-psychopaths> (last accessed on 2015-05-06).

users. What is interesting is that these buckets need not have labels but rather operate as a clustering system, to be matched with advertisers whose interests and target groups can be matched with these buckets.²⁹¹ The above is indicative of two trends: first, it highlights the trend away from accepting data at face value and towards interpreting the knowledge carried by the data but that may not be visible to the human eye and second, it highlights a trend away from the emphasis on the importance of identity specific knowledge, such as age, gender and other personal data associated with an individual.

2.4.1.6.3 Target

The example of Target is often used to illustrate the characteristics and concerns of predictive modelling: it proves its power as a predictive tool, it shows how mainstream its use has become, it shows how concealed and unobtrusive a technology it is and most of all it reinforces the fears associated with it. Target is a US-based retail outlet.²⁹² The company achieved notoriety due to the publicity it received in connection with a predictive model it had constructed in order to identify its pregnant customers and their due date.²⁹³

Research has shown that people exhibit a fixed shopping behaviour over time. There are however periods in a person's life, which due to their impressionability, can cause people to change their behaviour. One such event occurs when one is expecting a child. During this period, a woman's (or couple's) shopping behaviour is susceptible to influence. Therefore, a commercial actor wishing to gain a competitive advantage over a rival, needs to approach a pregnant woman earlier than its rival can.²⁹⁴ For a company like Target, wishing to get a head start against any commercial rivals, the key is to determine

291 Gould, Jeff, *Court Docs Show How Google Slices Users Into 'Millions of Buckets'*, available at <https://medium.com/@jeffgould/courts-docs-show-how-google-slices-users-into-millions-of-buckets-ec9c768b6ae9> (last accessed on 2015-05-07).

292 Target, available at <http://intl.target.com/> (last accessed on 2016-12-20).

293 Duhigg, Charles, *How Companies Learn Your Secrets*, New York Times, 16 February 2012, available at <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all> (last accessed on 2017-04-14).

294 In some countries, one way of finding out if someone has just had a child is by consulting a public register, for example, a births registry database at a public authority or

when a customer is pregnant before any of the other stores can do so. Target set out to do this using predictive modelling and with the utilization of correlation data.²⁹⁵ First, Target required test data for an algorithm to learn from, which was acquired from the baby gift registry, where women voluntarily provided data concerning the fact that they were pregnant and also the expected due date. In addition, Target employed other targeted marketing programmes in order to get prospective mothers to reveal themselves.²⁹⁶ The predictive analytics department noticed how a woman's shopping habits changed as she approached her due date. For example, they often bought lotion, but at the beginning of the second trimester pregnant women bought larger quantities of unscented lotion. Also, within the first twenty weeks of pregnancy, women started to buy supplements like calcium, magnesium and zinc. Customers also regularly bought soap and cotton wool but when a woman suddenly started buying large amounts of cotton wool together with cloths and disinfectant, it was a sign that the due date was fast approaching. With this knowledge, Target was even able to trigger shopping habits by means of a coupon sent via email that would entice a purchase on the internet, or where an advertisement on a Friday would possibly result in a purchase during a shopper's routine shopping excursion to the store on the weekend.²⁹⁷ Using this predictive technology, Target was able to contact its pregnant customers before their rivals could do so.

This example also highlights the value of the information that consumers part with, which seems rather harmless, unimportant and far from sensitive. In other words, the information being revealed may seem rather innocuous at the time it is being parted with, but once connected with other data or used for other purposes, can prove to be sensitive in nature.

the tax office. Such a register may be public information and it is usual for new parents to receive advertisements for baby products from companies who monitor these registries.

295 Ibid.

296 Siegel, above n. 118, at p. 39.

297 Duhigg, *How Companies Learn Your Secrets*, above n. 293.

2.4.1.6.4 *Hewlett-Packard*

Another example of predictive modelling comes from Hewlett-Packard, which wanted to determine which of its employees have a higher propensity for leaving the company, the behaviour in need of prediction being referred to as ‘flight risk’. From a business perspective, the flight of employees is undesirable as it is expensive to find and train new employees and much experience and knowledge leaves the company with the employee. Two employees at Hewlett-Packard developed a predictive model to determine which employees were likely to quit. The predictive model identified certain factors that were relevant in the prediction of such behaviour as well as the relationship between these factors. The predictive model was also able to identify factors that one would assume would have the opposite effect. For example, a factor that increased the risk of an employee leaving was his or her promotion, which, while being a positive step, also resulted in the belief on the part of the employee that he or she was no longer being adequately remunerated, leading to increased dissatisfaction. The company was able to identify which employees were high risk and which measures needed to be put in place in order to reduce the risk from the point of view of the company. The company estimated that the predictive model identified \$300 million in potential savings with respect to employee replacement and productivity.²⁹⁸

2.5 Influencing Human Behaviour

The mere identification and prediction of human behaviour acquired from the predictive modelling process is not where it ends. With this knowledge, companies have the ability to alter the behaviour of individuals, using means which may be more overt, for example marketing campaigns, or more subtle means of manipulation, which is the focus of this section.

Extensive reference is made to the work of Thaler and Sunstein, who in their work ‘Nudge’, provide some reasons as to why human beings are susceptible to manipulation and the effects thereof.²⁹⁹ The point of departure is

298 Siegel, above n. 118, at p. 45.

299 Thaler and Sunstein, above n. 10.

that all human interaction occurs within an environment. The manner in which this environment is constructed is important, both from a symbolic point of view but also because changes to a physical environment influence behaviour. This is particularly well put by Churchill, where, after the House of Commons was damaged by a bomb in 1941, it had to be decided whether to re-build it according to its previous design or whether to adopt a more modern design:

Here is a very potent factor in our political life. The semicircular assembly, which appeals to political theorists, enables every individual or every group to move round the centre, adopting various shades of pink according as the weather changes ... The party system is much favoured by the oblong form of the chamber. It is easy for the individual to move through those insensible gradations from Left to Right, but the act of crossing the Floor is one which requires serious attention.³⁰⁰

An example of an environment, offered by Thaler and Sunstein, is that of the school cafeteria, whereby the person who controls this space has a key position to the extent that he or she is able to manipulate the behaviour of those making their way through this environment. For example, how the food is arranged influences behaviour and the person in control, referred to as the ‘choice architect’, has the following choices: 1) arrange the food in order that the students are best off, 2) arrange the food at random, 3) arrange the food to get the students to choose the food they would have on their own, 4) arrange the food prioritising the suppliers that provide the largest bribes or 5) arrange the food so as to maximise profits. Irrespective of the choice made, what is of prime importance is the notion that there is no such thing as a neutral design and irrespective of motivations, any design, intentional or unintentional, will have an impact. Another point made is that ‘everything matters’ and that small alterations can have a large impact on the behaviour of people. Above all, the choice architect has power. A concept put forward by the authors, favouring option one above, is what they term ‘libertarian paternalism’. Admittedly contradictory in nature, the authors propose a stance whereby people are free to make choices and are essentially able to opt out of an architecture (libertarian) while at the same time, choice architects should be able to do what is necessary

300 Churchill, Winston S., *The Second World War, Volume V, Closing the Ring*, Cassell & Co, 1952, at p. 150 in Klang, Mathias, *Disruptive Technology – Effects of Technology Regulation on Democracy*, Gothenburg Studies in Informatics, Report 36, October, 2006, at p. 1.

to put people in a better position and nudge them in the right direction (paternalism), the rationale being that in general, people do not make good choices.³⁰¹ This is best described by the authors themselves:

A nudge, as we will use the term, is any aspect of the choice architecture that alters people's behaviour in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, the intervention must be easy and cheap to avoid. Nudges are not mandates. Putting the fruit at eye level counts as a nudge. Banning junk food does not.³⁰²

That people are susceptible to being nudged, according to Thaler and Sunstein, originates in research within social science that has shown that human beings are not particularly rational when making decisions or when required to use their judgement, because of the manner in which they think.³⁰³ A distinction is made between two ways in which human beings think. Researchers within psychology have developed so-called 'dual-process models of social information processing', which have been applied to social attitudes, stereotyping, person perception, memory, judgement and decision-making, stating that:

Dual-process models ... all share the basic assumption that two qualitatively different modes of information processing operate in making judgements and decisions and in solving problems. In essence, the common distinction in dual-process models is between a fast, associative information-processing mode based on low-effort heuristics, and a slow, rule-based information-processing mode based on high-effort systematic reasoning. Related dual-processing perspectives distinguish between controlled versus uncontrolled, conscious versus unconscious, and affective versus cognitive models of processing.³⁰⁴

The first mode of information processing is the intuitive and automatic way of thinking, which is fast and instinctive. It occurs almost as a reflex and is associated with a gut reaction. The second is the reflective and rational way of thinking, which is deliberate, self-conscious and associated with conscious

301 Thaler and Sunstein, above n. 10, at pp. 1-6.

302 Ibid, at p. 6.

303 Ibid, at pp. 8 and 21.

304 Chaiken, Shelly and Trope, Yaacov (eds.), *Preface* in *Dual-Process Theories in Social Psychology*, The Guilford Press, 1999, at p. ix.

thought.³⁰⁵ In addition, two types of people are introduced by the authors. First, based on ideas from within economics, ‘homo economicus’ or ‘econs’ are the economic man that makes good decisions most of the time and falls within the image of the human being portrayed within economics. The second category of people are ‘homo sapiens’ or ‘humans’, which are essentially most people who do not live up to the expectations assumed of the ‘econ’.³⁰⁶ The problem is that the choices made using the automatic mode of thinking may result in human beings making decisions that are unfavourable. Considering the increased complexity of society, with the pressures to make more decisions on a daily basis, the automatic mode of thinking is relied on more extensively, which can be problematic considering its imperfections. The aim with the implementation of libertarian paternalism is to protect human beings from the bad decisions they make from of relying on their automatic way of thinking.³⁰⁷

Associated with the automatic way of thinking is the notion of habit. Research at MIT’s department of brain-and-cognitive sciences, examining the brain activity in rats, has shown that the first time a rat is required to navigate a structure to find strategically placed food, its brain activity is high. The brain activity decreases each time the exercise is repeated and as the rat increasingly relies on habit.³⁰⁸ A term referred to is ‘chunking’, whereby the brain converts behavioural action into automatic routine, with hundreds of chunks being created and corresponding with numerous daily actions that are required to be executed.³⁰⁹ The formation of a habit is described as a three-step loop: first there is a cue, telling the brain to go into automatic mode and which habit to use, second there is the routine, which can be mental, physical or emotional and third, there is the reward, which assists the brain in determining whether this loop should be retained for the future.³¹⁰ There are a number of reasons for relying on habit. The human brain is always looking for ways to decrease the necessity of constantly making minor decisions, in order that the major

305 Thaler and Sunstein, above n. 10, at p. 21, referring to dual-process theories as canvassed in Chaiken and Trope, above n. 304.

306 Ibid, at p. 7.

307 Ibid, at p. 24.

308 Duhigg, *How Companies Learn Your Secrets*, above n. 293.

309 Duhigg, Charles, *Habit: Why We Do What We Do in Life and Business*, Random House Trade Paperback Edition, 2012, at p. 17.

310 Duhigg, *How Companies Learn Your Secrets*, above n. 293.

decisions can take preference, a crucial element in this process being the brain's ability to identify situations where habit can be relied on.³¹¹

What is certain is that companies are aware of this research as well as of the manner in which the brain works and it is in this way that the knowledge gained from predictive modelling can be utilized in order to maximize the profits of commercial actors. A case in point is that of the company Procter and Gamble, that initially struggled in promoting the product 'Febreze', a liquid spray that could remove bad smells. The marketing campaign initially promoted the removal of bad smells from the home, not attaining much success. However, the marketing department had missed one fundamental fact, namely, that people who are continually exposed to a certain odour become immune to it. Here, they had missed an elementary fact concerning the cue aspect of habits, and that those people who needed Febreze most, were unable to identify this. Rather, what these people wished for was a reward, the reward here being a nice smell from Febreze after the act of cleaning. In addition, this reward was desired despite there being no bad smell from the start.³¹² In this manner, knowledge of the habit cycle allowed a corporation to maximize an advertising campaign and align it better with the consumers' habit pattern, thereby influencing behaviour.

2.6 Summary and Conclusions

An initial observation is that for many different reasons, the amount of available data has increased exponentially, resulting in the notion big data. What must also be borne in mind is that the nature of big data is also significant. Previously, as far as was possible, data were collected and stored in databases. This data can be characterised as being of a more static and structured nature. While this is still the case, big data has become more dynamic or fluid in nature, the notion of 'streaming' data or 'live' data relevant in this regard. Also, there is no longer the need to store the data in databases to the same extent as has been the case up until recently. Once the knowledge is extracted from the data, using modern technology such as predictive models, it can be discarded.

311 Duhigg, *Habit*, above n. 309, at pp. 17-18.

312 For an extensive description of the Febreze case, see Duhigg, Charles, *Habit*, above n. 309, at pp. 37-55.

This has also led to new approaches to analysing data, for example, from a theory driven approach to a data driven approach.

The applications of predictive modelling are in their infancy. While the basics of predictive modelling, namely, the practical application of statistics, essentially has remained the same, technological developments have increased the power of this tool. This includes the unprecedented availability of large amounts of data, the development of modern algorithms to extract new knowledge from these data and the ability of predictive models to be self-learning. Predictive models are also incorporated into decision-making systems that have varying degrees of independence. Those who have access to this technology also have access to power, including the ability to manipulate people. For the masses, however, the technology remains a ‘black box’.

A closer investigation of predictive models reveals that there are different types, which utilize different methods for arriving at the decisions they suggest. This in turn allows for different degrees of human control, which is relevant from a responsibility perspective. What is certain is that the reliance on predictive models and their ambit of operation is likely to increase as big data develops. For example, as more biometric data at the molecular and cellular level becomes available, so too will the possibility to predict a predisposition for a certain illness, resulting in predictive medicine being applied, instead of the reactionary methods available presently.³¹³

While technology is neither good nor bad, it can be put to negative uses. For example, search engines facilitate peoples’ interaction with the digital environment and much can be learned about individuals by examining their search queries. It was reported that advertising companies, with the help of special code, were monitoring the search habits of users that employed the Safari browser, even though such monitoring was blocked by default.³¹⁴ Technology can also be used for unintended purposes. Web site visits can be monitored using Google Analytics, which places a text file on the visitor’s computer and also stores the IP (Internet Protocol) address from where the search was made, enabling the correlation between IP address and Gmail account and the subsequent identification of individuals.³¹⁵

313 Hood, Leroy, *Systems Biology: Integrating Technology, Biology and Computation, Mechanisms of Ageing and Development*, 124, pp. 9-16, 2003, at p 16.

314 Angwin and Valentino-Devries, above n. 195.

315 Örstadius, Kristoffer, *Websidor avslöjar ditt besök för Google*, Dagens Nyheter, 27 September 2012.

In addition, it is worth noting that knowledge gained from disciplines, such as the behavioural sciences, is increasing the effectivity of the uses to which technology can be put. For example, as knowledge concerning how the human mind works becomes available, or the manner in which physical appearances reflect the human personality, technologies can be adapted to take advantage of this knowledge. This in turn is starting to put in question the ability of human beings to make decisions that are in their best interests, especially in the digital environment and where complex technologies are concerned.

A final consideration refers to the correlation of data, especially big data, and touches upon the notion of how data is represented, mentioned above. The power of predictive models lies in the ability of this technology to make correlations between data points. Of more importance are the actual correlations between data and not necessarily the actual data points themselves. In other words, an individual may be notified that a certain data point was used to make a decision about him or her. However, if that data point was correlated with another data point to arrive at the decision, unless information is provided concerning the influence the second data point had in relation to the outcome, access to the original data point is almost useless. In other words, any meaningful access to data requires access to the big picture and all data points as correlated and used to arrive at a decision.

It is in the context of the future application of predictive technologies that the next chapter provides a theoretical foundation for the study of the potential harms associated with the use of predictive technologies.

3 A Theoretical Background

3.1 Introductory Remarks

This chapter examines to what extent predictive modelling diminishes personal autonomy and restricts its development. It provides a theoretical context to predictive modelling and the reasons for the proliferation within society of surveillance techniques to support it. What becomes apparent is that the use of predictive models and accompanying technologies, amounts to the surveillance of individuals, employees, customers and society in general. Predictive models are used, not because it is fun or because companies are evil, but because, in the face of a more mobile population and globalization, they diminish risk and assist with decision-making, thereby increasing profit. Placing predictive modelling in the context of surveillance is beneficial in a number of respects. It draws attention to the fact that individuals are being subjected to constant monitoring, using a barrage of digital tools, and it allows for reflection concerning its effects on human beings and ultimately society in general. This chapter describes different justifications of the progression to the surveillance society. A common theme is that surveillance provides knowledge and knowledge is power. This chapter also examines the notion of autonomy and identity, providing a brief philosophical orientation. Personal autonomy is a central notion in that it is identified as a common denominator linking the potential harms associated with predictive modelling, an inventory of which is provided in the next chapter. Personal autonomy is also a pre-condition in order to build identity, two aspects of which are discussed below. First, identity is an instrument by which humans regulate their interaction with others and second, it is the product of the predictive model in the form of a digital representation of the individual.

3.2 Surveillance and Social Change

People have always profiled each other, even before computers existed. Sometimes this profiling has been performed based on ‘gut feel’, physical appearance playing a role in how an individual has been judged by society. Prior to large scale urbanization, people lived in villages, with the individual’s existence closely entwined with all the other individuals of that village. Everyone knew each other, which gave the notion of reputation a function within society. Due to the fact that everyone knew each other personally, one’s reputation was important, as having it tarnished or even destroyed could have disastrous consequences to one’s social standing. The inhabitants of the village, in their interaction with one another, would come to decisions about each other based on socially adapted tools such as reputation or gossip.³¹⁶ A person with a destroyed reputation had two main alternatives, namely to move to another village and make a fresh start, or to repair the tarnished reputation, for example, by means of explanation.

Society has become fluid and mobile, influencing human interaction and therefore the function that reputation has as a regulatory mechanism. Not only has human interaction been altered, but the interaction between humans and the institutions of society has also been influenced. Modernization and urbanization have brought with it cultural changes but also changes in the relationships between people, where the number of relationships or contacts with strangers has increased, and where the length of these encounters has become shorter, affecting the extent to which people are able to effectively determine trust.³¹⁷ Consequently, large scale urbanization has influenced the function that reputation once had within the village. Within the urban confines, the close personal connection that people had, vanished, increasing the ability to become anonymous, the individual being judged to a large degree at face value. Not too much was known about the individual and everything to be learned about the individual in order to judge his or her character was based on social interactions that spanned a relatively short period of time. In addition, the size of modern cities allowed for different contexts or social spheres,

316 Solove, *The Future of Reputation*, above n. 192, at p. 32.

317 Heimer, Carol, A., *Solving the Problem of Trust*, in *Trust in Society*, p. 40, available at https://www.researchgate.net/publication/261707664_Solving_the_Problem_of_Trust (last accessed on 2016-09-28), at p. 65.

in turn allowing a person to determine the border between these social spheres and allowing for privacy.

As the village society disintegrated and with an increase in societal mobility and urbanization, it became more difficult for central institutions to keep track of the individuals with which they previously had dealings. Amidst the large increase in urbanization, and as the population became more mobile and anonymous, the close relationship between the individual and the institutions that they interacted with, became weaker. It was precisely these close relationships between individual and institution that formed the basis on which the institutions could arrive at a (business) decision concerning the individual. It is within this context that the relationship between commercial actor and individual changed. Heimer argues that this relationship is characterised by either trust or distrust, with distrust of the individual being the default starting point. It is within this relationship that the factor of power becomes relevant, where companies are able to use their position of power to their advantage, insisting that individuals part with vast amounts of data about themselves in order to diminish the distrust.³¹⁸

In order to address this problem caused by modern mobility, the institutions that had contact with these individuals, had to rely on a new method for seeking and gathering information about the individuals with which they interacted. Within sociology, organizations are characterised as systems for coping with uncertainty in their environments:

... formal organizations are not the only social forms which coordinate and facilitate human action in the face of otherwise uncertain conditions. But only formal organizations in the modern sense devote themselves so systematically and self-consciously to searching for unpredictable or disruptive elements in the environment, and attempting to master them so as to achieve desired results ... For the organizational activities of interest here, the environment is people; the uncertainties to be mastered are ambiguities as to what people 'deserve' what organizational responses.³¹⁹

318 Ibid.

319 Perrow, Charles, *Complex Organizations: A Critical Essay*, Glenview, Ill, Scott Forsman and Co, 1972 in Rule, James B., McAdam, Douglas, Stearns, Linda and Uglow, David, *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies*, Elsevier, 1980, at p.44.

In other words, in dealing with humans there are uncertainties, which organizations are required to identify and curtail.

A reason often provided for the progression from privacy to data protection, dealt with in Chapter 5 below, is technology. However, in the context of changing societal relationships, it is also seen as an effect of the increase in the scale of organizations as well as the increase in the distance between the individual and the social and economic institutions with which they deal.³²⁰ Lessig refers to ‘hierarchies of social rank’, which require information in order to be able to make distinctions based on rank, or what he refers to as ‘subtle distinctions of rank’.³²¹ The mobility of people took away the ability to gauge trust and social status, especially in the commercial setting.

The digital environment has resulted in the development of the ‘global village’, a term coined by McLuhan, describing a world interconnected by an electronic nervous system, allowing for events taking place in one part of the world to be experienced in other parts of the world in real time.³²² Society has come full circle in that the means for judging people, required in order to counter the distrust of companies, lost in the age of urbanization and mobility, has been reacquired, albeit in a different form. The anonymity that was possible in the urbanized society has disappeared with the advent of digital technologies and the accompanying ability to track individuals as they make their way through this digital space. While the internet has revolutionized peoples’ on-line social relationships, monitoring their presence in the digital environment as sources of information from which to make judgements about them has a number of consequences. First, the time available to gauge a person’s reputation is shorter, with credit institutions, for example, being expected to make a decision about a potential customer in real time. Second, the trust (or lack thereof) that characterized the commercial actor and individual relationship is dependent not on the person’s reputation as such but rather on the person’s digital reputation, that is the image of a person ascertained from within the digital environment and as perceived by technological agents. Third, the

320 Clark, Roger, *What’s Privacy?*, Prepared for a workshop at the Australian Law Reform Commission, 28 July 2006, available at <http://www.privacy.org.au/Resources/PLawsIntl.html> (last accessed on 2014-05-21), at p. 4.

321 Lessig, above n. 53, at p. 221.

322 The term ‘global village’ is attributed to McLuhan, Marshall, *The Gutenberg Galaxy*, University of Toronto Press, 1962. See also *The Living Internet*, Marshall McLuhan *Predicts the Global Village*, available at http://www.livinginternet.com/i/ii_mcluhan.htm (last accessed on 2016-10-07).

digital environment does not forget. While an individual's transgressions in the village could possibly be forgotten over time, the memory of the digital sphere is absolute, this leading to the call for legal arrangements, such as the inclusion of a right to be forgotten in legal instruments such as the GDPR.

The norms being created in the digital environment are also different from those that existed in the village. Solove highlights the way in which organizations nowadays establishes an individual's reputation by the collection of fragments of data, more specifically personal data.³²³ An example of this trend is highlighted by the employer versus employee relationship. This relationship is described by Packard in his book *The Naked Society*, where he paints a bleak picture of the frenzy in the US during the 1960's, where employers went to great lengths to find out personal details concerning prospective employees in order to gauge whether they wanted to hire them. It was not uncommon for prospective employers to hire private detectives, the most intimate details seen as relevant to identifying the productive, dependable and loyal employee. Tools such as lie detectors, questionnaires and personality tests were common, all with the goal of rooting out the undesirable applicants.³²⁴ These measures were expensive, time consuming and intrusive. The process ended with a profile of the prospective employee being compiled and provided to the employer for a fee.³²⁵ The introduction of computers into mainstream society together with large-scale digitalisation, would soon change this process.

The development and popularity of the digital environment, spurred on by the internet, has changed the manner in which companies are able to gauge prospective employee suitability in a more cost effective and less intrusive manner. For example, using digital technologies associated with the social media, it is possible to measure job performance. One research project found that the perusal of a person's Facebook profile can be used to determine per-

323 Solove, *The Future of Reputation*, above n. 192, at p. 32.

324 Packard, Vance, *The Naked Society*, IG Publishing, 1964, at pp 73-122.

325 Ibid.

sonality factors such as conscientiousness, agreeability and intellectual curiosity.³²⁶ It is more cost effective than hiring a private detective, it is less intrusive in that it can take place without the person ever knowing about it and the process can be automated.

Predictive models are one of many mechanisms that help commercial actors acquire information about their customers, considering that the traditional relationships between companies and individuals have become weaker. However, what they do require is data. One manner of obtaining data is through surveillance. The next section provides a theoretical context for the increased surveillance of the digital environment.

3.3 A Context for Surveillance

Many theories are provided explaining the development of, and increase in the use of, surveillance techniques within society, which may differ from one academic discipline to another. Therefore, while context bound, briefly examining these theories sheds light on the differing attitudes to surveillance and the technologies that enable them.

A general definition of surveillance is the following:

The systematic investigation or monitoring of the actions or communications of one or more persons. Its primary purpose is generally to collect information about them, their activities, or their associates. There may be a secondary intention to deter a whole population from undertaking some kind of activity.³²⁷

Within the digital environment, the term ‘dataveillance’ has been coined, described by Clarke as, ‘the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more

326 Kwow, Leslie, *Facebook Profiles Found to Predict Job Performance*, Wall Street Journal, available at <http://www.wsj.com/articles/SB10001424052970204909104577235474086304212> (last accessed on 2015-05-05).

327 Clarke, Roger, *Information Technology and Dataveillance*, November 1987, available at <http://www.rogerclarke.com/DV/CACM88.html> (last accessed on 2016-09-28) at p. 3.

persons’.³²⁸ The manner in which surveillance takes place, may also influence its legitimacy. For example, making the distinction between ‘personal dataveillance’ and ‘mass dataveillance’, Clarke points to the increased dangers when surveillance is carried out on the masses.³²⁹ This development towards the ability to monitor the masses in the digital environment, has been described as a progression from surveillance being about ‘watching’ to being about ‘seeing with data’, a definition of surveillance in the digital environment being, ‘... any systematic focus on personal information in order to influence, manage, entitle, or control those whose information is collected’.³³⁰ In addition to the monitoring of individuals by organizations becoming commonplace, an identified trend is that of the increase in individuals monitoring each other.³³¹ It is argued that individuals have always monitored each other for various reasons: it gives them a power advantage over others but it is also an essential element if a person is to lead a ‘gregarious life’.³³² What has changed, however, is the accessibility of individuals to technologies that, while not as powerful as predictive modelling, are commercially available and facilitate the monitoring of others. This has resulted in what Bennett et al. refer to as the, ‘... surveillance culture, where watching has become a routine and unremarkable part of social life’.³³³

3.3.1 Panopticism

One manner in which the modern technologies of surveillance are couched is in terms of the analogy of the Panopticon. The architectural association with Panopticism is that of a space, where the individuals housed in that space,

328 Ibid.

329 Ibid, at p. 14.

330 Bennett, Colin J., Haggerty, Kevin D., Lyon, David and Steeves, Valerie, *Transparent Lives: Surveillance in Canada*, Athabasca University Press, 2014, at p. 6. Reference is also made to Schneier’s use of the phrase ‘data as surveillance’, in Schneier, above n. 152, at pp. 20-32.

331 Ibid, at p. 167.

332 Locke, John L., *Eavesdropping: An Intimate History*, Oxford University Press, 2010, at pp. 6-7.

333 Bennett, Haggerty, Lyon, and Steeves, above n. 330, at p. 168.

could easily be monitored with a minimum of resources. It was a blueprint for industrial buildings, hospitals, and schools although the most famous association has become that of the prison. Designed by Jeremy Bentham, and called the Panopticon, it was subsequently studied by Foucault, who identified it as the concretization of the imposition of a system of domination.³³⁴ As a prison, the Panopticon could house large numbers of prisoners, whom could be monitored by relatively few guards. The jarring description of the Panopticon by Foucault, not only describes the physical attributes of the design, but also provides insight into the emotional impact that the structure could potentially have, even in a commercial context, such as on the factory floor:

At the periphery, an annular building; at the centre, a tower; this tower is pierced with wide windows that open onto the inner side of the ring; the peripheric building is divided into cells, each of which extends the whole width of the building; they have two windows, one on the inside, corresponding to the windows of the tower; the other, on the outside, allows the light to cross the cell from one end to the other. All that is needed, then, is to place a supervisor in a central tower and to shut up in each cell a madman, a patient, a condemned man, a worker or a schoolboy. By the effect of backlighting, one can observe from the tower, standing out precisely against the light, the small captive shadows in the cells of the periphery. They are like so many cages, so many small theatres, in which each actor is alone, perfectly individualized and constantly visible. The panoptic mechanism arranges spatial unities that make it possible to see constantly and to recognize immediately. In short, it reverses the principle of the dungeon; or rather of its three functions - to enclose, to deprive of light and to hide - it preserves only the first and eliminates the other two. Full lighting and the eye of a supervisor capture better than darkness, which ultimately protected. Visibility is a trap.³³⁵

The rationale behind this architecture was that the prisoners never knew when they were being monitored, with the guard tower a constant reminder that they were being watched, this internalized assumption of being monitored discouraging deviant behaviour. The prisoners were also isolated from each other, which prevented communication and therefore the spreading of undesired be-

334 Poster, Mark, *The Mode of Information: Poststructuralism and Social Context*, Polity Press, 1990, at p. 90.

335 Foucault, Michel, *Discipline and Punish: The Birth of the Prison* (Alan Sheridan trans.), Peregrine Books (1977), Reprinted in Penguin Books, 1991, at p. 200.

haviour. The architectural structure led to control via complete visibility coupled with continuous monitoring, the long-term goal being social control where the prisoners ultimately monitored themselves. Simon also captures the emotional aspect of the Panopticon:

The panoptic structure seems to speak to the sense of helplessness individuals often feel in the face of the overwhelming force of institutions (prisons, hospitals, schools, workplaces, families) to determine life within their confines ... the sense that there is nowhere to run and nowhere to hide.³³⁶

Foucault continues his description of the Panopticon by referring to the power of the structure creating not only the conditions for total visibility of the prisoners, but also total invisibility of the watchers. He states that, '[t]he Panopticon is a machine for dissociating the see/being seen dyad: in the peripheric ring, one is totally seen, without ever seeing; in the central tower, one sees everything without ever being seen'.³³⁷

Poster reflects on the aims of both Bentham and Foucault in their reference to the Panopticon. For Bentham, the goal of the prison was to make non-prisoners of the prisoners, to be accomplished by constant monitoring and a regime in place to effect that change. The Panopticon was a structure that, 'deflected the criminal's mind from the irrationality of the transgression to the rationality of the norm', and with no escape from monitoring, the prisoner would accept the authority of the norm. Foucault, taking the Panopticon out of the context of this liberal theory provided by Bentham, viewed it not as a system for the purpose of transforming prisoners into non-prisoners, but rather as a system of domination.³³⁸

Both Poster and Foucault recognized the advance of technology:

Our society is one not of spectacle, but of surveillance; under the surface of images, one invests bodies of depth; behind the great abstraction of exchange, there continues the meticulous, concrete training of useful forces; the circuits of communication are the supporters of an accumulation and a centralization of knowledge; the play of signs defines the anchorages of power; it is not that the beautiful totality of the individual is amputated, repressed, altered by our

336 Simon, Bart, *The Return of Panopticism: Supervision, Subjection and the New Surveillance*, *Surveillance and Society* 3(1), pp. 1-20, 2005.

337 Foucault, above n. 335, at p. 201.

338 Poster, above n. 334, at p. 90.

social order, it is rather that the individual is carefully fabricated in it, according to a whole technique of forces and bodies.³³⁹

The Panopticon is used as a metaphor for highlighting the relationship between surveillance and power. In the words of Foucault, the Panopticon, 'is a diagram of a mechanism of power reduced to its ideal form'.³⁴⁰ Foucault argued that the Panopticon, with its methods of discipline, allowed for the birth of the modern industrial society, where the prevalent forms of violent power demonstration could fall away and be replaced by other forms of power demonstrations, which were more subtle and used the 'technology of subjection' to further state that power:

... insidiously objectifies those on whom it is applied; to form a body of knowledge about these individuals, rather than to deploy the ostentatious signs of sovereignty. In a word, the disciplines are the ensemble of minute technical inventions that made it possible to increase the useful size of multiplicities by decreasing the inconveniencies of the power which, in order to make them useful, must control them.³⁴¹

3.3.2 Orwell and Nineteen Eighty-Four

In 1949 the English author George Orwell published the novel *Nineteen Eighty-Four*, which has since become a famous reference within privacy literature, the metaphor of 'Big Brother' being extensively used and where the slogan 'Big Brother is watching you' is referred to in order to convey the notion of constant surveillance. It is set in the fictional totalitarian state of Oceania where the political system results in a constant and omnipresent surveillance by the Government, also known as 'Big Brother'. The system of total surveillance and the accompanying manipulation is carried out by the 'Inner Party' that puts down all forms of individualization and free thinking. Big Brother demands total obedience and controls every aspect of its citizens' lives, the goal being the establishment of a society of uniform individuals. This is to be attained through total control where even the thoughts of people

339 Foucault, above n. 335, in Poster, above n. 334, at p. 93.

340 Foucault, above n. 335, at p. 205.

341 Ibid, at p. 220.

are read and the notion of privacy eradicated. Technology plays a central role, with Big Brother utilizing multiple forms of technology to provide the means of total and continuous monitoring, an example being the ‘telescreen’, which is a television that is installed in every home, its unique attribute being its two-way communication ability, where Big Brother can monitor those watching the television. The power lies in the fact that people watching the telescreen cannot tell if they are being watched, in turn leading to the internalized assumption that they are always being watched, ultimately influencing their behaviour accordingly.³⁴²

There are resemblances between the Panopticon and Nineteen Eighty-Four. Those being watched cannot see the watchers, leading to the internalized assumption of always being watched and resulting in conformist behaviour. In addition, the technology employed is a technology of power. The metaphor of Nineteen Eighty-Four can be applied to modern technologies of surveillance, especially in the digital environment, where the internet’s architectural characteristics facilitate the constant monitoring of every action. As with Nineteen Eighty-Four, actual monitoring is not required in order to influence behaviour. Just the suspicion that monitoring may be taking place suffices. It is also from this metaphor of Big Brother that the term ‘Little Brother’ has been coined, referring to commercial actors that utilize surveillance technologies in order to monitor consumers.³⁴³

3.3.3 Kafka and The Trial

Another well-known metaphor used in the surveillance narrative is that of The Trial, a novel written by Franz Kafka and published in 1925. The protagonist Joseph K. is woken one day by the police. He is arrested, but does not know why and nor can the police answer this question. Joseph K. spends the remaining time trying to determine why he was arrested. From the scraps of information he can find, and by meeting various characters, he determines that a large bureaucratic court has compiled a dossier on him, which is sent backwards and forwards through the bureaucratic administration. However, he has

342 Orwell, George, *Nineteen Eighty-Four*, Penguin Books Ltd., 2008.

343 Solove, *The Digital Person*, above n. 67, at p. 32.

no access to the Court or his file. Eventually, Joseph K. is called to an interrogation by the Court, where the officials are indifferent to the matter. The peculiarity about the Court being its secrecy, where the court officials are not identifiable and interaction with the public non-existent. Finally, Joseph K. is taken away in the middle of the night and executed.³⁴⁴ The value of the metaphor is eloquently summarized by Solve:

Kafka depicts an indifferent bureaucracy, where individuals are pawns, not knowing what is happening, having no say or ability to exercise meaningful control over the process. This lack of control allows the trial to completely take over Joseph K.'s life. The Trial captures the sense of helplessness, frustration and vulnerability one experiences when a large bureaucratic organization has control over a vast dossier of details about one's life. At any time, something could happen to Joseph K.; decisions are made based on his data, and Joseph K. has no say, no knowledge, and no ability to fight back. He is completely at the mercy of the bureaucratic process ... [t]here is no diabolical motive or secret plan for domination; rather, there is a web of thoughtless decisions made by low-level bureaucrats, standardized policies, rigid routines, and a way of relating to individuals and their information that often becomes indifferent to their welfare.³⁴⁵

3.3.4 The Panspectron

DeLanda in his work *War in the Age of Intelligent Machines*, makes reference to the 'Panspectron', which also is a follow-on from the Panopticon metaphor, this time in a military context.³⁴⁶ The Panspectron is referred to as a, 'new non-optical intelligence-acquisition machine', the importance of which has come to the fore as communications have moved from cables in the ground to wireless signals, in turn necessitating the need for new methods of encoding the messages that use this communication medium.³⁴⁷ Yardley, a civilian, founded the Black Chamber, the first American crypto-agency, which was to

344 Kafka, Franz, *The Trial*, Dover Publications Inc., 2009.

345 Solove, *The Digital Person*, above n. 67, at pp. 38-41.

346 DeLanda, Manuel, *War in the Age of Intelligent Machines*, Swerve Editions, 1991, at pp. 205-206.

347 Ibid, at p. 205.

later become the NSA, which in turn, according to DeLanda, is continuing the task of building the Panspectron, with notable differences:

Instead of positioning some human bodies around a central sensor, a multiplicity of sensors is deployed around all bodies: its antenna farms, spy satellites and cable-traffic intercepts feed into its computers all the information that can be gathered. This is then processed through a series of ‘filters’ or key-word watch-lists. The Panspectron does not merely select certain bodies and certain (visual) data about them. Rather, it compiles information about all at the same time, using computers to select the segments of data relevant to its surveillance tasks.³⁴⁸

3.3.5 The Superpanopticon

Poster has Foucault and Panopticism as his point of departure in describing the role that technology and more specifically databases have played as far as the database discourse is concerned. Initially, he refers to the development of ‘home networking’, popular during the 1980’s in America. It consisted of the phenomenon whereby companies would make available product databases to consumers via the medium of television.³⁴⁹ The consumer, by purchasing products via these databases, in turn created new databases for the companies, these new databases comprising information about these consumers and their purchasing habits. This is an example of what Poster refers to as the ‘Superpanopticon’, following his discussion of Panopticism.

It is this increase in surveillance using technology, or as Poster puts it, ‘circuits of communication’ together with the databases that are generated with the collection and storage of data from this increased surveillance, that results in the ‘Superpanopticon’, which is a system of surveillance without the architectural constraints of the Panopticon.³⁵⁰ The Superpanopticon is not merely a development in the ability to monitor people, but encompasses an element of social engineering, whereby society has been trained to participate in their own surveillance. Therefore, technologies such as credit cards, driving licenses, social security cards and the like are applied for and used to perform

348 Ibid, at p. 206.

349 Wikipedia, *Shop at Home Network*, available at https://en.wikipedia.org/wiki/Shop_at_Home_Network (last accessed on 2016-06-15).

350 Poster, above n. 334, at p. 93.

transactions, each transaction eventually ending up in a database. It is in this context that Poster refers to a new language situation, where the transformation of information into the language of databases, in other words into one's and zero's, or from analogue to digital, results in a loss of data.³⁵¹ Transforming natural language into the database language, results in a natural deterioration of that information in so far as the digital language is more rigid than other forms of language and as a result cannot adequately reflect them:

I contend that the database imposes a new language on top of those already existing and that it is an impoverished, limited language, one that uses the norm to constitute individuals and define deviants ... the structure or grammar of the database creates relationships among pieces of information that do not exist in those relationships outside of the database. In this sense, databases constitute individuals by manipulating relationships between bits of information.³⁵²

The Superpanopticon is also a method of control. It is comprised of technologies of surveillance that transcend the physical constraints of the Panopticon. It is also characterized by the presence of databases that transform all language into a digital format that fits the rows and columns of the database. This process alters the meaning of natural language, since society is willing to utilize these new technologies, in effect making people their own guards. It is a medium of control with consequences:

We see databases not as an invasion of privacy, as a threat to a centred individual, but as the multiplication of the individual, the constitution of an additional self, one that may be acted upon to the detriment of the 'real' self without that 'real' self ever being aware of what is happening.³⁵³

The Superpanopticon therefore is everywhere, facilitated by the technologies individuals use and not confined to physical constraints. It has the databases at the centrum, as the databases are the main technological driving force behind surveillance. Its main objective is to transform natural language into the language of the database, thereby transforming every individual into a recordable format.

351 Ibid, at p. 94.

352 Ibid, at pp. 95-96.

353 Ibid, at pp. 97-98.

3.3.6 The Surveillant Assemblage

Following on the metaphors of the Panopticon and Big Brother, Haggerty and Ericson refer to the creation of the ‘surveillant assemblage’. They highlight the development from previously discrete surveillance systems to the convergence of surveillance systems. The data being produced from the mechanisms of surveillance are combined to form the surveillant assemblage:

This assemblage operates by abstracting human bodies from their territorial settings and separating them into a series of discrete flows. These flows are then reassembled into distinct ‘data doubles’ which can be scrutinized and targeted for intervention. In the process, we are witnessing a rhizomatic levelling of the hierarchy of surveillance, such that groups which were previously exempt from routine surveillance are now increasingly being monitored.³⁵⁴

The assemblage is the bringing together of all the modes of surveillance, where practices and technologies are woven into a single entity, allowing for an increase in the capacity of the systems of surveillance. Packard reiterates the idea that technologies in themselves may not be intrusive, however, the danger lies in the amalgamation of these technologies:

Individually the new social controls we are seeing are cloaked in reasonableness. And some perhaps have comic overtones. But when we view them collectively we must consider the possibility that they represent a massive, insidious impingement upon our traditional rights as free citizens to live our own lives.³⁵⁵

Haggerty and Ericson make special reference to the surveillance of the physical body, stating that, ‘[f]irst it is broken down by being abstracted from its territorial setting. Then it is reassembled in different settings through a series of data flows. The result is a decorporealized body, a “data double” of pure virtuality’.³⁵⁶ In other words, the human as an object of surveillance, has its characteristics broken down into data, after which it is reconstituted in a dif-

354 Haggerty and Ericson, above n. 66, at p. 606.

355 Packard, above n. 324, at p. 34.

356 Haggerty and Ericson, above n. 66, at p. 611.

ferent form, context or setting. The human body is broken down into information, in order for it to be more mobile and also in order to facilitate comparison.³⁵⁷ The automatic nature of this process is also alluded to, where the surveillant assemblage requires machines to ‘make and record discrete observations’, the body in turn being broken down into ‘a series of discrete signifying flows’.³⁵⁸ Once the body has been broken down, there arises the need to reassemble it, such centres of reassembly being identified as ‘forensic laboratories, statistical institutions, police stations, financial institutions and corporate and military headquarters’ and where strategies of governance, commerce and control are formulated.³⁵⁹

What is noteworthy is the utility of the surveillant assemblage:

Rather than being accurate or inaccurate portrayals of real individuals, they are a form of pragmatics: differentiated according to how useful they are in allowing institutions to make discriminations among populations ... it is productive of a new type of individual, one comprised of pure information.³⁶⁰

Referring to Bauman, the authors state that the modern notion of surveillance is now less about discipline and power and more about people being ‘constituted as consumers and seduced into the market economy’.³⁶¹ Just as with the Panopticon, where the inmates were conditioned to self-monitor, it is argued that consumers are encouraged to monitor themselves. Consumers give up information about their habits, in return for perks, such as customer loyalty bonuses, travelling points or better service, leading to the phrase ‘the disappearance of disappearance’, where individuals no longer have a place to hide.³⁶²

357 Ibid, at p. 613.

358 Ibid, at p. 612.

359 Ibid, at p. 613.

360 Ibid, at p. 614.

361 Bauman, Zygmunt, *Intimations of Postmodernity*, Routledge, 1992 in Haggerty and Ericson, above n. 66, at p. 615.

362 Ibid, at pp. 615-619.

3.3.7 The Commercial Dimension

It is within this context that data has been described as the ‘new oil’.³⁶³ Haggerty and Ericson alluded to the commercial value associated with surveillance and the metaphor of the Panopticon has become popular in many disciplines, for example in sociology, where it has come to represent an administrative technique.³⁶⁴ In the commercial context, it is referred to as an ‘ordering machine’ for categorizing and sorting people in order that they can be seen and understood.³⁶⁵ Gandy, transposing the notion of the Panopticon to the commercial sector, states:

The Panopticon represents the idea that control over individuals is made possible where one has a system that provides for the continuous, automatic and disciplinary surveillance of people who have been determined to be in need of normalization or correction, and framed in technology of power, it involves the organization of individuals into space by placing them in categories, where surveillance serves the goal of correction and control.³⁶⁶

Gandy takes the metaphor of the Panopticon further by referring to the ‘panoptic sort’:

The panoptic sort is the name I have assigned to the complex technology that involves the collection, processing, and sharing of information about individuals and groups that is generated through their daily lives as citizens, employees, and consumers, and is used to coordinate and control their access to goods and services that define life in the modern capitalist economy ... the panoptic sort is a difference machine that sorts individuals into categories and classes on the basis of routine measurements. It is a discriminatory technology that allocates options and opportunities on the basis of those measures and the administrative models they inform ... it moves into action solely in response to an action by the object of its control ... [t]he panoptic sort is a system of power.³⁶⁷

363 Rotella, Perry, *Is Data the New Oil?*, Forbes, available at <http://www.forbes.com/sites/perryrotella/2012/04/02/is-data-the-new-oil/> (last accessed on 2015-05-22).

364 Gandy, above n. 187, at p. 22, note 23.

365 Simon, above n. 336.

366 Gandy, above n. 187, at p. 21.

367 Ibid, at p. 15.

The panoptic sort categorizes people in relation to their profitability or their potential risk to profitability, the term ‘cyber triage’ used to describe the process by which individuals are divided into groups or categories depending on their potential economic or political value.³⁶⁸ In other words the aim is to identify those clients that have the least value and simply discard them. This sorting process requires data, information and knowledge.

Robins and Webster refer to the concept of ‘cybernetic capitalism’, in their investigation of information and knowledge in the ‘information economy’, referring to the process whereby commercial actors collect, store and process as much information as possible in order to control individuals to an extent that these individuals would never have anticipated.³⁶⁹ Gandy, in his reference to the panoptic sort, also acknowledges the capitalistic perspective in relation to data, information and knowledge.

Robins and Webster contend that as a result of the ‘information revolution’, it is not just certain physical architectures that resemble the Panopticon, but rather that society is becoming a ‘hierarchical and disciplinary Panoptic machine’.³⁷⁰ They describe the process of the depletion of social skills, knowledge and self-sufficiency on the part of individuals, which knowledge is transferred to centres of power, such as companies, only to be sold back to the consumers in a different form, stating that ‘[t]he centres of power are multiple and differential; the archives of commerce and control are relatively dispersed. But in each of them social knowledge and resources are appropriated and transformed into power and capital’, emphasising that information and knowledge negotiate power relations, also contending that information is not a thing or an entity, but rather a social relation. In the capitalistic society, where knowledge is an inherent part of the relations of power, it is becoming the arena for the battle for power.³⁷¹ Cohen too refers to control of the ‘modes of prediction’, highlighting the economic relationship between knowledge and power.³⁷²

368 Ibid, at p. 2.

369 Robins, Kevin and Webster, Frank, *Cybernetic Capitalism: Information, Technology, Everyday Life*, pp. 44-75 in Mosco, Vincent and Wasko, Janet, *The Political Economy of Information*, The University of Wisconsin Press, 1988.

370 Robins and Webster, above n. 369, at p. 59.

371 Ibid, at pp. 69-72.

372 Cohen, Julie E., *Examined Lives: Informational Privacy and the Subject as Object*, 52 *Stanford Law Review*, 1373-1438, 2000, at p. 1406.

3.3.8 The Minority Report

The Minority Report is a 1956 science fiction short story by the author Philip K. Dick. The story involves three mutants ('precogs'), whom are able to foresee the commission of crime, allowing the 'Precrime Division' to arrest criminals before a crime is committed. The main character, John Anderton, who is head of Precrime, receives a report in which it is stated that he is going to kill a person by the name of Leopold Kaplan, a man he has never met, and which results in an adventurous plot.³⁷³

The Minority Report serves an important function within the surveillance context. It refers to the notion of the prediction and thereby control of human behaviour, something which is lacking in the other surveillance theories. It portrays the situation whereby undesired (criminal) human behaviour is eradicated, not under threat of consequences but by proactively incarcerating the criminal before the crime can be committed. While seemingly futuristic, it is not extreme taking into account current policing methods being utilized to combat crime. For example, in the US, predictive analytics is being used in a joint project between the Memphis Police Department and the University of Memphis. Called 'Blue Crush' (Crime Reduction Using Statistical History), a new methodology is being used to detect crime in advance, whereby police investigators, sociologists and mathematicians are combining their expertise and utilizing technology in order to predict what crime will take place, when and where. With this knowledge, extra resources can be allocated to the identified areas.³⁷⁴

The Minority Report is a fictional novel, it concerns law enforcement and the technology depicted does not yet exists (the ability to foresee crime). However, what it does is capture the notion of prediction, where human behaviour is predicted and influenced.

373 Dick, Philip K., *Minority Report*, Gollancz, 2012.

374 Vlahos, James, *The Department of Pre-Crime*, Scientific American, January 2012, at p. 50.

3.3.9 Concluding Remarks

Many of the above theories concern the relationship between state and individual. However, it is important to note their applicability also to the commercial setting. For example, Bentham's Panopticon was an industrial design for a variety of environments, including factories. Second, while the state versus individual relationship may be at the centre, this should not be a hinder to the use of analogy in applying them to other relationships. Third, some of the theories specifically refer to the commercial setting, for example, Gandy, Haggerty and Ericson and Robins and Webster. Consequently, it is submitted that the commercial setting is represented by these theories.

One theme that is highlighted by examining the above theories is the role of technology and the manner in which it has altered the static nature of surveillance. From being confined by physical constraints, modern technology, accompanied by the reliance on the digital environment, has allowed surveillance to occur unhindered by physical constraints, such as a structure's architecture. This development is also characterized by a potential intrusion that is unprecedented, considering the nature and amount of information and knowledge that can be gained about individuals without detection. For example, Solove reflects that many of the technologies associated with the internet, for example databases, have the same aim as Big Brother, namely social control and the suppression of individuality.³⁷⁵ Cohen argues that while much of the focus on Bentham's Panopticon concerns the notion of discipline through 'visibility', its treatment by Foucault concerns 'normalization' through discipline, where in the modern society, discipline is attained through statistical methods.³⁷⁶ In support of this, she cites Foucault, who stated that:

... whereas the juridical systems define juridical subjects according to universal norms, the disciplines characterize, classify, specialize; they distribute along a scale, around a norm, hierarchize individuals in relation to one another and, if necessary, disqualify and invalidate.³⁷⁷

375 Solove, *The Digital Person*, above n. 67, at p. 32.

376 Cohen, Julie E., *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*, Yale University Press, 2012, at p. 136.

377 Foucault, above n. 335, at p. 223.

In the modern society, the surveillance is decentralized and performed by multiple institutions, both public and private, that regulate everyday life.³⁷⁸

On the topic of technology, the focus of Nineteen Eighty-Four, *The Trial* and the *Superpanopticon* is the database, in other words a certain computer hardware and software solution used to store data. Here reference is made to the trend, identified in Chapter 2, where the notion of storing data in a structured form is diminishing in favour of accessing the fluid and dynamic constellations of data that make up big data. The value is not in the actual data but rather in its meaning, in other words, in the knowledge that it potentially holds. This technical development, it is argued, contradicts slightly the central role attributed to the physical database in the surveillance theory.

The objective of surveillance is power. This is illustrated in the context of the NSA's ambition to know about everything happening on the internet. Greenwald writes:

Ultimately, beyond diplomatic manipulation and economic gain, a system of ubiquitous spying allows the United States to maintain its grip on the world. When the United States is able to know everything that everyone is doing, saying, thinking and planning – its own citizens, foreign populations, international corporations, other government leaders – its power over those factions is maximized. That's doubly true if the government operates at ever greater levels of secrecy. The secrecy creates a one-way mirror: the US government sees what everyone else in the world does, including its own population, while no one sees its own actions. This is the ultimate imbalance, permitting the most dangerous of all human conditions: the exercise of limitless power with no transparency or accountability.³⁷⁹

The above citation also illuminates the economic aspect connected with state surveillance. This elevates the relevance of the above theories of surveillance despite the potential criticism that they relate to the state versus individual relationship and not the commercial sector. For example, one document leaked by Snowden revealed the economic aspect of state surveillance.³⁸⁰ The NSA spied on purely industrial targets, for example the Brazilian Ministry of Mines

378 Cohen, *Configuring the Networked Self*, above n. 376, at p. 136.

379 Greenwald, above n. 85, at p. 169.

380 Edward Snowden is a US citizen who worked for the intelligence services and who in 2013 revealed documents showing the mass surveillance activities pursued by the NSA. More information is available at Free Snowden, available at <https://edwardsnowden.com/> (last accessed on 2017-03-26).

and Energy, the gains related to such economic espionage being the ability to gain the upper hand in trade negotiations, thereby benefitting US industry and indirectly US companies.³⁸¹

The emotional harm that results from the modes of surveillance mentioned above are also relevant. There is a certain discomfort associated with being constantly monitored. There is also the feeling of helplessness in being characterised or depicted in a manner that does not correspond with a self-image. Being categorized in a certain light, based on data points, statistics, mathematics, machine learning and artificial intelligence, where human action is predicted based on probability, is harmful to humans. Adding insult to injury, there is no means of altering this image as it is created by the ‘black box’ of technology and the logic of which is accessible to only a few. The words of Cohen, once again most eloquently put, portrays a life constituted by the monitoring of an individual’s every single move:

Pervasive monitoring of every first move or false start will, at the margin, incline choices to the bland and the mainstream. The result will be a subtle yet fundamental shift in the content of our character, a blunting and blurring of rough edges and sharp lines. But rough edges and sharp lines have intrinsic, archetypal value within our culture. Their philosophical differences aside, the coolly rational Enlightenment thinker, the unconventional Romantic dissenter, the sceptical pragmatist, and the iconoclastic postmodernist all share a deep-rooted antipathy toward unreflective conformism. The condition of no-privacy threatens not only to chill the expression of eccentric individuality, but also, gradually, to dampen the force of our aspirations to it.³⁸²

A final point concerning the surveillance that humans are being exposed to is its indiscriminate nature. The words of Solove, describing the public surveillance apparatus, resonates in the commercial sector as well:

In sum, the privacy problem created by the use of databases stems from an often careless and unconcerned bureaucratic process – one that has little judgement or accountability – and is driven by ends other than the protection of people’s dignity. We are not just heading toward a world of Big Brother or one composed of Little Brothers, but also toward a more mindless process – of

381 Ibid, at pp. 135-141.

382 Cohen, *Examined Lives*, above n. 372, at p. 1426.

bureaucratic indifference, arbitrary errors, and dehumanization – a world that is beginning to resemble Kafka’s vision of *The Trial*.³⁸³

3.4 Autonomy and Identity

What follows is a brief analysis of the philosophical dimension associated with the context of technology and law. The philosophical dimension becomes relevant, in circumstances where a problem arises to which there is no right or wrong answer, but where a stance is required to be taken despite the difficult implications. This is especially relevant in adjudicating the desirability of new technologies that, despite their advantages, also harbour risks. In such circumstances, where there are conflicting interests, the philosophical perspective is usually helpful in determining where to draw the line in order to achieve a balance.

Two concepts are discussed below, namely ‘autonomy’ and ‘identity’. Not only are they important when assessing the impact of technologies on peoples’ lives, but they are interrelated in that personal autonomy is a necessary precondition for identity building. Both autonomy and identity are impacted by the predictive modelling process and are therefore in need of examination.

Finally, concrete examples are provided of scenarios from the digital environment where autonomy and identity are harmed.

3.4.1 A Philosophical Background

The estimation of whether a technology is desirable or where to draw the line regarding its use often boils down to issues of morality or ethics. There are different ways of applying the ethical approach. For example, Brownsword refers to the ‘three-cornered matrix’.³⁸⁴ While he uses it in the context of biotechnology, it can be applied to all types of technology. The three corners of the triangle are ‘goal-orientated’ (consequentialism), ‘rights-based’ and ‘duty-

383 Solove, *The Digital Person*, above n. 67, at p. 55.

384 Brownsword, Roger and Goodwin, Morag, *Law and the Technologies of the Twenty-First Century*, Cambridge University Press, 2012, at p. 184.

based' forms. The normative frameworks corresponding with the above three-corner model are utilitarianism (goal-orientated), liberalism (rights based) and deontology (duty based).³⁸⁵

Utilitarianism has its roots in the seventeenth century thinking of the British philosopher Jeremy Bentham. The basic principle of utilitarianism is that an act is determined to be morally right when it maximizes the happiness of the community, happiness being the quantitative measure of pleasure and the absence of pain, pain and pleasure being the sole motives behind all human action.³⁸⁶ Bentham writes:

By the principle of utility is meant that principle which approves or disapproves of every action whatsoever, according to the tendency which it appears to have to augment or diminish the happiness of the party whose interest is in question: or, what is the same thing in other words, to promote or oppose that happiness.³⁸⁷

The utilitarian approach is referred to as a consequentialist approach as it holds the view that human action is determined solely by the consequences for human well-being. The consequences of actions are more important than their inherent character.³⁸⁸ The formula involves weighing up the benefits of something against the costs to human well-being, determining whether an action is to be considered legitimate from the utilitarian point of view. The equation does not treat human beings in their own right when measuring human well-being, but rather focusses on the well-being of all, allowing for the sacrifice of the rights of individuals within society for the greater good of society at large.³⁸⁹ John Stuart Mill, a supporter of utilitarianism, conceded however, that some pleasures were more valuable than others.³⁹⁰ It is argued that this

385 Ibid, at p. 185.

386 Cahn, Steven M., and Markie, Peter, *Ethics: History, Theory and Contemporary Issues*, 6th edition, Oxford University Press, 2016, at p. 354.

387 Bentham, Jeremy, *An Introduction to the Principles of Morals and Legislation*, Hafner Publishing Company, Darien Conn. 1970, at p. 2, in Cahn and Markie, *Ibid*, at p. 354.

388 Brownsword and Goodwin, above n. 384, at p. 186.

389 *Ibid*, at p. 186.

390 Cahn and Markie, above n. 386, at p. 363.

utilitarian lens is used for the most part when regulating technology in the Western world.³⁹¹

A deontological basis for morality looks to the morality of the actions themselves. The most famous proponent of this approach was Immanuel Kant, who argued that one cannot treat people as a means to an end, but rather they should be treated as an end in themselves, this approach having a religious grounding and coming to the fore in discussions surrounding topics such as dignity.³⁹² Kant formulated a standard of morality that he named the ‘categorical imperative’, described as, ‘a moral law that is unconditional or absolute for all agents, the validity or claim of which does not depend on any ulterior motive or ends.’³⁹³ Kant argued that an action should not be judged by its consequences, but rather by the principle that gave rise to the action, the only true principles being those that are universal in that they can be applied to all people and at any time.³⁹⁴ The categorical imperative was a command of reason that was not dependent on anyone’s particular desires.³⁹⁵ Kant described the categorical imperative as a principle that was objective, rationally necessary and unconditional, with all immoral actions lacking rationality as they breached the categorical imperative, which was based on the notion that moral requirements were essential to rational agency and that a rational will must be regarded as autonomous in the sense of being the law that binds it.³⁹⁶ Kant criticised utilitarianism in that it devalued individuals, since the utilitarian calculation ultimately determined a person’s welfare in terms of its benefit to others, thereby treating a person only as a means and not as an end in themselves.³⁹⁷ Another philosopher opposed to utilitarianism was John Rawls, who

391 Brownsword and Goodwin, above n. 384, at p. 186.

392 Ibid, at p. 186.

393 Encyclopaedia Britannica, *Categorical Imperative*, available at <https://global.britanica.com/topic/categorical-imperative> (last accessed on 2016-10-05).

394 Cahn and Markie, above n. 386, at p. 314.

395 Ibid.

396 Stanford Encyclopedia of Philosophy, *Kant’s Moral Philosophy*, available at <http://plato.stanford.edu/entries/kant-moral/> (last accessed on 2016-10-05).

397 McCormick, Matt, *Immanuel Kant: Metaphysics*, Internet Encyclopedia of Philosophy, available at <http://www.iep.utm.edu/kantmeta/#H9> (last accessed on 2017-02-28).

authored the work entitled *A Theory of Justice*.³⁹⁸ This opposition to utilitarianism was based on the grounds that maximizing the happiness of the greatest number of people allowed individual concerns to be sacrificed for the sake of social preferences.³⁹⁹ The act of the ‘ideal legislator’ promoted by utilitarianism, according to Rawls, was no different than that of the entrepreneur seeking to maximise profit or the consumer seeking to maximize the satisfaction of the purchase:

In each case there is a single person whose system of desires determines the best allocation of limited means. The correct decision is essentially a question of efficient administration. This view of social cooperation is the consequence of extending to society the principle of choice for one man, and then, to make this extension work, conflating all persons into one through the imaginative acts of the impartial sympathetic spectator. Utilitarianism does not take seriously the distinction between persons.⁴⁰⁰

Liberalism, a political school of thought that focuses on the individual, places a burden on the state and society at large to provide the conditions in order that individuals be able to make the decisions that best correspond with the way they wish to live. Liberalism focuses on individual rights, this line of thought also being described as a ‘human rights perspective’, where freedom (free speech and freedom of thought) is important but not unlimited, equality being an example of one factor limiting this freedom.⁴⁰¹

Schwartz illuminates the fact that much of the scholarly thought concerning privacy has revolved around the liberal paradigm and the ability to control privacy, more specifically the right to control the use of one’s data, putting the individual at the centre of the decision-making process.⁴⁰² In this regard, Cohen refers to the struggle between the supporters of ‘information-as-freedom’ and ‘information-as-control camps’, stating that the latter camp viewed the

398 Rawls, John, *A Theory of Justice*, Cambridge, Mass., The Belknap Press of Harvard University Press, 1971 in Cahn and Markie, above n. 386, at p. 571.

399 Ibid.

400 Ibid, at p. 579.

401 Brownsword and Goodwin, above n. 384, at p. 186.

402 Schwartz, Paul, M., *Privacy and Democracy in Cyberspace*, 52 *Vanderbilt Law Review*, 1607, 1999, available at <http://scholarship.law.berkeley.edu/facpubs/1162> (Last accessed on 2017-04-14), at pp. 1659-1660.

internet as being governed by a ‘natural law of the market’.⁴⁰³ She continues by criticising legal theorists for applying a liberal political theory and for failing to ask questions about culture, subjectivity and social ordering that have become common with new technologies.⁴⁰⁴ There are a number of limits associated with the liberal individualism conception of the legal subject: first, this person is an autonomous entity capable of exercising acquired rights irrespective of context, second, this person possesses the capacity for rational deliberation, also separated from context and third, the selfhood this person possesses is distinct from the body.⁴⁰⁵ It is from within the liberal political philosophy that utilitarianism has been chosen with which the law identifies.⁴⁰⁶ Cohen states that in the US legal context, legal academics are primarily trained to take the liberal political theory perspective, for example, when examining notions such as autonomy, one of the consequences being the study of cultural and social institutions from the detached, value-neutral distance of liberal theory.⁴⁰⁷ She adds:

Legal scholarship posits simplistic models of individual behaviour derived from the first-order liberal commitments and then evaluates emerging legal and technical regimes that govern information flows according to the models. Theoretical frameworks organized around the core liberal individualist themes of expressive and market liberty predominate, regardless of their fit with the phenomena under investigation.⁴⁰⁸

Instead, Cohen argues that the development of the information society should occur, taking into account, ‘ways that promote the well-being of the situated, embodied beings who inhabit it’. The basis of this stance is attributed to the work of Nussbaum, who promotes the law as a mechanism for promoting human flourishing.⁴⁰⁹ In order to achieve the goal of human flourishing, Cohen

403 Cohen, Julie E., *Configuring the Networked Self*, above n. 376, at pp. 12-13.

404 Ibid, at p. 15.

405 Ibid, at p. 16.

406 Ibid, at p. 21.

407 Ibid, at pp. 4-5.

408 Ibid.

409 Nussbaum argues that traditionally, economic factors such as profit have been used to measure human development. For example, the quality of life is said to be improving when a country’s Gross Domestic Profit (GDP) is increasing. Nussbaum, however, refers to a new paradigm, called the ‘Human Development’ approach or ‘Capabilities

argues that the law should take into account the, ‘ordinary, everyday ways in which situated, embodied subjects experience their culture and their own evolving subjectivity, and when they consider the ways in which networked information technologies reshape everyday experience’.⁴¹⁰ It is argued that the factors that best achieve a position of human flourishing in the networked society are access to knowledge, operational transparency and room for play of everyday practice.⁴¹¹ In other words, Cohen argues that a new paradigm is required in the information society that has a different focus compared to liberal political theory.

3.4.2 Autonomy

The notion of autonomy takes centre stage because it is the common denominator linking the potential harms associated with predictive modelling, addressed below. There are countless definitions of what autonomy is and how it should be defined, its meaning ultimately depending on perspective. Autonomy is a concept that is difficult to define and is not easily explained. It may differ from person to person and may be influenced by external factors, for example, cultural attitudes. One of the more well-known works on autonomy

Approach’, which asks the simple question, ‘what are people actually able to do and to be? Nussbaum argues that what is required is that respect be shown to real people and that they are empowered, instead of reflecting on the biases of the intellectual elite. She continues, ‘[a] new theoretical paradigm is evolving, one that is the ally of people’s demands for a quality of life that their equal human dignity requires. Unlike the dominant approaches, it begins from a commitment to the equal dignity of all human beings, whatever their class, religion, caste, race, or gender, and it is committed to the attainment, for all, of lives that are worthy of that equal dignity. Both a comparative account of the quality of life and a theory of basic social justice, it remedies the major deficiencies of the dominant approaches. It is sensitive to distribution, focusing particularly on the struggles of traditionally excluded or marginalized groups. It is sensitive to the complexity and the qualitative diversity of the goals that people pursue. Rather than trying to squeeze all these diverse goals into a single box, it carefully examines the relationships among them, thinking about how they support and complement one another. It also takes account of the fact that people may need different quantities of resources if they are to come up to the same level of ability to choose and act, particularly if they begin from different social positions. Nussbaum, Martha C., *Creating Capabilities*, The Bellknop Press, 2013, pp.ix-xi and 186.

410 Cohen, *Configuring the Networked Self*, above n. 376, at p. 6.

411 Ibid.

was produced by Gerald Dworkin and is entitled *The Theory and Practice of Autonomy*.⁴¹² Also, Joseph Raz investigates the concept of autonomy in the work entitled *The Morality of Freedom*.⁴¹³ Both these scholars take the legal philosophical perspective in their respective works on autonomy.

3.4.2.1 Autonomy Defined

Autonomy, according to normal language usage, is described as, ‘the state of existing or acting separately from others’.⁴¹⁴ In other words, it is the state in which an individual is free to make a decision based on the factors that a person him or herself chooses to base that decision upon. The word autonomy is derived from the Greek words ‘self’ and ‘law’ or ‘rule’ and means ‘the having or making of one’s own laws’.⁴¹⁵ On an individual level, autonomy has four meanings, namely capacity to govern oneself, the actual condition of self-government, the ideal of character or the sovereign authority to govern oneself.⁴¹⁶ A general definition states that:

Individual autonomy is an idea that is generally understood to refer to the capacity to be one’s own person, to live one’s life according to reasons and motives that are taken as one’s own and not the product of manipulative or distorting external forces ... to be autonomous is to be one’s own person, to be directed by considerations, desires, conditions, and characteristics that are not simple imposed externally upon one, but are part of what can somehow be considered one’s authentic self. Autonomy in this sense seems an irrefutable value, especially since its opposite – being guided by forces external to the self and which one cannot authentically embrace – seem to mark the height of oppression.⁴¹⁷

412 Dworkin, G., *The Theory and Practice of Autonomy*, Cambridge University Press, Cambridge, 1988.

413 Raz, Joseph, *The Morality of Freedom*, Oxford Scholarship Online 2003, first publication 1998.

414 Merriam Webster Dictionary, *Autonomy*, available at <http://www.merriam-webster.com/dictionary/autonomy> (last accessed on 2015-12-15).

415 Feinberg, Joel, *Autonomy*, in *The Inner Citadel, Essays on Individual Autonomy*, John Christman (ed.), Oxford University Press, 1989, at p. 27.

416 *Ibid*, at p. 28.

417 Stanford Encyclopedia of Philosophy, above n. 340.

At the core of Kant's theory of morality is the fact that all rational human wills are autonomous, where one is bound by laws of one's own creation. A person is free, therefore, when he or she is bound by his or her own will and not by the will of others. The categorical imperative claims its legitimate morality in that it is grounded in a person's own rational will.⁴¹⁸ Dworkin acknowledges the difficulty in defining autonomy:

It is apparent that although not used just as a synonym for qualities that are usually approved of, 'autonomy' is used in an exceedingly broad fashion. It is used sometimes as equivalent of liberty (positive or negative in Berlin's terminology), sometimes as equivalent to self-rule or sovereignty, sometimes identical with freedom of the will. It is equated with dignity, integrity, individuality, independence, responsibility and self-knowledge. It is identified with qualities of self-assertion, with critical reflection, with freedom from obligation, with absence of external causation, with knowledge of one's own self interests. It is even equated by some economists with the impossibility of interpersonal comparisons. It is related to actions, to beliefs, to reasons for acting, to rules, to the will of other persons, to thoughts, and to principles. About the only features held constant from one author to another are that autonomy is a feature of persons and that it is a desirable quality to have.⁴¹⁹

This passage illustrates how autonomy can mean different things to different people and is, as a result, difficult to define precisely. Nevertheless, it is something that is desirable to human beings and Dworkin attempts to provide a definition:

Autonomy is conceived of as a second-order capacity of persons to reflect critically upon their first-order preferences, desires, wishes, and so forth and the capacity to accept or attempt to change these in the light of higher-order preferences and values. By exercising such a capacity, persons define their nature, give meaning and coherence to their lives, and take responsibility for the kind of person they are.⁴²⁰

418 Johnson, Robert, *Kant's Moral Philosophy*, *The Stanford Encyclopedia of Philosophy* (Summer 2014 Edition), Edward N. Zalta (ed.), available at <http://plato.stanford.edu/archives/sum2014/entries/kant-moral/> (last accessed on 2014-11-10).

419 Dworkin, above n. 412, at p. 6.

420 Ibid, at p. 20.

Dworking goes on to describe autonomy as a human characteristic whereby a person is able to reflect upon and have an awareness regarding his or her desires, intentions and general motivational structure and to make changes to that structure. It is therefore not merely a reflective characteristic but also the ability to take action in order to effect change in relation to one's preferences.⁴²¹

For Raz, autonomous agents are required to meet three conditions: first, they must possess certain mental capacities, second, they must have a range of valuable options and third, they must enjoy independence from coercion and manipulation.⁴²² He argues that the main idea behind autonomy is that people should make their own lives, and continues by providing a definition of autonomy where, '[t]he autonomous person is a (part) author of his own life. The ideal of personal autonomy is the vision of people controlling, to some degree, their own destiny, fashioning it through successive decisions throughout their lives'.⁴²³ Consequently, a person does not suddenly, one day, decide what his or her goals are and subsequently attempt to attain them. These personal goals may take time to materialize, changing over time. Of interest is the reference by Raz to the fact that autonomy, 'is opposed to a life of coerced choices ... [t]o choose one must be aware of one's options' and that it is not the quantity of choices that a person has, but rather the variety of choice.⁴²⁴ In other words, a person that is presented with multiple choices that really do not make a difference to his or her circumstances, cannot be said to possess autonomy.

Another attribute of autonomy refers to an individual's capacity for self-regulating, which encompasses concepts such as self-esteem, self-awareness, self-acceptance, self-responsibility and self-assertion.⁴²⁵ Autonomy is also the ability to reflect on one's motivational structure and to make changes to that motivational structure. For example, a person may, having identified the influences that move him or her in a certain manner, associate him or herself positively with those influences and appreciate being moved in that manner

421 Ibid, at p. 108.

422 Raz, above n. 413, at p. 369.

423 Ibid.

424 Ibid, at p. 371.

425 Klang, *Disruptive Technology – Effects of Technology Regulation on Democracy*, above n. 300, at p. 185.

by those influences, while on the other hand, a person may frown upon the influences moving him or her and wish to have other influences, for example, other values or ideals.⁴²⁶ It becomes apparent that autonomy is not just something passive or the desire to be left alone and in seclusion. There is an active aspect to autonomy, which reinforces the notion of an individual as being an independent agent, with a freedom of movement and a freedom of association.

Not only is freedom of movement essential, but also a freedom of communication. The bi-directional nature of communication is important where the individual is able to communicate with others but also where he or she is able to receive communications from others.⁴²⁷ This is necessary as it allows the individual access to the facts, which in turn allows for informed decisions to be made, where any attempt to interfere with this communication process must be viewed as unwarranted.

Autonomy comprises not only negative duties, but also positive ones. According to Raz, in addition to refraining from actions of coercion and manipulation, one can create conditions for living an autonomous life, for example by providing a person with the capability for absorbing, remembering and using information, as well as providing a person with an adequate number of choices to choose from.⁴²⁸

In summarizing the meaning of autonomy, an apt description is that it is a, ‘conception of the person able to act, reflect, and choose on the basis of factors that are somehow her own (authentic in some sense)’.⁴²⁹

3.4.2.2 The Value of Autonomy

Autonomy’s value lies in its being an essential part of what it means to be an agent and grounds an individual’s notion of what it means to have a ‘character’.⁴³⁰ This highlights the interrelation between autonomy and identity. Raz, on the other hand, simply states that, ‘[a]utonomy is a constituent element of

426 Dworkin, above n. 412, at p. 6.

427 Klang, above n. 300, at p. 187.

428 Raz, above n. 413, at p. 408.

429 Stanford Encyclopedia of Philosophy, *Autonomy in Moral and Political Philosophy*, available at <http://plato.stanford.edu/entries/autonomy-moral/> (last accessed on 2016-05-17).

430 Dworkin, above n. 412, at p. 32.

the good life'.⁴³¹ What both have in common is the fact that they view autonomy as an essential element, the existence of which is beneficial from the individual's perspective. In addition, according to Dworkin, it is deemed a prerequisite for defining the self:

Our idea of who we are, of our self-identity, is linked to our ability to find and refine ourselves. The exercise of the capacity of autonomy is what makes my life mine. And, if I am to recognize others as equal persons, there is a requirement that I give weight to the way they define and value the world in deciding how I should act.⁴³²

Autonomy therefore involves, first, an ability to change one's self, or according to Dworkin, 'refine ourselves'. In this regard, modern technologies and especially the internet have a tendency not to allow people to change or re-define themselves, for example, by the inability to erase information once uploaded. In addition, technology opposes this re-definition of the self. Predictive modelling is reliant on, but also contributes to, the categorizations of persons, making it difficult to shed a label due to the lack of insight into and control over the categorization process. In addition, the above also suggests that the notion of autonomy is not absolute. There are limitations, which are established by taking into account that others too have a desire for autonomy, which should be respected. This results in the notion of autonomy that is restricted in relation to other peoples' autonomy. It can also be limited by other factors, for example, in its relation with other concepts such as privacy, power and liberty. Dworkin states that these latter notions are not on a par with autonomy, yet are a necessary precondition for its existence.⁴³³

There are two ways to evaluate why something is to be considered good, according to Dworkin, referring to the 'instrumental value' and the 'intrinsic value'. According to the instrumental value outlook, something is good because it leads to something else that is good, whereas according to the intrinsic value outlook, something is to be considered good in itself. Dworkin argues that autonomy possesses both these values, asserting that a person's life will be more satisfying if he or she is able to shape it, as opposed to others doing the shaping, adding that the act of shaping and determining for oneself is in

431 Raz, above n. 413, at p. 408.

432 Dworkin, above n. 412, at p. 111.

433 Ibid, at p. 108.

itself satisfying to the individual. As far as the intrinsic value of autonomy is concerned, Dworkin suggests that our self-respect is linked to the respect we gain from others but also that there are certain values, such as risk-taking, creativity, responsibility and adherence to principle, that are dependent on the existence of autonomy. He states that, '[i]n general, autonomy is linked to activity, to making rather than being, to those higher forms of consciousness that are distinctive of human potential'.⁴³⁴ There is a good in autonomy that is derived due to the fact that it leads to other desired consequences, and intrinsically, there is also a value in being able to decide things for oneself. Here, it can be argued that even if the risks associated with a person's independent choice are higher, as opposed to another entity making the choice on behalf of that individual, there is an inherent value in letting the individual make the decision, even if the end result is negative from his or her perspective. In addition, there is a certain value to be associated with activity, that is, with the ability to move to action. Autonomy, it is argued, is a pre-condition for action. Without it, the individual lacks the ability to act freely, the alternative being a passive individual susceptible to manipulation.

An ever-present threat to autonomy is manipulation, clouding a person's ability to reflect critically. Cohen states that:

'Autonomy' connotes an essential independence of critical faculty and imperviousness to influence. But to the extent that information shapes behaviour, autonomy is radically contingent upon environment and circumstance. The only tenable resolution – if 'autonomy' is not to degenerate into the simple, stimulus–response behaviour sought by direct marketers – is to underdetermine the environment. Autonomy in a contingent world requires a zone of relative insulation from outside scrutiny and interference – a field of operation within which to engage in the conscious construction of self ... [w]e do not experiment only with beliefs and associations, but also with every other conceivable type of taste and behaviour that expresses and defines self.⁴³⁵

Autonomy can be studied from various perspectives. The following sections illustrate the value of autonomy from the perspectives of democracy, the law and technology.

434 Ibid, at p. 112.

435 Cohen, *Examined Lives*, above n. 372, at pp. 1424-1425.

3.4.2.3 Autonomy and Democracy

It is argued that human autonomic capabilities are an essential aspect of any democratic society. In this regard it is suggested that privacy derives its importance from the fact that it is the instrument that ensures the protection and existence of this autonomy, which is necessary for sustaining the democratic society.⁴³⁶ Autonomy is also perceived as a core value in any democratic state in that everyone should be treated as the best judge of his or her own interests. This is so, first, as they are in the best position to know what is best for themselves and second, that they have an interest in self-determination, which is closely linked to self-development due to the fact that one is required to make one's own decision and also be responsible for the outcomes of these decisions.⁴³⁷

Also, there is a common good in preserving autonomy. This becomes most apparent when viewing it as an essential element of a democratic society. Klang referring to autonomy in the context of democracy, states that internet censorship can affect individual autonomy as a person does not have access to the facts and as a result is manipulated, the consequence being that he or she cannot make an autonomous decision.⁴³⁸ Here we see the connection between concepts such as autonomy, democracy and manipulation. Cohen too states that, '[t]he cornerstone of a democratic society is informed and deliberate self-governance'.⁴³⁹ It is in this context that autonomy possibly takes on a notion closest to its natural language meaning, namely, to govern oneself or make one's own laws. Cohen points out that close scrutiny by outside forces stifles an individual's desire or daring to experiment. This experimentation sometimes occurs with ideas that are not considered mainstream or sometimes with incomplete ideas, where an awareness on the part of the individual that his or her every move is being monitored, can diminish this experimentation. The point made by Cohen, is not that experimentation will cease to exist in its

436 Rouvroy, Antoinette and Poullet, Yves, *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy* in Gutwirth, S., et al. (eds.), *Reinventing Data Protection*, Springer Science and Business Media, 2009, at p. 46.

437 Dahl, *On Democracy*, New Haven, Yale University Press, cited in Klang, above n. 300, at p. 185.

438 Klang, above n. 300, at p. 203.

439 Cohen, *Examined Lives*, above n. 372, at p. 1426.

entirety in the face of constant surveillance, but rather that self-government is required in order to prevent what she refers to as ‘precautionary conformism’.⁴⁴⁰

Reference was made above to the fact that an element ensuring autonomy is communication, this notion including the ability to both receive but also disseminate communications. Following from this, it is noteworthy that in the commercial setting, some of the companies that restrict autonomy by means of employing predictive modelling techniques are the very same companies that control the access to information. In this regard, special reference is made to search engines that determine access to information on the internet. For example, when Google entered the Chinese market under Google.cn it agreed to block certain content from Chinese users.⁴⁴¹ By removing links to information, the information essentially disappears as far as the individual is concerned, thereby depriving him or her of the ability to make an autonomous decision. The individual is manipulated by not receiving access to all the facts, affecting autonomy and democracy.⁴⁴²

Not only does the ability to access information disappear, but so too does the ability to voice one’s opinions, as any reference to dissenting views are removed. An argument is that if one is unaware that censorship is being carried out, one cannot attempt to circumvent these censorship ‘rules’.⁴⁴³ In this regard, it has become popular for companies to publish ‘transparency reports’. For example, Google makes public instances where content has been removed after official requests by states or content holders.⁴⁴⁴ While access to the actual content is not available, knowledge is provided as to the fact that censorship

440 Ibid, at p. 1427.

441 Klang, above n. 300, at p. 198.

442 The intersection between democracy and manipulation is illustrated by the technological methods used by the company Cambridge Analytica, contracted by the Donald Trump campaign in the 2017 presidential elections. The main method used to engage the electorate was by means of first examining their individual digital footprints in the digital environment, Cambridge Analytica allegedly having acquired data on 220 million americans. With this knowledge as well as considering the possibility to tailor a person’s interaction with the digital environment, a political message could be formed in a manner tha best catered to a person’s outlook as far as the issues at hand were concerned. See Grauers, Karl, *Gigantisk database hjälpte Trump vinna*, Dagens Etc, 16 December 2016, at p. 10.

443 Ibid, at p. 199.

444 Google, *Transparency Report*, available at <https://www.google.com/transparencyreport/> (last accessed on 2016-05-23).

has occurred and the user can seek other means to attempt to gain access to the required information. Here an analogy can be drawn to the example of Apartheid South Africa, where paper-based newspapers that had articles censored by the state censor elected to retain blank spaces where an article would have been placed as a means of indicating that censorship had taken place.⁴⁴⁵

As mentioned, internet service providers (ISP's) also have the ability to decide what content individuals have access to. For example, the Swedish telecommunications operator Telia recently decided to provide its customers free access to content on Facebook.⁴⁴⁶ Arguably contradicting the notion of net neutrality, it highlights the fact that private companies, controlling the internet infrastructure, have the capacity to control users' access to content and therefore the facts, which in turn can harm autonomy and also democracy.

3.4.2.4 Autonomy and the Law

Autonomy is also a concept that is entrenched in law. Autonomy may take a procedural form, for example, a lawyer's relationship with his or her client, or it may take a substantive form, for example, a law addressing autonomy through the notion of consent. Therefore, a central objective of the law is the protection of autonomy.⁴⁴⁷

Arguably, autonomy finds reference in the law in various forms. One example is where a person under a certain age is considered ineligible to enter into a contract, not deemed to have the legal capacity to do so. This is an illustration where the law does not recognize minors as having the autonomy to enter into a contract. Another example is the availability of certain defences that can be raised in order to negate the existence of a contract. For example, a defence according to section 28 of the Swedish Contracts Act is that of extreme duress.⁴⁴⁸ A party to a contract can plead the invalidity of a contract in

445 Parks, Michael, *Blank Spaces in S. Africa Papers Protest Censorship*, Los Angeles Times, available at http://articles.latimes.com/1986-06-18/news/mn-11057_1_winnie-mandela (last accessed on 2016-08-23).

446 Clover, Julian, *Telia-Facebook Move Sparks Swedish Net Neutrality Row*, Broadband TV News, available at <http://www.broadbandtvnews.com/2016/05/03/telia-facebook-move-sparks-swedish-net-neutrality-row/> (last accessed on 2016-05-23).

447 Sellers, Mortimer (ed.), *Autonomy in the Law*, Springer, 2008, at p. 1.

448 Lag (15:218) om avtal och andra rättshandlingar på förmögenhetsrättens område.

cases where he or she was under extreme duress, for example where he or she entered into a contract under the threat of violence, an explanation being that the person is seen to lack autonomy in the circumstances, in turn reflecting the non-existence of the coinciding wills of the contracting parties.

From the American perspective, autonomy is closely associated with liberty, which address the right not to be interfered with, be it by the state or by other individuals. If a strict definition of autonomy entails that an individual can do whatever he or she desires, then it is liberty that provides the constraints on autonomy in that it cannot be exercised to the extent that it interferes with another person's liberty. Therefore, in the American legal system, it is via liberty that the law protects autonomy, be it the autonomy of individuals, groups or states, from unwarranted intrusion by other entities.⁴⁴⁹

In certain health sector instances, the law is specifically required to determine at what point a person may retain or lose his or her autonomy. For example, at what point can a patient be forced to undergo a certain medical procedure against his or her will? This question takes on an even greater relevance within the realm of psychiatric care, where the law takes on a decisive role in determining the circumstances under which a patient can be forced to undergo involuntary psychiatric care with reference not only to his or her own best interests but also in relation to the best interests of society, where the law attempts to clarify the patient's legal status with respect to making decisions.⁴⁵⁰

3.4.2.5 Autonomy and Technology

Autonomy is referred to in the context of technological development. Writing on the philosophy of technology, Ellul argues that technology itself is 'autonomous':

449 Sellers, above n. 447, at p. 2.

450 For an in-depth investigation on this topic, reference is made to the PhD thesis of Dahlin, Moa Kindström, *Psykiatrirätt: Intressen, rättigheter och principer*, Jure, 2014 at p. 353 (This thesis is in Swedish with the English summary at p. 353).

This means that technology ultimately depends only on itself, it maps its own route, it is a prime and not a secondary factor, it must be regarded as an 'organism' tending towards closure and self-determination: it is an end in itself. Autonomy is the very condition of technological development.⁴⁵¹

This autonomy of technology exists in relation to other concepts, namely the political establishment, ethics and legitimacy.⁴⁵² First, technology is autonomous in relation to the state, or put another way, the political establishment. Ellul argues that the traditional legislative mechanisms do not exert meaningful control over technology and that it is invariably a technician that decides how a certain technology will be designed and what functionality it will possess. He argues against the popular and traditional view of the relationship between technology and law, where the assumption is that, 'the state decides, technology obeys' and that we 'have to ask who in the state intervenes, and how the state intervenes, that is, how a decision is reached and by whom in reality not in the idealist vision'.⁴⁵³ Technology is autonomous in relation to ethics in that it disregards moral ideal, being perceived as neutral and objective, the result being that people are reluctant to question it, with technology bearing the characteristic that it is not prepared to be halted by moral considerations.⁴⁵⁴ This neutrality, argues Ellul, allows unhindered progress, with only its application (not its existence) being questioned in relation to normative ideals and where the technician is able to argue that 'his research, quite simply is'.⁴⁵⁵ Finally, technology's autonomy is acquired from its association with the legitimacy of scientific progress in general.⁴⁵⁶ In other words, technology's legitimacy is gained from the perception that it is scientific and objective. It is in relation to this legitimacy that Ellul states:

Hitherto, man has always tried to refer his actions to a superior value, which both judged and underpinned his actions, his enterprises. But this situation is

451 Ellul, Jacques, *The 'autonomy' of the technological phenomenon*, 2003, in Scharff, RC and Dusek V., (eds), *Philosophy of Technology: The Technological Condition*, Malden, Blackwell Publishing Ltd, at p. 386.

452 Ibid.

453 Ibid, at p. 388.

454 Ibid, at p. 394.

455 Ibid.

456 Ibid, at p. 395.

vanishing for the sake of technology. Man in our society both discerns this autonomy demanded by the system (which can progress only if autonomous) and grants this system autonomy by accepting it as legitimate in itself ... It is man who, becoming a true believer in, and supporter of, technology, views it as a supreme object. For it must be supreme if it bears its legitimacy in itself and needs nothing to justify it!⁴⁵⁷

Gertz, picking up from this, draws the conclusion that human beings believe that they are in control over technology while in actual fact it is the opposite. Consequently, describing Ellul's stance as an examination of the efficiency of technology, Gertz states that while technology was intended to become more efficient for human demands, humans have instead become more efficient for the sake of the demands of technology, with humans conforming to a technology-centric world instead of vice versa.⁴⁵⁸

3.4.3 Concluding Remarks

The systems architect affects autonomy in that it is the system code that determines what a user can or cannot do and what content a person has access to. This in turn affects autonomy. This line of argument can be illustrated by reference to information retrieval systems, where the systems architect determines the extent of 'recall' and 'precision'. If one has a system and knows how many relevant documents the system contains, then one can calculate the number of relevant documents found and retrieved by an algorithm. Recall is the ratio between the number of retrieved documents and the number of relevant documents, and precision is the ratio between the number of relevant documents and the number of non-relevant documents.⁴⁵⁹ The point here is that all systems are built with certain pre-conceived purposes and constraints, with the digital environment, just like any physical environment, either intentionally or unintentionally, influencing action.

457 Ibid.

458 Gertz, Nolen, *Autonomy online: Jacques Ellul and the Facebook emotional manipulation study*, Research Ethics, Vol. 12, Issue 1, pp. 55-61, at p. 56.

459 Karlgren, Jussi, *Legal Information Retrieval*, in Magnusson-Sjöberg, Cecilia, (ed.), *Legal Management of Information Systems: Incorporating Law in e-solutions*, Studentlitteratur, 2005, at p. 300.

The above illustrates the phenomenon referred to by Pariser as the ‘Filter Bubble’. Put briefly, it describes the situation where users of a digital system, oblivious to its manipulative capabilities, are prone to such manipulation to the extent that the digital system inhibits their view of the world. Pariser highlighted this phenomenon by describing his own personal experiences, where he noticed that Facebook had scrubbed his feed of material of a conservative nature. He had clicked more extensively on the links of his liberal friends, which resulted in Facebook taking the decision to edit out his more conservative feeds.⁴⁶⁰ The commercial rationale for this is the idea that showing a client only that content which corresponds to his or her ideals or view of the world will encourage the client to remain a client.

Within the context of autonomy and technology, reference is also made to the ‘autonomy trap’. This term is used by both Zarsky and Schwartz, albeit in slightly different contexts. Zarsky refers to the autonomy trap in the context of profiles and the knowledge they provide. A person, having no knowledge of the existence of his or her profile, the knowledge that it represents and its application as a proxy, may be manipulated in a manner that would not have taken place were it not for the knowledge gained from the profile. Thus the existence of the profile circumvents individual autonomy.⁴⁶¹ The autonomy trap is also used by Schwartz in relation to privacy protection, more particularly his criticism of privacy control. Privacy control was advocated by Westin, who argued that privacy required, ‘individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others’.⁴⁶² In other words, it was up to the individual to decide for him or herself which facts were parted with and under what circumstances this was to take place. Schwartz refers to a number of problems with this control approach, the one highlighted here being what he refers to as the ‘autonomy trap’. A core notion of the control theory is that the individual has a certain amount of freedom to decide for him or herself as to whether personal data should be parted with or kept private. Schwartz argues that this notion of freedom underlying privacy control theory does not exist for the simple reason that in the information age, individual self-determination itself

460 Pariser, Eli, *Beware Online “Filter Bubbles”*, TED, 2011, available at https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles/transcript (last accessed on 2016-05-12).

461 Zarsky, above n. 225, at p. 6.

462 Westin, Alan F., *Privacy and Freedom*, Athenum, 1967, at p. 7.

is shaped by the processing of personal data, stating that, ‘the autonomy trap ignores the extent to which the use of personal data helps set the terms under which we participate in social and political life and the meaning that we attribute to information-control’.⁴⁶³ It is a ‘lock-in’ of personal choice, argues Schwartz, stating that this ‘glorification of freedom of action neglects the actual conditions of choice’.⁴⁶⁴ In other words, technology creates the impression that individuals retain a certain degree of autonomy and freedom to act, while in reality, this is limited. Lessig highlights a similar theme where human interaction with an information system results in a spiral of influence. A person interacts with a computer, and receives a response, upon which response a new decision is taken, the result being a continued spiral of reliance by individuals on the system. He describes this cycle by stating that, ‘the system watches what you do; it fits you into a pattern; the pattern is then fed back to you in the form of options set by the pattern; the options reinforce the pattern; the cycle begins again’.⁴⁶⁵

Technical developments that have altered interaction with the media have also resulted in a filter bubble. Negroponte refers to ‘The Daily Me’, identifying a trend within the media where newspapers are being specifically tailored to each individual’s particular tastes:

That’s because there’s pretty good evidence that we generally don’t truly want good information — but rather information that confirms our prejudices. We may believe intellectually in the clash of opinions, but in practice we like to embed ourselves in the reassuring womb of an echo chamber.⁴⁶⁶

These personalized services have also been described as, ‘[a] service that passively delivers and recommends prioritized breaking and timeless content to the user based on their ever changing interests and social graph’.⁴⁶⁷ Humans are drawn to people and ideas that reinforce their own ideas, thoughts and

463 Schwartz, Paul, M., *Privacy and Democracy in Cyberspace*, above n. 402, at p. 1661.

464 Ibid, at p. 1163.

465 Lessig, above n. 53, at p. 220.

466 Kristof, Nicholas, *The Daily Me*, New York Times, available at http://www.ny-times.com/2009/03/19/opinion/19kristof.html?_r=0 (last accessed on 2016-01-21).

467 Schlicht, Matt, *How the Personalized Newspaper Can Save Journalism*, Business Insider, available at <http://www.businessinsider.com/how-to-save-journalism-with-personalization-2011-3?IR=T> (last accessed on 2015-05-20).

principles, shying away from opposing opinions. The advent of modern technology – from the paper newspaper to the digital version of that newspaper – creates the ability of those who control content to tailor it specifically to every reader. In other words, in theory, every single reader of an on-line newspaper could receive a different version of that newspaper, with the version received more in line with that person’s morals, ideas, convictions, thoughts and outlook on life.

Another issue is that of altered human behaviour. Hildebrandt indicates that the concern is not that machines will start to learn but rather that humans will start to think like machines.⁴⁶⁸ The argument is that an awareness of constant surveillance and accompanying treatment results in human beings altering their actions in the hope that this will cause their digital image to be a favourable portrayal of their personality. Once again the argumentation of both Ellul and Gertz is echoed here, where the autonomy of human beings is shrinking in that human action is being altered for the sake of and to fit in with the architecture and functioning of machines.

Also, a relevant philosophical consideration here is whether more choice is preferable for individuals, if autonomy is associated with the freedom of choice. For example, being presented with a choice between two versions of a product, when in actual fact there are ten versions of that product available, influences that person’s autonomy as the freedom to choose and decide for him or herself is diminished. Dworkin is a proponent of greater choice for the inherent value in choice itself, where the greater the choice, the greater the chance of satisfying one’s desires.⁴⁶⁹ This is portrayed only as a rule of thumb by Dworkin, who states that, ‘... given the relatively bad fit between people’s wishes and the objects of their satisfaction, one is well advised to have a broader rather than narrower range of options’.⁴⁷⁰ Dworkin provides an example of where a greater option allows for a change in taste: in a situation where an individual only likes red t-shirts, the offer of another colour t-shirt is meaningless. However, even here choice is beneficial as a person’s taste may change, in which case, a greater choice is preferable.⁴⁷¹ There are other reasons for preferring greater choice: choice in itself provides satisfaction; practising

468 Hildebrandt, *Slaves to Big Data*, above n. 59, at p. 28.

469 Dworkin, above n. 412, at p. 78.

470 Ibid.

471 Ibid, at p. 79.

making choices is a part of character development and making choices allows a person to discover more about what kind of person he or she is.⁴⁷²

Finally, it is also important to recognize the fact that lots of choice may not necessarily only be beneficial. In this regard reference is made to the work of Schwartz, who argues that the reduction of choice results in less stress and anxiety in addition to the fact that more options leads one to speculate about the alternative that were rejected, thereby leading to dissatisfaction instead.⁴⁷³

3.4.4 Identity

Identity means many different things to different people depending on diverse factors, such as background and culture. It can be expressed in individual terms or in the context of the group, where an individual identifies with the attributes assumed by a group. Identity can differ depending on what perspective and discipline it is studied from, for example, philosophy, psychology, sociology, security studies and the law, to mention but a few. The concept of identity also has a time aspect associated with it and it may change over time. Identity has always been an instrument facilitating an individual's social interactions. Simply put, identity is essential for wellbeing.⁴⁷⁴

The extent to which humans are spending more time in the digital environment, is affecting the notion of identity as well as the social mechanisms for dealing with it. For example, it is becoming more accepted to have multiple identities in the digital environment, something that is challenging to the notion of identity from the legal perspective.⁴⁷⁵ A difference with the digital environment, though, is that only a part of a person's identity may be available in a particular context. These incomplete identities have been referred to as

472 Ibid.

473 Schwartz, Barry, *The Paradox of Choice: Why More is Less*, Ecco Press, 2016, at pp. 99-217. Here Schwartz explores some of the consequences associated with too much choice. Examples are the loss of happiness, the feeling of missed opportunities, the problem of regret, the fact that people make extensive use of comparison and disappointment and depression.

474 Bodstrom, Nick and Sandberg, Anders, *The Future of Identity*, Report Commissioned by the UK's Government Office for Science, 2011, available at <http://www.nick-bodstrom.com/views/identity.pdf> (last accessed on 2017-03-27), at p. 4.

475 Ibid.

‘digital partial identities’, where fragments of the digital identity are dispersed within the digital environment.⁴⁷⁶ The increase in time spent on-line has resulted in identity becoming a tool by means of which people are assessed, especially in the context of the digital village.

Identity is also entwined with the notion of privacy, which is sometimes described in terms of an individual’s ability to decide what information to part with in the presence of others, thereby creating the best circumstances for social interaction. It is this function of identity that the digital profile does not take cognizance of.⁴⁷⁷ It is also in this respect that privacy has been described as, ‘the freedom from unreasonable constraints on the construction of one’s own identity’.⁴⁷⁸

The function of identity was scrutinized in the Future Identities report, which provides a number of conclusions regarding the concept of identity in the digital age: it was referred to as the sum of those characteristics which determine who a person is, including a person’s conception of themselves as similar to, or different from, other people; a person may choose to make public certain aspects of his or her identity or to keep it secret; aspects of an identity may be imposed on a person by others; a person’s identity is central to their values and affects health and well-being, where freedom of expression is important; and on-line, people tend to achieve their ‘true identity’.⁴⁷⁹

One of the most noteworthy observations of the above study was the manner in which people are seamlessly switching between the digital environment and the physical world as the divide between these two spaces diminishes, blurring the lines between private and public, and ceding control by publishing personal information that becomes a permanent record in this sphere.⁴⁸⁰

476 Nabeth, Thierry, *Identity of Identity*, in Rannenberg, Kai, Royer Denis and Deuker André (eds.), *The Future of Identity in the Information Society – Challenges and Opportunities*, Introduction, Springer, 2009, at page 39.

477 Bylund, *Personlig integritet på nätet*, above n. 178, at p. 67.

478 Agre, Philip E. and Rotenberg, Marc, *Technology and Privacy: The New Landscape*, MIT Press, 2001, available at <http://jolt.law.harvard.edu/articles/pdf/v11/11HarvJL-Tech871.pdf> (last accessed on 2017-04-13), at page 7.

479 Foresight, *Future Identities*, above n. 203, at p. 4. The above report refers to the concept ‘true identity’.

480 Ibid.

3.4.4.1 Defining Identity

Identity originates from the Latin ‘idem’, meaning sameness or similarity. A general definition provided is, ‘who someone is: the name of a person ... the qualities, beliefs, etc., that make a particular person or group different from others’.⁴⁸¹ This definition distinguishes between the two distinct approaches to identity, namely, identity as a composition of what attributes a person has (who someone is) and identity as a means of confirming that a person is who he or she says they are. One can refer to the former function of identity as having a ‘structural perspective’, where it is viewed ‘as a representation’.⁴⁸² The second function is that of being able to ascertain that a person is who they say they are, for example, by using an identifier such as a name. This is commonly referred to as the ‘process perspective’, in other words ‘for identification’.⁴⁸³ In the former, identity is seen as a group of attributes that characterize a person while in the latter, identity is seen as a process relating to disclosure of information about a person and the use of this information.⁴⁸⁴ The first concept of identity can be described as certain characteristics associated with an individual so as to determine what sort of person he or she is and what kind of character or personality attributes he or she has. The latter concept can be said to be associated with security and can be described as the need to identify an individual so as to determine who that person is and what he or she is and is not allowed to do within a certain context and for attaching responsibility. Certain technologies may be used to re-inforce the latter definition of identity, for example, identification cards, which in turn may have features that physically connect the human being to the technology, such as biometric information. Identity as a means of establishing a person’s character is emphasised in the context of predictive modelling.

481 Merriam-Webster on-line dictionary, *Identity*, available at <http://www.merriam-webster.com/dictionary/identity> (last accessed on 2015-02-05).

482 Nabeth, above n. 476, at page 36.

483 Ibid.

484 Ibid.

3.4.4.2 Abstract Models of Identity

A number of abstract models illustrate the complexity of identity. They highlight the fact that a person's identity has different spheres or confines, some of which a person may wish to keep private while making others public, a dominant factor being choice regarding which confines to make public and in which contexts.

3.4.4.2.1 *The 'I', the 'Implicit Me' and the 'Explicit Me'*

There are a number of ways of perceiving identity taking the digital environment into account. One study separates the digital identity into three categories, namely, the 'I', the 'Implicit Me' and the 'Explicit Me'. The 'I' refers to the indeterminate first person, the 'Implicit Me' to how a person perceives him or herself, while the 'Explicit Me' refers to how a person is perceived and represented, in other words, the image that a person portrays to his or her environment.⁴⁸⁵ The 'Explicit Me' is particularly interesting in relation to the digital environment, where this aspect of an individual's identity exists in the form of diverse constellations of data. In this regard, reference is made to a theory of identity, where Rost argues that the 'Explicit Me' is made up of a number of 'digital partial identities'.⁴⁸⁶ These are not complete representations, but are rather fragments of a person's complete identity. Nabeth argues that two considerations must be taken into account: first, the 'Explicit Me' in the digital environment is by default imperfect or incorrect as it can never be in line with what a person thinks of him or herself and second, an individual only really controls a small part of his or her own identity, the remainder in essence being controlled by others.⁴⁸⁷

485 Ibid, at p. 39.

486 Ibid.

487 Ibid, at p. 40.

3.4.4.2.2 *Identity as Three Tiers*

In the commercial setting, Durand presents a model called the ‘Three Tiers of Identity’. Tier one is the personal identity, also referred to as the inner and timeless identity, which is the true personal identity that is owned and controlled by the individual. Tier two is the corporate or assigned identity, which is the identity of a person in a particular context and represents a temporary assigned characteristic of a person. Tier three comprises the marketing identity, also referred to as the abstracted or aggregated identity, and refers to the end product of some form of profiling. On this tier, the person is not considered an individual but rather is seen as belonging to a certain category.⁴⁸⁸

In his analysis of this model of identity, Nabeth refers to the concepts of temporality and conditionality. He states that the personal identity is timeless and unconditional, while the corporate identity is temporary, conditional and context-bound, to be considered as attached to a person as opposed to being part of a person as is the case with the personal identity. He furthermore analyses the marketing identity and describes it as an abstraction of an individual with which a person can be identified. Therefore, while being an abstract representation of the individual, it can be used for taking very concrete steps against that individual.⁴⁸⁹

3.4.4.2.3 *Identity and Philosophy*

The concept of identity has also been the focus of research within the discipline of philosophy, with much attention given to the work of Ricoeur, whom in his book entitled *Oneself as Another*, refers to the concept of identity by breaking it down into two distinct, yet related, concepts, namely the ‘ipse-identity’ and the ‘idem-identity’. The ipse-identity refers to selfhood and is the identity of the self, representing who that person really is and which is fluid and not reachable by information and identification technologies. The idem-identity is the identity of a person reduced to a characterization of that person, being a representation of a person as reduced to a more static format

488 Ibid, at pp. 41-42.

489 Ibid.

by information and identification technologies.⁴⁹⁰ There is a distinct relationship between the idem and ipse identities in that while the inner ipse-identity is not in direct contact with a person's environment, it is influenced through contact with the idem-identity, which is in contact with the environment. The concept of 'sameness' is also relevant in that while something may change over time, it has an element of sameness to the extent that it can be identified as the same thing over time.⁴⁹¹

3.4.4.2.4 *Identity and Psychology*

The discipline of psychology has also grappled with the notion of identity. Within Jungian psychology, a person's personality is said to be divided into two parts, the 'anima', which is the inner personality of a person and the 'persona', which is the public personality that is presented to the world, based on physical appearance and behaviour.⁴⁹² According to Jung, the persona is the appearance people present to the world and is important to personal development. The anima as expressed by Jung is seen as the compliment of the persona and is an unconscious structure and includes that psychological material that does not fit in to the individual's conscious self-image.⁴⁹³ This once again reflects a perspective of identity where there is a splitting of the concept of identity into two parts, an inner, personal part and another part that comes into contact with the external environment.

3.4.4.3 **A Common Denominator**

The above abstract theories contain certain similarities, in that they portray identity as something that can be divided into a personal, inner sphere and an

490 Ibid, at p. 37.

491 Ricoeur, Paul, *Oneself As Another*, translated by Blamey K, The University of Chicago Press, 1992, at p. 2.

492 Sofia University, *Transpersonal Pioneers: Carl Jung*, available at <http://www.sofia.edu/about/history/transpersonal-pioneers-carl-jung/> (last accessed on 2015-02-03).

493 Ibid.

external, more outward or publically available sphere.⁴⁹⁴ It is this outer sphere that comes into contact with the external environment, for example in the interaction with friends, family, co-workers and society at large. There may also be multiple outer identities that can be switched between depending on context. The inner identity is that aspect of the personal identity that is not in direct contact with the outside environment. Its development is however dependent on its contact with those parts of the identity that are in contact with the outer environment, and it is in this manner that the outer environment influences identity-building. Consequently, any attempts to influence the outer identity, for example by the use of coercion or manipulation, also influence the inner identity.

The above distinction has a practical dimension, where, for example, in surveillance studies, research has identified instances where an individual's self-perception is not aligned with this same person's social environment. In a study conducted regarding attitudes to speeding, it was found that individuals caught speeding had a different notion of their identity compared to society. The reality was that individuals broke the law by speeding but refused to perceive themselves as 'law-breakers', the 'self-ascribed' identity being one of a normal, respectable and non-criminal driver.⁴⁹⁵ This example illustrates that a certain technology can portray an individual as being a certain type of person, which may not correspond with the self-image.

Predictive modelling technologies attach sameness, for example, where members of a group may have the same characteristics.⁴⁹⁶ These technologies detect sameness in terms of the idem-identity only, the ipse-identity being out of reach. It is this detection of sameness that indirectly influences the identity-building process, in that a person's environment determines the idem-identity, which in turn influences the ipse-identity.⁴⁹⁷

494 Bodstrom and Sandberg refer to the term 'exoself', being that part of a person's identity that will permanently reside in the information and software of the digital environment, in Bodstrom and Sandberg, above n. 474, at p. 4.

495 Wells, Helen and Wills, David, *Individualism and Identity: Resistance to Speed Cameras in the UK*, *Surveillance and Society*, Vol. 6, No. 3, pp. 259-274, at p. 260, available at <http://www.surveillance-and-society.org> (last accessed on 2015-05-25).

496 Hildebrandt, *Profiling and the Identity of the European Citizen*, above n. 282, at p. 313.

497 Ibid.

Hildebrandt, drawing on this model of identity as a relationship between the idem and ipse identities, also refers to Agre and Rotenberg, who refer to privacy as, ‘the freedom from unreasonable constraints on the construction of one’s own identity’.⁴⁹⁸ Hildebrandt examines what she terms the ‘legal persona’ in terms of the ‘freedom to’ (a positive freedom that allows an individual to interact with his or her environment in order to establish identity) and the ‘freedom from’ (which allows the individual to withdraw to a place of solitude, to reflect on issues without having to contend with outside influences).⁴⁹⁹ She contends that it is the freedom of the individual to construct an identity that is the aspect of privacy most threatened by profiling.⁵⁰⁰

3.4.4.4 The ‘Digital Identity’ versus the ‘True Identity’

It is argued that technology and the accompanying hyper-connectivity has blurred the distinction between the digital environment and the physical world. For example, previously when entering the on-line world, a telephone line was accessed via a modem from a stationary desktop computer and it was clear when one was on-line. The boundary between ‘on-line’ and ‘off-line’ worlds is diminishing, however a distinction nevertheless remains between that environment characterised by digital technologies and that which is not.⁵⁰¹ It is under this assumption that one possible understanding of the notion of identity is to distinguish between the ‘digital identity’ and the ‘true identity’.

The notion of identity presents itself at different stages of the predictive modelling process illustrated by Figure 2, referred to in Chapter 2. As early as

498 Agre and Rotenberg, above n. 478, at p. 7, in Hildebrandt, *Profiling and the Identity of the European Citizen*, above n. 282, at p. 312.

499 Hildebrandt, *Profiling and the Identity of the European Citizen*, above n. 283, at p. 303.

500 Ibid.

501 Hildebrandt acknowledges the degree to which the distinction between these two environments has collapsed by referring to the term ‘onlife’. Presentation by Mirielle Hildebrandt, 21 February 2017, at SNS (Centre for Business and Policy Studies), *Hur påverkas den personliga integriteten av Big Data och AI?*. More information about SNS available at <https://www.sns.se/en/about-sns/> (last accessed on 2017-03-24). A podcast is available at <https://www.sns.se/aktuellt/hur-paverkas-den-personliga-integriteten-av-big-data-och-ai/> (last accessed on 2017-03-24) and the slides for this presentation are available at <https://www.sns.se/wp-content/uploads/2017/02/hildebrandt-presentation.pdf> (last accessed on 2017-03-24).

stage one already, there may be partial identities of a person residing in big data. For example, this could be a partial identity in the form of a profile created by a person using a social network site. In addition, an identity of a person may be created at stage three by the predictive model and represented in a certain form at stage four. It is this stage four representation of a person's identity that is referred to as the 'digital identity'.⁵⁰² It is an identity engineered by the 'black box' and based on the sources of data chosen at stage one of the predictive modelling process as correlated by the predictive model.

The digital identity is a proxy identity, in other words an identity that is created by a predictive model and that is imposed on the individual by other entities and by means of accumulating all the data about the individual available digitally. It is created without the consultation of the individual involved and it is the image whose construction is determined by big data and the predictive model. The 'true identity' is the antithesis of the digital identity, even though some similarities may exist. It is the individual's own perceived and subjective identity, in other words, how the individual sees him or herself or alternatively an identity that the individual wishes to portray in certain contexts. It is therefore true from the individual's subjective perspective. It is argued that the true identity is true to the extent that the individual assumes it to be a true reflection of him or herself and that it corresponds with that individual's perception of the prevailing reality. This as opposed to the digital identity, which is, for example, a commercial actor's construction of the individual, constructed by means of a predictive model. The true identity is 'true' also to the extent that it is that identity that an individual wishes to portray to a certain audience in a specific context. Important, however, is that 'true' is not

502 Subsequent to resorting to the term 'digital identity' other references to the notion 'digital identity' have been noted. For example, Bodstrom and Sandberg refer to the concept of a 'digital identity'. They describe it as, 'digital representations of real-world entities that link a number of attributes. For example, a computer user's digital identity links a password, an online name, and ownership of various files in such a way that the user can log in to the system using the password and access the files, other users can send messages to the online name and the computer system can keep track of what activities occur related to the digital identity'. They continue describing this digital identity in relation to the terms 'authentication' and 'identifier'. This use of the term digital identity remains narrower than that used in this thesis and implies the creation of an identity using a digital platform, for example within the social media. The notion of digital identity used in this thesis refers not only to the identity attained from the various systems that allow a person to create an identity in the digital environment, but also includes other data as identified as relevant by the black box, such as knowledge identified via the correlation of data by means of an algorithm. See Bodstrom and Sandberg, above n. 474, at p. 8.

used to contend that the true identity is not made up of lies. An individual, wanting to defraud others, may construct an identity consisting of lies or incorrect data. Even though it is filled with untruths, it is a ‘true’ identity in that it is how the individual wishes to portray him or herself in a specific context, irrespective of whether the intentions are good or bad.

Attempting to classify an individual’s digital identity as applied to that individual by other entities is not new. For example, Clarke coined the term ‘digital persona’ and describes it as, ‘a model of an individual’s public personality based on data and maintained by transactions, and intended for use as a proxy for the individual’.⁵⁰³ There are various ways in which the digital persona can be created. It can be created by the individual him or herself or by other people or organizations, referring also to the ‘projected persona’ over which an individual has some measure of control and the ‘imposed persona’, which is the digital persona as created by another entity and over which the concerned individual has a lower degree of control. It is important to note that the interpretation of the digital persona is in the hands of the interpreter.⁵⁰⁴ Clarke puts forward two additional concepts, namely, the ‘informal digital persona’, which is based on human perceptions and the ‘formal digital persona’, which is based on the collection of structured data.⁵⁰⁵ It is submitted that with the increase in predictive modelling, the usefulness of the formal digital persona will also increase.

Roosendaal distinguishes between the concepts of the ‘digital persona’ on the one hand and the ‘profile’ on the other.⁵⁰⁶ He provides a definition of the digital personae, namely that it is, ‘a digital representation of a real-world individual, which can be connected to the real-world individual and includes a sufficient amount of (relevant) data to serve, within the context and for the purpose of its use, as a proxy for the individual’.⁵⁰⁷

It is argued that the concepts ‘digital persona’, ‘digital dossier’ or ‘data double’, referred to above, describe this external identity in a manner that creates the impression that the image representing the individual is digital and

503 Clarke, *The Digital Persona and its Application to Data Surveillance*, above n. 64.

504 Ibid.

505 Ibid.

506 Roosendaal, Arnold, *Digital Personae and Profiles in Law: Protecting Individual’s Rights in Online Contexts*, Wolf Legal Publishers, 2013, at p. 39.

507 Ibid, at p 41.

made up of data, and is therefore totally correct, objective and true. However, predictive models are designed to create nuanced representations of individuals and are far from objective in nature. The more information the better and the more information about such things as habits and personality, the more beneficial for the accuracy of the predictive model. This in turn highlights the two dimensional nature of the digital identity. It is physical in nature, and can be recorded, stored and even traded, yet it has an extremely subjective side as well, representing very subjective aspects of the individual, including personality traits.

The distinction between the ‘digital identity’ and the ‘true identity’ is best illustrated with the aid of an example. Individual ‘A’, makes use of various identities in his social interactions and in various contexts. In a professional context, he cultivates and promotes his identity as a legal academic (Identity 1). ‘A’, however, is not only a legal academic, he is also a member of a motorcycle club, an identity (Identity 2) that he uses when socializing with his motorcycle club friends. ‘A’ chooses to keep these identities separate, as the fact that he belongs to a motorcycle club may tarnish his reputation as a legal academic and vice versa. Both these identities are true identities as far as ‘A’ is concerned in that they are intentional representations of his character, albeit separated. A commercial actor, using predictive modelling, creates a digital identity (Identity 3) representing ‘A’. It may combine attributes of both Identities 1 and 2 or it may be a totally different identity compared with Identities 1 and 2. The point is that Identity 3 is composed by a third party and attributed to ‘A’ irrespective of its correctness, irrespective of whether ‘A’ likes or dislikes the characterization it makes of him and irrespective of the harms caused to him.

3.4.5 Concluding Remarks

The notion of identity has always had an important function within society. However, this function of identity has become increasingly important with the increased popularity of and reliance on the digital environment. The availability of various technologies associated with the internet and social media have increased the range of tools available to individuals with which to give expression to the various forms of their identity.

It is in this sense that the role of technology has been rather contradictory. The technology that has enabled this ability to find multiple routes for the expression of an individual's many different identities to a large extent incorporates the same technology as that of predictive models. At the same time, predictive models and other 'black box'-type solutions are now reducing the ability for an individual to keep the expression of multiple identities separated. Now that technology has the ability to correlate data and extract knowledge unavailable to humans, the ability for individuals to keep their respective identities apart is diminishing.

The predictive modelling process creates the digital identity. Whereas the interaction between commercial actor and individual previously consisted of a bi-directional relationship, predictive models have become the de facto intermediaries between these parties. Predictive models draw conclusions about individuals, based on data points, the reality being that the digital identity produced may very well not match the individual's true identity. Yet, there is little that the individual can do to influence the composition of his or her digital identity, save for refraining from the use of all digital technologies.

Companies can predict what individuals' want before they know this themselves. This in turn can lead to the individual being manipulated in his or her actions. This ever-narrowing spiral diminishes the individual's view of reality and what may be perceived to be the sum of options may in actual fact only be a sum of options as provided by a commercial actor. The digital identity pinpoints the desires as well as the weaknesses of the consumer. Manzerolle and Smeltzer state:

The belief is that outward behaviour can be turned into datum that, when sufficiently assembled, will embody (as information) the will of the consumer ... data about consumers reflect some reality of their inner selves, providing a window not only into actions, but also motivations, values, predispositions, habits and vulnerabilities. The entire personal data economy is, therefore, premised on the analysis (and manipulation) of these "irrational" motivations, values, and so forth ... identity is held to reflect the essence of an individual; consumer profiles stand-in for, and speak on behalf of, the embodied individual.⁵⁰⁸

508 Manzerolle, Vincent and Smeltzer, Sandra, *Consumer Databases and the Commercial Mediation of Identity: A Medium Theory Analysis*, Surveillance and Society, Vol. 8, No. 3, pp. 323-337, 2011, at pp. 325-326, available at <http://www.surveillance-and-society.org> (last accessed on 2015-05-13).

Lessig refers to the anonymity of consumers as being an essential mechanism in order to maintain ‘equality’ in their relationship with commercial actors. Human mobility provided this anonymity and prevented companies from discriminating between individuals, lacking the necessary information to do so. Technology has now remedied this, but in turn society has lost a benefit of anonymity, namely the benefit of equality.⁵⁰⁹

The digital identity is altering how companies and clients do business. Technology has allowed for the possibility that every person, visiting a web site, could receive a different, specially tailored version of that web site. The traditional manner in which consumers have been said to choose products is by starting with a wide range and variety of products and narrowing down the choice after a selection process based on various factors, this process being referred to as ‘the consumer decision journey’.⁵¹⁰ In response to the availability of technology to compare products and prices, companies have resorted to ‘proactive personalization’, which ‘uses information about a customer—either based on past interactions or collected from external sources—to instantaneously customize the experience. Remembering customer preferences is a basic example of this capability, but it extends to personalizing and optimizing the next steps in a customer’s journey, such as immediately putting a valued traveller on an upgrade list’.⁵¹¹ In addition, the digital identity may be the basis for targeted marketing. Egan, the chief privacy officer at Facebook, remarked that, ‘Facebook serves you ads based on your identity’.⁵¹² It is also noteworthy that the digital identity not only may be used for the purpose of interacting with individuals on-line but also can be used as a form of leverage in the off-line environment, where salespeople can benefit from having the upper hand in terms of knowledge.⁵¹³

509 Lessig, above n. 53, at p. 221.

510 Edelman, David and Singer, Marc, *The new consumer decision journey*, available at <http://www.mckinsey.com/business-functions/marketing-and-sales/our-insights/the-new-consumer-decision-journey> (last accessed on 2016-05-19).

511 Ibid.

512 Valentino-Devries, Jennifer and Singer-Vine, Jeremy, *They Know What You’re Shopping For*, Wall Street Journal, available at <http://online.wsj.com/news/articles/SB10001424127887324784404578143144132736214> (last accessed on 2017-04-12).

513 Ibid.

There are a number of problems concerning the digital identity. First, there is a risk that the data used to construct it has been disconnected from its original context. For example, a bank that collects data about a client or potential client does so within a context. If the bank constructs a digital identity of the client, then the context is the relationship between bank and client/potential client and the transaction that it concerns. As data is transferred from one entity to another, the context is likely to be lost, which can lead to problems in relation to privacy.⁵¹⁴ In this way, digital identities built with non-context data, run the risk of being inaccurate, resulting in a discrepancy between digital identity and true identity. Second, the digital identity is a representation of only a part of an individual's identity.⁵¹⁵ In other words, a person's identity can be complex in nature and it is questionable whether any attempt to fully re-create this identity from data is in fact possible. Finally, the use of digital identities has an effect on the human being it represents. These potential harms are addressed in Chapter 4 below.

3.5 Summary and Conclusions

This chapter introduced a number of theories regarding the notion of surveillance. These theories provided a basis for understanding the reasons why surveillance is resorted to. It also mapped out the progression of surveillance in relation to the development of technology. Consequently, while the Panopticon was confined to the limitations of a physical architecture, for example, the surveillant assemblage recognized the availability of multiple sources of surveillance and also its digital nature. While many of the forms of surveillance discussed referred to the state versus individual relationship, it is argued that all could be related to the commercial setting.

The concepts of 'autonomy' and 'identity' are central when discussing the phenomenon of predictive modelling. This is so with the advent of predictive modelling techniques, where autonomy runs the risk of diminishing to the detriment of human identity. Identity creation is an important human pastime and

514 Bylund, *Personlig integritet på nätet*, above n. 178, at p. 46.

515 Clarke, *The Digital Persona and its Application to Data Surveillance*, above n. 64, at p. 3.

identity itself is a mechanism that has a special function within society in that it provides humans with the ability to switch between different identities in different contexts, arguably a desirable quality associated with privacy. However, as autonomy diminishes in the face of predictive modelling techniques, so too does this function of identity.

Having examined both the technology of predictive modelling as well as the notions of autonomy and identity, and considering the extent to which the technology potentially erodes an individual's personal autonomy, a critical issue to consider is whether there is even a place for personal autonomy in the face of a continuously expanding digital environment. This in turn leads to the questioning of the place of humanity in the digital age. It is with this in mind that the potential harms resulting from predictive modelling are addressed in more detail in the next chapter.

4 Predictive Modelling and the Potential Harms

4.1 Introductory Remarks

This chapter examines the potential harms associated with the use of predictive modelling. Notwithstanding the benefits to individuals and society that predictive modelling confers, there are potential harms that result. The inventory provided here is not intended to be a complete list of all the possible harms, but is presented as an illustration of the potential harms arising from predictive modelling and their nature. Some of these harms can be said to be more recognized in traditional law. By this is meant that the law already refers to them clearly and in a well-defined manner, providing legal remedies. Reputation is one such example, that is protected by the law. In the US, for example, redress is provided either via the legal remedy of privacy or from within the bounds of defamation law, where the torts of libel and slander exist.⁵¹⁶ Other harms resulting from predictive modelling have a weaker connection to the law. For example, the harm of self-censorship is not as established in traditional law. This is a harm that is novel, as technology these days provides the ability for each and every individual to be a publisher, while at the same time technology may lead to greater self-censorship, especially with the rise of technologies such as predictive modelling.

The goal of predictive modelling is to identify human behaviour and ultimately influence it. The potential harms of such a practice are not apparent to the individuals being monitored due to a general lack of awareness of modern digital technologies as well as the characteristics of the digital environment that are conducive to surveillance. Predictive modelling can also be disadvantageous for the companies that use this technology as it may not be their aim to scare off or anger customers and destroy goodwill. It is in this context that

516 Solove, *The Future of Reputation*, above n. 192, at p. 117.

many companies potentially refrain from utilizing the vast depositories of data at their disposal and the power that these bring. Therefore, preventing harm from the utilization of predictive modelling is not only in the interests of individuals, but also in the interests of other entities, like companies and even society.

The following are the potential harms identified as resulting from predictive modelling. It can already be revealed that a common denominator between these potential harms is the notion of autonomy. They all reduce personal autonomy in some fashion and it is the diminishing sphere of autonomy that is the red thread running through them.

4.2 Privacy

There have been many attempts to define privacy, however, no single definition has been able to capture all its nuanced characteristics. The challenge is that privacy means many different things to different people, the words used to describe it differing from one jurisdiction to another. This uncertainty and vagueness is reflected in the various terminologies that attempt to capture privacy's essence. It is probably the degree of difficulty in trying to establish what privacy is that has created the abundance of specialized terminology attempting to describe it. Nevertheless, in order to investigate the consequences of predictive modelling, a working definition is required. In addition, while privacy as a concept is challenging to define, it has become enshrined in the law, more specifically, common law, constitutional law, statutory law and international law.⁵¹⁷ Privacy also operates as an underlying norm in relation to the various European legal frameworks, where the DPD and GDPR have as one of their aims the protection of privacy.

A number of approaches to privacy are addressed below. Investigating privacy through these 'lenses' narrows down the wide field of the study of this abstract notion.

517 Solove, Daniel J. and Schwartz, Paul M., *Information Privacy Law*, Wolters Kluwer, 2011, at p. 39.

4.2.1 Privacy in General

Privacy is a subjective and dynamic concept, its meaning dependent on many factors making up the context that it is studied in. For example, what an individual may find private in a professional context may not necessarily be so amongst friends. These values also potentially change over time. Another example is the manner in which privacy is given a certain meaning within the practice of research, where the norms and principles within that research discipline may influence the manner in which privacy is perceived.⁵¹⁸ The academic perspective it is studied from may also define its boundaries or meaning. There are additional factors as to why privacy is so difficult to define. Seipel provides three reasons for this: first, much depends on the individual's subjective feeling of discomfort and disempowerment, second, many of the notions of privacy depend on the attitude of groups as well as political values and third, legislation must take the form of a framework and pre-empt an interpretation from case to case.⁵¹⁹ Social norms, which have a tendency to change over time, may also affect the notion of privacy. For example, during the 1960's in the US, insurance companies perceived wealthy females to be a higher risk, from an insurance perspective, as the attitude was taken they had a tendency to be more unstable if a romantic relationship went badly and where pregnancy was viewed as a risk.⁵²⁰

Even though privacy may be difficult to define, what is clear is that it is a concept valued by most people, even if expressed in different ways. Many use the fact that some teenagers are relatively open with their private information within the social media as 'proof' that they are no longer interested at all in privacy. However, research has shown that teenagers are interested in privacy, but, they show it in a different way and use different tactics to protect it.⁵²¹

518 Kaye, Jane, *The Tension between Data Sharing and the Protection of Privacy in Genomics Research*, in Mascalcioni, Deborah (ed.), *Ethics, Law and Governance of Biobanking*, The International Library of Ethics, Law and Technology, Vol. 14, Springer, 2015, at p. 102.

519 Seipel, Peter, *Juridik och IT*, Norstedts Juridik, 2001, at p. 251, translated from the Swedish. Furthermore, the term in the Swedish language used to describe privacy is that of 'personlig integritet', translated as 'personal integrity'.

520 Packard, above n. 324, at p. 194.

521 boyd, danah, *Networked Privacy*, *Surveillance and Society*, Vol. 10 No. 3/4, pp. 348-350, at p. 349, available at <http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/networked/networked> (last accessed on 2014-03-24).

The work of boyd and Marwick is interesting in this respect, pointing out that teenagers do not view privacy as binary, that is, in terms of ‘access’ or ‘no access’. Rather, it is the control over how information flows that concerns them, a central notion being that teenagers do not possess the agency to influence the social norm of privacy and a context seen as ‘public’ does not correspond with the notion of making everything accessible to everyone. This confusion has in large part to do with technological advances, such as the development of ‘networked publics’, which are ‘a highly accessible space where wide audiences, have common interests’.⁵²² A public consists of a group of strangers who have a common interest, and provides a space for conversation existing only so long as its members continue to participate in these conversations.⁵²³ Technical platforms such as these have resulted in blurring what was once a clear boundary between the traditional concepts of ‘public’ and ‘private’. This leads the above authors to the claim that in the physical world interactions are ‘private-by-default’ and ‘public-through-effort’, while in the digital environment, the opposite is true.⁵²⁴ Also, the manner in which privacy is viewed is different for so-called ‘digital natives’ as opposed to previous generations, with a shift in the expectation of privacy in an environment where there are fewer checks on imprudent behaviour and the more one reveals, the more friends one makes.⁵²⁵ Important in this context is the extent to which privacy is or should be seen in terms of its value for the individual or if it is rather to be seen in terms of being a societal value. The privacy debate in the US has focussed on the former value.⁵²⁶ The opposite argument is also provided in terms of privacy as a societal need and something that should be strived after for the benefit of society as a whole. Regan focuses on this social aspect:

522 boyd, danah and Marwick, Alice, *Social Privacy in Networked Publics: Teens’ Attitudes, Practices, and Strategies*, Microsoft Research, available at <http://ssrn.com/abstract=1925128> (last accessed on 2014-04-08).

523 Doty, Jeffrey S., *What is a Public?*, available at <http://project.makingpublics.org/research/what-do-you-mean/> (last accessed on 2014-04-08).

524 Boyd and Marwick, above n. 522.

525 Palfrey, John and Gasser, Urs, *Born Digital. Understanding the First Generation of Digital Natives*, Basic Books, 2008, at p. 54.

526 Bygrave, *Privacy Protection in a Global Context*, above n. 69, at p. 334.

Privacy has value beyond its usefulness in helping the individual maintain his or her dignity or develop personal relationships. Most privacy scholars emphasize that the individual is better off if privacy exists; I argue that society is better off as well when privacy exists. I maintain that privacy serves not just the individual interests but a common, public, and collective purpose.⁵²⁷

Traditionally, privacy has been viewed from the perspective of the individual. However, in searching for a fresh and more dynamic solution to the challenge of protecting privacy, it is useful to view privacy from the societal perspective. Lundblad takes up the issue of the divide between individual privacy and what he terms ‘the collective expectation’ of privacy, where he identifies the high expectation of collective privacy and a low expectation of individual privacy.⁵²⁸ The development of privacy described in Chapter 5, highlights the importance given to privacy as an individual attribute and something that the individual should be able to control. However, this notion becomes problematic when viewing privacy as a public good and something that is required for human agency, especially in a democracy.⁵²⁹

4.2.1.1 Traditional Approaches to Conceptualizing Privacy

A traditional approach to privacy is advocated by Seipel, who separates it into a number of theoretical areas. First, the ‘sphere theory’ (‘sfärteorin’) states that an individual has an inner sphere where actions, relationships and other characteristics are not known to others. From the inner sphere there are other spheres with gradually diminishing sensitivity, from which information should be more accessible to the outside world. Second, the ‘data category theory’ (‘datakategoriteorin’) denotes different categories of data with different levels of sensitivity, for example data regarding a person’s address being less sensitive than data concerning political convictions. Third, the ‘theory of ownership’ (‘äganderättsteorin’) views data as the property of the individual,

527 Regan, Priscilla M., *Legislating Privacy: Technology, Social Values, and Public Policy*, University of North Carolina Press, 1995, at p. 221.

528 Lundblad, above n. 61, at p. 351.

529 Hildebrandt, Mirielle, *Profiling into the Future: An Assessment of Profiling Technologies in the Context of Ambient Intelligence*, in Bus, Jacques et al. (eds.), *Digital Enlightenment Yearbook 2012*, IOS Press, 2012, at p. 8.

where consent is required for its use. Fourth, the ‘autonomy theory’ (‘autonomiteorin’) views privacy as the right to be left alone, where the individual can decide under which circumstances and under what conditions to enter into relations with the outside world. Fifth, and finally, the ‘empirical theory’ (‘empiriteorin’) treats privacy as something to be determined statistically, for example, by conducting investigations.⁵³⁰

Another approach to privacy views it as ‘decisional autonomy’.⁵³¹ Within the US context, a case cited to highlight this approach is that of *Griswold v. Connecticut*.⁵³² The case emanated from a law at state level prohibiting the provision of contraceptives to married couples. The US Supreme Court stated that the marital relationship was a special one that should not be intruded or controlled by the state. Here privacy was portrayed as the right to make one’s own decisions in circumstances that are regarded as requiring freedom from the control of others. This can be associated with the definition of privacy as, ‘[...] the interest that individuals have in sustaining a “personal space”, free from the interference from other people and organizations’.⁵³³

In the legal context, the most famous reference to privacy is provided in the article written by Warren and Brandeis entitled ‘The Right to Privacy’. In this article, the authors advocate the introduction of a right to privacy, which they described as the ‘right to be let alone’.⁵³⁴ The article was authored as a response to privacy invasive technological advances at the time, which were part of a new type of journalism. Advances were being made concerning cameras and printing, where cameras, a technology that was previously available only to a core of professional photographers, in 1884 became available to society at large in the form of the Eastman Kodak Company snap camera, which was cheap and mobile.⁵³⁵ In addition to this development, Warren and Brandeis were disturbed by the new trend in journalism, with the printing of gossip and

530 Seipel, *Juridik och IT*, above n. 519, at p. 251, loosely translated from the Swedish by the author.

531 Rouvroy and Pouillet, above n. 436, at p. 64.

532 *Griswold v. Connecticut*, 281 US 479, 493 (1965).

533 Clark, *What’s Privacy?*, above n. 320, at p. 5.

534 Warren, Samuel D. and Brandeis, Louis D., *The Right to Privacy*, Harvard Law Review, Vol. 4, Number 5, December 1890, at p. 195.

535 Solove, Daniel J., *Understanding Privacy*, Harvard University Press, 2008, at p.15.

other material that was seen to be of an indecent and sordid nature at that time. They wrote:

Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the housetops’. For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of the invasion of privacy by the newspapers [...].⁵³⁶

It was within this context that the authors investigated whether the common law could be used in order to establish a right to privacy, called the ‘right to be let alone’. They stated that the right to privacy was part of the right to be let alone, which was first advanced by T. Cooley.⁵³⁷ The argument was that in order to achieve privacy, the access to personal information would need to be controlled.⁵³⁸ This right to privacy advocated by Warren and Brandeis was influential on privacy law in that soon after its publication, courts and legislatures began to recognize this new right.⁵³⁹ Altman, another influential figure concerning privacy conceptualization, described it as a ‘process’ that takes place every time one needs to make a decision between being private or being public, the goal being to reach the optimal balance in a situation where privacy is not determined by one party only.⁵⁴⁰ Bylund, who seemingly favours this approach, highlights the advantages of explaining privacy in terms of a process for creating a balance between the private and public, arguing that the aim of privacy is not secrecy, but rather the ability to decide over one’s presence in a certain context by deciding what information to make public and what information to keep private. In other words, privacy is the freedom for the individual to manoeuvre along the private/public continuum depending on the context (the contextual factors surrounding privacy being just as important

536 Warren and Brandeis, above n. 534, at p. 195.

537 Cooley, Thomas M., *Treatise on the Law of Torts or the Wrongs Which Arise Independently of Contract*, 29 (2nd ed. (1888)) in Gavison, Ruth, *Privacy and the Limits of the Law*, Yale Law Journal, Vol. 89, No. 3, pp. 421-471, 1980, at p. 437.

538 Warren and Brandeis, above n. 534.

539 Solove, *Understanding Privacy*, above n. 535, at p. 16.

540 Altman, Irvin, *The Environment and Social Behavior: Privacy, Personal Space, Territory and Crowding*, Monterey, CA Brooks/Cole Pub. Co., Inc, 1975.

as privacy itself) and to decide which privacy enhancing mechanism is best suited for that particular situation.⁵⁴¹

Westin described privacy as the right to control the flow of personal information. He envisaged privacy as a concept that was relative to the counter-concept of social interaction, where total privacy was possible, but would entail total and absolute isolation, in other words placing oneself at the extreme end of the spectrum.⁵⁴² Bylund criticises this approach in two respects: first, in this day and age of technology reliance, it is not possible to isolate oneself to the degree required in order to achieve privacy and second, social values fluctuate from one context to another, creating difficulties.⁵⁴³

4.2.1.2 Alternative Approaches to Privacy

Two alternative approaches to privacy are provided, namely, the privacy taxonomy of Solove and the notion of ‘contextual integrity’ advocated by Nissenbaum. The former is interesting in that instead of trying to conceptualize privacy in the abstract, it starts with problematic scenarios associated with privacy and seeks common elements linking these, the aim being to attain a meaning or definition of privacy. The second theory, advocated by Nissenbaum, is dominated by the notion of context. Both approaches are therefore context related, which is useful considering that many of the harms associated with predictive modelling are context orientated.

4.2.1.2.1 A Privacy Taxonomy

Solove approaches privacy in a novel and less abstract manner, the main reason being that all conventional attempts to define it in an abstract manner have up until now not led to any success and have merely caused more confusion. He conceptualizes privacy in the following way:

541 Bylund, *Personlig integritet på nätet*, above n. 178, at p. 37.

542 Westin, above n. 462.

543 Bylund, *Personlig integritet på nätet*, above n. 178, at p. 23.

Under my conception, we should understand privacy as a set of protections against a plurality of distinct but related problems. These problems are not related by a common denominator or core element. Instead, each problem has elements in common with others, yet not necessarily the same element – they share family resemblances with each other. We label the whole cluster ‘privacy’, but this term is useful primarily as a shorthand way of describing the cluster. Beyond that, it is more useful to discuss and analyse each type of problem specifically.⁵⁴⁴

By defining privacy in a bottom-up manner and by focusing on the problems that arise, a better understanding of what privacy is can be attained. He thus produces a taxonomy for easier identification of privacy problems, a problem being defined as, ‘a situation that creates harms to individuals and society’.⁵⁴⁵ The taxonomy is composed of four types of problems and sixteen subgroups. The first type of problem is labelled ‘information collection’ (subgroups: surveillance, interrogation), the second type of problem ‘information processing’ (subgroups: aggregation, identification, insecurity, secondary use, exclusion), the third type of problem is labelled ‘information dissemination’ (subgroups: breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, distortion) and the fourth type is labelled ‘invasion’ (subgroups: intrusion, interference).⁵⁴⁶ By highlighting the problems that arise in society, attention is drawn to values that are identified as being in need of protection. A resolution of these problems, as highlighted in the above taxonomy, will automatically result in a ‘realm of freedom we call “privacy”’.⁵⁴⁷

4.2.1.2.2 *Contextual Integrity*

Nissenbaum, in conceptualizing privacy, refers to ‘contextual integrity’. Contexts are stated to be everywhere within society. Visiting a doctor takes place in a context and taking part in some form of education takes place in a different context. These contexts also have norms that govern them, more specifically, the roles, expectations, actions and practices within them and from

544 Solove, *Understanding Privacy*, above n. 535, at p. 171.

545 Ibid, at p. 174.

546 Ibid.

547 Ibid.

which norms originate, for example, legal conventions or cultural attitudes.⁵⁴⁸ To expand on this theory, contexts are described as, ‘structured social settings characterized by canonical activities, roles, relationships, power structures, norms (or rules), and internal values (goals, ends, purposes).⁵⁴⁹ A role can be a lawyer, an activity can be providing a legal service and a value underpins a context. For example, the legal profession has certain values that are inherent and which set out the goals of the profession. And finally norms describe the duties and obligations associated with a certain role. At the core of contextual integrity, Nissenbaum states, is the context-relative informational norm.⁵⁵⁰

Each context has its own informational norms, and these can be characterised in terms of contexts, actors, attributes and transmission principles.⁵⁵¹ She states that, ‘[c]ontext-relative informational norm functions descriptively when they express entrenched expectations governing the flows of personal information, but they are also a key vehicle for elaborating the prescriptive (or normative) component of the framework of contextual integrity’.⁵⁵²

There are two types of informational norms, namely, ‘norms of appropriateness’ and ‘norms of flow or distribution’. If both these norms are followed and upheld, contextual integrity (and therefore privacy) are upheld. Breaching either of these informational norms results in a breach of contextual integrity. A norm of appropriateness dictates what type of information can be revealed about a person and by whom, for that particular context. For example, in the lawyer-client context, the client may be expected to reveal certain types of information to the lawyer, whereas he or she is not expected to share that same information with colleagues over lunch. The second type of informational norm is that of ‘distribution’.⁵⁵³ For example, in the context of a friendship, it can be assumed that one can be candid to a friend without fear of the information being revealed to a third party.

548 Nissenbaum, Helen, *Privacy as Contextual Integrity*, Washington Law Review, 2004, available at <https://crypto.stanford.edu/portia/papers/RevNissenbaumDTP31.pdf> (last accessed on 2016-01-19), at p. 119.

549 Nissenbaum, *Privacy in Context*, above n. 230, at p. 132.

550 Ibid, at p. 129.

551 Ibid, at p. 181.

552 Ibid, at p. 129.

553 Nissenbaum, *Privacy as Contextual Integrity*, above n. 548, at p. 124.

4.2.2 Remarks

There are theories of privacy that can be regarded as ‘traditional’ and those that can be said to be more progressive in nature. Examining both types, it is argued that the more progressive theories may be better equipped to deal with technological developments. For example, Seipel’s reference to categories of data, while remaining an integral component of the forthcoming GDPR, can be criticised from the technical point of view, where the ability of algorithms to correlate all data makes every single data point potentially sensitive. The alternative, more progressive, approaches to privacy are relevant in that they focus on context. For example, the theory of contextual integrity is relevant from the point of view of predictive modelling, which has the potential harm of collapsing contexts and completely disregards the above-mentioned informational norms. This is illustrated by the situation where an individual wishing to have a different identity for different digital contexts may not be able to keep these identities separate in the face of predictive technologies. In this manner, predictive modelling, by not respecting differing contexts as well as informational norms, threatens privacy.

Solove’s taxonomy of privacy and consequential harms is interesting from the predictive modelling perspective as well. Under the heading ‘information processing’, reference is made to the aggregation of information, which is an integral part of predictive modelling. Aggregation occurs where bits of data are compiled in order to create a comprehensive and general picture of a person, that is, the digital identity. Aggregation is harmful as it ‘unsettles expectations’.⁵⁵⁴ It has the effect of finding out information about people that they did not themselves intend to reveal (if they at all knew about it themselves in the first place). A person may have wished to reveal bits and pieces about him or herself in different contexts, however, by aggregating the data a new type of knowledge is attained. Solove, within the context of aggregation, states that ‘a piece of information here or there is not very telling, but when combined, bits and pieces of data begin to form a portrait of a person’.⁵⁵⁵

554 Solove, *Understanding Privacy*, above n. 535, at p. 119.

555 *Ibid.*, at p. 118.

4.3 Reputation

Reputation has long been important to humans. While it has historically been protected in various forms, such as by means of the right to a duel, modern history has seen reputation acquire protection in the law, with civil as well as criminal sanctions awaiting those who taint the reputation of others. Also, the societal function of reputation is changing and in the digital era, the issue of reputation on the internet is gaining attention, especially in the context of the social media.

The word ‘reputation’ means ‘the common opinion that people have about someone or something: the way in which people think of someone or something’.⁵⁵⁶ Alternatively, it is ‘a shared, or collective, perception about a person’.⁵⁵⁷ In other words, it is not something that the individual creates, but rather something that is created by the people associated with the individual and who perceive that individual in a certain manner. The individual may have some influence over the way he or she is portrayed outwardly, resorting to various techniques to improve or alter his or her reputation, however, this control is limited for the most part. It is essentially created by others and can be elevated or tarnished by others. Extended to the digital environment, not only is reputation determined by other people, it may be determined by technology, where algorithms determine a person’s digital identity.

Historically, the concept of reputation has had an important societal function, operating as a measure of trust. In many relationships, both personal and business, with little known about a prospective party, reputation was the main vehicle for determining trust in the absence of other societal mechanisms.⁵⁵⁸ It was for this reason that a person’s dignity, honour and reputation were of vital importance.

Reputation protection has not always been something that just anybody could claim in a court of law. For example, for centuries in Europe, only persons of a certain social stature and belonging to the aristocracy, had access to the courts to enforce their personal honour, this ability slowly filtering down

556 Merriam-Webster, *Reputation*, available at <http://www.merriam-webster.com/dictionary/reputation> (last accessed on 24-01-2014).

557 Nock, Steven L., *The Cost of Privacy: Surveillance and Reputation in America*, Aldine Transaction, 1993, in Solove, above n. 192, at p. 30.

558 Solove, *The Future of Reputation*, above n. 192, at p. 34.

to the masses over time.⁵⁵⁹ In addition, a deeply entrenched method for protecting reputation was by means of the duel, where the rights to reputation protection were only afforded to the duelling classes.⁵⁶⁰ The duel originated in Italy in the 1500's and became a popular mechanism amongst gentlemen of Europe during the 1600's and 1700's, being considered a civilized dispute resolution mechanism as compared with brawls.⁵⁶¹ It has even been argued that the main catalyst of World War I was not the actual assassination of Franz Ferdinand, but rather the notion of taking to arms to protect one's honour, war being a duel between states.⁵⁶² Duelling also found its way to the US and despite making it illegal, the practice continued due to the social pressure of being required to protect one's honour.⁵⁶³ One theory as to why duelling as a mechanism faded, in the US at least, was the increase in commerce and trade, where the aristocratic ideal of honour was replaced by the notion of creditworthiness in the commercial setting.⁵⁶⁴

An aspect that Post advocates is that defamation law, in protecting reputation, presupposes how people are or should be tied together socially. Post sets out three concepts of reputation that the law of defamation protects, namely 'reputation as property', 'reputation as honour' and 'reputation as dignity'. Reputation as property can be compared to goodwill. It entails individuals being connected to each other via the institution of the marketplace. It is within this marketplace that one's reputation has a value and the law seeks to protect reputation by preventing it from being deprived of the correct market value. 'Reputation as honour' is not earned but rather is acquired through a person's standing in society, in other words through the status afforded by a social role. Unlike reputation as property, reputation as honour is in a fixed state. Therefore, in situations where a person's honour has been defamed, the role of the law is to restore this honour. Finally, 'reputation as dignity' relates to the respect that a person is accorded from society and where the individual is accepted as being a part of that society. Society as a whole has rules of civility

559 Solve and Schwartz, *Information Privacy Law*, above n. 517, at p. 1061.

560 Ibid.

561 Solove, *The Future of Reputation*, above n. 192, at p. 114.

562 Danielsen, Andreas, *Hederskriget: hur Österrike-Ungern startade första världskriget*, Atlantis, 2014.

563 Solove, *The Future of Reputation*, above n. 192, at p. 114.

564 Ibid, at p. 116.

that ensure the maintenance of the dignity of society. The law of defamation, in protecting dignity, protects the individual's interest to be included in society while at the same time acting as a tool for society to enforce its rules of civility.⁵⁶⁵

Reputation does not exist in a vacuum and closely connected to the issue of reputation is the notion of norms. A norm can be described as a rule of conduct, which is seen as improper to transgress.⁵⁶⁶ It does not, however, have the same status as an official law and is usually not written down in a code of any type and cannot be extracted from case law. Norms are collectively determined and constrain individuals in a way that is, 'so familiar as to be all but invisible'.⁵⁶⁷ In other words, it is 'those normative constraints imposed not through the organized or centralized actions of a state, but through the many slight and sometimes forceful sanctions that members of a community impose on each other ... deviation from which makes you socially abnormal'.⁵⁶⁸ While breaching a law may lead to an official sanction, the breach of a norm can lead to a form of punishment meted out by the community. Norms are not written down yet they are known by everyone and there seems to be public consensus as to when they are breached. Solove highlights the fact that an individual's reputation is an important asset and that it is created when people make judgements about people with available information, pointing to the inherent irony that reputation is a central element of personal identity yet it is not something that we create.⁵⁶⁹ He writes:

Reputation is a core component of our identity – it reflects who we are and shapes how we interact – yet it is not solely our own creation. Individuals generally require social contact with each other and whom we interact with and how we interact, is to a large degree shaped by the way in which we are outwardly portrayed ... our freedom, in short, depends in part about how others in society judge us.⁵⁷⁰

565 Post, Robert C., *The Social Foundations of Defamation Law: Reputation and the Constitution*, 74 California Law Review, 691, 1986, at pp. 691-742.

566 Solove, *The Future of Reputation*, above n. 192, at p. 84.

567 Lessig, above n. 53, at p. 11.

568 Ibid, at p. 340.

569 Solove, *The Future of Reputation*, above n. 192, at p. 33.

570 Ibid, at p. 33.

In addition to being a mechanism of trust, reputation can also be used as a mechanism of social control. The threat of destroying a person's reputation can be used as leverage in order to ensure that a person remains trustworthy, as the tarnishing of the reputation can have potentially catastrophic effects.⁵⁷¹

4.3.1 Reputation and the Law

The crime of harming someone's reputation dates back to Roman law, where the crime of *libellis famosus* existed, with the punishment of death a possible consequence.⁵⁷² Protecting reputation occurs on both a constitutional law level as well as by means of statutory instruments. An example of the former is the United Nations Declaration of Human Rights, where, Article 12 states that no-one shall be subject, 'to attacks upon his honour or reputation'.⁵⁷³ Article 10 ECHR establishes the right to the freedom of expression (Article 10(1)) yet places a limitation on this right, 'for the protection of the reputation or the rights of others', being one such restriction (Article 10(2)).⁵⁷⁴ It has even been acknowledged that reputation is something that is starting to be included under Article 8 ECHR, the ECtHR stating that, '[q]uite tentatively, the Court seems lately to be moving towards the notion that "reputation" could well be an issue under Article 8'.⁵⁷⁵ It can therefore be argued that ECtHR recognizes Article 8 of the ECHR to include a right to reputation.⁵⁷⁶

571 Ibid.

572 International Press Institute and Media Legal Defence Institute, *Freedom of Expression, Media Law and Defamation*, available at http://www.freemedia.at/fileadmin/user_upload/FoE_MediaLaw_Defamation_ENG.pdf (last accessed on 2016-01-22), at p. 17.

573 UN General Assembly, *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III), available at, <http://www.refworld.org/docid/3ae6b3712c.html> (last accessed on 2016-01-22).

574 Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5, available at, <http://www.refworld.org/docid/3ae6b3b04.html> (last accessed on 2016-01-22).

575 *Rotaru v. Romania*, (App. No. 28341/95) (unreported), 4 May, 2000, para. 13.

576 International Press Institute and Media Legal Defence Institute, above n. 572, at p. 17.

4.3.2 Reputation in the Era of the Internet

Reputation has acquired a new function as individuals have started to spend more time in the digital environment. The term ‘NetRep’ (short for ‘internet reputation’) is mentioned in a report by the Australian Law Reform Commission.⁵⁷⁷ The term appeared in research commissioned by Viadeo⁵⁷⁸ and which was performed by YouGov.⁵⁷⁹ The study primarily examined the extent to which potential employers used the internet, and more specifically the social media, to do background checks on prospective employees as well as the extent to which potential employees used the internet to portray a better image of themselves. The research showed that an increasing number of young adults, mainly in the age group eighteen to twenty four, were posting personal information on social network sites and that, ‘all of this is contributing to our personal online brand – our very own “Netrep”’.⁵⁸⁰ Interesting was that this information was being published by others, such as friends, family and acquaintances and that it was in fact others that were contributing to the individual’s ‘Netrep’.⁵⁸¹

The increase in the importance of a person’s reputation on the internet is supported by the availability of social media sites dedicated to determining the status of one’s reputation. PeekYou considers itself a search engine for the

577 Australian Law Reform Commission, *For Your Information, Australian Privacy Law and Practice (ALCR Report 108)*, at <http://www.alrc.gov.au/publications/your-information-australian-privacy-law-and-practice-alrc-report-108/terms-reference>, Chapter 67, *Children, Young People and Attitudes Towards Privacy*, available at <http://www.alrc.gov.au/publications/67.%20Children%2C%20Young%20People%20and%20%20Attitudes%20to%20Privacy/online-social-networking>, (last accessed on 2017-04-14).

578 Viadeo described itself as a business social network, which can be used to find suppliers, clients and business partners. It is part of The Viadeo Group, available at <http://corporate.viadeo.com/en/> (last accessed on 2017-03-05).

579 Yougov is an international market research company, available at <https://yougov.com/>, *What Does Your NetRep Say About You? A Study of How Your Internet Reputation Can Influence Your Career Prospects*, commissioned by Viadeo, Spring, 2007, available at <http://corporate.viadeo.com/wp-content/uploads/media/pdf/2007/en/2007-03-28%20-%20recruiter%20say%20no.pdf> (last accessed on 2014-01-28).

580 Ibid.

581 Ibid.

purpose of finding individuals on the internet and does this by means of associating URL's with individuals.⁵⁸² A by-product of PeekYou is called 'Peekscore', which is the process by which individuals are ranked on a scale from one to ten, depending on their presence or importance on the internet.⁵⁸³ An individual feeling that he or she does not have a suitable ranking can increase it by being more visible in blogs, on Twitter and other social media. Klout is a social media site based company using analytical tools to determine how much influence an individual exerts on the internet.⁵⁸⁴ It provides a score of one to one hundred, with forty being the average. It also measures an individual's influence within the social media, where what is important is not the number of connections, but rather the ability to engage people, where the Klout score is the aggregation of various pieces of data acquired from your activity within the social media.⁵⁸⁵ What both these services have in common is that they rank an individual's influence on the internet by analysing data associated with that individual's reputation.

PeekScore and Klout suggest ways to increase one's ranking. These programmes build this functionality into the application that makes the judgement about the individual. In the discourse of Lessig, the code of the applications allows the individual to influence the end result.⁵⁸⁶ The extent to which this is possible depends on the code, its developers and most importantly on the developer's goals.

Another tendency that has become possible in the digital environment is to judge a person's reputation via his or her 'friends' reputation. In August 2015, Facebook applied for and was granted a patent, described in the patent application, as follows:

582 Peekyou, available at <http://www.peekyou.com/> (last accessed on 2017-02-07).

583 Material originally accessed at <http://score.peekyou.com/> (accessed on 2013-08-03). This link is no longer active. An alternative source is PR Web, *PeekYou Launches First Digital Footprint Ranking System for Individuals; PeekScore Gauges One's Relevance and Reach on the Web*, available at <http://www.prweb.com/releases/peekyou/peekscore/prweb4148084.htm> (last accessed on 2017-02-07).

584 Klout, available at <https://klout.com/home> (last accessed on 2017-02-07).

585 Wired, *What your Klout Score Really Means*, available at https://www.wired.com/2012/04/ff_klout/ (last accessed on 2017-02-07).

586 Lessig, above n. 53, at p. 5.

When an individual applies for a loan, the lender examines the credit ratings of members of the individual's social network who are connected to the individual [...]. If the average credit rating of these members is at least a minimum credit score, the lender continues to process the loan application. Otherwise, the loan application is rejected.⁵⁸⁷

Here the issue of reputation slips even further away from the individual's control and it is no longer the individual's own circumstances that determine his or her own economic reputation. Rather, it is dependent on the economic stability of his or her friends. One could go so far as to say that an individual's credit worthiness has almost nothing to do with his or her financial situation and has everything to do with how an algorithm interprets the credit worthiness of his or her friends within the social media. Novel to the issue of reputation in the digital environment is the fact that a person's friends are a reflection of that person. The dangers with this are apparent. It may very well lead to a situation where a person does not dare to accept friends for fear that they may tarnish his or her credit worthiness and as a consequence his or her reputation. This is an example of Lessig's reference to the phrase, 'subtle distinctions of rank', where the digital environment allows for the creation of a class structure.⁵⁸⁸ The following examples illustrate the importance of reputation in the context of technology.

4.3.2.1 Netflix

Netflix is a commercial actor that provides for the streaming of on-demand content via the internet.⁵⁸⁹ Netflix's algorithm monitors an account holder's viewership of content and based on this makes recommendations to the account holder. In other words, the Netflix predictive software, using algorithms to process historical data, predicts what the account holder will want to watch based on what he or she has already watched. When logging on to Netflix, an

587 Meyer, Robinson, *Could a Bank Deny Your Loan Based on Your Facebook Friends?*, The Atlantic, September 25th, 2015, available at <http://www.theatlantic.com/technology/archive/2015/09/facebooks-new-patent-and-digital-redlining/407287/> (last accessed on 2015-11-30).

588 Lessig, above n. 53, at p. 221.

589 Netflix, available at <https://signup.netflix.com/> (last accessed on 2013-11-25).

account holder sees is his or her ‘top ten recommendation list’.⁵⁹⁰ By default this list reflects the predictions for the ‘household’, however, it is possible for each family member to create a separate profile, thereby enabling Netflix to make individual predictions.

There are a number of reasons why this situation is undesirable. First, the viewer may be aware that Netflix is monitoring his or her movie selection, which in itself could be viewed as an undesirable form of surveillance, leading to self-censorship. Second, by compiling a recommendation list based on a specified individual’s past choice of movies, Netflix is making a statement about that individual, which could potentially affect his or her reputation in circumstances where ‘others’ may have the opportunity to see this recommendation list, be it another member of that household or acquaintances who are present when Netflix is accessed. What is important here is that the recommendation list says something about a person, be it sexual orientation or political affiliation. It puts a label on a person and potentially brands him or her in an undesirable light, thus damaging reputation.

4.3.2.2 You Are What You Drive

Another example of technology utilized to gauge a person has been used in shopping centre parking garages. When a car drives into the parking garage, a sensor determined what kind of car it was and the age of the car. Thereafter, the digital screen in front of the car displays an advertisement directed at the occupants of that car. A new, modern and expensive car could result in an advertisement for luxury items that could be purchased at the shopping centre, while an older car, which was not in such great shape, received an advertisement for cheaper items at the shopping centre.⁵⁹¹ The technology has since been updated so that a camera identifies a car’s registration number and based on that data, together with information on the postal code of the area that the car is registered in, an advertisement is flashed on the digital display in front of the car. The company responsible for the application has stated that the

590 The Netflix Tech Blog, <http://techblog.netflix.com/2012/04/netflix-recommendations-beyond-5-stars.html> (last accessed on 2017-04-14).

591 Ginner, Viktor and Olsson, Mattias, *Smart teknik vet vad du vill köpa*, Mitt i Nacka, 13 December 2011, at p. 5. Since referring to this development, this technology has been removed from the location referred to.

software is compliant with legislation and that no ‘personal data’ is stored by the system.⁵⁹² From the company’s home page, mention is made of ‘privacy’ and that the system has the following functionality to protect privacy: the data concerning registration number is erased immediately, the registration number of the car is made anonymous by means of encryption using a hash key and finally, the system does not possess the functionality for surveillance.⁵⁹³ The system may be legally compliant yet this does not mean that it is without a consequential harm, for example, where reputation is at stake. While the advertisements remain on a general and harmless level the technology could potentially be developed such that an advertisement suggesting a certain health-related drug could reveal sensitive health information.⁵⁹⁴

4.3.2.3 Creditworthiness in China

Creditworthiness is becoming the measure of the model citizen in China. A number of companies in conjunction with the state have produced a system whereby a citizen’s reliability is reduced to a score produced by predictive models. The task of determining the model citizen has been left to technology and the criteria being used to determine this is creditworthiness. The system uses big data, against which an algorithm is run, in order to monitor every action that person takes in the digital environment. A digital image of the person is compiled based on this data. The main factor determining whether a person is deemed a good, reliable and dependable citizen is creditworthiness. It is possible to acquire a maximum of 950 points. If you have a score of 650, that is considered good and you are entitled to a number of benefits and some of the obstacles that would normally need to be overcome in order to gain certain societal benefits, are removed. A low score, for example under 300 points, makes life more difficult. You are not eligible for the better jobs in society and many obstacles appear that make everyday life more difficult.

592 Ibid.

593 Facility Labs, *Facility Labs och den personliga integriteten*, available at <http://www.facilitylabs.com/> (last accessed on 2017-04-14) as translated and summarised by the author of this thesis.

594 This is merely a hypothetical example. In reality the advertisements are suggestions for shops that are likely to be of interest, but this does not prevent the technology from being used on a more personal level and in doing so, being more invasive.

The Chinese authorities are open about the system and about how the model citizen is determined. They even provide advice on how one can improve one's score, for example, by purchasing the right goods such as electrical appliances, by refraining from buying frowned upon products such as certain computer games, by refraining from using those social media considered unacceptable and by paying bills on time. Also, having friends with a low score can bring down a person's score and the only way to remedy this is to cut all contact with these 'undesirable' friends. There is also an app that can be downloaded to view what your score is and the trend is to publish the result for everyone to see.⁵⁹⁵ It is the predictive model that is at the heart of this programme, where an algorithm compiles a digital identity of an individual and produces a score. This is a typical instance where reputation is determined by a computer system and the data points associated with a particular individual.

4.3.3 Remarks

As individuals spend more time in the digital environment, new ways are being developed in order to assess their reputation, the predictive algorithm central in this respect. The advent of predictive modelling has brought into focus the notion of control. On the one hand control over one's reputation is lost to the algorithm, that determines an individual's digital identity and reputation, yet on the other hand, it can be argued that more control is given to the individual in certain circumstances. The Chinese example portrayed above, provides control to the individual over his or her reputation. The individual knows exactly what is required in order to attain the reputation of a model citizen and the technology in the form of apps are provided in order to facilitate this process. A follow-up issue, however, is whether this development is desirable?

Another issue for consideration is whether a digital identity compiled by an algorithm is better than one created by a human being, considering that the

595 Åkerblom, Tobias Andersson, *Så blir du en kinesisk mönstermedborgare*, available at <https://kit.se/2015/09/25/11823/sa-blir-du-en-kinesisk-monstermedborgare/> (last accessed on 2015-12-01). See also Chin, Josh, *China's New Tool for Social Control: A Credit Rating for Everything*, The Wall Street Journal, available at <https://www.wsj.com/articles/chinas-new-tool-for-social-control-a-credit-rating-for-everything-1480351590> (last accessed on 2017-02-07).

latter are susceptible to subjectivity. Put another way, will too much control not allow the individual the leeway to create a false image of him or herself, thereby causing great difficulty for those, without an in-depth knowledge of the person, to make a judgement of trust?

A theme within the area of law and information technology is that of embedding law in technology. Whereas law is a mechanism with which to regulate technology, more specifically the risks associated with a technology, law can also be embedded into technology, thereby increasing effectivity.⁵⁹⁶ This theme is illuminated by Lessig where his main point is that ‘code is law’.⁵⁹⁷ The China example is a typical scenario where law is built into technology. If one takes the point of departure that one of the functions of the law is to influence behaviour, then this example is just that: a technology is created to influence behaviour in a certain direction, failure to comply resulting in a predetermined sanction. It is also argued that within this context, the concept of reputation is also transformed into a technologically based notion. So while reputation is protected by the law, the notion of reputation is also embedded into technology. Consequently. The technology becomes the law due to the part that it plays in the overall socio-technological system for social steering.

4.4 Discrimination

Predictive modelling in itself is to some extent discriminatory in that it classifies individuals based on certain characteristics, which can lead to the different treatment of these individuals in similar circumstances. However, the fact that predictive modelling is discriminatory in the general sense does not necessarily mean that it is discriminatory according to anti-discrimination law. In other words, the distinction between discrimination in practice and discrimination according to the law is illuminated by the predictive modelling technology. This section investigates the phenomenon of predictive modelling in relation to EU anti-discrimination legislation, with the goal of illustrating the challenges that technologies can create in relation to existing law.

596 Wahlgren, Peter, *Inbyggda lagar*, in *Festskrift till Peter Seipel*, Norstedts Juridik, 2006, at p. 649.

597 Lessig, above n. 53.

Discrimination is ‘the practice of unfairly treating a person or group of people differently from other people or groups of people’.⁵⁹⁸ Alternatively, discrimination is, ‘the prejudiced treatment of an individual based on their membership in a certain group or category’ and the attributes encompassing discrimination include race, ethnicity, religion, nationality, gender, sexuality, disability, marital status, genetic features, language and age.⁵⁹⁹ This list is exhaustive in that for discrimination to be present, one of these specific attributes needs to form the basis of or be incorporated into a decision to qualify as discriminatory. For example, discriminating against a person for having a yellow car is not discrimination according to the law, even if it was this attribute that resulted in the disadvantageous treatment. From the computer science perspective, discrimination is, ‘the prejudiced treatment of an individual based on their membership in a certain group or category’. In relation to the predictive modelling process, a model is said to be discriminatory in situations where two individuals have the same characteristic relevant to a decision making process, yet they differ with respect to a sensitive attribute, which results in a different decision produced by the model.⁶⁰⁰

Using predictive models to predict future behaviour by examining historical data usually encompasses the situation where specific attributes associated with human behaviour are built into a predictive model. For example, attributes may include income, postal code, current debts, student loan, marital status, age, education etcetera. Included in the predictive model may also be attributes that are discriminatory in nature according to law, for example, gender or race. In this manner, the predictive process may be built upon discriminatory bases.

The point stressed here is that a decision can be discriminatory yet not contravene any anti-discrimination law in that the legislation requires the presence of certain pre-determined criteria in order to activate the anti-discrimination legislation.

598 Merriam-Webster Dictionary, *Discrimination*, available at <http://www.merriam-webster.com/dictionary/discrimination> (last accessed on 2017-02-07).

599 Calders, Toon and Zliobaite, Indre, *Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures*, in Custers, Bart, et al. (eds.), *Discrimination and Privacy in the Information Society – Data Mining and Profiling in Large Databases*, Springer, 2013, at p. 43.

600 Ibid, at p. 45.

4.4.1 On a European Level

Within the European context, the law regarding discrimination has been described as a 'patch-work'. In other words, the coverage is provided through multiple pieces of legislation that complement each other to provide a measure of protection for the individual. There are a number of Directives that make up the anti-discrimination legislation and it is also addressed in the Treaty on the Functioning of the European Union in articles 18 to 25.⁶⁰¹ The Race Equality Directive (Directive 2000/43/EC) protects against discrimination that is based on racial or ethnic origin. Its main aim is to give effect to the principle of equal treatment.⁶⁰² The Gender Recast Directive (Directive 2006/54/EC) regarding employment situations and the Gender Goods and Services Directive (Directive 2004/113/EC) have applicability in the area of the supply of goods and services.⁶⁰³ As far as employment is concerned, the Employment Equality Directive (Directive 2000/78/EC), prohibits discrimination on grounds of religion and belief, age, disability and sexual orientation.⁶⁰⁴ The European context encompasses a legal regime that protects against discrimination, where a number of basic principles form the basis of this discrimination legislation. First, a distinction is made between discrimination on the one hand that is based on specific grounds and a general principle of equal treatment on the other hand.⁶⁰⁵ Examples of the special grounds of discrimination are race, gender, disability or age.⁶⁰⁶ It is argued that the general principle of

601 Consolidated Version of the Treaty on the Functioning of the European Union, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0047:0199:en:PDF> (last accessed on 2014-03-21).

602 European Union Agency for Fundamental Rights, *The Racial Equality Directive – Application and Challenges*, <http://fra.europa.eu/en/publication/2012/racial-equality-directive-application-and-challenges> (last accessed on 2014-03-17).

603 Fabeni, Stefano and Agius, Silvan, *Transgender People and the Gender Recast Directive*, <http://www.changelingaspects.com/PDF/ILGA%20GUID-LINES%20for%20transsexuals.pdf> (last accessed on 2014-03-17).

604 European Commission, The Employment Equality Directive, http://europa.eu/rapid/press-release_MEMO-08-69_en.htm?locale=en (last accessed on 2014-03-17).

605 Gellert, Raphael, de Vries, Katja, de Hert, Paul and Gutwirth, Serge, *A Comparative Analysis of Anti-Discrimination and Data Protection Legislation* in Custers, Bart et.al (eds), *Discrimination and Privacy in the Information Society – Data Mining and Profiling in Large Databases*, Springer, 2013, at p. 64.

606 Ibid.

discrimination arises out of the constitutional traditions of Member States, international human rights treaties (particularly the ECHR) and EU Charter. This general principle is determined on a marginal level, meaning that if there is some sort of rationality to different treatment and that it is not totally arbitrary, the consideration of this treatment being discriminatory is dropped.⁶⁰⁷ Also, a distinction is made between direct and indirect discrimination, the former occurring when an individual is treated in a less favourable manner and this unfavourable treatment is based on a certain forbidden ground, as stipulated in the anti-discrimination legislation, and the latter occurring when an individual is treated differently based on what appears to be a neutral criteria but which has the effect of leading to discrimination on one of the specific grounds.⁶⁰⁸ In other words, discrimination is present if two individuals have the same characteristics that are relevant for a certain decision but are treated differently (the outcome of a decision is different) and this was due to the fact that the only difference between these two individuals is an attribute that is considered sensitive, and which is stipulated, such as race or gender.⁶⁰⁹

Much of the discrimination that takes place can be described as indirect discrimination. Article 2 of Directive 2000/43/EC states that:

Indirect discrimination shall be taken to occur where an apparently neutral provision, criterion or practice would put persons of a racial or ethnic origin at a particular disadvantage compared with other persons, unless that provision, criterion or practice is objectively justified by a legitimate aim and the means of achieving that aim are appropriate and necessary.

Finally, anti-discrimination legislation is described as having an asymmetrical scope, mainly in that it is highly specified, which in turn, results in a situation where the presence of discrimination depends on which specific ground is being examined.⁶¹⁰

Therefore, despite the fact that an established legal regime exists regarding acts of discrimination within the European context, in order for an action to activate it, the discrimination must be based on race, ethnicity, religion, na-

607 Ibid, at p. 65.

608 Ibid.

609 Ibid, at p. 45.

610 Ibid, at p. 66.

tionality, gender, sexuality, disability, marital status, genetic features, language or age. This is problematic in that the type of discrimination taking place in the context of predictive modelling may not be covered by existing legislation.

4.4.2 The Context of Price Discrimination

Price discrimination can be described as the act of ‘charging different prices to various customers for the same goods or services’.⁶¹¹ Generally, prices for goods and services are determined by the principles of supply and demand. In normal circumstances, determining demand may be difficult and would be determined by the general circumstances of the public and factors such as what is fashionable at a certain point in time. The digital era has changed this and demand can be determined on an individual basis.

The airline industry can be used in order to illustrate this. An airline company may use different methods to find out more about a customer or potential customer. The person may have a customer loyalty card where points are collected or the person’s activities while browsing the airline’s web page may be monitored, for example, how many times he or she has gone to the web page during a certain time period or how long the mouse cursor has hovered over a certain type of ticket. Feeding this data into a predictive model, a person may be identified as having a certain tendency when purchasing plane tickets. For example, the predictive model may show that Person A has a tendency to purchase his plane tickets at the last moment, while Person B always purchases her ticket well in advance. When Persons A and B go on to the internet in order to purchase a plane ticket on the same flight on the same route, they may get offered tickets of different price levels solely due to their anticipated behaviour. Person A may be offered a more expensive ticket while Person B a cheaper ticket. The difference between these two tickets is the circumstances under which they were bought as predicted by the predictive model. A consequence of this is that we now have the situation where human behaviour is

611 Odlyzko, Andrew, *Privacy, Economics and Price Discrimination on the Internet*, <http://www.dtc.umn.edu/~odlyzko/doc/privacy.economics.pdf> (last accessed on 2013-10-08), at p. 2.

predicted and humans are judged not according to what they did but rather according to what it is predicted that they will do.⁶¹²

History, it is said, repeats itself, and price discrimination also occurred in the US during the latter part of the 19th century in relation to the railroads. This price discrimination took the form of ‘versioning’, where the process of creating different versions of the same product with minor differences occurred in order to create a basis on which to price discriminate.⁶¹³ The instances of versioning that were apparent within the US railroad system, where physical differences between the first, second and third class train carriages were created in order to legitimize the different prices of ticket for the different classes. Third class carriages had no roof as opposed to first and second class carriages and third class carriages also had wooden benches. In addition, the third class carriages were usually placed directly behind the steam locomotive in order that third class customers would be burned by cinders flying from the locomotive. The idea, Odlyzko argues, was that second class customers would be discouraged from travelling third class and the same applied for the first class customers, who would be discouraged from travelling second class, the idea being not to punish the poor but rather frighten the rich.⁶¹⁴

The public reaction to price discrimination was such that it was deemed unfair even if prices on average decreased as a result. People preferred fairness, transparency and predictability over cheaper train fares. The railroad controversy later resulted in the drafting of the Interstate Commerce Act of 1887, which incorporated the following principles: rates were to be just and reasonable, personal discrimination was forbidden, ‘undue or unreasonable preference’ was forbidden, charging more for a short haul than a long haul was forbidden, pooling was forbidden, rates were to be published and impediments to continuous travel of freight was forbidden.⁶¹⁵ The difference today is that companies are able to determine demand on an individual basis and according to a person’s ‘maximal willingness to pay’, something which the

612 Mayer-Schönberger and Cukier, above n. 149, at p. 175.

613 Odlyzko, above n. 611, at p. 2. Odlyzko also provides the example of hard cover books and their soft cover equivalent. Hard cover books usually are much more expensive, more expensive than the difference justifies. Hard cover books usually come out some time before the soft cover equivalent, which entices the impatient customer to pay the difference for the hard cover version.

614 Ibid.

615 Ibid.

railroad companies could not do back in the 19th century due to the lack of technology.⁶¹⁶

Staples is a US based stationary company that has an outlet on the internet.⁶¹⁷ People accessing the staples.com website in order to make a purchase, receive a price relative to their location in relation to an off-line competitor.⁶¹⁸ In other words, people received different versions of the web offer depending on certain predetermined factors, proximity to a competitor in the off-line environment being one of them. There may be legitimate reasons for prices in one geographical area being higher than prices for the same products in another geographical area. However, in the case of Staples, tests seemed to show that it was ZIP code that determined price, in turn determined by IP address.⁶¹⁹ What is interesting also is that generally the areas in the off-line environment, where a lower price was quoted, were areas where the individuals on average had a higher income.⁶²⁰

The main argument here is that price discrimination will not be deemed discrimination according to EU anti-discrimination laws unless it can be proven that it was based on one of the stated grounds required by law. This, however, does not mean that price-discrimination is not a form of discrimination that is harmful and unwarranted as far as society is concerned.

616 Ibid.

617 <http://www.staples.com/office/supplies/home> (last accessed on 2014-10-01).

618 Valentino-Devries, Jennifer, Singer-Vine, Jeremy and Soltani, Ashkan, *Websites Vary Prices, Deals Based on Users' Information*, Wall Street Journal, 24 December 2012, available at <http://online.wsj.com/news/articles/SB10001424127887323777204578189391813881534> (last accessed on 2014-10-01).

619 Ibid. An IP address is a unique identifier assigned to every device on a network and together with geolocation technology, can be used to determine a person's geographic location, see Mitchell, Bradley, *What is an IP Address?*, Lifewire, available at <https://www.lifewire.com/what-is-an-ip-address-818393> (last accessed on 2017-02-07).

620 Valentino-Devries, Singer-Vine, and Soltani, above n. 618.

4.4.3 Discrimination on a Technical Level

Discrimination may not only occur in the form of an effect on a human being. It may be an inherent part of the actual predictive modelling process. In working with data sets as part of the predictive modelling process, mentioned above, two assumptions are common: first, the characteristics of the population on which the predictive model is applied are the same as that of the training data and second, the training data represents the population well.⁶²¹ The main point here is that the workings of the predictive model may lead to discriminatory decisions depending on how they are constructed and also on what data have been used for them to train on before being applied to novel situations.

Calders and Zliobaite state that the process of modelling has as its main aim the attainment of accuracy, but that discrimination may occur on a technical level where, ‘a classifier discriminates with respect to a sensitive attribute, for example gender, if for two persons which only differ by their gender (and maybe some characteristic irrelevant for the classification problem at hand) the classifier predicts different labels’.⁶²² They highlight that the attributes at the basis of the model need to be relevant for that instance, providing the example of the attribute of ‘wearing a skirt’ as not only being discriminatory due to its close association with gender, but also that it is irrelevant, for example, in the request for a loan situation.⁶²³ Another example is that of insurance companies attempting to identify high risk drivers, where the attribute ‘driving style’ is the one that most aptly determines the risk associated with an individual. However, it is costly to determine this by following the individual as he or she drives around town. Instead, one uses a proxy, which is an attribute that is most closely associated with the attribute not available. For example, males of a certain age, investigations have shown, have a tendency to drive in a riskier fashion. However, this may lead to situations where a calm male driver is required to pay a higher car insurance premium than an aggressive female driver of the same age, driving the same car.⁶²⁴

621 Calders and Zliobaite, above n. 599, at p. 46.

622 Ibid, at p. 49.

623 Ibid, at p. 50.

624 Ibid, at p. 45

4.4.4 Remarks

Anti-discrimination legislation is specific in its nature and specified criteria must be present in order for it to become applicable. In the digital environment, an attribute not recognized by law as being discriminatory, may still lead to a discriminatory or unfair result, while the remedies for recourse under existing anti-discrimination legislation are not available. This holds true also in instances where proxies are utilized. The argument is twofold, in that not only may proxies be used that do not fall within the bounds of anti-discrimination law, but that the predictive modelling process may be complicated, resulting in difficulties in identifying discrimination. For example, imagine a correlation established between the propensity for accidents and the colour of a car. Utilizing a car's colour in the determination of driving style may first be difficult to identify, and may also lead to a discriminatory result while not being covered by discrimination legislation. In this regard, Mayer-Schönberger and Cuckier provide insight into the use of proxies within the insurance industry.⁶²⁵

Despite the negative arguments above, technology is also part of the remedy. For example, insurance companies are already fitting the cars of their insured clients with technology, which records and transmits data concerning how the car is being driven. The Discovery Health insurance company in South Africa has a programme whereby good driving is rewarded with free petrol. The technology called 'DQ-Track' measures driving behaviour and a score is obtained at the end of each month, called the 'driver quotient', which factors in driver behaviour, driver knowledge and knowledge about how safely a car is being driven. Factors monitored in real time are acceleration, speed, braking, how corners are taken, night time driving, distance and smartphone activity. The more extreme these factors, the lower the score attained.⁶²⁶ Apart from problems identifying who the actual driver of the car is at a certain point in time, the insurance company is able to ascertain the attribute 'driving style' at a minimal cost. This diminishes the need to use proxies in such circumstances and a more exact determination of driving style can result in a fairer calculation of insurance premium. This in turn eradicates the

625 Mayer-Schönberger and Cuckier, above n. 149, at pp. 56-57.

626 Discovery, *DQ-Track Helps Measure Your Driving Ability*, available at <https://www.discovery.co.za/portal/individual/insure-measure-driving> (last accessed on 2016-01-20).

possible harm of discriminatory decisions in such circumstances and an aggressive driver will pay a higher premium irrespective of factors such as gender.

A final consideration pertains to a balancing of interests. While a technology may result in less discrimination, it may affect other notions, for example privacy. The above example of fitting cars with technology to gauge how the car is driven is illustrative of this. Determining how a person drives, by means of technology, may turn out to be privacy-invasive, necessitating a balancing of the interests at stake.

4.5 Self-Censorship

Censorship is defined as, ‘the system or practice of censoring books, movies, letters, etc.’⁶²⁷ A definition of ‘self-censorship’ states that it is, ‘control of what you say or do in order to avoid annoying or offending others, but without being told officially that such control is necessary’.⁶²⁸ Yet another definition states that it is, ‘the act of censoring one’s own work or what one says without overt pressure from any specific party or institution of authority, often for fear of sanctions.’⁶²⁹

In examining the effects of technology on democracy and focusing on the topic of censorship on the internet, it has been argued that the increased reliance on ICT by users of the internet can lead to a stifling of the freedom of expression and thereby affect democracy negatively, with reference being made by Klang to the works of Milton and Mill.⁶³⁰ Milton published his work *Areopagitica*⁶³¹ in response to the British Parliament’s decision to introduce a

627 Merriam-Webster, *Censorship*, <http://www.merriam-webster.com/dictionary/censorship> (last accessed on 2015-12-04).

628 Cambridge Dictionaries Online, available as <http://dictionary.cambridge.org/dictionary/english/self-censorship> (last accessed on 2015-12-04).

629 Your Dictionary, Self-censorship, available at <http://www.yourdictionary.com/self-censorship> (last accessed on 2015-12-04).

630 Klang, above n. 300, at p. 202.

631 Milton, John, *Areopagitica*, Project Gutenberg, 2006. Retrieved at May 4, 2008, from the website temoa: Open Educational Resources (OER) Portal, available at <http://www.temoa.info/node/799> (last accessed on 2015-12-10).

law requiring that all works be perused by the official censor prior to publishing, thereby attaining greater control over published works. Mill in his work *On Liberty*⁶³² provides four reasons for allowing free speech: first, the opinion we would suppress may be true, second, the opinion we would suppress may be partly true, third, the false opinion is useful in order to make sure the true opinion is not held as a mere uncontested prejudice and fourth, we need the false opinion in order to understand the meaning of the true opinion. Therefore, according to Mill, there is a benefit to publishing everything, even if parts are untrue, in that the untruths re-inforce the truths.

Cook and Heilmann, in examining self-censorship, make the distinction between two kinds of self-censorship, namely public and private self-censorship. Dealing first with public self-censorship, it is described as situations where individuals restrain themselves from expression in response to a public censor and where there are two parties, namely the censor and censee, where the censee internalizes some aspects of the censor.⁶³³ The public censor can take various forms. For example, a legal system functioning in a certain sphere and setting limitations, can be regarded as a censor. Taking this broader view of the notion of the public censor, even norms, culture, religious bodies and companies can be considered a public censor. This is particularly relevant in the context of the internet where self-censorship may take place as a result of individuals not wanting to face legal sanction as a result of disseminating material or even do not want to upset society at large.

In this regard, reference is made to a study by Dent and Kenyon, who examine how certain ambiguities with regards to how a law should be interpreted can lead to a ‘chilling effect’, where people are inclined not to print something in case it would breach a law.⁶³⁴ The notion of chilling effect is used also by

632 Mill, John Stuart, *On Liberty*, fourth edition, London: Longman, Roberts & Green, 1869; Bartleby.com, 1999. Available at www.bartleby.com/130/ (last accessed on 2015-12-10).

633 Cook, Philip and Heilmann, Conrad, *Censorship and Two Types of Self-Censorship*, March 20, 2010, available at SSRN: <http://ssrn.com/abstract=1575662> or <http://dx.doi.org/10.2139/ssrn.1575662> (last accessed on 2015-12-12) at p. 2.

634 Dent, Chris, and Kenyon, Andrew T., *Defamation Law's Chilling Effect: A Comparative Content Analysis of Australian and US Newspapers*, Media and Arts Law Review, Vol. 9, No. 2, at pp. 89-112.

Solove in his privacy taxonomy, being used in the sense that it is a harm associated with some of the privacy problems outlined in his taxonomy and is present when people are inhibited from engaging in certain activities.⁶³⁵

Solove in turn refers to Schauer, who states that, '[a] chilling effect occurs when individuals seeking to engage in activity protected by the first amendment are deterred from doing so by governmental regulation not specifically directed at that protected activity'.⁶³⁶ Here, the relationship between government and individual is the backdrop and what is highlighted is the indirect nature that self-censorship may take. In other words, the focus of limiting free speech may be the by-product of some other governmental action. Here the link between privacy and self-censorship is illustrated, where the failure to provide a large enough space for individuals to act upon their liberty and freedom can result in self-censorship.

The digital environment has blurred the distinction between regular censorship in the paper world and censorship on the internet. With the former, something is produced but censored prior to publishing whereas with the latter, dissemination has usually taken place and here censorship is concerned with limiting access to that content, the most common technical means being via content filtering.⁶³⁷ The consequence of this is partnerships between private actors and governments in order to control access to information, enabling a much harsher type of control.⁶³⁸

Private self-censorship occurs where individuals show personal restraint by means of the self-imposed suppression of personal attitudes, which takes place in the absence of a public censor.⁶³⁹ This type of censorship is characterised by the censor and censee roles being fulfilled by the same agent, namely the individual.⁶⁴⁰ Two categories of private self-censorship are highlighted. First, self-censorship by proxy and second self-censorship by self-constraint. The former occurs when there is an internalization of some external values. This

635 Solove, *Understanding Privacy*, above n. 535, at p. 178.

636 Schauer, Frederick, *Fear Risk and the First Amendment: Unravelling the 'Chilling Effect'*, 58, *Boston University Law Review*, 685, 693 (1978) in Solove, *Understanding Privacy*, above n. 535.

637 Klang, above n. 300, at p. 189.

638 *Ibid*, at p. 219.

639 Cook and Heilmann, above n. 633, at p. 14.

640 *Ibid*, at p. 2.

could be, for example, the rules set out within an organization. The latter arises when the self-censorship occurs as a result of a personal attitude or belief system. This type of self-censorship is the product of an internal conflict within the censee, referred to as ‘the actual expressive attitudes held by an agent and the set of permissible expressive attitudes that they endorse.’⁶⁴¹ In addition, it is not necessarily a fear of something that is the catalyst of self-censorship, for example the respect of something or someone such as religious beliefs can result in self-censorship.⁶⁴²

A relevant issue is whether the concept of free speech applies to both types of self-censorship. Schauer argues that free speech is only relevant in the context of public self-censorship because censorship is something that exists only in the context of the government versus individual.⁶⁴³ This portrays a more restricted notion of the censor, compared to Cook and Heilmann, who argue that the notion of the public censor is wider than that proposed by Schauer, although they do concede that this does not mean that the principle of free speech is applicable to all.⁶⁴⁴ A finding made is that in the case of private self-censorship, there is no external censor, resulting in the fact that the censorship is ‘non-coercive’ in nature and as a result, the principles of free speech do not apply.⁶⁴⁵ An internalized struggle over the expression of ideas, therefore, cannot result in a form of coercion, the result being that the principles of free speech are not violated.

4.5.1 Remarks

The notion of self-censorship is gaining in relevance as more people flock to the social media for communication purposes and as a medium for documenting their lives. It has also become more relevant as the surveillance activities of the NSA were made public by Snowden, after which, in a survey of 520 American writers by PEN America, they admitted to self-censorship of their

641 Ibid, at p. 3.

642 Klausen, Jytte, *The Cartoons that Shook the World*, Yale University Press, 2009, at p. 16.

643 Schauer, Fredrick, *Free Speech*, Cambridge University Press, 1982, at p. 122.

644 Cook and Heilmann, above n. 633, at p. 24.

645 Ibid, at p. 3.

work out of fear that it might cause them harm.⁶⁴⁶ It is argued that both public and private self-censorship become relevant within the predictive modelling context. Extending the notion of the public censor to companies, predictive modelling can have the effect of causing individuals to refrain from expressing a personally held attitude. This is so within the context of the widespread surveillance apparatus used to collect data concerning individuals and which ultimately ends up in the digital identity. A greater awareness of the predictive modelling process can result in the fear that a publicized attitude, having been converted into data, may find its way into the digital identity and ultimately the predictive model, having a detrimental effect on the way a person is judged and resulting in a negative decision being made by an algorithm. Within the context of predictive modelling, private self-censorship may also result out of an internalized conflict. Considering that an objective of predictive modelling is to influence behaviour, an effect may be the manipulation of an individual's internal belief system or a reinforcement of that system. For example, being fed content of a conservative nature may result in a more conservatively orientated value system, which, when used as a measure to determine the acceptability of making an opinion public, may result in a decision to self-censor instead. The notion of brainwashing is relevant in that what may have started out as public self-censorship, may in time evolve into private self-censorship as the norms reflected in the public self-censorship context become internalized.

The notion of self-censorship also comes to the fore in the 'creditworthiness in China' example cited above, and depicts a development from more traditional public censorship to private censorship, albeit in the government versus individual relationship. The authorities determine what should and should not be read, however, the action of censorship is no longer performed by a government official. This task has been transferred to the censee, where the censee and censor reside in the same individual. Material may be publicly available but the effect of reading it results in a lower predictive score. This in turn leads to private self-censorship, where individuals voluntarily refrain from reading or accessing certain content as it may affect the light in which they are seen.

646 PEN American Center, *Chilling Effects: NSA Surveillance Drives Writers to Self-Censorship*, November 2013, available at <http://www.pen-international.org/read-pen-american-centres-report-chilling-effects-nsa-surveillance-drives-writers-to-self-censor/> (last accessed on 2017-02-24) in Greenwald, above n. 85, at p. 178.

Another aspect relating to self-censorship is that as the social media and other digital media become an integral part of peoples' lives, they are becoming subjected to more harassment. A recent report in Sweden has shown that one in three young girls has been sexually harassed online, three of every ten young people say that racial harassment has occurred online and one in three young people has been bullied online.⁶⁴⁷ A recent Swedish Government Report highlights a gender aspect in that women are more frequently sexually harassed on the internet than men, which could lead to self-censorship, especially from a gender equality perspective, and which could impact the freedom of expression as well.⁶⁴⁸ The same Report also referred to the increased harassment by organizations as far as the media was concerned, the aim being to stop journalistic scrutiny.⁶⁴⁹ It is with these developments in mind, that the notion of self-censorship is only going to increase in importance in the future.

4.6 Deindividualization

Deindividualization has been described as, 'to remove or destroy the individuality of, deprive of individuality'.⁶⁵⁰ It is identified as a harm resulting from predictive modelling.⁶⁵¹ This line of thought is highlighted by Vedder, albeit referring to the KDD process, where the dangers of seeing human beings only

647 Friends Online Report 2016, available at <https://friends-brandmanualswede.netdna-ssl.com/wp-content/uploads/2016/03/Friends-natrapport-2016-eng.pdf> (last accessed on 2017-02-07), at p. 5.

648 Swedish Government Official Reports, *Integritet och straffskydd (Privacy and Protection Provided by Criminal Law)*, SOU 2016:7, available at <http://www.regeringen.se/contentassets/207048837827439b9d1dce919d0dd6f9/integritet-och-straffskydd-sou-20167> (last accessed on 2017-02-08).

649 Mattmar, Ulf, Eriksson, Hedvig, *Grävande journalist blev måltavla för proryska troll (Investigative Journalist Targetted by Pro-Russian Trolls)*, published on 2016-03-13, available at <http://www.svt.se/nyheter/utrikes/gravande-journalist-blev-maltavla-for-proryska-troll> (last accessed on 2017-02-08).

650 Merriam-Webster, *Deindividualize*, <http://www.merriam-webster.com/dictionary/de-individualize> (last accessed on 2015-12-03).

651 Shermer, B., *Risks of Profiling and the Limits of Data Protection Law*, in Custers, Bart et al. (eds), *Discrimination and Privacy in the Information Society – Data Mining and Profiling in Large Databases*, Springer, 2013, at p. 138.

in relation to the categories they are placed in are highlighted and that there is an inherent value in seeing human beings as individuals.⁶⁵² The categorization aspect of the predictive modelling process allocates human beings to pre-determined categories where their behaviour is determined by the group to which they were assigned. This can result in a number of undesirable consequences. First, individuals are affected indirectly as they are treated as members of a group, their individual characteristics and traits disappearing into those of the group's. Second, the use of generalizations and profiles is unfair, where, in this context, it is the non-distributive generalizations and profiles that are particularly damaging, having been derived from probabilities, medians and averages.⁶⁵³ As a result, whereas the members of a distributive group all share the characteristics of that group to which they have been assigned, this is not necessarily true of the non-distributed group, where not all members necessarily bear the characteristics described by and associated with that group. Thus the use of generalizations and profiles is even more damaging to the individual, as compared with what is referred to as 'real' personal data.⁶⁵⁴ In other words, taking personal data from an individual and applying it to that individual is less harmful than making a generalization about a group of people and then applying it to that same individual, since a decision based on personal data is more accurate and creates a more accurate digital identity.

These challenges transcend the KDD process.⁶⁵⁵ Predictive modelling can entail sorting people into groups. In addition, representing a person as a score, has the indirect effect of creating a group. In the credit application scenario, those individuals with a score that make them ineligible to be granted credit become de facto members of that group. These individuals are not treated as individuals, but rather as members of the group that they have been sorted into. There is also a link between individuality and privacy, that is highlighted by Cohen, who states that, 'a realm of autonomous unmonitored choice ... promotes a vital diversity of speech and behaviour' and that where there is no

652 Vedder, Anton, *KDD: The Challenge to Individualism*, Ethics and Information Technology, 1: 275-281, Kluwer Academic Publishers, 1999, at p. 275.

653 Ibid, at p. 277.

654 Ibid.

655 Ibid.

privacy, the result ‘threatens not only to chill the expression of eccentric individuality, but also, gradually, to dampen the force of our aspirations to it’.⁶⁵⁶

As was depicted above, there are benefits to treating human beings as individuals. The liberal political theory places the individual in the centrum, advocating that conditions should be such so as to allow the individual to make decisions that best reflect his or her needs. In the realm of political philosophy, there is a tradition that looks to the writings of Aristotle, who examines the notion of ‘the good’. This notion of the good, ‘... regards as fundamental the question of what counts as an excellent, valuable life for a human being’.⁶⁵⁷ A consequence flowing from this conception of the good is that a philosopher will look to the institutions, both political and social, that can achieve this.⁶⁵⁸ The law is important in this regard as it is the mechanism that creates the environment within which the individual can enjoy the freedom to make decisions (‘right of subjective freedom’) and where the individual can pursue his or her notion of a good life in a sphere of liberty, free from interference. In this context, it is argued that notions such as ‘rights’, ‘justice’ and ‘equality’ gain importance.⁶⁵⁹

4.6.1 Remarks

The predictive modelling process affects the individual in a number of ways. First, it identifies the probability of individual behaviour occurring, which is separated from the guarantee that a certain behaviour will occur. In other words, the individual is treated as if he or she will behave in a certain manner before this has occurred, in effect disregarding the role played by human free will. Second, the prediction of behaviour may be made in relation to the group, also diminishing individuality. The individual is not treated as an individual but as a member of a group, where the group attributes override any individuality, and a person disappears into the mechanics of the predictive model. It reduces a human being to a score that ultimately can prevent him or her from

656 Cohen, *Examined Lives*, above n. 372.

657 Simmonds, Nigel E., *Central Issues in Jurisprudence- Justice, Law and Rights*, Sweet and Maxwell, 2008, at p. 6.

658 Ibid.

659 Ibid, at p. 7.

being in a position to make the choices that best reflect his or her notion of the good. If society is to cherish the liberal notion of the individual, then the law should position itself in order to promote the individual.

4.7 Loss of Agency

A potential harm resulting from predictive modelling is the loss of agency. Agency can be described as, ‘the free will by which people choose their actions’ and encompasses the notion that individuals should be held accountable for their behaviour and not their propensity.⁶⁶⁰ It is at the core of most, if not all modern legal systems, that human beings are held responsible for their actions (or failure to act).⁶⁶¹ A summary of the progression of the notion of agency is provided by De Mul and Van den Berg, who trace the origins of agency. They start with the philosophy of Descartes, who referred to rationality as being the catalyst for human action. Next they refer to critics of this view and state that there are other factors besides rationality that motivate human action and second, that a large portion of a person’s decisions are implicitly taken with rationality being totally absent.⁶⁶² There is a wide spectrum, where at the one end, agency is regarded as being grounded on rationality whereas at the other end, agency is regarded as being void of all free will and autonomy. De Mul and Van den Berg place themselves somewhere in the middle:

In our everyday lives we experience ourselves as agents with some level of control and freedom of choice, even if we are willing to grant the postmodern suspicion that our levels of control are far from complete, and that our freedom of choice may often be informed by motives and processes that are either unknown to us or principally not (completely) insightful for us.⁶⁶³

660 Mayer-Schönberger and Cukier, above n. 149, at p. 175.

661 Exceptions to this rule arise, for example, in the case of minors who do not have the legal capacity to act in certain situations according to the law.

662 De Mul, Jos, and Van den Berg, Bibi, *Remote Control: Human Autonomy in the Age of Computer-Mediated Agency*, in Hildebrandt, Mirille and Rouvroy, Antoinette, *Law, Human Agency and Autonomic Computing: The Philosophy of Law Meets the Philosophy of Technology*, Routledge, 2011, at p. 51.

663 Ibid.

The authors refer to a ‘reflexive loop’, which is the ability for persons to judge the internal and external forces that motivate them.⁶⁶⁴ In other words, the reflexive loop can be described as a person having the ability to step away and reflect on the driving forces relevant to the decisions that he or she has made. A main assertion made by the authors is that human agency is based on ‘reflexive remote control’, where human action is controlled remotely, in other words, where humans are influenced in their actions by factors yet they also control these factors (a remote control of the self).⁶⁶⁵

4.7.1 Agency and Law

The danger in relying too heavily on the prediction of behaviour, is that it can result in people being judged not for what they did but rather on the probability of what they will do in the future. It is suggested that the notion of judging based on probability is not restricted to future action but can be applied to past actions, where someone is found guilty based on the probability that he or she committed a crime.⁶⁶⁶ In other words, the evidentiary yardstick may not require evidence that an act was committed, but rather, it may be sufficient to prove that the individual possessed the character traits or personality characteristics to have probably committed the act in question.

The above reinforces some core themes associated with technological advances. First, it is based on the notion that generally, data are considered objective and that data do not lie. This, it is submitted, is not entirely true. The data may be in the form of ones and zeros, but there is a certain subjectivity associated not only with the collection and sorting of data, but behind technology in general. In the words of Kranzberg:

That is why I think that my first law - Technology is neither good nor bad; nor is it neutral – should constantly remind us that it is the historian’s duty to compare short-term versus long-term results, the utopian hopes versus the spotted

664 Ibid.

665 Ibid.

666 Mayer-Schönberger and Cukier, above n. 149, at p. 176.

actuality, the what-might-have-been against what actually happened, and the trade-offs among various “goods” and possible “bads”.⁶⁶⁷

In other words, technologies influence the environments that they co-exist in, and have social and human consequences that may differ from one context to another and under different circumstances. Hildebrandt utilizes the term ‘selection’, stating that technology is effective and ineffective as well as legitimate and illegitimate, ultimately stating that any type of selection that takes place and which affects people’s lives, needs to be justified.⁶⁶⁸ The second notion is that technology is always one hundred percent correct and true. However, in predictive modelling, the aim is not to predict exact behaviour. Many predictive models aim at increasing productivity and effectiveness. The Hewlett-Packard flight risk model used to identify employees about to leave the company achieved a \$300 million potential saving for the company, with the model accurately identifying seventy-five percent of the quitters.⁶⁶⁹ The aim is not for the predictive model to succeed in every imaginable case, but rather to increase effectiveness and boost profitability.

Connected to the issue of human agency is that of legal responsibility. Brenner, in highlighting the challenges that technology poses to the law, states that legal systems will be required to adjust to new technologies that are smart in nature, distinguishing between the ‘dumb’ technologies of the past and ‘smart’ technologies of the present and future. She states that we ‘use’ dumb technologies while we ‘interact’ with smart technologies. These smart technologies have two main characteristics: first, they are ambient in nature and work in the background without our noticing them and second, they are intelligent, constantly making decisions for us and on behalf of us in order to make everyday tasks less burdensome.⁶⁷⁰

Berk, a criminology professor, has developed an algorithm predicting the probability of a person, jailed for murder, killing again once released from jail. Predictive modelling also has consequences in relation to public entities. This algorithm is now being used as part of the decision as to whether parole should

667 Kranzberg, Melvin, *Technology and History: 'Kranzberg's Laws'*, *Technology and Culture*, Vol. 27, No. 3, pp. 544-560, 1986, at pp. 547-548.

668 Hildebrandt, *Profiles and Correlatable Humans*, above n. 226, at p. 270.

669 Siegel, above n. 118, at p. 49.

670 Brenner, above n. 171, at p. 5.

be granted to such persons.⁶⁷¹ A number of questions arise in connection with this example. First, in the event that parole is denied and part of the decision not to grant parole is based on the algorithm ‘saying no parole’, is that not tantamount to finding a person guilty based not on action but rather on probability and propensity for action? Second, does this scenario not amount to punishment prior to a criminal act being committed? Third, how does this fit in to established legal concepts such as fairness, predictability and innocence until proven guilty? Fourth, is this ethical? Fifth, if the algorithm predicts a high risk of relapse and that parole should not be granted, to what extent would it be likely that members of the parole board would contradict this decision (especially in light of the attitude to data that it is always correct and objective)?

Algorithms are not only being used at the parole application, but throughout the entire criminal process, where a decision must be taken as to whether a suspected criminal should be set free. Accusations are surfacing that these predictive models are racially biased. ProPublica, in studying cases where predictive models were used to decide the risk attached to a particular suspect being freed, claims to have proved that they were racially biased in that White people were treated more favourably than African Americans.⁶⁷² First, examining 7000 people, the results showed that the algorithm proved unreliable, with only 20 percent of those predicted to commit a crime again (recidivism), actually doing so. Second, the algorithm incorrectly flagged African Americans at twice the rate of White people, the statistics showing the following: of those labelled ‘high risk but did not re-offend’, 23.5% were White and 44.9% African American and of those labelled ‘low risk yet did re-offend, 47.7% were White and 28% African American.⁶⁷³ Algorithms have also become a tool at the sentencing stage.⁶⁷⁴ Judge Horne in La Crosse County, Wisconsin

671 Vlahos, above n. 374, at p. 54.

672 Angwin, Julia, Larson, Jeff, Mattu, Surya and Kirchner, Lauren, *Machine Bias*, ProPublica, available at <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> (last accessed on 2016-09-09).

673 Ibid.

674 The referral to numerical factors to produce guidelines in order to arrive at a decision regarding sentencing is not new. In this regard, see Wahlgren, Peter, *Lagstiftning: rationalitet, teknik, möjligheter*, above n. 54, at p. 187.

declared that a defendant had been, ‘identified, through the COMPAS assessment, as an individual who is at high risk to the community’.⁶⁷⁵ A judge who reduced a sentence on appeal, from the original 2 years to 18 months, admitted that, ‘[h]ad I not had the COMPAS, I believe it would likely be that I would have given one year, six months’, admitting that the predictive model encouraged a longer sentence. Another point is highlighted by the defendant, who said that, ‘[n]ot that I’m innocent, but I just believe people do change’, reflecting on the fact that the predictive algorithm did not take into account that people can change, an argument which has a connection to the potential harm of stereotyping, addressed below.⁶⁷⁶

4.7.2 Remarks

The notion of human agency is complex, and considering the extent to which society is becoming more reliant on the digital environment for every-day activities and as this environment becomes more integrated with aspects of human activity, the extent to which human agency and personal autonomy will thrive in the future should be questioned. Predictive models are increasingly being used by companies as an intermediary in their interaction with individuals. Considering the ‘black box’ nature of this technology, humans are losing the opportunity to exert persuasive influence over these relationships. In other words, acting on behalf of a commercial actor, the decision-system, essentially a ‘black box’ from the perspective of the individual, makes decisions based on big data whereby the digital identity is formed and where the individual loses the ability to get a personal point of view across.

The notion of human agency is raised by Thaler and Sunstein who discuss the ability of individuals to make decisions that are in their own best interests. They do not argue that individuals should not have complete agency, however question the ability of individuals to make decisions that are best for them. Having stated this, there is the argument that the autonomy of individual choice, even if the outcome is disadvantageous, is a good in itself. It is in this context that the future act of having to draw the line regarding human agency will require determination.

675 Ibid.

676 Ibid.

4.8 Stereotyping

Stereotyping is the use of ‘widely accepted beliefs about groups of people’.⁶⁷⁷ It is also argued to be a form of generalization, or as Schauer aptly puts it, ‘painting with a broad brush’.⁶⁷⁸ Providing a more concise definition of what it means to generalize, he states that, ‘[o]n the basis of a characteristic of some members of a class, we reach conclusions or make decisions about the entire class’.⁶⁷⁹ Stereotyping is also referred to as a type of profiling employed by human beings, which is unique in that they are able to reflect upon these profiles and accept or reject them, in effect making humans autonomous agents.⁶⁸⁰ Stereotypes can also be alternatively regarded as a mechanism that underlies inequality and discrimination.⁶⁸¹ People, it is argued, use generalizations extensively, for example, where employers recruit employees on the assumption that good grades are an indication of job performance. Another example is that of actuaries, whose guidance to insurance companies is based on generalizations concerning large categories of people.⁶⁸² However, one argument is that no matter how many categories one has created and no matter how many labels these categories have, they can never adequately account for the richness, diversity and complexity of the human personality and in the long run this is harmful to an individual’s identity.

There is a connection between stereotyping and de-individualization in that the stereotype assigned to a person may be associated with a group stereotype. These notions, in turn are also connected to the issue of personalization, where the trend is to tailor services more precisely to the perceived desires of the individual. Hildebrandt, in the context of profiling, refers to the notion that once an individual has been placed in a category, it may be difficult to break out, or shed the stereotype attributed to that individual, as an individual or as

677 Timmer, Alexandra, *Toward an Anti-Stereotyping Approach for the European Court of Human Rights*, *Human Rights Law Review*, 11:4, pp. 707-738, 2011, Oxford University Press, at p. 708.

678 Schauer, Fredrick, *Profiles, Probabilities and Stereotypes*, Harvard University Press, 2003, at p. 1.

679 Ibid, at p. 4.

680 Hildebrandt, *Profiling into the Future*, above n. 529.

681 Timmer, above n. 677, at p. 708.

682 Schauer, above n. 678, at p. 4.

part of a group. She states that, '[b]oth group profiling and personalization judge your needs, expectations, and desires on the basis of past behaviour, building a well-fitted and usually comfortable cage from which escape will be nearly impossible, precisely when profiling becomes ever more ubiquitous and intelligent'.⁶⁸³

First, it is submitted that with the advent of ubiquitous and ambient intelligence, it will become difficult to recognize the fact that one has been placed in this cage or category. Second, Hildebrandt refers to the important fact that the cage may be 'comfortable'. This in turn may lead to the situation that the individual, even having gained knowledge that he or she is in this cage, may not want to make the effort to break out, which can lead to a negative spiral in the sense that once an individual is placed in a category, it may be extremely difficult, if not impossible, to leave that category.⁶⁸⁴ This is contingent on the individual knowing that he or she was placed in a category in the first place.

The existence of the process of stereotyping comes to the fore in a matter where a judge ordered Google to make certain email correspondence public. From the emails it could be ascertained that Google's business operations included sorting its users into 'buckets', where there were literally millions of bucket, which were described as clusters of people who share a characteristic that might be of interest to an advertiser. The software is called Content One-Box (COB) and in addition to variables such as postal code, it tried to understand the meaning of email messages using machine learning methods. What is particularly interesting is that these 'buckets' were not required to be labelled as all they did was connect users to each other, that is create clusters of connections.⁶⁸⁵ Processes like these are described by Gandy, where he states that profiling or predictive modelling, utilized to predict behaviour, incorrectly assumes that 'the identity of the individual can be reduced, captured or represented by measurable characteristics'.⁶⁸⁶

683 Stehr, Nico and Weiler, Bernd (ed.), *Who Owns Knowledge?: Knowledge and the Law*, Transaction Publishers, 2008, at p. 271.

684 Shermer, B., *Risks of Profiling and the Limits of Data Protection Law*, in Custers, above n. 651, at p. 139.

685 Gould, Jeff, *Courts docs show how Google slices users into "millions of buckets"*, available at <https://medium.com/@jeffgould/courts-docs-show-how-google-slices-users-into-millions-of-buckets-ec9c768b6ae9#.2gqyh6p6g> (last accessed on 2017-04-14).

686 Gandy, Oscar H., *Exploring Identity and Identification in Cyberspace*, Notre Dame Journal of Law, Ethics and Public Policy, Vol. 14, 2000, at p. 1100.

4.8.1 The Computer Assisted Passenger Pre-screening System

The act of stereotyping is illustrated by the Computer Assisted Passenger Pre-screening System (CAPPS II), an application used by the United States Transportation Security Administration (TSA) to prevent acts of terrorism within the aviation industry. Using both governmental and commercial databases, it determines how big a threat an individual is, each passenger given a score in the form of a colour code. For example, ‘green’ indicates that you are no threat, while ‘yellow’ indicates that you are a potential threat and must undergo additional security checks. ‘Red’ indicates that you are an imminent threat and must not be allowed to board the plane, with additional questioning or even arrest a possible consequence.⁶⁸⁷ One incident involved a rower with the US national rowing team, who having been flagged by the system, was denied access to a flight, allegedly, due to his being on a no-fly list because of his Muslim-sounding name.⁶⁸⁸

It is clear that the act of stereotyping is harmful to the innocent individual. Materially assessing the damages can be difficult as well as categorizing the harm suffered by stereotyping, something that is relevant in the legal context. There is the humiliation, the time wasted, the loss of dignity, the financial aspect and of course the fact that one cannot escape the stereotype. According to Sobel, the danger with the system, is that, ‘[a] system does all this data mining of disparate information and then spits out a name ... does this person then bear a secret government-imposed tag, “Possible Terrorist”? Does he have an opportunity to know about it and challenge it?’⁶⁸⁹

687 Electronic Frontier Foundation, *CAPPS II: Government Surveillance via Passenger Profiling*, <https://w2.eff.org/Privacy/cappsii/background.php> (last accessed on 2017-04-14).

688 Berkow, Ira, *Rower With Muslim Name Is an All-American Suspect*, The New York Times, available at <http://www.nytimes.com/2003/02/21/sports/othersports/21ROWWW.html> (last accessed on 2015-12-03).

689 Kumagai, Jean and Cherry, Steven, *Sensors and Sensibility*, IEEE Spectrum, at p. 5, available at <http://spectrum.ieee.org/computing/networks/sensors-and-sensibility> (last accessed on 2015-05-11).

4.8.2 Stereotyping and the Law

Stereotyping as an independent notion is established in the law, but only to a limited extent. It can be argued that this is due mainly to the fact that it has been subsumed by other areas of the law, for example, anti-discrimination law. For example, stereotyping is established within US and Canadian equal protection law, while in human rights law, the ECtHR has only recently started to recognize stereotyping.⁶⁹⁰

For example, in the matter of *Konstantin Markin v. Russia*, the ECtHR referred to the Chamber's condemnation of the gender stereotype according to which mothers were seen to be better than men at child raising.⁶⁹¹ In the context of the US, Title VII of the Civil Rights Act of 1964 and related case law make it illegal to discriminate against someone on the basis of race, colour, religion, national origin, or sex. The law also makes it illegal to retaliate against a person because the person complained about discrimination, filed a charge of discrimination, or participated in an employment discrimination investigation or lawsuit.⁶⁹²

Two types of stereotyping exist, namely, 'ascriptive' and 'prescriptive'. Ascriptive stereotyping occurs when a characteristic is assigned to a person without judging his or her individual qualities. This was the case in *Slack v. Havens*⁶⁹³, where Slack, an African American industrial worker, was asked to clean her workplace while her white co-worker was excused, the rationale given being that coloured workers are hired because they clean better. Her supervisor assumed that all black women were good at cleaning and associated Slack with this group stereotype. Prescriptive stereotyping occurs where the individual characteristics of a person are recognized but are then judged against an inappropriate gendered baseline.⁶⁹⁴ This situation was addressed in

690 Timmer, above n. 677, at p. 239.

691 *Konstantin Markin v. Russia*, Application No. 30078/06, 7 October 2010, Grand Chamber, para. 99, in Timmer, above n. 677, at p. 708.

692 US Equal Employment Opportunity Commission, *Laws Enforced by EEOC*, available at <http://www.eeoc.gov/laws/statutes/> (last accessed on 2016-01-21).

693 *Slack v. Havens*, 522, F.2d 1091, 1091-93 (9th Cir. 1975).

694 Herz, Zachary R., *Price's Progress: Sex Stereotyping and Its Potential for Antidiscrimination Law*, Yale Law Journal, 124:36, pp. 398-446, 2014, available at http://www.yalelawjournal.org/pdf/c.396.Herz.446_eou7btj2.pdf (last accessed on 2016-01-21), at p. 398.

*Price Waterhouse v. Hopkins*⁶⁹⁵, where Hopkins was asked to dress, speak and act in a manner appropriate to her sex. The difference between these two cases is that Slack was stereotyped as belonging to a group due to certain characteristics while Hopkins was penalized for not conforming to a stereotype.⁶⁹⁶

4.8.3 Remarks

Stereotyping as a concept is generally not as recognized in the law. Where it is afforded attention, it is seen as a sub-category of anti-discrimination law. It is nevertheless recognized as a harm that is worth protecting against by means of the law. While stereotyping has received attention within the law enforcement sphere, labelled as racial profiling, it is argued that stereotyping as a separate notion will receive more attention as predictive modelling becomes more commonplace.

Stereotyping has a negative connotation, yet this need not necessarily be the case. An individual confronted by a stereotype of him or herself, may find this useful as it can be used to adjust identity, and consequently can be an inherent part of the identity-building process. The problem within the area of predictive modelling, however, is the lack of knowledge that stereotyping is taking place.⁶⁹⁷

In addition, there are proponents of the advantages of the use of generalizations. People use generalizations as a mechanism for day-to-day interactions and they have become entrenched in society as a tool. Schauer strongly supports the act of making generalizations, although distinguishing between ‘spurious’ and ‘nonspurious’ generalizations, the difference being that the former type of generalizations has a strong statistical basis.⁶⁹⁸ An example of a weak statistical basis is a situation where a trait is the basis for a generalization yet

695 *Price Waterhouse v. Hopkins*, 490 U.S. 228 (1989).

696 Herz, above n. 694, at p. 398.

697 Hildebrandt, *Profiles and Correlatable Humans*, above n. 226, at p. 278.

698 Schauer, above n. 678, at p. 7.

this trait is irrelevant in relation to a characteristic being predicted, a case being where sexual orientation is irrelevant in relation to courage.⁶⁹⁹ An argument in response to this is that where predictive modelling is concerned, the differentiation between data that are relevant and irrelevant has weakened considering the ability for algorithms to find correlations in data.

4.9 Manipulation

It can be argued that manipulation is a common human activity, where one is nudged into acting in a manner different than one otherwise would have. Manipulation can take multiple forms, including physical, psychological or even optical manipulation. Manipulation is also a concept associated with the law, for example, in the form of a regulatory tool at the disposal of the legislator.⁷⁰⁰ In this regard, a utilized legislating mechanism is termed ‘Procrustean rules’.⁷⁰¹ The legislator gives the individual, who is the target of a piece of legislation, a number of options for adhering to the legislation. While providing the impression of choice, one of the options, which is preferred by the legislator, is made less burdensome to follow while the others are made more complex, manipulating the individual into following the option preferred by the legislator.⁷⁰²

The increased reliance by individuals on technology coupled with a decrease in knowledge or awareness concerning how these technologies work or even of the fact that they exist, results in individuals being more susceptible to increased manipulation by programming code that is unavailable to the user.

699 Ibid, at p. 15.

700 Here the term ‘legislator’ is used in the strict sense to mean that organ or those people who are responsible for the drafting and passing of laws in a country.

701 Procrustes is a figure from Greek mythology. He was said to have placed his victims on a bed and force them to the size of the bed. If they were too short, he would stretch their bodies and if too long, cut off their feet. The metaphor of Procrustes is used to describe the forcing of people into a certain predetermined pattern. Encyclopedia Britannica, *Procrustes*, available at <http://global.britannica.com/EB-checked/topic/477822/Procrustes> (last accessed on 2017-04-14).

702 Wahlgren, P., *Manipulation: Lagstiftningsteknik eller integritetskränkning?*, in Henrichsen, C., Rytter, J. and Rønsholdt, S. (eds.), *Ret, Informatik og Samfund*, DJØF, 2010, at p. 146.

For Lessig, code is a ‘regulator’ and those who have control of the code also control those who navigate through this coded space:

This regulator is what I call ‘code’—the instructions embedded in the software or hardware that makes cyberspace what it is. This code is the ‘built environment’ of social life in cyberspace. It is its ‘architecture’ ... my argument is that we must come to understand how in the twenty-first century it is a different regulator—code—that should be our current concern.⁷⁰³

Manipulation can also be psychological, an example being the 1996 Minnesota Department of Revenue tax compliance experiment on 47 000 payers of income tax. Various methods were tested on different groups of taxpayers. The first group was informed that their tax returns would be examined more closely, the second group was given a new form to fill in, the third group was promised better services for filling out the tax return and the fourth group was provided a letter stating that it was not as common as was generally perceived that people cheated on their taxes. What the study showed was that different tax groups were influenced differently depending on what method of communication was used. Those who received a message that reinforced the social norms regarding tax compliance generally had a positive effect.⁷⁰⁴

Manipulation may be optical, which also may have legal effects. For example, in order to manipulate motorists to slow down in certain areas, so-called ‘optical speed bars’ are used. They consist of white plastic strips that are placed on the road surface at decreasing lengths from each other, which gives the driver of a car the illusion that he or she is driving faster and faster, thereby causing him or her to slow down.⁷⁰⁵ The black letter law, complemented with road signs, determines how fast one may drive. However, technology that manipulates behaviour can also be effective in combatting speed-

703 Lessig, above n. 53, at p. 121.

704 Coleman, S., *The Minnesota Income Tax Compliance Experiment State Tax Results*, Minnesota Department of Revenue, 1996 available at http://www.revenue.state.mn.us/research_stats/research_reports/19xx/research_reports_content_compliance.pdf (last accessed on 2015-04-08).

705 Rondeaux, C., *An Optical Illusion Might Slow Drivers*, The Washington Post, 2006, available at <http://www.washingtonpost.com/wp-dyn/content/article/2006/05/03/AR2006050302306.html> (last accessed on 2015-04-08).

ing, especially if it is a complement to traditional law. Tailored content, referred to above, is also a form of technical manipulation, the danger here being that the manipulation is hidden from the manipulated:

But what happens when the motive is not so obvious? When options just seem to appear right when you happen to want them? When the system seems to know what you want better and earlier than you do, how can you know where these desires really come from? ... profiles will begin to normalize the population from which the norm is drawn. The observing will affect the observed. The system watches what you do; it fits you into a pattern; the pattern is then fed back to you in the form of options set by the pattern; the options reinforce the pattern; the cycle begins again.⁷⁰⁶

One of the main arguments against the use of manipulation are the moral and ethical implications. In an open and democratic society, there should be transparency; instead the use of manipulation threatens privacy.⁷⁰⁷ An additional threat in the commercial setting is the lack of attention paid to the effects of manipulation on individuals.

Psychological manipulation may also have a negative connotation, as in the below definition. It is described as the act of finding out the psychological vulnerabilities of a person in order to influence that person's behaviour:

Psychological manipulation changes the perception or behavior of others through underhanded, deceptive, or even abusive tactics. Such methods are often considered as exploitative, abusive, devious, and deceptive. It is often used in an attempt to control the behavior of others. It uses various forms of psychological abuse, brainwashing or bullying, emotional blackmail, to coerce others to do things which they naturally do not want to do.⁷⁰⁸

Here the ethical dimension arises in that while the goals of manipulation may be good, such as saving lives by getting people to drive more slowly, the actual mechanism of manipulation may have a negative implication.

706 Lessig, above n. 53, at p. 154.

707 Wahlgren, *Manipulation*, above n. 702, at p. 151.

708 US Legal Definitions, *Psychological Manipulation Law and Legal Definition*, available at <http://definitions.uslegal.com/p/psychological-manipulation%20/> (last accessed on 2015-12-14).

The notion of manipulation also derives its importance from its close association with democracy. According to Schwartz, a person's capability of reflection must be insulated from manipulation and coercion and consequently from certain acts of data collection.⁷⁰⁹ He highlights the notion of democracy as not being just gathering of the group in the town square, be it situated in the digital environment or off-line. Rather, democracy requires a capacity for individuals to be able to act on the notion of the good, when considering how to live their lives.⁷¹⁰ This notion of self-determination is threatened by the actions of private or governmental entities that control an individual's reasoning process and 'colonize' a person's thinking process.⁷¹¹

4.9.1 Unfair Commercial Practices Directive

A practical example of manipulation is illustrated within the context of unfair commercial practices where the Unfair Commercial Practices Directive is applicable.⁷¹² The main aims of this Directive are to increase consumer confidence as well as make it easier for businesses to carry out cross-border trading.⁷¹³ One way of increasing consumer confidence is by outlawing business practices deemed threatening from a consumer perspective, for example, the provision of inaccurate information in relation to a product, or due to aggressive practices. An action is determined to be unfair if it is, according to Article 5(2)(a), contrary to professional diligence and if, according to Article 5(2)(b), '[i]t materially distorts or is likely to materially distort the economic behaviour with regard to the product of the average consumer ...'. Article 2(e) defines

709 Schwartz, *Privacy and Democracy in Cyberspace*, above n. 402, at p. 1653.

710 Ibid, at p. 1654.

711 Ibid, at p. 1656.

712 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive').

713 European Commission, *Unfair Commercial Practices Directive*, available at http://ec.europa.eu/consumers/consumer_rights/unfair-trade/unfair-practices/index_en.htm (last accessed on 2016-01-13).

the concept of ‘material distortion’ as, ‘to materially distort the economic behaviour of consumers’ means using a commercial practice to appreciably impair the consumer’s ability to make an informed decision, thereby causing the consumer to take a transactional decision that he would not have taken otherwise.’

It is submitted that the notion of manipulation is implied in the transactional test as enshrined in Article 2(e). It attempts to prohibit practices that result in the consumer taking action or making a decision that he or she would not ordinarily have made were it not for the unfair practice of the commercial actor. In other words, it can be argued that practices that manipulate the consumer into making a decision that he or she would not ordinarily have made, are deemed illegal.

4.9.2 Remarks

Manipulation can arise as a consequence of predictive modelling in the commercial setting and may be harmful in that it is applied without knowledge of those that it is applied on. Manipulation may exist as a legislative tool, however, this process is transparent (in Western democracies at least), since a lengthy public consultation process is the norm. The manipulation of the individual by commercial actors and using predictive modelling, on the other hand, is not as transparent.

Just as it is acknowledged in consumer protection legislation that consumers need protection from commercial actors in certain instances, so too, it is argued that individuals require protection from the undesired effects of predictive modelling. The manipulation within predictive modelling can be automatic, to a large extent machine based and far more discrete, in turn preventing its identification.

4.10 Lost Human Dignity

From the outset, it is noteworthy that entertaining the notion of ‘dignity’ is itself an indicator of a moral position, in that it is more associated with liberal

thinking entrenched in the deontological way of thinking.⁷¹⁴ The concept of human dignity is complex as its meaning is subject to a normative framework, which may differ from one context to another. Human dignity has been described as, ‘the preeminent value that every human be recognized as a full person, independently of his or her individual characteristics and social relations’.⁷¹⁵ The notion of dignity, it is argued, has a special function within the European privacy context as compared with the US context, where privacy law in the US is based on liberty.⁷¹⁶ The historical explanation was briefly addressed above in the context of reputation, where for centuries, only a few individuals of certain social status had access to the courts in order to enforce their respect and seek redress for their damaged dignity. Over time this ability was demanded by the masses with dignity eventually becoming a general norm entitled to all.⁷¹⁷ Human dignity is arguably being threatened by technology, where ‘philosophical humanism is threatened to the extent that humans are being rendered obsolete by machines’.⁷¹⁸

Dignity can be ascribed various labels. Brownsword and Goodwin distinguish between ‘faith-based dignity’, ‘human dignity as human nature’ and ‘dignity as autonomy’. A faith-based view of dignity has a divine or religious grounding where human beings, by virtue of their relationship with the Creator, should be afforded certain rights but also have certain obligations. ‘Human dignity as human nature’ has as its core the notion that humans share a human nature that is more important than individual autonomy. Finally, ‘dignity as autonomy’ sees the ability to reason as separating humans from other species, with the consequence that humans are able to best decide for themselves.⁷¹⁹

Brownsword and Goodwin refer to certain concepts as ‘boundary marking concepts’. These are concepts, they explain, that can be used in discussions about the desirability of certain technologies, and which mark the acceptable

714 Brownsword and Goodwin, above n. 384, at p. 190.

715 Belley, Jean-Guy, *The Protection of Human Dignity in Contemporary Legal Pluralism*, Springer Science and Business Media Dordrecht, 2013, at p. 3.

716 Whitman, James Q., *The Two Western Cultures of Privacy: Dignity versus Liberty*, Vol. 113, No. 6, Yale Law Journal, 1151, 2004, in Solove and Schwartz, above n. 517, at p. 1067.

717 Whitman, above n. 716, at p. 1067.

718 Belley, above n. 715, at p. 5.

719 Brownsword and Goodwin, above n. 384, at pp. 194-205.

border of a technology in relation to morality.⁷²⁰ In other words, these are concepts that draw the line for what is morally acceptable. Boundary marking concepts have certain distinguishing characteristics. First, they have the goal of being an instrument in determining the boundary of what technology is to be permitted. Second, they are not only concerned with prohibition. Third, a boundary marking concept may have within it a pre-defined notion of what is morally acceptable. For example, the notion that human dignity arises out of a religious belief in itself sets a boundary that is not open for negotiation. Fourth, boundary marking concepts do not exist in a vacuum, but rather reflect the norms of society, which themselves may not remain constant. A certain normative belief system will result in a certain boundary marking concept having a greater importance than another, for example, those encompassing normative outlooks associated with a religious belief.⁷²¹ The notion of human dignity as a boundary marking concept, therefore, has a specific function in relation to technological development. Boundary marking concepts have two functions, namely empowering and constraining, this dual function being supported by reference to Kant:

Every human being has a legitimate claim to respect from his fellow human beings and is in turn bound to respect every other. Humanity itself is a dignity; for a human being cannot be used merely as a means by any human being ... he is under an obligation to acknowledge, in a practical way, the dignity of humanity in every other human being.⁷²²

On the one hand, human dignity is seen as something empowering. It allows for humans, who are rational and have the ability to reason and think for themselves, to make decisions, which are best for them, considering the circumstances. It is here that human dignity connects with the notion of autonomy and is synonymous with freedom. On the other hand, this freedom is not absolute, as humans are required to acknowledge the human dignity of others. In this way, freedom and autonomy is curtailed and human dignity restricted in the sense that it is a guarantor of freedom in all human beings. The notion

720 Ibid, at p. 188.

721 Ibid, at p. 190.

722 Kant, Immanuel, *The Metaphysics of Morals*, translated and edited by Mary Gregor, Cambridge University Press, 1996, at p. 209, cited in Brownsword and Goodwin, above n. 384, at p. 193.

of human dignity is not only complex, but can be used to argue both sides of an issue. The above authors refer to the abortion debate, where human dignity can be empowering in that it can be used to argue for giving women the power to choose in situations that affect their bodies, yet on the other hand is restrictive in that it can be used to argue for the right to life of the unborn child, thus limiting the freedom of women to choose.⁷²³ The notion of ‘dignity as autonomy’ assumes that human beings are in the best position to make decisions for themselves as they know what is important to them. It is argued that human beings have dignity because they are able to identify what is important to them, in turn leading to the understanding that humans are fundamentally free, and it is upon this basis that dignity is thought of in terms of autonomy.⁷²⁴

4.10.1 Human Dignity and Law

The notion of human dignity finds expression in the law. The relationship between freedom and autonomy extends to the notion that people’s lives are valuable, a notion that is entrenched in Article 1 of the Universal Declaration of Human Rights (UDHR), which states that, ‘[h]uman beings are born free and equal in dignity and human rights’. For illustrative purposes, mention is made of the the notion of human dignity in the context of the regulation of technological advances within the area of bioethics. A memorandum to a draft of the Universal Declaration on Bioethics and Human Rights states, ‘that such development occurs within the framework of ethical principles that respect human dignity and protect human rights and fundamental freedoms, and ... prevent practices contrary to human dignity’.⁷²⁵ Reference is made below to two instances that place dignity in the legal context.

723 Brownsword and Goodwin, above n. 384, at p. 193.

724 Ibid, at p. 194.

725 Explanation to Article 2 of *Elaboration of the Declaration on Universal Norms on Bioethics: Third Outline of a Text* (Paris, August 2004), cited in Brownsword and Goodwin, above n. 384, at p. 195.

4.10.2 American Constitutional Law

The Fourth Amendment protects against searches that are indiscriminate and against searches conducted under ‘general warrants’, where no specific individual is suspected of wrongdoing.⁷²⁶ Lessig argues that this protection provided by the Fourth Amendment can be seen as having the function of protecting an individual’s dignity, therefore such searches are tolerated only where there are sufficiently strong suspicions that exist prior to the search.⁷²⁷ Historically, the Fourth Amendment was written to prevent abuse in connection with search and seizures where King George II and King George III would give their officers a ‘general warrant’ that enabled them to search through private homes seeking evidence of a crime, without any prior suspicion.⁷²⁸ It read as follows:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.⁷²⁹

Lessig, questioning the application of this Amendment to the technological context, puts forward the hypothetical scenario of an algorithm conducting a wide and indiscriminate search of all data, with a court providing permission for any action based on the information attained. The rationale subsequently provided by Lessig is that despite the search not being burdensome, the Fourth Amendment is applicable in that its aim is to protect a kind of dignity. Reference is also made to the concept of human dignity in the Eighth Amendment, where it is stated that, ‘[e]xcessive bail shall not be required, nor excessive fines imposed, nor cruel and unusual punishments inflicted’.⁷³⁰ This too has

726 Lessig, above n. 53, at p. 210.

727 Ibid.

728 Ibid, at p. 19.

729 Legal Information Institute, *The Fourth Amendment*, available at https://www.law.cornell.edu/constitution/fourth_amendment (last accessed on 2015-12-21).

730 Ibid.

been interpreted to suggest that even if a certain punishment were to effectively curtail crime, it should not be allowed, as it is contrary to human dignity.⁷³¹

4.10.3 European Patent Law

The notion of human dignity is also referred to in European Patent law. This has occurred in the context of technological developments within the sphere of biotechnological inventions, where the issue of morality has received attention. The main aim of the patent system is to protect technical inventions, which is achieved by the granting of exclusive rights to patent applicants fulfilling the formal and substantive patentability criteria.⁷³² Developments within the biotechnological sphere have brought to the fore issues of morality and ethics, which in turn focusses attention on the notion of dignity.

In Patent law, certain inventions are considered unpatentable due to their being contrary to a certain moral standard. For example, Preamble 38 of Directive 98/44/EC on the Legal Protection of Biotechnological Inventions, in reflecting upon the notion that certain inventions are beyond a discussion of morality and therefore unpatentable, by referring to the notion of ‘order public’, states that certain inventions are not patentable due to their being contrary to human dignity.⁷³³ This example portrays how human dignity has made its way into Patent law, where it forms the basis for determining which technological developments within the biotechnological sphere should be disallowed due to their moral unacceptability.

731 Brownsword and Goodwin, above n. 384, at p. 9, citing *Roper v. Simmons* 543 US 551 (2005).

732 Hellstadius, Åsa, *A Quest for Clarity – Reconstructing Standards for the Patent Law Morality Exclusion*, Doctoral Thesis in Civil Law at Stockholm University, Sweden, 2015, at p. 61.

733 Directive 98/44/EC of the European Parliament and of the Council of 6 July 1998 on the Legal Protection of Biotechnological Inventions.

4.10.4 Remarks

Human dignity is a concept that can be utilized in order to determine the ethical boundaries of technology, also relevant within the predictive modelling setting. Lessig's scenario above occurs within the individual versus Government scenario, where the injury to dignity resulting from an unjustified Government search should act as a limit on the Government's power. While limiting administrative power, a similar limit can be argued to be of significance in the commercial setting. Within human rights law, as will be shown hereunder, states have a duty to limit the human rights abuses of companies within their jurisdictions while companies also have certain human rights obligations. In this manner Constitutional law becomes relevant to the commercial setting.

The importance of a concept like dignity is its function as a boundary marker designating the area of acceptability in relation to developing technology. In addition, some would suggest it is also a human quality that is worth protection. In this sense, the extent to which predictive models erode individual dignity is important to note. Dignity is also important from the societal perspective, the German Constitutional Court stating that, '[h]uman dignity means not only the human dignity of the person but the dignity of man as a species. Dignity is therefore not at the disposal of the individual'.⁷³⁴

4.11 Lost Human Identity

Starting with a perspective on identity-building, from the disciplines of philosophy and psychology, this section examines the effect of predictive modelling on the human identity creation process referred to as the 'narrative identity'. This is then juxtaposed with another identity creation process, namely the 'database discourse', which has its basis in technology. The potential harm to the individual resulting from predictive modelling is framed in the comparison between these two processes of identity creation.

734 BVerfGE 45, 187, 229 (1997), cited in Brownsword and Goodwin, above n. 384, at p. 196, footnote 23.

4.11.1 The Narrative Identity

‘Narrative identity’ is a theory regarding individual identity creation, from within both the disciplines of philosophy and psychology. The philosopher Ricoeur, in constructing the theory of narrative identity, argued that it is a means of bridging the distinction between the idem and ipse identities, that make up the individual identity.⁷³⁵ The narrative identity has the following attributes: first, ‘knowledge of the self is an interpretation’, second, ‘the interpretation of the self, in turn, finds narrative, among other signs and symbols, to be privileged mediation’ and third, ‘this mediation borrows from history as much as fiction making the life story a fictive history or, if you prefer, an historical fiction, comparable to those biographies of great men where both history and fiction are found blended together’.⁷³⁶ Narrative identity is a dynamic manner of identity creation through the narrative, be it in writing or orally, where individuals acquire an understanding of their own identity by telling stories about themselves.⁷³⁷ Also, within the discipline of psychology, McAdams put forward a theory of narrative identity.⁷³⁸ Here too, the narrative identity is depicted as the story of the self, which has the function of integrating a person’s life with time and culture, providing a subjective story of how a person came to be and where his or her life may be going.⁷³⁹ A formal conceptualisation of the narrative identity states the following:

Narrative identity is the internalized and evolving story of the self that a person constructs to make sense and meaning out of his or her life. The story is a

735 Ricoeur, Paul, *Narrative Identity*, *Philosophy Today*, 35:1, Springer, 1991, at p. 73, (The original article was published in French as *L’identité narrative* in *Esprit* nos 7-8 (1988), 295-304, translated by Mark. S. Muldoon), at p. 74.

736 Ibid.

737 Dauenhauer, Bernard, *Paul Ricoeur*, *Stanford Encyclopedia of Philosophy*, available at <http://plato.stanford.edu/entries/ricoeur/> (last accessed on 2015-05-29).

738 McAdams, Dan P., *The Psychology of Life Stories*, *Review of General Psychology*, Vol. 5, No. 2, 2001, at p.100.

739 McAdams, Dan P., *Narrative Identity*, in Schwartz, Seth J., Luyckx, Koen and Vignoles, Vivian L., (eds.), *Handbook of Identity Theory and Research*, Springer, 2011, at p. 111.

selective reconstruction of the autobiographical past and a narrative anticipation of the imagined future that serves to explain, for the self and others, how the person came to be and where his or her life may be going.⁷⁴⁰

It is an internalized story of the self and is dynamic in that it is constantly evolving. It can have a setting, scenes, plot and themes and is a construct of the past and imagines the future, with individuals constantly able to alter the self as situations change and as time passes.⁷⁴¹

4.11.2 The Database Discourse

Another narrative, which has a technological foundation, is the ‘database discourse’. This term originates from Poster who notes that computerized databases function as discourses and have their own ‘rules of information’, being linguistic configurations that constitute individuals according to these rules of information.⁷⁴² The lens used by Poster to view the social role of the database investigates the relationship between language and the constitution of humans. Just as with individuals, who have a narrative with which to mold their identity, so too do databases have a certain discourse, which differs from that used by individuals.⁷⁴³ Essentially, the human narrative is transformed into a database discourse, which has the function of creating a proxy identity of the individual.⁷⁴⁴ There are a number of ways of seeing databases: the Marxist view on databases perceives them in the context of the power struggle between companies and individuals and the Liberal view on databases sees them in the context of the power that government exerts over its population. Poster, in

740 Ibid, at p. 99.

741 Ibid, at p. 102.

742 Poster, Mark, *Databases as Discourses; or, Electronic Interpellations*, in Lyon, David, and Zureik, Elia (eds.), *Computers, Surveillance and Privacy*, University of Minnesota Press, 1996, at p. 175.

743 Franko Aas, *From Narrative to Database: Technological Change and Penal Culture*, *Punishment and Society*, Sage Journals, Vol. 6, Issue 4, 2004, available at <http://pun.sagepub.com/content/6/4/379.abstract> (last accessed on 2015-06-02), at p. 379.

744 Poster outlines the notion of the database discourse by referring to the manner in which they constitute the individual, see Poster, *The Mode of Information*, above n. 334, at pp. 69-98.

referring to these ‘other’ views on databases, is critical of the fact that they tend to miss the discursive effects of databases, and do not take into account the effect of language on the subject.⁷⁴⁵ He remarks that it is often forgotten that databases are composed of symbols, and that they are representations of something.⁷⁴⁶ They are a tool with a function and a purpose and consideration should be taken of the fact that they are structured in a certain manner with a certain functionality in mind. And the manner in which databases are constructed are a form of language. According to Poster, databases constitute individuals according to columns and rows, creating relationships between information, these relationships non-existent outside of the database.⁷⁴⁷ The agency, using the database, constitutes the individual according to these pre-defined parameters.⁷⁴⁸ This results in a de-contextualization and a standardized view of identity.⁷⁴⁹ Calhoun refers to the concept of ‘categorical identity’, which is the categorization of individuals according to social categories, which results in a circumstance that:

... allows a kind of abstraction from the concrete interactions and social relationships within which identities are constantly negotiated, in which individuals present one identity as more salient than other, and within which individuals achieve some sense of personal continuity and balance among their various sorts of identities ... The abstractness of categories encourages framing claims about them as though they offered a kind of trump card over the other identities of individuals addressed by them. This encourages an element of repression within the powerful categorical identities.⁷⁵⁰

Franco Aas refers to the database discourse theory in her examination of the penal system, making a number of points: first, the information amassed becomes much easier to disseminate, with the penal system becoming more transparent and accountable and second, the traditional practice of penal sys-

745 Poster, *Databases as Discourses*, above n. 742, at p. 175.

746 Ibid, at p. 176.

747 Poster, *The Mode of Information*, above n. 334, at p. 96.

748 Ibid.

749 Franko Aas, above n. 743, at p. 379.

750 Calhoun, Craig, *Critical Social Theory: Culture, History, and the Challenge of Difference*, Blackwell, 1995, at p. 220.

tem narration may have to adjust itself in order to fit into the database discourse, stating that, ‘... the new cultural and linguistic situation may transform the process of creating offenders’ identities. The stories of violence, pain, social deprivation and frustration now need to be told within the new parameters’. A poignant question, she asks, is whether the stories of the inmates, after being transformed into the database discourse, remain the same stories.⁷⁵¹

A relevant example in this regard is the recent introduction by French authorities of a Bill in relation to immigration. In order to reduce immigration to France, immigrants applying for entry into the country based on a family member already living there, would be allowed to submit a DNA sample in order to prove a connection to that family member, thereby proving eligibility for entry into the country. Here, it is genetic data that is the main factor determining a person’s identity as opposed to ‘biographic narratives’.⁷⁵² In other words, the digital identities created from data act as a proxy for people, and are increasingly being used as a means of establishing identity, as opposed to the person being given the opportunity to explain who he or she is.

4.11.3 Accompanying Themes

The following ideas are useful as a complement to contextualize the database discourse. First, technology is never neutral. Postman argues this point of view stating that, ‘embedded in information technology, as in every other tool, is an “ideological bias” – a predisposition to construct the world as one thing rather than another, to value one thing over another, to amplify one sense of skill or attitude more loudly than another’.⁷⁵³ In addition, we are urged not to see technology as apolitical, without social actors, but rather as being closely connected to society and culture, where new technologies are created with a certain purpose in mind when they are conceived.⁷⁵⁴ Franco Aas also questions

751 Franko Aas, above n. 743.

752 Rouvroy and Poulet, above n. 436, p. 51.

753 Postman, Neil, *Technopoly: The Surrender of Culture to Technology*, Vintage Books, 1993, at p. 13.

754 Williams, Raymond, *Televisions, Technology and Cultural Form*, Fontana, 1974, at p. 7.

the neutrality of technology, considering it a tool through which the actual nature of penal knowledge is being changed.⁷⁵⁵

A second observation of importance in the context of the database discourse regards the notion of knowledge and the manner in which society is structured in relation to this knowledge. Böhme states:

In order for a society to be controllable through knowledge, it must itself be organized in terms of knowledge. Social processes must be differentiated according to function and arranged according to models, and social actors must be disciplined in a way that makes their behaviour amenable to data collection or makes their social roles and activities relevant only insofar as they produce data.⁷⁵⁶

A third observation is provided by Manovich. He states that databases have a cultural influence, and that while they were created as a mechanism by which computers would store and retrieve data, they are becoming, ‘a new form of cultural expression’, where the world is expressed as a collection of items, against which various operations can be run. In addition, they are not governed by the law of cause and effect, they do not tell stories and they do not have a beginning and an end nor any thematical development. He states, therefore, that the database is the opposite of the narrative, which has thus far been the preferred form of cultural expression. Manovich in turn describes the internet in this vein, stating that it has an ‘anti-narrative logic’ due to the fact that it can change over time and does not have the same logical build-up as a story, where every page on the internet can in fact be the first page.⁷⁵⁷

A fourth observation concerns database information, more specifically how it differs from the human narrative. The information or data in a database can be described as having certain qualities. First, it is ‘byte-like’ whereas:

Narrative as in the novel works form a beginning, middle and end. The subjective intentions of the protagonist are the motor of the plot and events follow from one another as causes and effects. Discourse – as in say philosophic or social scientific texts – is comprised in conceptual frameworks, of serious

755 Franko Aas, above n. 743.

756 Böhme in Ericson, Richard V., and Haggerty, Kevin D., *Policing the Risk Society*, Oxford University Press, 1997, at p. 46.

757 Manovich, Lev, *The Language of New Media*, MIT Press, 2001, at p. 225.

speech acts, of propositional logic, of speech acts backed up by legitimating arguments. Information is none of these.⁷⁵⁸

In addition, information is 'indexical' in that 'it has an effect on you without the sort of legitimate argument that you are presented with in a discourse'.⁷⁵⁹ Franco Aas, in reflecting on this, in turn refers to risk assessment guidelines and sentencing guidelines, characterised by a lack of narration, with no beginning, middle and ending, and having no sequence and being able to be completed in any order.⁷⁶⁰

4.11.4 Remarks

The database is a central component of many predictive models, despite the trend towards accessing more unstructured forms of data. Historical data, representing real life stories, yet stored in the neat rows and columns of the database, is parsed by the algorithm, which applies the examples represented in the database, to new scenarios.

The above results in a conflict. It is a conflict between two narratives – the narrative identity on the one hand and the database discourse on the other. Alternatively phrased, the database and narrative are 'natural enemies'.⁷⁶¹ It is a conflict for supremacy between the individual's digital identity as created by means of the database discourse and the individual's own narrative identity. Predictive modelling, incorporating databases, reduces the individual's ability to compose his or her own identity, the database becoming an obstacle to the human narrative. This is disempowering for individuals.

758 Lash, Scott, *Critique of Information*, Sage Publications, 2002, at p. 2.

759 Ibid, at p. 3.

760 Franko Aas, above n. 743, at p. 385.

761 Manovich, above n. 757, at p. 225.

4.12 Summary and Conclusions

The above section examined the potential harms associated with predictive modelling. Some observations are necessary in this regard. The harms are considered potential to the extent that they do not necessarily exist in every case where predictive modelling has been used or partly relied on. However, it is necessary to flag the possibility that the process may inflict some measure of harm covered by the above inventory. A common denominator among the above harms is the manner in which they negatively influence personal autonomy by shrinking its ambit of influence. For example, privacy relies on autonomy and manipulation involves influencing personal autonomy, by altering the ability of individuals to make decisions freely and without being hindered.

Apparent from the above inventory is the effect of digitalization on society and the manner in which the internet is challenging the traditional notion of what is harmful. It is within this context that the existential question regarding the future of humanity within the digital environment becomes relevant. In other words, consideration needs to be taken of the diminishing margin of influence that humans are able to have on their environment and communications, in the onslaught of digital decision-making systems that act as intermediaries between humans and their contact with others via the digital environment.

The above harms were placed in a legal perspective. Some of them are already recognized in the law, such as the harm to reputation, whereas others will become more established as they acquire publicity and are identified as a harm from which society requires protection. It is in this context that the role of the law becomes relevant and the reason why the next chapter investigates the extent to which autonomy and predictive modelling are addressed by traditional legal frameworks.

5 The Data Privacy Legal Regime

5.1 Introductory Remarks

This chapter addresses predictive modelling using the ‘data privacy’ legal framework. This legal regime is judged to be the most applicable to predictive modelling considering that it is technology centred with the aim of protecting personal integrity. This chapter illuminates the challenges posed by predictive modelling for the current data privacy regime, considering the potential harms resulting from predictive models. A brief examination will be made of how the instruments comprising the data privacy legal regime are positioned to address the potential harms resulting from predictive modelling as well as ensure an adequate level of personal autonomy. To this end, a brief historical overview of the development of data privacy will be provided.

Data privacy is approached from the European perspective. This chapter discusses the legal redress a person situated in Europe would have under EU law and/or the ECHR if subjected to the technology of predictive modelling. The notion ‘data privacy’ represents both privacy and data protection, each of these areas being represented by a different international legal regime in turn developed by separate political entities. One applicable international legal regime is human rights law, which is a branch of public international law and within the European context there are a number of institutions and corresponding legal frameworks that are relevant. Of these, the CoE’s ECHR is considered the most relevant for two reasons. First, the case law from the ECtHR is the most well-developed. Second, only the CoE has legislative and judicial functions essential for developing human rights law.⁷⁶² The second applicable legal regime, representing the data protection notion, is the EU data protection regime. Within the European legal space the legal structures of both the CoE and EU operate. A complication when examining privacy and data protection

762 Greer, Steven, *Europe*, in Moeckli, Daniel, Shah, Sangeeta and Sivakumaran, Sandesh (eds.), *International Human Rights*, Oxford University Press, 2014, at p. 417.

is that there is no clear distinction between these two legal regimes, and they do in fact overlap. One of the reasons for this overlap is the fact that the areas of privacy and data protection are so tightly interwoven, especially within the constitutional instruments and case law of these two actors. This has resulted in speculation as to how the interaction between these two actors should be viewed.

In examining the privacy and data protection legal regimes, cognizance is taken of recent case law, which is also interesting to the extent that it is an indicator of future trends.

5.2 Two Actors within the European Legal Space

The two main protagonists within the European legal space are the CoE, which represents human rights and created the ECHR, and the EU, which developed an extensive data protection framework in the form of the Data Protection Directive (DPD) and the forthcoming General Data Protection Regulation (GDPR). This section provides a brief account of these two political actors. In addition, considering that the areas of application of their respective data privacy instruments are so interdependent and intertwined, a brief description will be made concerning how data privacy is referred to within the respective constitutional instruments.

5.2.1 The Council of Europe (CoE)

The CoE was founded in Strasbourg in 1949 by ten West European liberal democracies.⁷⁶³ It has generated approximately 200 treaties, the most well-known being the ECHR.⁷⁶⁴ In 1950 the Member States of the CoE signed the

763 Ibid. The founding states were Belgium, France, the United Kingdom, Denmark, Ireland, Italy, Norway, Sweden, Luxembourg and the Netherlands.

764 Ibid.

ECHR⁷⁶⁵, which entered into force in 1953.⁷⁶⁶ There were two main reasons for the creation of the ECHR: first, an attempt to prevent a repeat of the human rights violations that took place during World War II and second, as a measure to protect Member States against the spread of Communism.⁷⁶⁷ Therefore, the four main objectives of the CoE were to prevent another war in Europe, a statement of common values (opposing Communism), to establish a common identity in the face of the cold war and to provide a warning for any authoritarian tendencies arising in any member state.⁷⁶⁸ Another reason for the creation of the ECHR was the frustration with the length of time that it was taking to reach agreement on the provisions of the ICCPR and ICESCR (18 years) being developed under the auspices of the UN.⁷⁶⁹ At the start, the main aim of the ECHR was to allow for settling differences between states, where human rights was the means for encouraging international cooperation.⁷⁷⁰

5.2.2 The European Union (EU)

In 1951 the European Coal and Steel Community was founded by six Member States, integrating the French and German coal and steel industries, thereby decreasing the future risk of conflict between these two nations. In 1957, the Treaty of Paris resulted in the Treaties of Rome, which created the European Atomic Energy Community and the European Economic Community (EEC).⁷⁷¹ In 1965 the EEC amalgamated with the European Coal and Steel

765 Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5.

766 Dixon, Martin, *Textbook on International Law*, sixth edition, Oxford University Press, 2007, at p. 353.

767 Ovey Clare and White, Robin, Jacobs and White, *The European Convention on Human Rights*, fourth Edition, Oxford University Press, 2006, at p. 2.

768 Greer, above n. 762, at p. 418.

769 Bring, Ove, Mahmoudi, Said and Wrangle, Pål, *Sverige och folkrätten*, fourth edition, Norstedts, Juridik, 2011, at p. 212.

770 Greer, above n. 762, at p. 423.

771 Schütze, Robert, *European Union Law*, Cambridge University Press, 2015, at p. 5.

Community and the European Atomic Energy Community to create the European Communities (EC).⁷⁷² In 1992 the EU was formed by means of the Maastricht Treaty, where the identity of the EC was incorporated into the ‘first pillar’ with a common foreign and security policy being the ‘second pillar’ and justice and home affairs the ‘third pillar’.⁷⁷³

EU law can be divided into primary EU law and secondary EU law. The former comprises treaties, the EU Charter, protocols and declarations. Primary EU law includes the Treaty on the European Union (TEU), Treaty on the Functioning of the European Union (TFEU), Charter of Fundamental Rights of the EU (EU Charter) and the General Principles of EU law, whereas secondary EU law is comprised of International Agreements and Secondary legislation (Regulations, Directives and Decisions).⁷⁷⁴ Secondary EU law comes into being by means of adoption by the EU institutions that have been granted the authority to do so according to the above treaties.⁷⁷⁵

Article 288 TFEU states the following:

To exercise the Union's competences, the institutions shall adopt regulations, directives, decisions, recommendations and opinions. A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States. A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods. A decision shall be binding in its entirety. A decision which specifies those to whom it is addressed shall be binding only on them. Recommendations and opinions shall have no binding force.

Another integral institution of the EU is the Court of Justice of the European Union (CJEU), previously referred to as the European Court of Justice (ECJ), which according to Article 19(1) TFEU has the function of interpreting EU law, making sure that it is applied consistently in every EU country and providing remedies in order to ensure protection in accordance with the scope

772 Greer, above n. 762, at p. 435.

773 Ibid, at p. 435.

774 Ibid.

775 European Union Agency for Fundamental Rights, Council of Europe, *Handbook on European Data Protection Law*, 2014, at p. 17.

of EU law.⁷⁷⁶ The CJEU has the jurisdiction to review the legality of legislative acts (Article 263 TFEU) and to provide preliminary rulings concerning the interpretation of the Treaties and the validity of acts of the EU institutions (Article 267 TFEU). Where such a question has been raised before a court in a Member country, it may send the matter to the CJEU for a ruling. In such a case, the CJEU is able to make a ruling only on the facts submitted and the matter is usually referred back to the national court to make a judgement in light of the CJEU's interpretation.⁷⁷⁷

5.2.3 The Council of Europe and European Union Regulatory Interplay

Considering the establishment and roles of both the CoE and EU, the European legal sphere incorporates two organizations implementing separate transnational legal regimes that intersect each other with respect to certain issues. One such intersection is that of data privacy, where both the CoE and EU address the notions of privacy and data protection, both being recognized as fundamental rights. The historical goals of these two organizations are relevant when studying this interplay as well as the manner in which they have influenced each other. The main post-World War II goal in Europe was the establishment of a lasting peace, something that the above two organizations aspired to. However, the route to the achievement of this common goal was different, with the CoE preferring the protection of human rights and the EU preferring the establishment of the integrated market in order to achieve this end.⁷⁷⁸ Initially distinguishable, the ability to maintain this distinction soon collapsed, with the CJEU as early as the 1960's identifying human rights as falling within its ambit of jurisdiction.⁷⁷⁹ The interplay between the CoE and

776 Trzaskowski, Jan, *EU Law and the Internet*, in Trzaskowski, Jan, Savin, Andrej, Lundqvist, Björn and Lindsoug, Patrik, *Introduction to EU Internet Law*, Ex Tuto Publishing, 2015, at p. 19.

777 *Ibid*, at p. 24.

778 Andersson, Helene, *Dawn Raids under Challenge: A Study of the European Commission's Dawn Raid Practices in Competition Cases from a Fundamental Rights Perspective*, Doctoral Thesis in European Law at Stockholm University, Sweden, 2017, at p. 96.

779 *Ibid*, at p. 97.

the EU is illustrated by the manner in which fundamental rights, and especially human rights, not only came to be included within the ambit of the CJEU's jurisdictional competence but also ignited a conflict between the CJEU and some courts within the Member States.

The ECHR is a legal instrument protecting human rights and promoting the rule of law, democracy and social development.⁷⁸⁰ However, it is also viewed as a data protection instrument, as facilitated by Article 8 ECHR.⁷⁸¹ This is evident from the case law of the ECtHR, where data protection has been interpreted to fall within the scope of the right to private life as enshrined by Article 8 ECHR. It is noteworthy that a large proportion of the case law from the ECtHR concerns data protection in relation to the actions of states, for example the interception of communications, surveillance practices and the storage of data.⁷⁸² Therefore, while there are a few cases where the actions of private entities invoked the data protection function of Article 8 ECHR, the main thrust of the application of data protection principles by the ECtHR has occurred within the realm of the state surveillance practices.⁷⁸³

The CJEU initially refrained from the adjudication of human rights matters, but it soon began to hear these matters. The fact that the applicable statutory legislation made no reference to human rights became problematic as cases relating to human rights started to come before the CJEU with more frequency. An initial response from the CJEU was the refusal to deal with cases concerning fundamental rights.⁷⁸⁴ A pivotal point, however, was the development of the doctrines of supremacy and direct effect by the CJEU, which in turn forced it to start adjudicating such matters.⁷⁸⁵ The doctrine of supremacy, established in *Costa v. ENEL*, stated that any law in a Member State contradicting EU law should be ignored by national courts.⁷⁸⁶ The doctrine of direct effect, established in *Van Gend en Loos*, stated that the preliminary ruling

780 European Union Agency for Fundamental Rights, above n. 775, at p. 14.

781 Ibid.

782 Ibid.

783 Bygrave, *Data Privacy Law*, above n. 69, at p. 86.

784 Andersson, above n. 778, at p. 98.

785 Ibid.

786 Case 6/64, *Flaminio Costa v. E.N.E.L.*, EU:C:1964:66.

procedure had as an aim the uniform interpretation of the Treaty by the national courts of the Member States, a consequence being the ability for individuals to rely on EU law in argument before a national court.⁷⁸⁷

The response in some Member States to the development of the doctrines of supremacy and direct effect was negative. For example, German and Italian constitutional doctrine and case law refused to accept them, the main sticking point being the supremacy of Community law, which did not protect human rights to the same extent as the constitutions of Member States.⁷⁸⁸ This conflict was reflected in case law both from the CJEU and, for example, the German courts. In the matter of *Stauder*⁷⁸⁹ the CJEU stated that the fundamental rights of persons were to be considered a part of the general principles of EU law.⁷⁹⁰ Thereafter, in the case of *Internationale Handelsgesellschaft*⁷⁹¹, the CJEU held that not even a fundamental rule in a constitution of a Member State was above EU law, thereby affirming the supremacy of EU law. In the case of *Nold*⁷⁹², the CJEU referred to guidelines for EU law found in treaties which Member States had ratified and which pertained to fundamental rights. In response, the German Constitutional Court stated in ‘*Solange I*’⁷⁹³ that it would uphold basic fundamental rights to the extent that they conflicted with Community law, that is, to the extent that Community law did not include a corresponding catalogue of rights comparable with the Basic Law of Germany.⁷⁹⁴ Finally, in *Rutili* explicit reference was made to the ECHR as a source of inspiration.⁷⁹⁵

787 Case 26/62, *NV Algemene Transport- en Expeditie Onderneming van Gend & Loos v. Netherland Inland Revenue Administration*, EU:C:1963:1.

788 Rosas, Allan, *Fundamental Rights in the EU, with Special Emphasis on the Case-law of the European Court of Justice (Luxembourg)*, in Alfredsson, Gudmundur, Grimheden, Jonas, Ramcharan, Bertrand G. and de Zayas, Alfred (eds.), *International Human Rights Monitoring Mechanisms: Essays in Honour of Jacob Th. Möller*, Brill Academic Publishers, 2009, at p. 580.

789 Case 29/69 *Erich Stauder v. City of Ulm*, EU:C:1969:57.

790 Rosas, above n. 788, at p. 580.

791 Case 11/70, *Internationale Handelsgesellschaft*, EU:C:1970:114, paras. 3 and 4.

792 Case 4/73, *Nold*, EU:C:1974:51, para. 13.

793 Order of 29 May 1974, BVerfGE 37, 271.

794 Rosas, above n. 788, at p. 581.

795 Case 36/75, *Rutili*, EU:C:1975:137.

Two aspects characterise the above interplay. First, fundamental rights made their way into EU law via the CJEU and can be characterised as ‘judge-made law’.⁷⁹⁶ Second, faced with opposition by various national courts to the CJEU’s progression to accepting fundamental rights as falling within its jurisdiction, the CJEU took the view that fundamental rights were an integral part of EU law and that they were to be recognized as general principles of law.⁷⁹⁷ It is within this context that human rights protection became a general principle of EU law.⁷⁹⁸

On the 7th of December 2000 in Nice, the EU proclaimed the Charter of the Fundamental Rights of the European Union (EU Charter). At this stage, however, it was a political document and not legally binding.⁷⁹⁹ It brought together all the fundamental rights protected within the EU, that is those rights referred to by the CJEU, the rights and freedoms elaborated on in the ECHR and the rights found in various constitutional traditions of EU countries. The Treaty of Lisbon came into force on the 1st of December 2009.⁸⁰⁰ Up until this point, the fundamental rights that were being applied in the EU existed only as general principles of law, becoming established law with the coming into force of the Treaty of Lisbon.⁸⁰¹ The Treaty of Lisbon also altered Article 6 of the TEU: Article 6(1) states that the EU Charter shall have the same legal status as the Treaties, Article 6(2) states that the EU shall accede to the ECHR and Article 6(3) states that the fundamental rights laid out in the ECHR shall constitute general principles of EU law. In this manner, the EU Charter became binding on all EU institutions as well as the national governments of the Member states.⁸⁰² The Treaty of Lisbon also did away with the three pillars structure of the EU, which in turn acquired a consolidated personality.⁸⁰³ Article

796 Rosas, above n. 788, at p. 580.

797 Andersson, above n. 778, at p. 99.

798 European Union Agency for Fundamental Rights, above n. 775, at p. 20.

799 Ibid.

800 [2012] OJ C326/02.

801 Lenaerts, Koen and Gutiérrez-Fons, José Antonio, *The Place of the Charter in the EU Constitutional Edifice*, in Peers et al. (eds.), *The EU Charter of Fundamental Rights: A Commentary*, Hart Publishing, 2014, at p. 1559.

802 EU Charter of Fundamental Rights available at http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm (last accessed on 2016-12-06).

803 Greer, above n. 762, at p. 435.

52(3) of the EU Charter addresses the overlapping different legal regimes as far as fundamental rights is concerned:

In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.

Also noteworthy is that the rights as set out in the EU Charter are not absolute in nature, with Article 52(1) allowing for limitations to be imposed on the enshrined rights as long as these limitations are founded in law, respect the rights concerned and are necessary taking proportionality into account. Article 52(1) reads:

Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

Prior to the Treaty of Lisbon, the CJEU, in identifying and applying general principles of law, did so by referring not only to principles common to all the Member States but also by looking to international agreements that Member States signed, and the ECHR was no exception in this regard.⁸⁰⁴ Consequently, the national constitutions of the Member States, the ECHR and EU law have all affected each other to some degree and by means of ‘cross-fertilisation’.⁸⁰⁵ The situation has been altered somewhat, by the Treaty of Lisbon, where the EU Charter has taken on a central role at the expense of the general principles of law.⁸⁰⁶ However, the role of the CJEU, in resorting to general principles of law, is not curtailed by the EU Charter and this gap-filling function of the CJEU may still be relevant, especially where a certain flexibility is required in order to be able to recognize new fundamental rights, since this flexibility

804 Lenaerts and Gutiérrez-Fons, above n. 801, at p. 1559.

805 Ibid, at p. 1560.

806 Eckes, Christina, *EU Accession to the ECHR: Between Autonomy and Adaption*, *The Modern Law Review*, Vol. 76, No. 2, 2013, at p. 258.

is not inherent in the EU Charter.⁸⁰⁷ The importance of this function becomes apparent in light of the argument that a reading of Article 6(1) TEU and Article 51(2) of the EU Charter leads to the opinion that the EU Charter cannot be used for this gap-filling function, as it cannot be applied to situations not foreseen by the authors of the treaties.⁸⁰⁸

5.3 Data Privacy

The importance of a nomenclature should not be underestimated, and this is especially so concerning ‘data privacy’, which has become the modern term incorporating both the privacy and data protection notions. In the American context, the term ‘privacy’ is most commonly used within the public, academic and judicial spheres, while other terms such as ‘liberty’, ‘freedom’ and ‘autonomy’ are also referred to in the privacy context.⁸⁰⁹ Privacy’s function in addressing the fears of increased computerization has occurred within this wider context.⁸¹⁰ Within the European privacy context, the focus has shifted to technology. A consequence of this is the reference to the term ‘data protection’, originating from the German ‘Datenschutz’.⁸¹¹ Just as with privacy, the meaning of ‘data protection’ is not completely settled, which is evident when studying its translation into the national legislation of the EU Member States, for example in Sweden, where it is termed ‘the protection of personal integrity’.⁸¹² In addition, it is noteworthy that ‘data protection’ both has privacy as its sphere of protection and also encapsulates other interests that require protection.⁸¹³ The context of the privacy debate is also relevant, in that in the US, the focus is on the individual, where terms such as ‘individuality’, ‘autonomy’, ‘dignity’, ‘emotional release’, ‘self-valuation’ and ‘inter-personal relation-

807 Andersson, above n. 778, at p. 114.

808 Lenaerts and Gutiérrez-Fons, above n. 801, at p. 1575.

809 Bygrave, Lee, *Privacy Protection in a Global Context*, above n. 69, at p. 320.

810 Ibid, at p. 23.

811 Ibid, at p. 26.

812 Ibid, at p. 321.

813 Bygrave, *Privacy and Data Protection in an International Perspective*, above n. 69, at p. 168.

ships' are referred to, while in Europe, concern is more with creating conditions within society that encourage public participation and therefore democracy.⁸¹⁴

The term 'data privacy' can be said to be gaining in popularity and replacing the terms 'privacy' and 'data protection'.⁸¹⁵ It is gaining popularity in the US and in Europe, in part due to its ability to communicate the norms and rationale that form its basis.⁸¹⁶ The term 'data privacy' is effective in two ways. First, it reflects the normative basis that lies at its centre, and second, it functions as a bridge over the Atlantic, reconciling the European and American attitudes to privacy and data protection.⁸¹⁷

5.3.1 The Symbiosis Between Data Protection and Privacy

Notwithstanding the close ties between the above two concepts, a clear distinction is made within the European context, between data protection and privacy. The most significant manifestation of this is found within the EU Charter, where data protection was granted the status as a legal right separate from the legal right to privacy. A joint reading of Articles 7(1) and 8 confirms that privacy and data protection are to be treated as separate rights.⁸¹⁸ Article 7(1) covers 'respect for private and family life', and states that, '[e]veryone has the right to respect for his or her private and family life, home and communications', while Article 8 guarantees the protection of personal data, stating that, '[e]veryone has the right to the protection of personal data concerning him or her'. Data protection is also addressed by the TFEU, Article 16(1) stating that, '[e]veryone has the right to the protection of personal data concerning them'. For some time now the right to privacy has existed within the EU as a

814 Bygrave, *Privacy Protection in a Global Context*, above n. 69, at p. 324.

815 *Ibid.*, at p. 322.

816 *Ibid.*, at p. 26.

817 *Ibid.*, at p. 29.

818 Gellert, Raphael, de Vries, Katja, de Hert, Paul and Gutwirth, Serge, *A Comparative Analysis of Anti-Discrimination and Data Protection Legislation* in Custers, Bart et al. (eds.), *Discrimination and Privacy in the Information Society – Data Mining and Profiling in Large Databases*, Springer, Heidelberg, 2013, at p. 64. Text of the EUCFR is available at http://www.europarl.europa.eu/charter/pdf/text_en.pdf (last accessed on 2014-03-21).

general principle of law.⁸¹⁹ The right to data protection, however, was absent from the EU Charter signed and proclaimed in 2000. The CJEU recognized this right later in *Promusicae*.⁸²⁰ Subsequently, the EU Charter as amended by the Treaty of Lisbon elevated data protection to an independent right.⁸²¹

There exists another connection between data protection and privacy in the form of human rights. For a large portion of its initial existence, the EU was not too interested in human rights for a number of reasons: it was not prioritised considering the economic goals of the EU, human rights were being addressed by the CoE and the CJEU generally adhered to the ECHR when interpreting EU law.⁸²² However, during the 1970's, challenges by some national constitutional courts compelled the CJEU to formulate its view of fundamental rights, and human rights started to become a condition for entry into the EU, Protocol No 14 to the ECHR allowing for the EU to become a party to the ECHR.⁸²³ It is therefore within this context that the normative values of privacy have made their way and subsequently become entrenched in the data protection framework in Europe.⁸²⁴ Also, data privacy law has its origins in human rights law, where, for example, privacy, autonomy, integrity and dignity are addressed.⁸²⁵

In addition, the case law from the ECtHR, that is based on traditional human rights legal documents, exerts an influence on the way other data privacy legislation is interpreted, with not only the right to privacy effective in this regard, but also other rights entrenched in human rights law, such as the right not to be discriminated against and the right of freedom of expression.⁸²⁶ As a result, human rights instruments have progressed from merely containing the

819 Case C-137/79 *National Panasonic v. Commission* [1980] ECR I-2033, paras. 18-20 in Lynskey, Orla, *The Foundations of EU Data Protection Law*, Oxford University Press, 2015, at p. 89.

820 Case C-275/06 *Productores de Música de España (Promusicae) v. Telefónica de España* [2008] ECR I-271, para. 63 in Lynskey, above n. 819, at p. 89.

821 Bygrave, *Data Privacy Law*, above n. 69, at pp. 58-59.

822 Greer, above n. 674, at p. 435.

823 Ibid, at pp. 435-436.

824 Bygrave, *Privacy and Data Protection in an International Perspective*, above n. 69, at p. 180.

825 Bygrave, Lee, A., *Data Protection Law: Approaching Its Rationale, Logic and Limits*, Kluwer Law International, 2002, at p. 167.

826 Bygrave, *Data Privacy Law*, above n. 69, at p. 83.

normative origins of data privacy to being effective instruments of data privacy.⁸²⁷

Another measure indicating the close relationship between privacy and data protection is the manner in which access can be sought to the CJEU. Instances that are characterised by the breach of fundamental rights can be sent to the CJEU by EU institutions against each other, by Member states against each other, by the Commission against Member states, by individuals against EU institutions and by individuals against Member states via referrals to the CJEU by national courts.⁸²⁸ As mentioned above, according to Article 267 TFEU, a national court can approach the CJEU for a preliminary ruling, although this mechanism is not provided as a right.⁸²⁹

Further evidence of the interrelationship between privacy and data protection is provided by means of the increased extent to which the ECtHR has entered into the realm of data protection. This should not seem strange in light of the fact that the CoE has also taken an interest in data protection via the creation of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108) ('Convention 108'), discussed below.

An issue that arises in this context is how to view the above interaction between the right to privacy and the right to data protection. Lynskey discusses three models explaining this relationship: according to 'model 1', data protection and privacy are complementary tools with the ultimate aim of protecting human dignity; according to 'model 2', data protection is a facet of the right to privacy; and according to 'model 3', data protection as a right has a number of purposes, one of which is to protect privacy, although it is not limited to this function.⁸³⁰ Lynskey advocates 'model 3' as best representing the nature of the data protection regime considering that it protects rights that are not addressed by Article 8 ECHR.⁸³¹ Lynskey provides examples of other purposes of data protection, one being the regulation of decisions made concerning the data subject based on automatic processing, and the another that of

827 Ibid, at p. 82.

828 Greer, above n. 762, at p. 436.

829 Ibid, at p. 437.

830 Lynskey, above n. 819, at pp. 94-106.

831 Ibid, at pp. 129-130.

data portability as included in the GDPR.⁸³² In other words, while data protection is to be viewed as having purposes outside of the realm of privacy, there is an overlap to the extent that certain privacy implications are addressed.

The close relationship between data protection and privacy is evident when examining the goals of data protection separately from data protection principles. Brouwer describes data protection as having three main goals: first, the protection of the individual as well as the protection of his or her privacy, second, the protection of the rule of law and third, good governance or good administration.⁸³³ The goal of privacy is rooted in the essay of Warren and Brandeis, advocating the ‘right to be let alone’. In addition, the ECtHR has entered the realm of data protection in cases relating to Article 8 of the ECHR, where the right to private life was alleged to have been invaded by governments. Reference is also made to *Rechnungshof v. Österreichischer Rundfunk and Others*⁸³⁴, where the court stated that the DPD is to be read together with Article 8 of the ECHR.⁸³⁵ Brouwer refers to a decision of the German Constitutional Court in the matter of *Volkszählungsurteil*⁸³⁶, where the court, reflecting on the role of data protection in the protection of liberty, stated that:

Anyone who is uncertain whether his or her deviating behavior will always be noted and recorded, used or transmitted in the longer term, will try not to attract attention by such behavior. Anyone who is concerned, for example, that his participation in a gathering or civil action could be recorded by the government and that this will involve risks for him, may refrain from exercising his constitutional rights. (...) This would not only be detrimental to the possibilities for individual self-development, but also to the public interest [common well-being], because individual self-determination is a basic condition for the functioning of a democratic society, based on the freedoms of citizens to act and to cooperate.⁸³⁷

832 Ibid.

833 Brouwer, Evelien, *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*, Martinus Nijhoff Publishers, Leiden, 2008, at p. 195.

834 *Rechnungshof v. Österreichischer Rundfunk and Others*, Joint Affairs C-465/00, C-138/01 and C-139/01.

835 Brouwer, above n. 833, at p. 197.

836 Judgement of 15 December 1983, 1 BvR 209/83, BVerfGE 65, cited in Brouwer, Ibid, at p. 197.

837 Brouwer, above n. 833, at p. 197.

The opinion of the German Constitutional Court, it is argued, established the notion of the right to informational self-determination.⁸³⁸ This reflects the right to control personal data, which has subsequently found its way into the principles of the DPD. In addition to the right of control, mentioned above, data protection provides a procedural guarantee to counter the power of public authorities, as reflected in the case law of the ECtHR. A practical example of a tool in this regard is the principle of transparency that is established within data protection.⁸³⁹ Finally, another objective of data protection is reflected in its principles, where, for example companies, are required to treat data in a fitting manner as well as take the necessary security precautions.⁸⁴⁰

5.3.2 The Tension Between Council of Europe and European Union

The relationship between the CoE and the EU can be argued to have received a set-back, the main catalyst for this being Opinion 2/13 of the CJEU. According to Protocol No 14 of the ECHR, the EU is able to become a party to the ECHR. According to the EU Charter as amended by the Treaty of Lisbon, the TEU states in Article 6(2) that the EU shall accede to the ECHR while Article 6(3) states that the ECHR shall constitute ‘general principles’ of EU law. Subsequently, in 2010, the Steering Committee on Human Rights and the European Commission were given the mandate to negotiate a treaty that would facilitate this, and a Draft Agreement was made public in April 2013.⁸⁴¹ The Draft Agreement was scrutinized by the CJEU, which rejected the Draft Agreement and stated in Opinion 2/13 that the EU could not accede to the ECHR due to incompatibility issues.⁸⁴² This stance was confirmed in *Åkerberg Fransson*⁸⁴³, where the CJEU held that the ECHR was not to be considered a

838 Ibid, at p. 199.

839 Ibid, at p. 201.

840 Ibid, at p. 202.

841 Greer, above n. 762, at p. 436.

842 Opinion 2/13 of 18 December 2014, EU:C:2014:2454.

843 *Åklagaren v. Hans Åkerberg Fransson*, Case C-617/10 of 26 February 2013.

legal instrument formally incorporated into EU law as long as the EU has not acceded to it.

5.4 International Law

International law can be described as the system of rules and principles that concern the relations between states and other institutions that are subjects of international law and is important for the functioning of the international community.⁸⁴⁴ It is not limited to states and institutions, and is also concerned with rights and obligations in relation to the individual, engaging topics such as nationality, extradition, the use of armed force and human rights.⁸⁴⁵ Therefore, while international law regulates the conduct of states in their relationship with other states, it also regulates the conduct of states in relation to individuals of other states as well as in relation to individuals in that state.⁸⁴⁶

Noteworthy is also that the distinction between formal and material sources of law, found on a domestic level, is not commonplace in international law, mainly because there is no constitutional machinery for the creation of rules in international law, making it difficult to maintain this distinction.⁸⁴⁷ There are a number of sources of law within international law, regarded as such by their incorporation into Article 38 of the Statute of the International Court of Justice. According to Article 38, the following are sources of law: international conventions, international custom, general principles of law and judicial decisions. The hierarchy of these sources is not specified but commonly accepted to be that of the order in which they occur in Article 38.⁸⁴⁸ Generally speaking, therefore, the main sources of international law are treaties and custom.

844 Dixon, above n. 766, at p. 3.

845 Ibid.

846 Ibid.

847 Brownlie, Ian, *Principles of Public International Law*, seventh edition, Oxford University Press, 2008, at pp. 3-4 and Klamberg, Mark, *Evidence in International Criminal Trials: Confronting Legal Gaps and the Reconstruction of Disputed Events*, Martinus Nijhoff Publishers, 2013, at pp. 10-11.

848 Dixon, above n. 766, at pp. 23-24.

International conventions, also called treaties, are created by states that enter into them and agree to their provisions, being either bilateral or multilateral. They are entered into voluntarily, bind only the parties that sign them, and are consequently a source of law only for the parties involved. A treaty may codify customary international law. In such a situation, a state may not be bound by the actual treaty while it may still be bound by the customary law that underlies a treaty.⁸⁴⁹ Consequently, two states may be bound by the same principle but via a different source of law, one country having signed a treaty and another not being a signatory to the treaty yet still being bound to the same underlying principle via customary law.

5.4.1 Human Rights Law

Human rights law, just as with international law in general, is created mainly by means of treaties or custom. A distinguishing factor as far as human rights law is concerned is the reference to concepts such as ‘morality’, ‘justice’, ‘ethics’ and the ‘dignity of Mankind’.⁸⁵⁰ The distinction is also made between on the one hand human rights law, encompassing legal instruments containing the obligations on states, and on the other hand, the soft law surrounding human rights, which are any means of influencing state behaviour, although not having been formally incorporated into a legal instrument.⁸⁵¹ The main purpose of human rights law is to protect individuals from the actions of states or governments.⁸⁵² The impetus to human rights development was the aftermath of World War II, and the United Nations (UN) was a central protagonist in this regard.⁸⁵³ The preamble to the UN Charter refers to, ‘faith in fundamental human rights, in the dignity and worth of the human person, in the equal rights of men and women and of nations large and small’. Articles 55 and 56 are also relevant, Article 55 (c) referring to the universal respect for, and observance of, human rights and fundamental freedoms for all without distinction as to

849 Ibid, at p. 27.

850 Ibid, at p. 341.

851 Ibid.

852 Ibid, at p. 343.

853 Ibid, at p. 344.

race, sex, language, or religion, and Article 56 reiterating a pledge by all countries to strive for this goal. It is argued that human rights law can be described in terms of generations: the first generation comprising civil and political rights, the second generation social and cultural rights, the third generation the rights of people collectively, and the fourth generation the impact of scientific and technological developments.⁸⁵⁴

5.4.2 Human Rights Protection at the Global Level

Human rights protection can occur by means of rules as laid down on the universal or global level as well as on the regional level. Noteworthy global level instruments are the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR)⁸⁵⁵, the International Covenant on Economic, Social and Cultural Rights (ICESCR), with customary international law also of relevance. The above three documents are significant as they form the so-called International Bill of Rights. While the goal was that the UDHR would shortly after taking effect be followed by the above two covenants, incorporating its principles into binding law, it would take eighteen years before this would be realized.⁸⁵⁶ The OECD Guidelines are also relevant since their core was the protection of the human right of privacy, even though in general they were not concerned with the issue of human rights.⁸⁵⁷

854 Ovey and White, above n. 767, at p. 6.

855 United Nations (UN) General Assembly resolution 2200A (XXI) of 16th December 1966, in force 23 March 1976.

856 Smith, Rhona K. M., *Textbook on International Human Rights*, sixth edition, Oxford University Press, 2014, at p. 37.

857 Kirby, Michael, *The History, Achievement and Future of the 1980 OECD Guidelines on Privacy*, International Data Privacy Law, Volume 1, Number 1, February 2011, at p. 8.

5.4.2.1 The Universal Declaration of Human Rights

On December 10th 1948 the UN General Assembly adopted resolution 217A, establishing the Universal Declaration of Human Rights (UDHR).⁸⁵⁸ It is not a legally binding document, although resolutions may lay the foundation for binding norms or later be transformed into treaty form or become custom.⁸⁵⁹ The importance of the UDHR was its role as a standard for adjudicating the behaviour of states, groups, individuals and multinational companies.⁸⁶⁰ A resolution retains its significance in situations where it has subsequently been transformed into a treaty yet not all countries have signed this treaty, in which case it can still be argued that the resolution has become customary international law.⁸⁶¹ The criteria for asserting that a resolution has become customary international law are the following: whether the resolution has been adopted by consensus, the inclusion of normative language and follow-up procedures.⁸⁶² The UDHR continues to form the basis of other human rights instruments and its importance arises from the fact that in cases where countries have not joined the ICCPR or ICESCR, the UDHR potentially remains the only human rights document that a country has joined.

Article 1 states that, '[a]ll human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood', while Article 2 reads:

Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Furthermore, no distinction shall be made on the basis of the political, jurisdictional or international status of the country or territory to which a person belongs, whether it be independent, trust, non-self-governing or under any other limitation of sovereignty.

858 United Nations (U.N.) General Assembly resolution 217 A (III) of 10th December, 1948.

859 Chinkin, Christine, *Sources* in Moeckli, Daniel, Shah, Sangeeta and Sivakumaran Sandesh (eds.), *International Human Rights*, 2nd edition, Oxford, 2014, at p. 91.

860 Dixon, above n. 766, at p. 345.

861 Chinkin, above n. 859, at p. 91.

862 Ibid.

While the UDHR is not a legally binding document, it has subsequently been codified in many instruments, both binding and non-binding.⁸⁶³ It is an important instrument in many respects: it illustrated the broad consensus as regards human rights, it allowed for the identification and inclusion of which human rights were important and it provided momentum for the creation of customary law and the creation of treaties.⁸⁶⁴

5.4.2.2 International Covenant on Civil and Political Rights (ICCPR)

Both the ICCPR and ICESCR were drafted in 1966 and entered into force in 1976.⁸⁶⁵ Article 17 ICCPR reads:

1. No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

The ICCPR is legally binding on all its signatories and they are bound to implement its provisions into national law as well as provide the availability of a remedy should its provisions be contravened.⁸⁶⁶ In addition, thus far 169 countries are parties to the ICCPR, making it an effective document.⁸⁶⁷ The parties to the ICCPR are obligated to submit a report to the Human Rights Committee every five years, wherein they must show the positive steps they have taken with regard to human rights promotion; inter-state complaints can also be submitted to this Committee.⁸⁶⁸ The Human Rights Committee can also make recommendations and issue statements, which have a strong moral force.⁸⁶⁹ It can also issue ‘General Comments’, which are public statements

863 Ibid, at p. 359.

864 Dixon, above n. 766, at p. 345.

865 Ibid, at p. 347.

866 Ibid, at p. 344.

867 United Nations Treaty Collection, available at https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-4&chapter=4&clang=en (last accessed on 2017-03-28).

868 Dixon, above n. 766, at p. 348.

869 Smith, above n. 856, at p. 49.

discussing compliance with the ICCPR and which provide guidance on the actions that the Human Rights Committee believes states should be taking.⁸⁷⁰ An Optional Protocol to the Covenant allows for individual complaints to the Human Rights Committee, however, the ratification of the Protocol is optional and a state can ratify the ICCPR without ratifying the Protocol, thereby side-stepping enforcement.⁸⁷¹ In General Comment 16 of 1988, the Human Rights Committee commented on Article 17 ICCPR, and provided the notion of privacy with a wide scope, stating that, ‘[t]he Committee considers that the notion of privacy refers to the sphere of a person's life in which he or she can freely express his or her identity, be it by entering into relationships with others or alone’.⁸⁷²

The ICESCR deals primarily with economic, social and cultural rights, for example, the right to work and the right to earn a living, the right to an adequate standard of living, food, physical and mental health education and a rich cultural life.⁸⁷³

5.4.2.3 Customary International Law

Customary international law has as its origin the practice or custom of states.⁸⁷⁴ Whether or not a practice of states becomes customary law depends on a number of ‘elements of customary law’, discussed in decisions of the International Court of Justice. The list of factors is not definite and the weight given to each element depends on the circumstances of each case.⁸⁷⁵ The elements determining state practice are: consistency of practice, generality of practice, duration of practice and *opinion juris* (where states recognize a practice as binding on them as a law).⁸⁷⁶

870 Dixon, above n. 766, at p. 348.

871 Ibid, at pp. 348-349.

872 *Coeriel and Aurik v. the Netherlands*, Communication No. 453/1991, U.N. Doc. CCPR/C/52/D/453/1991 (1994), para. 10.2, in Bygrave, *Data Privacy Law*, above n. 69, at p. 85.

873 Smith, above n. 856, at p. 46.

874 Dixon, above n. 766, at p. 30.

875 Ibid, at p. 31.

876 Ibid, at p. 36.

5.4.3 Human Rights Protection at the Regional Level

In examining human rights protection at the regional level, reference is made to the European Convention on Human Rights (ECHR), the European Court of Human Rights (ECtHR) and its case law, as well as to the EU Charter.

5.4.3.1 European Convention on Human Rights

The main aim of the ECHR was to provide an independent judicial process at Strasbourg for instances that violated its provisions.⁸⁷⁷ The ECHR has a number of characteristics: it contains civil and political rights, accession to it is conditional upon CoE membership and it applies to everyone within the boundaries of a member state.⁸⁷⁸ There is also no hierarchy as far as the rights contained in the ECHR are concerned, with each right given equal weight in relation to the others. The distinction can be made, however, between ‘unqualified’ and ‘qualified rights’, where the former category of rights does not allow for derogations, sometimes being referred to as ‘absolute’ rights and including such rights as the right to life. In contrast, qualified rights allow for derogations on the part of the state, where it is required to take certain interests into account, an example being Article 8.⁸⁷⁹ The judicial process was reformed by means of Protocol No. 11, which altered access to the ECtHR, whereby the process of the referral of matters to the European Commission on Human Rights was replaced by a system whereby any person suffering a violation of one of the rights enshrined in the ECHR could apply directly to the ECtHR.⁸⁸⁰ Any violation against an individual must be proven by that individual on a balance of probabilities. With regards to a qualified right, however, the state involved must prove on a balance of probabilities that the interference was justified by showing, first, that the interference was in accordance with the law, second, that it was necessary in a democratic society and third, that it was

877 Greer, above n. 762, at p. 422.

878 Ibid, at p. 420.

879 Ovey and White, above n. 767, at p. 7.

880 Solove and Schwartz, above n. 517, at p. 1071.

the minimum interference required in the circumstances, in other words proportional.⁸⁸¹ The formalities concerning applications were further altered by Protocol No. 14, which came into effect on the 1st of June 2010. It is argued that while the ECHR is materially similar to the ICCPR, its enforcement provisions are more effective, as the ICCPR relies on the First Optional Protocol for enforcement, which does not require signing by the parties who signed the main document.⁸⁸² In addition, the breach of the ECHR brings with it international responsibility, which means that a state will be required to make sure that its national law is in line with the ECHR.⁸⁸³ Furthermore, an individual can take a state to the ECtHR and receive a monetary award.⁸⁸⁴

5.4.3.2 The European Court of Human Rights (ECtHR)

The ECtHR hears applications by states or individuals concerning the alleged violation of human rights.⁸⁸⁵ This role has allowed it to take human rights forward via case law that is relevant, even in the face of new technologies.⁸⁸⁶ Of special interest is the method of interpretation employed by the ECtHR in adjudicating cases. First, it employs the same methods of interpretation as for the interpretation of treaties in international law. In addition, the process is viewed as one complex operation, where a hierarchical approach is not taken and where preparatory works, although deemed unreliable, can be referred to for guidance.⁸⁸⁷ The ECHR is treated as a ‘living instrument’ and a dynamic approach is taken in interpreting its clauses.⁸⁸⁸ Heed is also taken of the principle of effectiveness, where the ECHR is interpreted in such a manner to give it the fullest weight.⁸⁸⁹ A comparative interpretation is also employed, at times

881 Ovey and White, above n. 767, at p. 9.

882 Dixon, above n. 766, at p. 349.

883 Ibid, at p. 354.

884 Ibid.

885 Ovey and White, above n. 767, at p. 8.

886 Bygrave, *Data Privacy Law*, above n. 69, at p. 87.

887 Ovey and White, above n. 767, at p. 40

888 Ibid.

889 Merrills, J, *The Development of International Law by the European Court of Human Rights*, 1988, chapter 5, in Ovey and White, above n. 767, at p. 47.

comparing the different laws of the Member States in order to best reflect the law as common to these states.⁸⁹⁰ While the above human rights instruments in the past have been of important normative value, they have also come to be influential data protection instruments in themselves and while the actual instruments are dated in relation to modern information and communication technology, the expansive interpretation of their clauses has resulted in a considerable amount of case law.⁸⁹¹ A novel approach has also been taken in relation to technology, for example with regards to data protection, where the ECtHR has held that the processing of personal data shall take place subject to legal controls that reflect the notion of the ‘rule of law’ and be proportionate in relation to its aims.⁸⁹² The ECtHR has interpreted the ECHR in light of attitudes to new phenomenon in the CoE member countries.⁸⁹³

The ECtHR has used Article 8 ECHR and the right to ‘private life’ to meet the challenges posed by new technologies to human rights and has been prepared to use this article in circumstances not anticipated at the time of drafting.⁸⁹⁴ The ECtHR uses the dynamic interpretation stance, according to which concepts may change over time depending on the views of society.⁸⁹⁵ In this manner, the ECtHR has been able to address technologies such as telephone conversations, telephone numbers, computers, video surveillance, voice recording, internet and email within the scope of Article 8 and ‘private life’.⁸⁹⁶ Ovey and White refer to a description of the ECtHR’s interpretation methodology, by quoting Judge Bernhardt:

The general rules of treaty interpretation are in principle also applicable to human-rights treaties, but the object and purpose of these treaties are different,

890 Ibid, at pp. 48-49.

891 Bygrave, *Data Privacy Law*, above n. 69, at p. 83.

892 Ibid, at p. 86.

893 Ibid, at p. 87.

894 Ibid.

895 Gomez-Arostegui, Tomas, *Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations*, Vol. 35, No. 2, California Western International Law Journal, 2005, at p. 158.

896 De Hert, Paul and Gutwirth, Serge, *Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action*, in Gutwirth, Serge et al. (eds.) *Reinventing Data Protection?*, Springer Science and Business Media, 2009, at p. 16.

and therefore, the traditional rules need some adjustment. The notions contained in human-rights conventions have an autonomous international meaning; however, such meaning must be determined by a comparative analysis of the legal situation in the participating States. To the extent that this analysis shows considerable differences and disparities among the States, a National ‘margin of appreciation’ is and must be recognized. Human-rights treaties must be interpreted in an objective and dynamic manner, by taking into account social conditions and developments; the ideas and conditions prevailing at the time when treaties were drafted retain hardly any continuing validity. Nevertheless, treaty interpretation must not amount to treaty revision. Interpretation must therefore respect the text of the treaty concerned.⁸⁹⁷

Finally, ECtHR judgements are binding to the extent that they are declaratory, a consequence being that the defendant state can be made to make reparation according to international law, with ‘just satisfaction’ for the individual an alternative where state law only allows for partial reparation.⁸⁹⁸

5.4.3.3 Human Rights and Autonomy

In light of the role personal autonomy has in relation to the potential harms resulting from predictive modelling, the extent to which human rights law, more specifically the ECtHR, addresses the concept of autonomy is assessed. The concept of autonomy is dealt with under the principle of the ‘right to private life’ as enshrined in Article 8 ECHR. The ECtHR has also adjudicated cases involving technology, more specifically surveillance, where data protection was addressed. Here the link between technology and human rights is reiterated, where data protection not only has the protection of autonomy as a goal but has its origins in human rights.

897 Bernhardt, R, *Thoughts on the interpretation of human-rights treaties*, in F. Matscher and H. Petzold, *Protecting Human Rights: The European Dimension. Studies in Honour of Gerard J. Wiarda* (Köln, 1988), at 65-71, at p. 70-1, in Ovey and White, above n. 767, at p. 54.

898 Solove and Schwartz, above n. 517, at p. 1064.

5.4.3.4 The Protection of Private and Family Life in Article 8 ECHR

The protection of private and family life is enshrined in Article 8 ECHR. Article 8(1) specifies the rights enshrined in this Article while Article 8(2) specifies the circumstances under which a state can legitimately interfere with these rights.⁸⁹⁹ It reads:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and morals, or for the protection of the rights and freedoms of others.

Article 8(1) ECHR sets out the basic rule protecting private life as expressed in terms of ‘private and family life, his home and his correspondence’. It not only places a negative obligation on the state to protect private life, but also a positive one.⁹⁰⁰ A negative obligation constrains the state from interfering with an established right while the positive obligation compels a state to take steps to prevent any interference with that right. While Article 8 ECHR protects individuals against attacks by the state with respect to family and private life, the home and correspondence, the protection goes further in that it protects against the actions of institutions independent of the state, an example given being that of ‘private electronic data banks’, placing a positive obligation on the state.⁹⁰¹ The scope of Article 8 ECHR is wide, going so far as to protect

899 Kilkelly, Ursula, *The Right to Respect for Private and Family Life: A Guide to the Implementation of Article 8 of the European Convention on Human Rights*, Human Rights Handbook No. 1, Council of Europe, 2001, at p. 6.

900 *Marckx v. Belgium* (1980) 2 EHRR 330, para. 31. See also *Von Hannover v. Germany*, (2005) 40 EHRR 1, para. 51 for a succinct explanation of the negative and positive obligation on states. The Court stated that, ‘[t]he Court reiterates that although the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves’.

901 *Ovey and White*, above n. 767, at p. 243.

individuals against mental or physical integrity violations, moral and intellectual freedom, attacks on honour and reputation, the use of a person's name or identity, being spied on, watched or harassed and the disclosure of information where professional secrecy prevails.⁹⁰² The ECtHR has even stated that the existence of a law allowing for the secret monitoring of communications is in itself a threat to freedom of communication and therefore contravenes Article 8 ECHR irrespective of whether any actual surveillance takes place.⁹⁰³

The main effect of this positive obligation is that it places a duty on a state to take measures, either judicial (providing sanctions for breaching the ECHR) or practical, to protect a right of an individual.⁹⁰⁴ It is argued that the negative obligation on states has received more attention than the positive ones.⁹⁰⁵ The extension of the ambit of the positive obligations places additional duties on the state, and as a result, the ECtHR has always fixed a positive obligation to a specific article of the ECHR.⁹⁰⁶ Article 8 ECHR therefore broadens the scope of the right to private life in that the relationship between private bodies is also regulated.⁹⁰⁷ The positive obligation on states has a number of characteristics: it requires a state to take steps to protect private life, for example by making sure that there are laws in place with this positive obligation in mind; a breach of the above positive duty can occur even in situations where the interference was not directly caused by the state; and determining whether there is a positive duty on a state may be dependent upon a consideration of the interests of the individual as opposed to those of society at large.⁹⁰⁸ The above positive duty on a state entails that a national law violating the right to private life will violate Article 8(1) ECHR without the need to take into account the exceptions in 8(2).⁹⁰⁹

902 Ibid, at p. 242.

903 *Weber and Saravia v. Germany* (2008) 46 EHRR SE5, para. 78.

904 Akandji-Kombe, Jean-Francois, *Positive Obligations under the European Convention of Human Rights: A Guide to the Implementation of the European Convention on Human Rights*, Human Rights Handbook, No. 7, Council of Europe, 2007, at p. 7.

905 Ibid, at p. 5.

906 Ibid, at pp. 7-8.

907 Bygrave, *Data Privacy Law*, above n. 69, at p. 87.

908 Ovey and White, above n. 767, at p. 243.

909 Ibid.

There are a number of examples where technologies not in existence at the time of creation of the ECHR are included in its scope, for example the notion of ‘correspondence’, which was said to relate to the direct communication between people and in relation to surveillance techniques.⁹¹⁰ On the issue of what is included in the right to private life under Article 8 ECHR, the case of *Copland v. United Kingdom* is interesting.⁹¹¹ It brought telephone calls from business premises within the scope of ‘private life’ and ‘correspondence’ referred to in Article 8 ECHR. De Hert and Gutwirth indicate that building on the case of *Halford v. United Kingdom*, which recognized telephone calls as falling within the scope of Article 8 ECHR, emails sent from work as well as the monitoring of personal internet usage was also brought within the scope of Article 8 ECHR.⁹¹²

Article 8(2) sets out the subsequent limitations or exceptions to the general rule in Article 8(1) ECHR. It stipulates the circumstances under which interference with the right to private life under Article 8(1) ECHR is legitimate. The limitations function to balance the interests between society on the one hand and the individual on the other.⁹¹³ There are three limitations according to Article 8(2) ECHR: first, the interference must be ‘in accordance with the law’, second, it must occur in the pursuit of certain interests, which are perceived as legitimate and third, the interference must be ‘necessary in a democratic society’.⁹¹⁴

The first limitation necessitates that there be national law, written or unwritten, in the state that regulates the interference in question.⁹¹⁵ However, the measures could be considered illegitimate if not regulated by statute, but are regulated instead by, for example, administrative practice.⁹¹⁶ In addition, listening devices used by the authorities have been held to be an illegitimate interference due to the lack of a statutory mechanism to regulate such use.⁹¹⁷

910 Ibid, at p. 250.

911 *Copland v. United Kingdom* (2007) 45 EHRR 37.

912 Gutwirth and De Hert, above n. 896, at p. 16.

913 Ovey and White, above n. 767, at p. 219.

914 Klamberg, Mark, *FRA and the European Convention on Human Rights*, in *Overvågning i en rettsstat*, Schartum, Dag Wiese (ed.), Fagbokforlaget, 2010, at p. 107.

915 Ovey and White, above n. 767, at p. 223.

916 *Malone v. United Kingdom* (1985) 7 EHRR 14, para. 79.

917 *Kahn v. United Kingdom* (2000) 31 EHRR 1016, para. 27.

The second limitation provides a list of interests, such as national security, that must be pursued for the interference to be legitimate. These interests are rarely disputed by the ECtHR.⁹¹⁸

The third limitation, namely ‘necessary in a democratic society’, has been expanded upon by the ECtHR, which stated that, ‘the phrase “necessary in a democratic society” means that, to be compatible with the Convention, the interference must, inter alia, correspond to a “pressing social need” and be “proportionate to the legitimate aim pursued”’.⁹¹⁹ It therefore implies that there must be a pressing social need for that law and takes into account the notion of proportionality.⁹²⁰ This is argued to mean that there must be a legal regime governing the interference in question, with common law being adequate and statutory law not necessary.⁹²¹ This third limitation is further expanded upon by the notion of the ‘margin of appreciation’, which is a controversial development that essentially accepts that states are in a better position to judge whether a certain set of circumstances in a specific country in actual fact requires the response or penalty meted out by the state.⁹²² It is alternatively described as, ‘...an expression of moral relativism, based on the notion that each society is entitled to a certain amount of latitude in resolving the inherent conflicts between individual rights and nations interests or among different moral convictions’.⁹²³ The ECtHR has stated:

By reason of their direct and continuous contact with the vital forces of their countries, State authorities are in principle in a better position than the international judge to give an opinion on the exact content of these requirements as well as on the ‘necessity’ of a ‘restriction’ or ‘penalty’ intended to meet them.⁹²⁴

918 Klamberg, *FRA and the European Convention on Human Rights*, above n. 914, at p. 109.

919 *Silver and Others v. United Kingdom* (1983) 5 EHRR 347, para. 97.

920 Ovey and White, above n. 767, at p. 232.

921 Wadham, John, *Human Rights and Privacy – The Balance*, speech given at Cambridge, March, 2000, referred to in Solove and Schwartz, above n. 517, at p. 1072.

922 Ovey and White, above n. 767, at p. 233.

923 Klamberg, Mark, *Power and Law in International Society: International Relations as the Sociology of International Law*, Routledge, 2015, at p. 91.

924 *Handyside v. United Kingdom* (1979-80) 1 EHRR 737, para. 48.

In certain circumstances, states have been given broad discretion as regards the margin of appreciation, whereas in others situations, such as matters concerning an individual's existence or identity, a narrower leeway has been granted.⁹²⁵ On national security, states have been given a wide margin of appreciation.⁹²⁶ Walden states that few rights in the ECHR are absolute and that in deciding whether an action is legitimate in the circumstances requires an examination of whether it is 'proportionate to the legitimate aim pursued'.⁹²⁷ This means that an interest being pursued, even if legitimate from the perspective of the state, will not be justified if the action employed to achieve that aim is disproportionate to the interest being pursued.

Article 8 ECHR provided the framework for balancing the right of the individual to private life as opposed to the state's discretion to limit this right. The application of Article 8 ECHR has been described as a three-step process: first the court determines whether Article 8 is applicable, second whether the state has interfered with that right or omitted to take steps to prevent the interference with that right and third, whether the state's act or omission was justified in the circumstances.⁹²⁸ The ECtHR has stated that included in the right to private life is the necessity of protecting identity and personal development, that is the right to establish relationships with other human beings.⁹²⁹ Within the ECHR, there is no recognition of the rights to liberty, to the protection of human dignity, to autonomy nor to self-determination. The explanation for this is the fact that within Europe alone, many different interpretations have been given to the notion of privacy.⁹³⁰

925 Ovey and White, above n. 767, at p. 233.

926 Ibid at pp. 234-237. See also *Leander v. Sweden*, paras. 59 and 67, *Klass v. Germany*, para. 49, *S. and Marper v. United Kingdom*, para. 102 and *Weber and Saravia v. Germany*, para. 106.

927 Wadham, John, *Human Rights and Privacy – The Balance*, speech given at Cambridge, March 2000, referred to in Solove and Schwartz, above n. 517, at p. 1073.

928 Gomez-Arostegui, above n. 895, at p. 156.

929 Brouwer, above n. 833, at p. 153, citing the cases of *P.G. and J.H. v. United Kingdom*, *Peck v. United Kingdom* and *Niemietz v. Germany*.

930 Gutwirth and De Hert, above n. 896, at p. 14.

5.4.3.5 The Horizontal Effect

The positive obligation on states to protect the rights as set out in the ECHR forms the foundation for the notion of horizontal effect. Consequently, states are also required to regulate the relationships between individuals.⁹³¹ In the case of *Young, James and Webster v. United Kingdom*, the ECtHR established what was to be referred as the ‘horizontal effect’ of the ECHR, which enlarged the scope of the right to private life to encompass the relationship between individuals, in other words, private parties:

Although the proximate cause of the events giving rise to this case was the 1975 agreement ... it was the domestic law in force at the relevant time that made lawful the treatment of which the applicants complained. The responsibility of the respondent State for any resultant breach of the Convention is thus engaged on this basis.⁹³²

As a result, the right to private life of individuals as against non-state actors is protected, even though the ECHR primarily deals with protection from the power of the State.⁹³³ The positive obligation on states to provide the conditions under which to exercise the right to private life, together with the horizontal effect, requires states to take steps to protect the rights of private individuals against infringements by non-state parties.⁹³⁴ Notwithstanding the implications of the horizontal effect, any recourse taken by an individual must be directed towards the state concerned, and not towards the private actor that allegedly breached the individual’s right to private life. It is also noteworthy that a state cannot be held liable for the actual act perpetrated by an individual but is liable, rather, for not creating the conditions preventing this occurrence or for tolerating it.⁹³⁵ Accordingly, the ECtHR would then be called upon to adjudicate whether the state had the necessary framework in place in order to balance the interests of the parties, which adjudication would enquire as to

931 Akandji-Kombe, above n. 904, at p. 14.

932 *Young, James and Webster v. United Kingdom* (1982) 4 EHRR 38, para. 49.

933 Rouvroy, above n. 436, at p. 66.

934 *Ibid*, at p. 66.

935 Akandji-Kombe, above n. 904, at p. 14.

whether there was a proportionality that reflects the state versus private individual relationship referred to above.⁹³⁶ Consequently, this obligation on the state includes in it an obligation to take steps against private actors who breach the privacy of a person.⁹³⁷

5.4.3.6 Case Law on the Right to Private Life

The case law originating from the ECtHR that has developed surrounding Article 8 ECHR is relevant not only to the extent that it takes into account the developing nature of technology, but also because it addresses the notion of autonomy. Human rights and autonomy are closely associated in that human rights create a sphere of personal autonomy and therefore protect the individual from the ‘excessive steering of their lives’.⁹³⁸ The ECtHR has interpreted the notion of ‘private life’ as being further divided into two subsequent notions, namely ‘matters and information that should be kept secret or free from publicity’ and ‘matters that involve a person’s personality or autonomy’.⁹³⁹ In *X v. Iceland*, the right to be able to withdraw to a place of seclusion was described as a right to, ‘live, as far as one wishes, protected from publicity’, the Court also referring to the second dimension of the right:

In the opinion of the Commission, however, the right to respect for private life does not end there. It comprises also, to a certain degree, the right to establish and to develop relationships with other human beings, especially in the emotional field for the development and fulfilment of one’s own personality.⁹⁴⁰

Here the distinction between the two aspects of private life is visible and corresponds with that portrayal of autonomy provided by scholars within philosophy, namely the right to be able to withdraw to a place of seclusion as well

936 Bygrave, *Data Privacy Law*, above n. 69, at p. 89.

937 See, for example, *Von Hannover v. Germany*, in Bygrave, *Data Privacy Law*, above n. 69, at p. 87.

938 De Hert, P., and Gutwirth, S., *Privacy, Data Protection and law enforcement. Opacity of the individuals and transparency of the power*, in Claes, E., Duff, A., and Gutwirth, S., (eds.) in *Privacy and the Criminal Law*, Interscientia, 2006, at p. 5.

939 Gomez-Arostegui, above n. 895, at p. 160.

940 *X v. Iceland* (Application no. 6825/74), Commission Decision, 18 May 1976.

as the right to make relational contact with others in order to develop one's own personality.

5.4.3.6.1 *Autonomy*

Some scholars stress that autonomy is not a tangible object, capable of being given or taken away, nor can it be traded in.⁹⁴¹ Autonomy cannot be demanded and is not always present, although while one cannot demand actual autonomy, one can demand the right to pursue autonomy.⁹⁴² Where exactly autonomy is placed within the structure of a legal system may differ. For example, in the US, autonomy is reflected in terms of the 'right to be left alone' theory of privacy, whereas in Europe autonomy is addressed via the incorporation of the notion of privacy, notably in Article 8 of the ECHR.⁹⁴³ According to interpretations of the range of Article 8 ECHR, 'private life' not only protects an individual's private sphere, but also the development of inter-personal relationships and even events occurring in the public sphere.⁹⁴⁴ From the above interpretations of autonomy in relation to human rights and from an examination of Article 8 ECHR, a conclusion is that autonomy is clearly enshrined within the operation of Article 8 ECHR and comprises two clearly demarcated components. The first component concerns the ability to withdraw to a place of solitude while the second component entails a freedom to seek contact with other human beings with the aim of personality development. In the case of *Pretty v. United Kingdom*, the ECtHR emphasised the importance of the second component of autonomy:

Article 8 also protects a right to personal development, and the right to establish and develop relationships with other human beings and the outside world ... Although no previous case has established as such any right to self-determination as being contained in Article 8 of the Convention, the Court considers that the notion of personal autonomy is an important principle underlying the interpretation of its guarantees.⁹⁴⁵

941 Rouvroy and Pouillet, above n. 436, at pp. 59-60.

942 Ibid.

943 Ibid, at p. 63.

944 Gutwirth and De Hert, above n. 896, at p. 17.

945 *Pretty v. United Kingdom* (2002) 35 EHRR 1, para. 61.

While the claim in this case was rejected, the Court did concede that the notion of personal autonomy was an important principle underlying the right to self-determination. This linkage to self-determination in turn mirrors the aims of data protection, which has the protection of autonomy as an implied goal and which in turn encompasses a person's interest in informational self-determination or put another way, how personal data is processed.⁹⁴⁶

The case of *Niemietz v. Germany* also addressed the notion of autonomy. The ECtHR stressed that the right to private life not only included a right to a space of seclusion where the individual has autonomy, but that it also protected individuals in their relationships that extended outside of an 'inner circle', referring also to business relationships or relationships of a more professional nature.⁹⁴⁷ The Court stated the following:

The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of "private life". However, it would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world ... Thus, especially in the case of a person exercising a liberal profession, his work in that context may form part and parcel of his life to such a degree that it becomes impossible to know in what capacity he is acting at a given moment of time.⁹⁴⁸

This judgement is significant in three respects. First, it explicitly states that the notion 'private life' is too broad to define. Second, it expands upon the second component of autonomy, and in fact broadens the notion of whom the individual should be allowed to be in contact with and yet retain the protection of the right to private life as expressed in Article 8 ECHR. The reference to an 'inner circle' highlights that the individual, in exercising his or her autonomy,

946 Bygrave, *Data Protection Law*, above n. 825, at p. 150.

947 Bygrave, *Data Privacy Law*, above n. 69, at p. 88.

948 *Niemietz v. Germany* (1993) 16 EHRR 97, para. 29.

is not restricted to a group of close friends and possesses a substantial amount of leeway when establishing contact with other human beings for the purpose of personality building. Third, the distinction between the private and public is diminished, by stating that even contact of a business nature falls within the ambit of Article 8 ECHR, to the extent that private and professional life may be intertwined.

Two cases involving Princess Caroline von Hannover of Monaco and the media, which made their way to the ECtHR, are also relevant in the context of autonomy and the extent to which a person, even if famous, has the right to a private life.⁹⁴⁹ These cases highlight the tension between two rights enshrined in the ECHR, namely the right to private life (Article 8) and the right to the freedom of expression (Article 10). The first case of *Von Hannover v. Germany* concerned the right a person has to his or her image and engaged the state's positive obligation to protect a person's identity in relation to third parties, for example journalists as was the case here.⁹⁵⁰ The Court stressed that while Article 8 ECHR expressed the negative obligation on the state to refrain from interfering with a person's private life, the positive obligation required it to take steps to make any protection of private life more effective, even regarding the relationships between individuals.⁹⁵¹ The Court also highlighted the balancing process that was required, between the interests of the individual versus those of the community, adding that the state had a margin of appreciation in such circumstances.⁹⁵² The German media had printed photographs of Princess Caroline at a restaurant, horse riding, canoeing, shopping, playing tennis and tripping over an obstacle at a beach club. Princess Caroline alleged that German law did not protect her privacy as it had a narrow definition of 'secluded place'.⁹⁵³ The Court came to the conclusion that Princess Caroline did have a right to private life, the result being that Germany was liable for not upholding this. This case also concerned the second component of autonomy, namely the freedom of association for the purposes of personality building and ultimately the attaining of autonomy, where the actions of the media

949 *Von Hannover v. Germany*, and *Von Hannover v. Germany (no. 2)* (2012) 55 EHRR 15.

950 Akandji-Kombe, above n. 904, at p. 39.

951 *Von Hannover v. Germany*, para. 57.

952 *Ibid*, para. 57.

953 Solove and Schwartz, above n. 517, at p. 1076.

interfered with the autonomy of Princess Caroline by interfering with her freedom of association, coupled with the right to withdraw to a place of seclusion:

The Court reiterates that the concept of private life extends to aspects relating to personal identity ... Furthermore, private life, in the Court's view, includes a person's physical and psychological integrity; the guarantee provided by Article 8 of the Convention is primarily intended to ensure the development, without outside interference, of the personality of each individual in his relations with other human beings ... There is therefore a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life'.⁹⁵⁴

The Court reinforced this by stating that this right to private life, 'extends beyond the family circle and also includes a social dimension', adding that even if people are known to the public, they enjoy a 'legitimate expectation' to protection of their private life.⁹⁵⁵ Finally, from a technical perspective, the Court also mentioned the importance of preserving this right to the protection of private life considering the, 'new communication technologies which make it possible to store and reproduce personal data'.⁹⁵⁶ The case of *Von Hannover v. Germany (no. 2)* is relevant to the extent that the Court laid out the facts to be taken into account when determining the balance between the right to private life and freedom of expression.⁹⁵⁷

Odièvre v. France also dealt with autonomy.⁹⁵⁸ The case concerned a mother who, at birth, gave her child up for adoption while at the same time requesting the right to confidentiality, possible under French law. The child subsequently sought to attain the identity of her mother, arguing that the non-existence of the right to do so was a breach of Article 8 ECHR. The majority of the Court found no breach of Article 8 ECHR but of interest was the dissenting opinion of the judges. First, they disagreed with the majority of the Court, adjudicating a breach of Article 8 ECHR. In their rationale, they referred to the situation of competing rights. On the one hand, there was the right

954 *Von Hannover v. Germany*, para. 50.

955 *Ibid*, para. 69.

956 *Ibid*, para. 70.

957 *Von Hannover v. Germany (no. 2)*, paras. 108-113 in Bygrave, *Data Privacy Law*, above n. 69, at p. 90, footnote 237.

958 *Odièvre v. France* (2004) 38 EHRR 871.

of the child to have access to information about its origins, while on the other hand there was the right of the mother, in the light of her personal autonomy, to keep her identity secret.⁹⁵⁹ The Court stated:

Thus, certain aspects of the right to private life are peripheral to that right, whereas others form part of its inner core. We are firmly of the opinion that the right to an identity, which is an essential condition of the right to autonomy ... and development ... is within the inner core of the right to respect for one's private life. Accordingly, the fairest scrutiny was called for when weighing up the competing interests.⁹⁶⁰

The dissenting judges were of the opinion that this matter concerned the balancing of competing rights and that the fairest solution was necessary in determining which rights took precedence. The dissenting judges looked to the cases of *Pretty v. United Kingdom* and *Bensaid v. United Kingdom*, which stated that elements of social identity, such as gender identification, name and sexual orientation and sexual life fall within the sphere protected by Article 8 ECHR.⁹⁶¹ They described the right to private life as having a core and while some aspects of this right to private life were peripheral in relation to the core, there were others that were closer.⁹⁶²

5.4.3.6.2 *A Reasonable Expectation of Privacy*

The yardstick of a 'reasonable expectation of privacy' as well as the reference by the ECtHR to data protection are also noteworthy. While two separate aspects, they are intertwined and to a certain degree interdependent. A development noted in ECtHR case law concerning the right to privacy is the phrase 'reasonable expectation of privacy', which has crept in to the adjudication of

959 Ibid, para. 4, (dissenting opinion).

960 Ibid, para. 11, (dissenting opinion).

961 *Pretty v. United Kingdom*, para. 61, *Bensaid v. United Kingdom* (2001) 33 EHRR 205, para. 47.

962 In *Pretty v. United Kingdom*, the Court referred to autonomy as a 'principle', whereas in *Odièvre v. France* it was referred to as a 'right'. It is possible to argue that this is of great significance. However, in light of the lack of evidence to the effect that this difference in use of legal concept cannot be attributed to anything more than a semantic issue, the matter is not investigated further in this thesis.

the right to private life notion within the discourse of the ECtHR. The origin of the term is argued to be US case law, more specifically the case of *Katz v. United States*, where the Supreme Court, in assessing the Fourth Amendment right protecting people from unreasonable search and seizures, stated that anyone invoking this right must show an actual and reasonable expectation of privacy in the place or object at issue.⁹⁶³ The judge stated that, ‘[m]y understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person has exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as “reasonable”’.⁹⁶⁴ The ECtHR has infused the ‘reasonable expectation of privacy’ into its case law, especially in relation to data protection. Also, the majority of cases concerning data protection have come to the fore within the context of state surveillance.⁹⁶⁵

The first ECtHR case to use this test was that of *Halford v. United Kingdom*, where a policewoman’s telephone calls from her office telephone were allegedly recorded. After the right to privacy was evoked as a defence, the ECtHR adjudicated that the Applicant did not have a ‘reasonable expectation of privacy’ in relation to the calls that were made from a workplace telephone.⁹⁶⁶ Subsequently, the case of *P.G. & J.H. v. United Kingdom* took up this phrase.⁹⁶⁷ Here, reference was made to this phrase together with data protection and its relevance in relation to whether the right to private life was breached. It has been highlighted that references to data protection started to make their way into the judgements of the ECtHR already during the 1980’s.⁹⁶⁸

The case of *P.G. & J.H. v. United Kingdom* dealt with the recording of a suspect’s conversation with police at a charging procedure for voice analysis purposes. The Court stated that this voice recording indeed fell within the notion of private:

963 *Katz v. United States* 389 US 347 (1967) at p. 361, cited in Gomez-Arostegui, above n. 895, at p. 163.

964 *Katz v. United States*, at p. 361.

965 Bygrave, *Data Privacy Law*, above n. 69, at p. 90.

966 *Halford v. United Kingdom* (1997) 24 EHRR 523, para. 17.

967 *P.G. & J.H.* (2008) 46 EHRR 51.

968 Gutwirth and De Hert, above n. 896, at p. 19.

... a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene ... is of a similar character. Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain. It is for this reason that files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method ... where the storing of information about the applicant on a card in a file was found to be an interference with private life, even though it contained no sensitive information and had probably never been consulted ... the recording and analysis [...] on this occasion must still be regarded as concerning the processing of personal data about the applicants.⁹⁶⁹

Peck v. United Kingdom, concerning the recording by surveillance cameras of a person attempting to commit suicide in public, also addressed the 'reasonable expectation of privacy' notion and referred to the fact that the recording of personal data influenced the determination of whether Article 8 ECHR was applicable.⁹⁷⁰ Here the Court did judge Article 8 ECHR to be applicable because, 'the relevant moment was viewed to an extent which far exceeded any exposure to a passer-by or to security observation ... and to a degree surpassing that which the applicant could possibly have foreseen when he walked in [...]'.⁹⁷¹ According to Gomez-Arostegui, the ECtHR's absence of referral to data protection in the subsequent *Von Hannover* case, mentioned above, leads to the question of whether data processing is a 'test' in itself for the determination of whether private life has been breached or whether it is just one of many factors to be taken into account in the overall assessment of this.⁹⁷²

969 *P.G. & J.H.*, paras. 57-59.

970 *Peck v. United Kingdom* (2003) 36 EHHR 205.

971 *Ibid.*, para. 62.

972 Gomez-Arostegui, above n. 895, at p. 173.

5.4.3.6.3 Data Protection

A growing acceptance that privacy law at the time was not able to address the challenges of technology resulted in the CoE producing Convention 108 on data protection, which entered into force in 1985.⁹⁷³ While still applying Article 8 ECHR in privacy matters, the ECtHR broadened the notion of privacy by referring to the requirements set out in Convention 108. The first case to refer to Convention 108 was *Z v. Finland*, which concerned the disclosure of files related to health records, and more specifically of the fact that the Applicant was HIV positive.⁹⁷⁴ Here the Court provided an interesting reason for why the actions of the state were a contravention of Article 8 ECHR. It stated that files from the health sector were confidential, which was to protect privacy but was necessary also to protect a person's 'confidence in the medical profession and in the health services in general'. This was a novel rationale for implementing data protection principles and not formally a principle within more traditional data protection principles.

Leander v. Sweden also dealt with data protection.⁹⁷⁵ The Court held that the storage of data files, their dissemination as well as the refusal of the authorities to give the Applicant the opportunity to refute their contents, amounted to a breach of the right to private life according to Article 8 ECHR. A case with similar facts is that of *Segerstedt-Wiberg and others v. Sweden*, where five applicants had files stored with the security establishment.⁹⁷⁶ This was adjudicated to be a breach of the right to private life as the data had been stored for a lengthy period of time and the applicants were of no real threat to the security of the state.

The above shows how the general principles of data protection began to find application within the ambit of Article 8 ECHR. Subsequently, references have been made to data protection principles on a regular basis, for example

973 Kranenborg, Herke, *Article 8*, in Peers, Steve, Hervey, Tamara, Kenner, Jeff and Ward, Angela (eds.), *The EU Charter of Fundamental Rights: A Commentary*, Hart Publishing, 2014, at p. 228.

974 *Z v. Finland* (1998) 25 EHRR 371, para 95, see also Brouwer, above n. 833, at p. 155.

975 Brouwer, above n. 833, at p. 153.

976 *Segerstedt-Wiberg and others v. Sweden*, (Application no. 62332/00), Judgement, 6 June 2006.

the right to access of one's personal data,⁹⁷⁷ the right to the deletion of data⁹⁷⁸ and the right to have official data relating to gender corrected.⁹⁷⁹ In *Peck, Perry and P.G. and J.H.*, the Court acknowledged the purpose limitation principle found within data protection, which specifies that personal data can only be used for its initial purpose.⁹⁸⁰ In the case of *Gaskin v. United Kingdom*, the Applicant alleged being abused while in foster care and requested access to his file at a public authority. His request was partly denied in that he was granted access only to those parts of the file that had not been submitted by contributors under the condition of confidentiality. The Court did stress the importance of the right of access and that Article 8 ECHR in fact placed a positive duty on the government to ensure access to data within the context of Article 8 ECHR.

The 'reasonable expectation of privacy' is influenced by surveillance, the argument being that people living in societies with more intense surveillance do not have as high an expectation of privacy compared to those living in societies with a lower degree of surveillance.⁹⁸¹ This has two consequences. First, an increased knowledge of surveillance coupled with a low expectation of privacy, cannot counter the effects of monitoring and second, a lower expectation of privacy may lead to the situation where people no longer make the effort to claim their privacy.⁹⁸²

Also, even though the distinction between public and private has been diminished, it has not been completely dispensed with by the ECtHR, with Article 8(1) not completely relevant in the public sphere.⁹⁸³ However, it can be relied on when information from the public sphere has been recorded, used

977 *Gaskin v. United Kingdom* (1990) 12 EHRR 36.

978 *Leander v. Sweden* (1988) 9 EHRR 433.

979 *Rees v. United Kingdom* (1987) 9 EHRR 56.

980 Gutwirth and De Hert, above n. 896, at p. 19.

981 Rouvroy and Poullet, above n. 436, at p. 48.

982 *Ibid.*, at p. 45.

983 *Perry v. United Kingdom* (2004) 39 EHRR 3, para. 40 in Bygrave, *Data Privacy Law*, above n. 69, at p. 89.

and stored in a manner that conflicts with a person's 'reasonable expectations'.⁹⁸⁴ A challenge to the yardstick of the 'reasonable expectation of privacy' is that there is no clarity as to whose expectations are being referred to, there are no criteria ascertaining the concept of 'reasonable' and there is no guidance as to the weight that this criteria carries, for example in relation to other criteria.⁹⁸⁵

Two final points are made regarding data protection. First, the ECtHR has not adjudicated cases where data processing has taken place with consent, nor has the principle of re-purposing really been addressed.⁹⁸⁶ Second, the reference to data protection in the context of Article 8 ECHR does not necessarily apply to all types of data. For example, in *Leander v. Sweden*, the Court made the distinction between personal data that fell within the ambit of Article 8 ECHR and personal data that did not.⁹⁸⁷

5.4.3.6.4 Access to Information

Another dimension of human rights jurisprudence is the notion of information and the right of access to information, where Article 8 ECHR has been deemed relevant. *Gaskin v. United Kingdom* raised the issue of the relevance of Article 8 ECHR in relation to access to information. First, the Court held that considering that the file was the Applicant's only source of information about his past and formative years, Article 8 ECHR was applicable.⁹⁸⁸ Also, referencing *Leander v. Sweden*, the Commission referred to the fact that storing or releasing information, coupled with the inability to refute that information, amounted to a breach of Article 8 ECHR.⁹⁸⁹ A reason for deciding in favour of Gaskin was the lack of an independent body to assess whether the rights of a person requesting access to a file or the rights of the contributors to that file

984 *Halford v. United Kingdom, Copland v. United Kingdom*, para. 41, in Bygrave, *Data Privacy Law*, above n. 69, at p. 89.

985 Bygrave, *Data Privacy Law*, above n. 69, at p. 90.

986 *Ibid*, at p. 91.

987 *Leander v. Sweden*, para. 48.

988 *Gaskin v. United Kingdom*, para. 36.

989 *Leander v. Sweden*, para. 48.

weighed more.⁹⁹⁰ The Commission also argued that, within the notion of respect for private life, everyone should be entitled to establish details of their identity as individual human beings and should not be obstructed by the authorities from obtaining this information.⁹⁹¹

Guerra v. Italy concerned forty applicants from the town of Manfredonia, which was in close proximity to a chemicals factory. The applicants stated that they had not received important information from the authorities concerning the pending risks involved in living so close to the factory, or the procedures to be followed in the case of a major accident at the factory, which amounted to an infringement of the right to private life according to Article 8 ECHR.⁹⁹² First, the Court found that Article 8 ECHR included not only the negative obligation of protecting individuals from interference but also included a positive obligation to protect private life in an effective manner. Second, the Court held that not only did the environmental pollution prevent the individuals from enjoying their homes, in a manner that contravened Article 8 ECHR, but that they did not receive adequate information that would have enabled them to assess the risks that they were exposed to as well as the procedures in case of an accident. The Court agreed with the assertion that the matter pertained to family life, and also that the families were entitled to all the information necessary to make an informed decision.⁹⁹³

5.4.3.6.5 *Collection of Personal Information*

In *Leander v. Sweden*, mentioned above, the Applicant, a carpenter, was employed by the Naval Museum in Karlskrona in Sweden, which was situated adjacent to the Karlskrona Naval base. The Applicant needed a security clearance for his job in order to access some restricted areas. The Applicant's employment was terminated without reason and a communication from the Supreme Commander of the Armed Forces included a secret annex on the Applicant from the National Police Board. The Applicant alleged that his employment had been terminated based on secret information, which portrayed

990 *Gaskin v. United Kingdom*, para. 49.

991 *Ibid*, para. 39.

992 *Guerra v. Italy* (1998) 26 EHRR 357.

993 *Guerra v. Italy*, paras. 58 and 60.

him as a security risk and damaged his reputation. The Applicant argued that his being placed in the Security Police Register and being labelled a security risk amounted to a breach of Article 8 ECHR. The Court came to the conclusion that the storing of information of this nature, the release of this information and the refusal to allow the Applicant to refute it amounted to an interference with his right to private life in Article 8(1) ECHR. Considering that multiple authorities in Sweden oversaw the procedures and that these safeguards met the requirements of ‘in accordance with the law’ in Article 8(2) ECHR, the state’s national interests were judged to weigh more.

A notion referred to in the case law of the ECtHR is that of the ‘systematic collection and storage of personal information’, referred to in *Amman v. Switzerland*.⁹⁹⁴ A telephone call by a private person originating from the former Soviet embassy in Berne was intercepted by the Federal Public Prosecutor’s Office, resulting in an investigation into the Applicant and a security card on him being created and stored. The card indicated that the applicant had been ‘identified as a contact with the Russian embassy’ and was a businessman, with other references to ‘communist country’, ‘Soviet Union’, ‘espionage established’ and ‘various contacts with the Eastern Block’, amounting to a systematic collection of data with no purpose. The Court stated that, ‘the storing by a public authority of information relating to an individual’s private life amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding...’.⁹⁹⁵ In other words, the mere act of storing data concerning an individual can be judged as being in contravention of Article 8 ECHR even if these data are subsequently never used for any particular purpose.⁹⁹⁶ This attitude to stored data was also communicated in *Leander v. Sweden*, where it was held that, ‘[b]oth the storing and the release of such information, which were coupled with a refusal to allow Mr. Leander an opportunity to refute it, amounted to an interference with his right to respect for private life as guaranteed by Article 8 § 1 (art. 8-1)’.⁹⁹⁷ *Kopp v. Switzerland* was also referred to in the *Amann* case as support

994 *Amann v. Switzerland* (2000) 30 EHRR 843, para. 69.

995 *Ibid*, para. 69.

996 Bygrave, *Data Privacy Law*, above n. 69, at p. 111.

997 *Leander v. Sweden*, para. 48.

for the view that even if information is not used, this has no bearing on a finding.⁹⁹⁸

Bouwer also notes that reference to a systematic collection and storage of information has surfaced in other case law of the ECtHR. In *Rotaru v. Romania*, the ECtHR came to the conclusion that, ‘public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities’, something which Bouwer contends is exacerbated by the fact that information had been collected far back in the past.⁹⁹⁹ The case of *Rotaru v. Romania* concerned the Applicant who alleged that his right to respect for private life had been violated because the Romanian Intelligence Service (RIS) held a file containing personal information relating to him.¹⁰⁰⁰ The Court made some important points. First, referring to *Leander v. Sweden*, it noted that the storing of a secret file containing personal information on the Applicant did amount to a violation of Article 8(1) ECHR. Second, it referred to *Niemietz v. Germany* and *Halford v. United Kingdom*, where it was held that there was no reason to exclude activities of a professional or business nature from the notion of private life. The Court also stated that, ‘... public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person’s distant past’.¹⁰⁰¹ Therefore, considering the length of time over which the information was held and the private nature of the information, Article 8(1) ECHR was judged applicable. Ultimately, in determining whether there was any legitimate interference according to Article 8(2) ECHR, the Court found that domestic law was not clear on the scope and discretion conferred upon public authorities, and proceeded to find that the state’s actions were not in accordance with the law as required by Article 8(2) ECHR.

The notion of information of a public nature being treated as private was also considered in the case of *P.G. and J.H. v. United Kingdom*. Here the Court’s judgement revolved around the distinction between private and public and the role played by technology as far as that distinction was concerned. It referred to instances where a person’s actions in public, for example outside

998 *Kopp v. Switzerland* (1998) 27 EHHR 93, para. 53.

999 *Rotaru v. Romania*, in Brouwer, above n. 833, at p. 155.

1000 *Rotaru v. Romania*, para. 67.

1001 *Ibid*, para. 25.

his or her home or business, may be recorded or reported in a public manner. Here a person's reasonable expectation to privacy may be significant but not conclusive. However, such material from the public domain becomes part of the private, 'once any systematic or permanent record comes into existence of such material from the public domain'.¹⁰⁰²

5.4.3.6.6 *Mass Surveillance*

An issue that has received attention of late, especially after the revelations of Snowden, is that of mass surveillance. While concerning the issue of surveillance by state authorities, what becomes apparent is that many of the issues raised also are generally applicable to the commercial sector.

One case that came before the ECtHR was that of *Roman Zakharov v. Russia*, where Zakharov was deemed to be a victim of mass surveillance by the Russian secret service and police.¹⁰⁰³ The Court put forward a number of protective measures that were relevant in relation to surveillance, namely, the circumstances under which the authorities can resort to surveillance, the duration of these measures, the procedures in place for authorising interceptions and the storing and destruction of these intercepted data as well as the supervision of the interception. According to De Hert and Cristobal Bocos, these principles could be used in order to ascertain whether any system respects fundamental values.¹⁰⁰⁴ In order to be able to challenge any surveillance measure carried out, of utmost importance is knowledge of its existence. In this regard it has been noted that a duty to notify has gradually been established by the ECtHR.¹⁰⁰⁵ Also, in 1987 the CoE issued Recommendation R (87) 15 requiring that individuals be notified if they have been the subject of surveillance.¹⁰⁰⁶

1002 *P.G. and J.H. v. United Kingdom*, para. 57.

1003 *Roman Zakharov v. Russia*, (App. 47143/06), 4 December 2015.

1004 DeHert, Paul and Cristobal Bocos, Pedro, *Case of Roman Zakharov v. Russia: The Strasbourg follow up to the Luxembourg Court's Schrems judgment*, available at <https://strasbourgobservers.com/2015/12/23/case-of-roman-zakharov-v-russia-the-strasbourg-follow-up-to-the-luxembourg-courts-schrems-judgment/> (last accessed on 2017-03-07). See also *Roman Zakharov v. Russia*, para. 231.

1005 *Ibid.*

1006 Boehm, Franziska and De Hert, Paul, *Notification, an important safeguard against the improper use of surveillance - finally recognized in case law and EU law*, European Journal of Law and Technology, Vol. 3, No. 2, 2012.

Another aspect taken up in *Roman Zakharov* is that the technology used for surveillance did not produce any logs, in turn making it difficult for any supervisory body to review the surveillance activities.¹⁰⁰⁷

5.4.4 Data Protection

Within the European context, data protection is an entrenched concept, describing a series of principles that must be taken into account in connection with the processing of personal data.¹⁰⁰⁸ As a concept it has taken root in the European context, however, its underlying goals still remain the protection of privacy, protection against discrimination and promotion of the freedom of expression.¹⁰⁰⁹ Data protection law is mainly statutory, it establishes independent bodies to oversee its application, and its regulatory instruments are usually promulgated in the form of ‘framework laws’ that are intentionally vague and require subsequent interpretation, a role performed by the data protection agencies.¹⁰¹⁰

The EU data protection regime has not developed in a vacuum, with other institutions having had a significant effect on this legal framework. In this respect, reference is made to the ‘traditional’ role of the CoE and the ‘emerging’ role of the EU.¹⁰¹¹ Consequently, an investigation of the EU data protection framework would be incomplete without reference to two major interna-

1007 *Roman Zakharov v. Russia*, para. 272.

1008 Gutwirth, Serge and De Hert, Paul, *Regulating Profiling in a Democratic Constitutional State*, in Hildebrandt, Mireille and Gutwirth, Serge (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer Science and Business Media, 2008, at p. 281.

1009 Bygrave, *Privacy and Data Protection in an International Perspective*, above n. 69, at p. 180.

1010 Bygrave, *Data Privacy Law*, above n. 69, at p. 3.

1011 Solove and Schwartz, above n. 517, at p. 1064.

tional codes, namely, the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980)¹⁰¹² and the CoE Convention 108¹⁰¹³, referenced above in the context of human rights law. Two additional pieces of legislation examined have a clearer EU character, namely the Data Protection Directive 95/46/EC (DPD)¹⁰¹⁴ and the General Data Protection Regulation (GDPR).¹⁰¹⁵ The Data Protection Directive can also be described as having an international character in that it requires national implementation in each of the Member States. The GDPR, being a Regulation, is directly applicable in the Member States and has the character of both international as well as national legislation. The DPD is argued to be one of the most influential instruments regulating data protection and seen as a ‘trendsetter and benchmark’ for data protection around the world, with other instruments being updated to follow this trend.¹⁰¹⁶ Yet another reason for emphasising the DPD is that it has gained international importance due to the provision regulating the transfer of personal data to third countries (stipulating a prohibition on such a transfer to countries that do not have a sufficiently high level of data protection).¹⁰¹⁷ The OECD Guidelines and Convention 108 have also championed data protection concepts such as ‘fairness’, ‘transparency’, ‘lawful justification for processing’, ‘reasonable access to information’ and ‘appropriate security arrangements’.¹⁰¹⁸ The OECD Guidelines are dealt with under this section even though, as alluded to above, they have an origin in human

1012 Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (adopted 23 September 1980; (C (80)58/FINAL as amended on 11 July 2013 by C (2013)79).

1013 European Treaty Series No. 108, adopted 28th January 1981, in force 1st October 1985.

1014 Directive 95/46 of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995.

1015 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final, 25.1.2011.

1016 C.E.T.S. No. 181; adopted 23rd May 2001; in force 1st July 2004, in Bygrave, Lee, *Privacy and Data Protection in an International Perspective*, above n. 69, at p. 188.

1017 Bygrave, *Privacy and Data Protection in an International Perspective*, above n. 69, at p. 183.

1018 Kuner, Christopher, Cate, Fred H., Millard Christopher and Svantesson, Dan Jerker B., *Editorial*, *International Data Privacy Law*, 2011, Vol. 1, No. 1, at p. 1.

rights protection too. The close relationship between technology regulation and human rights becomes evident by the following statements made at the World Summit on the Information Society, where the Declaration of Principles states that:

We reaffirm, as an essential foundation of the Information Society, and as outlined in Article 19 of the Universal Declaration of Human Rights, that everyone has the right ... to seek, receive and impart information and ideas ... Everyone, everywhere should have the opportunity to participate and no one should be excluded from the benefits the Information Society offers.¹⁰¹⁹

5.4.4.1 The Development of Data Protection

Even though the terms ‘privacy’ and ‘data protection’ are indicative of the differences with which the topic is treated in the US and Europe, these two entities have influenced each other as far as the means of finding a solution to the effects of technology on personal privacy is concerned. At the same time as the HEW Committee was meeting in the US, the Younger Committee was meeting in the UK, ultimately producing a report entitled Privacy in Great Britain.¹⁰²⁰ While the concept of ‘fundamental principles of fair information practice’ were to have its origin in the HEW Committee, the phrase ‘fair information principles’ originated from the work of the Younger Committee.¹⁰²¹ What is clear is that European data protection instruments have been influenced by developments in the US, from where many of the principles making up data protection law were imported.

1019 World Summit on the Information Society Declaration of Principles, 12 December, 2003, available at <http://www.itu.int/net/wsis/docs/geneva/official/dop.html> (last accessed on 2016-10-05).

1020 Report of the Committee on Privacy (Younger Committee), Home Office, London: HMSO, 1973 available at <http://hansard.millbanksystems.com/lords/1973/jun/06/privacy-younger-committees-report> (last accessed on 2017-03-05).

1021 Brouwer, above n. 833, at p. 195.

5.4.4.1.1 *Alan Westin*

An influential scholar in the area of data privacy was Westin, who in 1967 produced the work *Privacy and Freedom*.¹⁰²² Rule et al., in their analysis of Westin's work, describe it as an analysis of the challenges to privacy, caused by the intrusion of previously balanced social relationships. This intrusion was caused by technology, creating pressures against privacy not anticipated before. Westin, they argue, was confident in the ability of law to 'restore the balance', especially by means of procedural rules.¹⁰²³ Westin based much of his thinking on the manner in which access to personal information was addressed in US Constitutional law, stating that, '[g]iven this setting, American constitutional, statutory, and common law concentrated on establishing shields of privacy to protect individual and organizational autonomy, ensure personal and family privacy in the home, and safeguard confidentiality in the basic modes of communication.'¹⁰²⁴ Westin also saw the utility in describing the situation then in terms of a property model as well as the utility of administrative rules:

With personal information so defined, a citizen would be entitled to have due process of law before his property could be taken and misused by government or by agencies exercising such enormous public power that they would be held to the same rules as government. Allowing for certain exceptions ... an individual would have to be notified when information was put into key central files. He would be able, if so desired, to examine the information that had been put into his file, to challenge its accuracy in some kind of administrative proceeding (with court review), and to submit a reply or explanation that would be coupled permanently to the information ... the growth of personal-data processing will necessitate the same high level of analysis and planning ... Provisions for confidentiality of information, restrictions on improper circulation, and sanctions against unauthorized use should be written into the basic legislation and administrative rules ...¹⁰²⁵

Westin envisioned privacy as having four main states, namely 'personal autonomy', 'emotional release', 'self-evaluation' and 'limited and protected

1022 Westin, above n. 462.

1023 Rule, McAdam, Stearns and Uglow, above n. 319, at pp. 74-77.

1024 Westin, above n. 462, at p. 330.

1025 Ibid, pp. 330-386.

communication', all these states influencing one another.¹⁰²⁶ On personal autonomy, Westin described how almost all democratic societies share the belief not only in the uniqueness of the individual but also in the value of having 'social processes' that protect this individuality.¹⁰²⁷ Autonomy, described as the 'desire to avoid being manipulated or dominated wholly by others', would protect individuality.¹⁰²⁸ He viewed autonomy as being made up of 'zones' or 'regions of privacy' surrounding the 'core self' – the core self being at the centre and housing the individual's 'ultimate secrets', which in turn was surrounded by multiple concentric circles, each circle protecting a less sensitive representation of the core self. Normally, no-one would be admitted to the core self, and as one moved further away from it, and the further the circle was from the core self, the more other people were provided with access to that aspect of the individual.¹⁰²⁹ Westin stated that penetration of the core self was the biggest threat to an individual's autonomy as this would leave him or her open to ridicule and those who were in possession of these secrets would be in control, another implication being that those who access the core zone would not appreciate the importance of privacy to that individual.¹⁰³⁰ For Westin, another aspect of autonomy was that the individual needed a place to which he or she could withdraw, in order to experiment and test. This individuality was an important component of the democratic society encouraging qualities such as independent thought, diversity of views and non-conformity. In addition, the ability to 'go public' was an important aspect of autonomy.¹⁰³¹ Rule et al. highlight Westin's dislike of the polygraph technology as it invaded an 'inner domain' where the individual was most vulnerable.¹⁰³²

Rule et al. are critical of the notion that due process and administrative rules could address the imbalance created by new technology, in that they could not bring society back to the situation where there was an even distribution of power.¹⁰³³ They argue that procedural rules can provide individuals with some

1026 Ibid, p. 32-39.

1027 Ibid, p. 33.

1028 Ibid.

1029 Ibid, p. 33.

1030 Ibid, p. 33.

1031 Ibid, p. 34.

1032 Rule, McAdam, Stearns and Uglow, above n. 319, at p. 79.

1033 Ibid, at p. 81.

degree of control, '[b]ut no one can live anything like a normal life in a modern bureaucratic society without providing significant amounts of personal information to organizations', asserting that if a person had absolute control over his or her personal information, then that data would be useless to the organization.¹⁰³⁴ In their opinion, Westin ignored the reality that large centralized data systems in the hands of centralized institutions put these institutions in a powerful position in relation to individuals. According to Westin, privacy was, 'the claim of individuals, groups, or institutions to determine for themselves, when, how and to what extent information about them is communicated to others'.¹⁰³⁵ Rule et al. argue that this definition of privacy allowed for the argument that limited control could protect it. Instead individuals would need absolute control over the data held by centralized organizations in order to reach a situation where privacy was really protected.¹⁰³⁶

5.4.4.1.2 *The Fair Credit Reporting Act*

A legal instrument addressing the issue of privacy in the face of technological developments in the US was the Fair Credit Reporting Act (1970). It had as its aim the regulation of personal data systems and was a reaction to public concerns, to what was thought of at the time as dubious practices within the credit rating industry by credit bureaus.¹⁰³⁷ Incorrect credit reports could damage a person's reputation permanently, especially where these credit reports were secret. The Fair Credit Reporting Act created awareness about the credit reporting industry, allowing for people to understand the practices and their effects. The Act included mechanisms for resolving disputes between individuals and consumers relating to a disagreement over credit information and placing legal responsibilities on the credit bureaus.

Rule et al., in examining the consequences of the Fair Credit Reporting Act, make one telling analytical point, namely, that it legitimized the activities reg-

1034 Ibid, at p. 82.

1035 Westin, above n. 462, at p. 7.

1036 Rule, McAdam, Stearns and Uglow, above n. 319, at p. 81.

1037 Ibid, at p. 88.

ulated by the Act and backed the status quo by siding with the establishment.¹⁰³⁸ In other words, the message it provided was that the practices of the credit bureaus could continue provided that the procedural regulations in the Act were adhered to. It did not limit the actions of the credit bureaus nor did it state that any part of their business was unacceptable, unlawful or unethical. In fact, as Rule et al. observe, the ability of consumers to correct certain data held by the bureaus made their data more accurate, which in turn provided them with the opportunity to make even more far reaching judgements about people.¹⁰³⁹

Despite criticism of the Fair Credit Reporting Act perpetuating the status quo, it did provide input into and was relied on in the creation of subsequent legislation on the EU level, most notably, the CoE Convention 108.¹⁰⁴⁰ In this way, the ideas of Westin, which shaped privacy norms at the time, made their way into the Fair Credit Reporting Act and ultimately into the EU data protection framework.

5.4.4.1.3 *The HEW Committee*

In 1973 the Report to the Secretary of the Department of Health, Education and Welfare as produced by its advisory Committee on Automated Personal Data Systems was published.¹⁰⁴¹ This report, later to be referred to as the ‘HEW Report’, reflected the ideology of Westin but also of Arthur R. Miller, while also incorporating much of the opinion that went into the Fair Credit Reporting Act mentioned above.¹⁰⁴² The main theme put forward by Westin and Miller was the erosion of privacy due to the development of technology, which upset the social balance and would lead to abuse if no corrective action was taken.¹⁰⁴³ The HEW Report authors were aware of the problems associ-

1038 Ibid, at p. 91.

1039 Ibid, at p. 94.

1040 Opened for signature 28 January 1981; in force 1 October 1985; ETS 108.

1041 US Department of Health, Education, and Welfare, Secretary’s Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* (Washington D.C.: Government Printing Office, 1993) (HEW Report).

1042 Rule, McAdam, Stearns and Uglow, above n. 319, at p. 96.

1043 Ibid.

ated with administrative and statistical personal-record systems, acknowledging that, '[t]hey are failures of systems to achieve the purposes for which they were created, or failures to provide for awareness and participation of the subject of the records'.¹⁰⁴⁴ The report suggested the need for regulatory involvement stating that, 'the natural evolution of [the] existing law will not protect personal privacy from the risks of computerized personal data systems'.¹⁰⁴⁵ As a result, the HEW Report suggested adherence to five basic principles in the Code of Fair Information Practices, namely that, 1) there must be no personal-data record-keeping systems whose very existence is secret, 2) there must be a way for an individual to find out what information about him or her is in a record and how it is used, 3) there must be a way for an individual to prevent information about himself being obtained for one purpose from being used or made available for other purposes without consent, 4) there must be a way for an individual to correct or amend a record of identifiable information about himself or herself and 5) any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.¹⁰⁴⁶

The following passage from the report highlights the attitude of the Committee:

An individual's personal privacy is directly affected by the kind of disclosure and use made of identifiable information about him in a record. A record containing information about an individual in identifiable form must, therefore, be governed by procedures that afford the individual a right to participate in deciding what the content of the record will be, and what disclosure and use will be made of the identifiable information in it. Any recording, disclosure, and use of identifiable personal information not governed by such procedures must be proscribed as an unfair information practice unless such recording, disclosure or use is specifically authorized by law ... This formulation does not provide the basis for determining *a priori* which data should or may be recorded and used, or why, and when. It does, however, provide a basis for establishing procedures that assure the individual a right to participate in a meaningful way

1044 Ibid, at p. 97.

1045 Regan, above n. 527, in Purtova, above n. 88, at p. 116.

1046 US Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Persona, above n. 1041, at pp. 29-30 and 41-42.

in decisions about what goes into records about him and how that information shall be used.¹⁰⁴⁷

The HEW Report is significant in a number of ways. Regan contends that the aim of the Code of Fair Information Practices was not to restrict the collection of information, but rather to promote individual privacy by highlighting fairness in information practices.¹⁰⁴⁸ Solove et al. describe them as an attempt ‘to correct [the] information asymmetries between an individual and the data-processing organisations resulting from massive data transfers.’¹⁰⁴⁹ The Fair Information Practices have been described as ‘empowering’ by Regan, who states that, ‘the Code was framed around the concept of giving individuals the means to protect privacy as they saw fit’.¹⁰⁵⁰ Just as with the Fair Credit Reporting Act, the effect of the HEW Report was contentious, with critics stating that the report producers neglected to ask the most important question, namely whether these systems should exist at all, and failed to address the issue of balancing the gains from the existence of these systems against the cost to privacy.¹⁰⁵¹

5.4.4.2 A Legal Framework

The OECD Guidelines and CoE Convention 108 are examined for their relevance in respect to the historical development of data protection within the European context. Although not legally binding, they have played an important role in the development of data protection law and have played a significant role in determining the fabric of EU data protection law.

5.4.4.2.1 *OECD Guidelines*

One of the most important instruments influencing data protection is the 1980 OECD Guidelines Governing the Protection of Privacy and Transborder

1047 Ibid, at pp. 40-41.

1048 Regan, above n. 527, at pp. 75-76.

1049 Solove et al., *Information Privacy Law*, p. 578, in Purtova, above n. 88, at p. 116.

1050 Regan, above n. 527, at pp. 76-77.

1051 Rule, McAdam, Stearns and Uglow, above n. 319, at p. 99.

Flows of Personal Data produced by the Organization for Economic Cooperation and Development (‘OECD Guidelines’).¹⁰⁵² This instrument, stressing self-regulation, applied to the processing of personal data, providing a minimum level of protection while taking the form of Guidelines that were not binding on members of the OECD.¹⁰⁵³ While formally having a lower normative status as compared to other legal instruments, it has had considerable influence within the EU legal regime and has been described as having gained the status of a ‘constitutional instrument of European public order in the field of human rights’.¹⁰⁵⁴ It has had a considerable influence as its broad principles allow many countries to identify with it, and has also influenced the development of the CoE Convention 108 in 1981.¹⁰⁵⁵

While the OECD is as a rule not concerned with the issue of human rights, the core of the OECD Guidelines has the goal of the protection of the human right of privacy. It also harmonises national legislation in the area of privacy and data protection in order to create an environment within which economic interests are considered. A reason for the development of the OECD Guidelines was the evolution of the transborder notion of data, which in turn created the need for a document that was international in nature.¹⁰⁵⁶ Hence, while taking human rights into account, the main aim of the Guidelines was to facilitate the transborder flow of data, in other words, create a climate for the free flow of facts, opinions and creative ideas, which in turn would encourage economic and social development.¹⁰⁵⁷ The effectiveness of the OECD Guidelines was increased because it operated globally, and not, for example, just within the EU. While the OECD Guidelines were not legally binding it was hoped that

1052 Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (adopted 23 September 1980; (C (80)58/FINAL as amended on 11 July 2013 by C (2013)79).

1053 Solove and Schwartz, above n. 517, at p. 1064.

1054 Polakiewicz, J. and Jacob-Foltzer, V., *The European Human Rights Convention in Domestic Law*, 12 Human Rights Law Journal, 65, 125 (1991) in Solove and Schwartz, above n. 517, at p. 1064.

1055 Brouwer, above n. 833, at p. 182.

1056 Kirby, above n. 857, at p. 7.

1057 Ibid, at p. 8.

the utility of the guidelines would be the driving force behind member countries implementing them.¹⁰⁵⁸ In addition, the rapid increase in technological developments necessitated the need for an international regime.

The OECD Guidelines spell out eight data privacy principles relating to processing personal data in both the public and private sectors.¹⁰⁵⁹ The principles are broad and loosely defined, thereby allowing for a large number of countries to identify with the ideals that they articulate. The following are the guiding principles incorporated in the OECD Guidelines: collection limitation principle (paragraph 7), data quality principle (paragraph 8), purpose specification principle (paragraph 9), use limitation principle (paragraph 10), security safeguards principle (paragraph 11), openness principle (paragraph 12), individual participation principle (paragraph 13) and the accountability principle (paragraph 14).

The OECD Guidelines also had to take into account the vastly different attitudes to privacy that existed in the US as compared to the EU. In the US it was thought that the European strategy of protecting privacy was too bureaucratic and heavy handed, while the EU was influenced by the experience of how the processing of data was abused during World War II. In the EU the priority was therefore a matter of keeping both public and private power under legal control and ensuring that the individual had ultimate control.¹⁰⁶⁰

As of September 2013, the OECD Guidelines were revised, which did not change any of the eight core principles. The aim of the revision was announced prior to the revision as, ‘addressing consumer protection and empowerment, privacy and security in light of changing technologies, markets and user behaviour and the growing importance of digital identities’.¹⁰⁶¹

1058 Ibid, at p. 10.

1059 Bygrave, *Data Privacy Law*, above n. 69, at p. 3.

1060 Kirby, above n. 857, at p. 9.

1061 Seoul Declaration for the Future of the Internet Economy (18 June 2008; C (2008)99) in Bygrave, *Data Privacy Law*, above n. 69, at p. 44.

5.4.4.2.2 Council of Europe Convention 108

In 1976 the European Committee for Legal Co-Operation was instructed to prepare a Convention for the protection of privacy, and to do so in collaboration with the OECD.¹⁰⁶² In 1968 the Council of Europe wished to investigate whether the ECHR was adequate to protect privacy in the face of modern technology.¹⁰⁶³ This resulted in the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108) (hereafter referred to as ‘Convention 108’) entering into force on the 1st of October 1985.¹⁰⁶⁴ It has been argued that the inspiration for Convention 108 was the ECHR’s inadequate protection of individuals in the face of advances in modern computerized technology.¹⁰⁶⁵ Identifying a need for renewal, the Council of Europe produced Convention 108 in 1981 in order to remedy what it considered to be shortcomings with the ECHR. The main aim of the Convention was the protection of the right to privacy in relation to the processing of personal data.¹⁰⁶⁶ It has since been updated by an Additional Protocol (2001).¹⁰⁶⁷ Yet another aim of Convention 108 was to ensure the free flow of personal data across borders.¹⁰⁶⁸ So while Article 1 states that an aim of Convention 108 is to protect the rights and freedoms of individuals, the Preamble refers to a second main goal, namely, safeguarding the free flow of information. The attainment of this goal was to be facilitated by harmonizing data protection rules so as to prevent national legislation from creating obstacles for this aim.¹⁰⁶⁹ Article 5 of Convention 108 states that:

1062 Brouwer, above n. 833, at p. 182.

1063 Ibid, at p. 181.

1064 European Treaty Series No. 108, adopted 28th January 1981, in force 1st October 1985.

1065 Bygrave, *Data Privacy Law*, above n. 69, at p. 34.

1066 Gutwirth and De Hert, above n. 896, at p. 5.

1067 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows (open for signature 8 November 2001, in force 1 July 2004, ETS 181).

1068 Ibid, at p. 3.

1069 Brouwer, above n. 833, at p. 183.

Personal data undergoing automatic processing shall be obtained and processed fairly and lawfully; stored for specified and legitimate purposes and not used in a way incompatible with those purposes; adequate, relevant and not excessive in relation to the purposes for which they are stored; accurate and, where necessary, kept up to date and finally preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Here one can see how the core principles of Convention 108 resemble the ‘fair information practices’ incorporated in the OECD Guidelines. Convention 108 is an international Code to the extent that non-CoE Member States can accede to it. Many of the changes that were made to the 2013 Amendment were done in order to meet the demands of globalisation, to keep pace with the forthcoming GDPR and to make sure that there was equality as far as accession to Convention 108 by non-EU and EU countries was concerned.¹⁰⁷⁰

5.4.4.3 The Data Protection Directive

The DPD provides guidelines on how data should be processed in addition to protecting other rights of the data subject. Data protection has an origin in human rights law and related instruments that enshrine these human rights, for example the UDHR and the ICCPR. Data protection has grown out of the notion of privacy, more specifically Article 8 ECHR.¹⁰⁷¹ The move towards data protection culminated in a number of directives on privacy and data protection, where the DPD became the most well-known.¹⁰⁷² The DPD was adopted in 1995 and has been described as an ‘omnibus’ instrument in that it regulates

1070 Greenleaf, Graham, *'Modernising' Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?*, *Computer Law and Security Review*, Vol. 29, Issue 4, 2013, at p. 2.

1071 Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*, above n. 825, at p. 116.

1072 There are other Directives that deal with privacy, for example Directive 97/66/EC (O. J., No L 24, 30-01-1998) concerning the processing of personal data and the protection of privacy in the telecommunications sector as replaced by Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive).

a large area of information law, as opposed to sectoral legislation that regulates a specific issue or industry.¹⁰⁷³ As a Directive, the DPD must be implemented into the national law systems of the Member States, which has provided them with a certain amount of leeway as regards its interpretation. The DPD has two main aims. First, it provides the legal framework within which the processing of personal data may occur. It provides both the circumstances under which personal data may be collected, stored and processed as well as the restrictions under which this processing is allowed to occur.¹⁰⁷⁴ In other words, as long as the rules and procedures as prescribed are followed, the processing of personal data may continue. Second, the aim of the DPD, just as with other data privacy laws, is to harmonize national data privacy laws in order to ensure the flow of data across the borders of the EU Member States.¹⁰⁷⁵ This dual objective has been described as slightly ‘paradoxical’ as the free flow of data within the EU is to be facilitated by ensuring Member States harmonize their privacy laws.¹⁰⁷⁶

The DPD encapsulates a number of basic principles. The historical development in the US of privacy enhancing initiatives is crucial in this regard as it is that ideology and attitude towards technology, as espoused by Westin and the authors of the HEW Report, that ultimately made its way into EU data protection legislation. It is with this in mind that the DPD closely resembles the fair information practices principles that originated in the US, gaining acceptance via the OECD Guidelines of 1980.

Focussing on the division between privacy and data protection, Gutwirth and De Hert refer to two types of tools, that highlight the differences between privacy legislation and data protection legislation. They refer to ‘transparency tools’ and what they call ‘tools of opacity’. This is a useful description as it highlights the distinctive nature of data protection legislation, such as the DPD. They argue that data protection legislation belongs to the category of transparency tools, which are tools that compel actors to act in a desired manner, for example, by increasing transparency and thus accountability. Privacy, they argue, is protected by opacity tools that ensure non-interference with an

1073 Solove and Schwartz, above n. 517, at p. 1110.

1074 Hildebrandt, *Profiling and the Identity of the European Citizen*, above n. 283, at p. 319.

1075 Bygrave, *Data Privacy Law*, above n. 69, at p. 123.

1076 Solove and Schwartz, above n. 517, at p. 1110.

individual's private sphere. These tools propagate a hands-off approach as regards an individual and allow the individual a certain amount of autonomy, liberty and therefore space for identity building.¹⁰⁷⁷ Opacity tools are characterised by prohibition rules while transparency tools are characterised by regulated acceptance.¹⁰⁷⁸ Data protection legislation is a transparency tool in that it is of a procedural nature and allows the processing of personal data to continue provided that the procedural rules are followed. The procedural rules allow for transparency and accountability as well as a limited amount of control. In doing so, they provide insight into the working of powerful actors, such as government or even private entities that control the technologies that utilize personal data. The authors point out that data protection legislation creates a set of rights, where the data subject has certain rights, such as the right to information and the right to have data corrected, and also sets numerous obligations on the controller to handle data in a certain manner.¹⁰⁷⁹

5.4.4.3.1 *Data Protection and Autonomy*

Autonomy, while not explicitly stated as such, is an implicit goal of the DPD.¹⁰⁸⁰ Autonomy has come to be a protected value through the incorporation of norms relating to human rights into the data protection regime (other values being privacy, integrity and dignity).¹⁰⁸¹ The values entrenched by the DPD have been categorized into two types, namely the quality of information and the interests in relation to the condition of the individual as data subject, autonomy here also being a central value (together with privacy, civility, democracy, pluralism, the rule of law and balanced control).¹⁰⁸² Autonomy is further described in three ways, namely as 'informational self-determination', in the sense that a person is able to determine how his or her data will be processed, as 'informational co-determination', where a person has some say

1077 Gutwirth and De Hert, above n. 1008, at page 271.

1078 Ibid.

1079 Ibid.

1080 Bygrave, *Data Privacy Law*, above n. 69, at p. 8.

1081 Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*, above n. 825, at p. 167.

1082 Ibid.

in how his or her data will be processed and finally ‘identificational self-determination’, where a person is able to determine and protect his or her identity in relation to others.¹⁰⁸³ Bygrave highlights that while the individual or data subject perspective fosters the view that privacy and autonomy remain values to be protected by data protection law, other perspectives result in privacy and autonomy having ‘less validity’ in comparison to other values.¹⁰⁸⁴

Rouvroy and Pouillet argue that privacy consists of two aspects, namely, a right to seclusion and a right of decisional autonomy, both of which are protected by data protection: seclusion by forbidding the processing of certain types of data and decisional autonomy by assuring the transparency of informational flows as well as limiting them so as to avoid what they term the ‘disproportionate informational power relationships to be developed or perpetuated between public and private data controllers and citizens’.¹⁰⁸⁵ Bygrave also argues that autonomy is included in the set of rights protected by data protection, suggesting that one of the main aims of the DPD is to protect the interests and rights of the data subject as far as the processing of personal data is concerned, which rights and interests are expressed in terms of privacy, autonomy and/or integrity.¹⁰⁸⁶

5.4.4.3.2 *The Principles of Data Protection*

Data protection is built on a number of core principles, which form the core of the DPD. The principles are fair and lawful processing, proportionality, minimality, purpose limitation, data subject influence over the processing of personal data, data quality, data security and finally sensitivity.¹⁰⁸⁷ Put slightly differently, these principles include the right to be properly informed, the right to access one’s own data, the right to have data rectified, the right against

1083 Ibid, at p 150.

1084 Ibid, at p. 168.

1085 Rouvroy and Pouillet, above n. 436, at p. 70.

1086 Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*, above n. 825, at p. 24.

1087 Ibid, at pp. 145-167.

automated profiling, the right to swift procedures in court, the right to assistance by the data authorities, the right to adequate security measures being implemented and the right to non-disclosure of data without consent.¹⁰⁸⁸

The principle of fairness and lawfulness combines these two concepts that are given effect in Article 6(1)(a) of the DPD. In the context of predictive modelling, the principle of fairness is particularly relevant. According to Bygrave the principle of fairness creates an obligation on the data controller to take into account the interests and reasonable expectations of the data subject. He also notes the extended application of this principle to the information systems supporting data processing and that there exists a requirement that they be designed with fairness in mind. He makes the link between the principle of fairness and that of purpose binding, where the use of data for a secondary purpose would contradict the principle of fairness if the data subject's consent for the secondary purpose was not obtained.¹⁰⁸⁹ Proportionality is argued by Bygrave to be a principle that, while not stated explicitly, can be read into the 'fair information practices' that form the basis of data privacy regulation.¹⁰⁹⁰ Proportionality balances the interests between the controller and the data subject, where in Article 6(1)(c) of the DPD it is stated that data collected shall be 'relevant' and not 'excessive'. The principle of purpose binding is comprised of two parts. First, the processing of data can only take place if it is in accordance with an explicit and specified purpose, and the processing of personal data is not allowed if the purpose no longer applies. As mentioned above, this principle is incorporated into Article 6(b), which states that personal data may only be collected for a specified, explicit and legitimate purpose, with no processing allowed that is not in accordance with the specified purpose. It can therefore be stated that once the purpose principle can no longer be satisfied, the processing of personal data becomes unlawful even with consent. The principle of data minimization is said to be constructed of three sub-principles: first and as mentioned above, the data may only be processed where they are adequate, relevant and not in excess in relation to the specific purpose for which they were collected, second, the data may not be kept for longer than is necessary with the purpose of the data collection in mind and third, another data minimization principle refers to the way data is

1088 Gutwirth and De Hert, above n. 896, at p. 4. See also Rouvroy and Poullet, above n. 436, at p. 68.

1089 Bygrave, *Data Privacy Law*, above n. 69, at p. 146.

1090 *Ibid*, at p. 148.

kept, in that the DPD is no longer applicable in situations where the data cannot be linked to an identifiable subject, for example, in cases where the data has been rendered anonymous.¹⁰⁹¹ The principle of data subject influence is present. According to Bygrave, it originated in the OECD Guidelines in the form of the ‘Individual Participation Principle’ and manifests itself in the DPD, for example, where the controller is required to furnish the data subject with certain types of information.¹⁰⁹² The principle of data quality finds expression in Article 6(1)(d) of the DPD and states that data shall be accurate and up to date.¹⁰⁹³ The principle of data security, as stipulated in Article 7(1), says that data shall be protected from unlawful and accidental destruction, alteration or disclosure. The principle of sensitivity recognizes that certain categories of data can be sensitive in relation to the data subject. Article 8(1) refers to different categories of sensitive data, that is, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership health and finally sexual life.

The DPD is applicable to the processing of personal data. Article 2(a) specifies what ‘personal data’ is:

Personal data shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or societal identity.

Recital twenty-six is relevant with regard to when a person is ‘identified or identifiable’, stating that:

... to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.

The Article 29 Data Protection Working Party has also commented on the concepts ‘identified’ and ‘identifiable’ natural persons. In opinion 4/2007 they

1091 Van der Sloot, Bart, *From Data Minimization to Data Minimumization*, in Custers, Bart et al. (eds.), *Discrimination and Privacy in the Information Society – Data Mining and Profiling in Large Databases*, Springer, 2013, at p. 278.

1092 Bygrave, *Data Privacy Law*, above n. 69, at p. 158.

1093 *Ibid*, at p. 163.

state that an individual can be considered identified when, in a group of other individuals, he or she can be ‘distinguished’ from the other members of the group. The notion of ‘identifiable’ occurs when the individual has not been identified but this may be possible. They continue by stating that identification normally takes place by means of pieces of information commonly referred to as ‘identifiers’, which are described as data that have a close relationship to a particular individual. Finally, it is highlighted that whether a piece of information can act as an identifier depends on context.¹⁰⁹⁴

Article 2(d) provides a broad definition of processing:

“processing of personal data” (‘processing’) shall mean any operation or set of operations which is performed on personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking erasure or destruction.

An integral tool within the DPD to ensure the protection of personal data relating to the data subject is that of ‘consent’. According to Article 2(h), the concept of consent is described in the following manner: the data subject’s consent shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

In the case of sensitive personal data, a higher threshold is employed, and consent must be ‘explicit’ in accordance with Article 2(a).

5.4.4.3.3 Articles 12(a) and 15 of the Data Protection Directive

Articles 12(a) and 15 of the DPD are most applicable in relation to predictive modelling. Article 12 is entitled ‘Right of Access’ and Article 12(a) states, among other things, that the data subject is entitled to receive information concerning ‘the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15(1)’. Preambles 27 and 41 are relevant with regard to Articles 12 and 15. Preamble 27 states that in addition to the DPD applying to both automatic and manual

1094 Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, Adopted on 20th June, at p. 12.

processing, the scope of protection of the DPD must not be determined by the technology used, so as to prevent the circumvention of the DPD.¹⁰⁹⁵ Preamble 41 restricts the ambit of Articles 12 and 15(1) by stating that this right granted to the data subject should not affect trade secrets and intellectual property rights, while at the same time these issues may not block a data subject's insight into the automatic processing. In other words, a balancing of interests is required.

The DPD bestows a right on data subjects not to be subjected to automated decisions, described as being, 'based not on personal judgement but upon an automated processing technique using an individual's personal data'.¹⁰⁹⁶ Article 15(1) is the only article to deal with the automated processing of data.¹⁰⁹⁷ Article 15(1) states that:

Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

Article 15(2) (a) and (b) lay down exceptions to this main rule, that is, when the decision is taken for the sake of entering into or for the performance of a contract or where it is stipulated by law.

Bygrave has commented extensively on Article 15. First, he argues that this article is relevant to the application of the profiling process and does not prohibit the creation of profiles as such. In addition, the right established by this article must be enforced by the individual. Four conditions must be met in order for the above right to be activated. First, a decision must be taken, second, the decision must have legal or significant effects on the person whom the decision targets, third, the decision must be based solely on automated data processing and finally, the data processed must be intended to evaluate certain

1095 Vermeulen, Mathias, *Regulating Profiling in the European Data Protection Regulation: An Interim Insight into the Drafting of Article 20*, EMSOC Working Paper, 2013, SSRN, available at <https://ssrn.com/abstract=2382787> or <http://dx.doi.org/10.2139/ssrn.2382787> (last accessed on 2017-03-30), at p. 7.

1096 Solove and Schwartz, above n. 517, at p. 1114.

1097 Bygrave, Lee, *Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, Computer Law and Security Report, Volume 17, pp. 17-24, 2001, at pp. 17-18.

personal aspects of the person who is targeted by the decision.¹⁰⁹⁸ It can be argued that the word ‘solely’ in the third condition can be interpreted to mean that if there is a minimal amount of human intervention in the profiling process, then Article 15(1) is not applicable. This view is taken by Hildebrandt, who states that, ‘[t]he fact that usually some form of routine human intervention is involved means that art. 15 is not applicable, even if such routine decisions may have the same result as entirely automated decision making’.¹⁰⁹⁹ Bygrave disagrees with this and argues instead that the word ‘solely’ must be read in a relative manner instead of in a strict manner, and that Article 15(1) must be interpreted as applying in situations where there is no real human influence on the outcome of a decision.¹¹⁰⁰ This interpretation therefore allows for the applicability of Article 15(1) in situations where there is some form of human involvement but where this human involvement is not of significance. Finally Bygrave states that the implications of Article 15(1) read together with Article 12(a) are that data controllers are required to understand the logic involved in the profiling process, and that the process be documented and easily available for communication.¹¹⁰¹

Of interest is the position taken by Bygrave that an individual’s failure to exercise the right created by Article 15(1) in effect allows profiling to continue.¹¹⁰² In other words Article 15(1) requires some form of positive action on the part of an individual in order to activate its applicability. This structuring of the rule assumes that the data subject has, or can relatively easily acquire, knowledge of the fact that the automatic profiling is occurring. Gutwirth and De Hert, rejecting this view, argue that the absence of an objection implies consent, which is problematic as this is not in line with the definition of consent as stipulated in the DPD.¹¹⁰³

1098 Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*, above n. 825, at p. 321.

1099 Hildebrandt, *Defining Profiling: A New Type of Knowledge*, above n. 56, at p. 28, footnote 22.

1100 Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*, above n. 825, at p. 324.

1101 *Ibid.*, at p. 325.

1102 Bygrave, *Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, above n. 1097, at p. 3.

1103 Gutwirth and De Hert, above n. 1008, at p. 283, footnote 317.

5.4.4.4 The General Data Protection Regulation

During January 2012 a draft proposal was released for a Regulation to replace the DPD, known as the General Data Protection Regulation (GDPR). Here too the close relationship with human rights was discernible. Recital 5 refers to respect for private and family life, reference is made to the ECtHR in Recital 41, Recital 73 stipulates that any restrictions made in the name of the GDPR should be in accordance with human rights law and Recital 104 states that the Commission, in deciding on the transfer of data to third countries, must take cognisance of, among other factors, the adherence to human rights in that country. The need for the GDPR arose due to the DPD becoming dated as well as the fragmented extent to which it was implemented in the different Member States.¹¹⁰⁴ Just as with the DPD, the GDPR has two main goals at its core, namely the protection of individuals from the risks associated with data processing, and the second aim of developing the internal market so as to facilitate the digital economy.¹¹⁰⁵ The main aim of the GDPR is the protection of individuals in relation to the processing of personal data as identified in the EU Constitution (Article 8(1) of the EU Charter and Article 16(1) Treaty on the Functioning of the European Union (TEFU)).¹¹⁰⁶ Of interest from the outset is that the data processing principles enshrined in the DPD and reflecting the fair information practices, are retained. An additional principle has been added, namely that of accountability. The main data protection principles are summarized in Recital 39 of the GDPR.

5.4.4.4.1 Addressing Predictive Modelling

An interpretation of Recital 71 suggests that its ambit of application addresses technologies that are comparable with predictive modelling. It enshrines the right not to be subjected to a decision based solely on automated data processing, where this decision evaluates the data subject and can lead to, for example, the refusal of credit. A portion of Recital 71 reads as follows:

1104 Recital 6 GDPR refers to the fact that technological developments necessitated a new regime and Recital 9 GDPR refers to the fragmented application of the DPD and the different levels of protection provided.

1105 See Recital 7, GDPR.

1106 See Recital 1, GDPR.

Such processing includes ‘profiling’ that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject’s performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her.

After laying out the area of application of the GDPR prohibiting these measures, a number of exceptions are made, the effect being that these automated decisions are allowed, should the factors activating the exceptions present themselves. First, a Member State can enact a law allowing this type of processing, second, it is allowed for the entering into or performance of a contract between data controller and data subject and third, explicit consent can be attained. The activation of the exceptions does not, however, negate the intended safeguards of the GDPR and the data subject is still entitled to information, to human intervention, to express his or her view and to an explanation as to how the assessment was made. Finally, the type of data processing referred to is never allowed to be applied to children.

Mention is also made to the technology behind the automated processing, where Recital 71 states that the mathematical and statistical procedures used should be appropriate to the circumstances and context within which the data is processed. More specifically, technical and organizational measures must be taken to correct factors that result in inaccuracies in personal data, and ensure the risk of errors is minimized. Also, the data must be secured so as to prevent discriminatory effects on natural persons based on the identified sensitive categories of data (racial or ethnic origin, political opinion, religion or beliefs, trade union membership, and genetic or health status or sexual orientation). Automated decisions and profiling based on these special categories of personal data are allowed, but only under specific conditions. Recital 24 takes up the issue of monitoring of individuals, and makes direct mention of this activity in order to determine the behaviour of people by tracking them on the internet and using data processing techniques to make a profile of that person in order to take a decision concerning him or her and predicting his or her behaviour or personal preferences. Recital 30 refers to the technologies available for tracking people on the internet, in order to produce these profiles.

Recital 63 is particularly relevant in the context of predictive modelling. It concerns the information that the data subject should have access to regarding

the data processing, including, ‘... the logic involved in any automatic personal data processing, and at least when based on profiling, the consequences of such processing’. However, Recital 63 then states that, ‘[t]hat right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software.’ Finally, Recital 63 states that, ‘the result of those considerations should not be a refusal to provide all information to the data subject’ and that any request from a data subject should, ‘specify the information or processing activities to which the request relates’.

5.4.4.4.2 Article 22 General Data Protection Regulation

Article 22 of the GDPR is entitled ‘Automated individual decision-making, including profiling’ and corresponds to Article 15 of the DPD. One of the main differences between Article 22(1) and its predecessor is the explicit reference to ‘profiling’. Article 22(1) reads as follows:

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
2. Paragraph 1 shall not apply if the decision: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent.
3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.
4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

This article differs from Article 15 DPD in a number of respects. First, profiling is defined, second, explicit consent is required, third profiling of sensitive

data is not allowed (unless with explicit consent) and fourth, the act of profiling a person must be communicated to him or her.¹¹⁰⁷ A reference to profiling is provided by Article 4(4) GDPR:

‘Profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

Profiling is widely defined and can include a large variety of business practices. In addition, Recital 24 makes a connection between data processing and monitoring the behaviour of data subjects. Processing of personal data can be considered to be monitoring of behaviour where it involves tracking natural persons as they make their way through the internet. This is the case if this processing is performed in order to make a decision about a person or determine the personal preferences of that person. Recital 24 also states that the GDPR is applicable where the behaviour of the data subject being monitored takes place within the EU and also widens the scope of the GDPR by stating that the above applies even where the data controller is established outside of the EU.

An initial reflection over Article 22 is that, as with Article 15 of the DPD, a decision concerning a person must have been arrived at ‘solely’ as a result of automatic processing in order for it to be prohibited under Article 22. It is argued that most, if not all, forms of predictive modelling have at least some human intervention involved, be it at the stage of data collection, data cleaning or even just interpreting the results of a predictive model. The extent to which Article 22 is applicable even where there is a limited amount of human intervention is debatable. Applying the override rules associated with predictive modelling, there is almost certain to be some form of human involvement at some point within the predictive modelling process. The extent to which this takes place will depend on business, legal, cultural and reputational factors,

1107 Proust, Oliver, *Getting to know the GDPR, Part 5: Your big data analytics and profiling activities may be seriously curtailed*, fieldfisher, available at <http://privacylaw-blog.fieldfisher.com/2015/getting-to-know-the-gdpr-part-5-your-big-data-analytics-and-profiling-activities-may-be-seriously-curtailed/> (last accessed on 2016-09-26).

with one especially big factor being what Finlay refers to as, ‘the cost of getting it wrong’.¹¹⁰⁸ This can be a financial cost but also a cost in human lives, for example, were a predictive model to be used in the health care sector. One could of course argue, as Bygrave does in relation to Article 15 DPD, that one should not take a literal interpretation of this stipulation but rather examine whether there is any real human influence.¹¹⁰⁹ Nevertheless, the uncertainty surrounding this requirement is problematic for determining the application of Article 22.

Article 22 is challenging in other respects too. Its scope of application is vague and the exceptions to the main rule are numerous, thereby diluting its applicability. These issues are addressed below.

5.4.4.5 Court of Justice of the European Union and Mass Surveillance

Two cases from the CJEU are worth mentioning at this juncture in that they raise a number of relevant issues. These are the cases of *Schrems*¹¹¹⁰ and *Tele2*.¹¹¹¹ Both these cases revolve around the issue of mass surveillance.

In the *Schrems* matter, Schrems filed a suit with the Irish Data Protection Commissioner following the Snowden revelations publicising the extent to which the NSA was employing mass surveillance techniques to monitor almost all internet traffic in the US. Schrems alleged that Facebook Ireland was transferring personal data to the US, which did not have the required level of security and as a result contravened the Safe Harbour Agreement as developed by the EU Commission to facilitate the transfer of personal data between the US and EU. As a consequence the CJEU struck down the Safe Harbour Agreement, the main reservation being that the unprecedented surveillance by the

1108 Finlay, above n. 1, at p. 65.

1109 Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*, above n. 825, at p. 324.

1110 *Maximillian Schrems v. Data Protection Commissioner*, C-362/14, EU:C:2015:650.

1111 *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others*, Joined cases, C-203/15 and C698/15, EU:C:2016:970.

NSA put into question the level of security adhered to by the US as required for the transmission of person data according to the Commission.¹¹¹² Subsequently, the Privacy Shield mechanism was established, replacing Safe Harbour and facilitating the continued transfer of personal data to the US.¹¹¹³

The matter of *Tele2* also dealt with mass surveillance, more specifically, the mass storage of data collected as a result of mass surveillance. The question that arose, after the *Digital Rights Ireland*¹¹¹⁴ case invalidated Directive 2006/24, was where the boundary lay as regards the ability of states to implement a policy of general and indiscriminate retention of all traffic and location data of users of electronic communications in terms of Directive 2002/58. The answer from the CJEU was as follows:

Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.¹¹¹⁵

In other words, states are allowed to use surveillance procedures in order to fight organized crime and terrorism. However, these surveillance procedures must be pinpointed and restricted to specific cases and people. The blanket monitoring of all traffic and location data exceeded the boundary of acceptability as it in effect lumped together the data of criminals and innocent people alike.

These two cases, in reflecting recent developments, are indicative of a number of relevant points. First, these cases illustrate how the ECtHR and CJEU are keeping pace with each other in taking a restrictive view of mass

1112 Court of Justice of the European Union, Press Release No. 117/15, Luxembourg, October, 2015, available at <http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf> (last accessed on 2017-03-08).

1113 Privacy Shield Overview, available at <https://www.privacyshield.gov/Program-Overview> (last accessed on 2017-03-08).

1114 *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, joined cases C-293/12 and C-594/12, EU:C:2014:238.

1115 *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others*, para. 112.

surveillance. Second, *Schrems* illustrates the connection between state surveillance and commercial activities. In chapter 3, mention was made of the fact that the Snowden revelations publicised the commercial perspective as far as state surveillance was concerned, as many of the NSA's targets were commercial actors and US companies indirectly benefitted from NSA surveillance activities. In this regard, *Schrems* also highlights the link between state surveillance and commercial activities, not only in terms of ramifications, but also in terms of the haste with which Safe Harbour was replaced by Privacy Shield, allowing for the continued and undisrupted transfer of personal data between the US and EU. Another indicator of the commercial connection is that both Safe Harbour and Privacy Shield fall under the control of the US Department of Commerce.¹¹¹⁶ The main point, therefore, is that it is difficult to distinguish activities of a public nature from commercial activities within the private sector.

Finally, the *Tele2* case brought up the relationship between the CoE and EU as addressed above. The CJEU reiterated that since the EU had not acceded to the ECHR, the interpretation of Directive 2002/58 could only take place in light of the fundamental principles of the EU Charter.¹¹¹⁷ In addition, the CJEU referred to the fact that for the sake of consistency, the rights protected by the EU Charter, according to Article 52(3) of the EU Charter, were to be given the same scope as the corresponding rights within the ECHR.¹¹¹⁸

5.5 Preliminary Analysis

This chapter in essence answers the fourth research question outlined above, namely, to what extent does the European data privacy legal framework address personal autonomy and predictive modelling, thereby diminishing the

1116 Safe Harbour, available at <http://2016.export.gov/safeharbor/index.asp> (last accessed on 2017-03-08).

1117 *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others*, para. 128.

1118 *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others*, para. 129.

potential harms? It examined the extent to which the European data privacy legal framework addresses personal autonomy and predictive modelling, and thus the ability to diminish the potential harms. In order to accomplish this, judgements from the ECtHR as well as the EU data protection framework, in the form of the DPD and GDPR, were examined.

5.5.1 Human Rights Analysis

The ECtHR jurisprudence is significant to the extent that it makes a clear and unequivocal mention of the notion of autonomy, as well as cementing autonomy's place within Article 8 ECHR. The ECtHR also defined autonomy's boundaries. Autonomy, as a notion, comprises two distinct components, namely, a sphere to which a person should be able to retreat from constant surveillance as well as a component comprising the freedom to enter into relationships. In determining the boundaries of the latter aspect, the Court was prepared to extend the notion of private life beyond a person's 'inner circle'. Moreover, the Court made a clear connection between the notions of autonomy and identity, stating that identity was required in order to be able to develop autonomy.

What is also significant is the willingness of the ECtHR to further develop its interpretation of Article 8 ECHR so as to make it applicable to evolving technologies that were not developed at the time of the creation of the ECHR. A second noteworthy development is the route taken by the ECtHR into the realm of data protection. While Article 8 ECHR initially treated only privacy infringements, an unequivocal reference to data protection has developed. While not surprising, considering the CoE's emphasis on the importance of data privacy regulation, the reference to data protection is relevant from the point of view of autonomy, to the extent that it is a value that is implicitly protected by data protection. The ECtHR also identified the value of access to information. A final observation is that most of the cases referred to can be characterised as falling into the category of individual versus state relationship. It is argued that this should not prevent the principles that form the bases of these judgements from being applied to other relationships, for example, the commercial actor versus individual relationship. This is coupled with the significance of the horizontal effect principle, which extends the positive ob-

ligation of the state to situations that are characterised as being between private parties. It is in this context that the above case law becomes relevant in relationships between individuals that are governed by these principles.

In addition, through cases regarding data protection, many principles can be identified that are potentially applicable to any system, irrespective of whether within the public domain or used by commercial actors. It is in such instances that analogies can be drawn and inferences made, which can be attributed to circumstances within the commercial sector. For example, the notions that the systematic collection of data is wrong or that a lack of access to information can be harmful to an individual are relevant within the commercial sector too, where technologies are being used to monitor people.

Some weak points can also be identified as far as the human rights framework is concerned. First, the notion of the ‘reasonable expectation of privacy’ has also crept in to the case law of the ECtHR. Consideration should be taken of how this notion is to be interpreted especially taking into account the technical advances being made. For example, as technology becomes more of an inherent part of people’s lives, won’t their expectation of privacy diminish? This could be argued to be even more true as individuals become increasingly manipulated by technology, thereby losing autonomy.

Another issue to take into consideration is that the human rights framework includes human rights that potentially contradict each other, in which case a determination must be made as to which human right shall take precedence. This is illustrated by both *Von Hannover* cases referred to above, where the right to private life (Article 8 ECHR) was pitched against the right to freedom of expression (Article 10 ECHR), and which required a balancing of these rights against each other. In *Von Hannover (No. 1)*, the Court found that Article 8 took precedence, finding in favour of Princess Caroline. However, in *Von Hannover (No. 2)*, Article 10 took precedence. Without delving into how the facts from these two cases differed, they do illustrate the complexities involved in weighing competing interests and that predictability may be diminished depending where the facts differ from case to case.

Finally, Brownsword and Goodwin refer to some shortcomings associated with human rights as far as technology regulation is concerned: first, that the universality and moral truth that human rights sometimes aspires to is often challenged, and being intangible and difficult to empirically verify, many people do not view human rights as legitimate; second, human rights are usually formed as individual claims against the state, which become irrelevant when the existence of the state is put in focus, for example, where states are seriously

threatened; third, human rights demands are an effective manner to phrase demands, however, these demands may have no legal standing (others may have a moral duty to address the human right demand, but not a legal one) and fourth, human rights do not function as practical legal entitlements in relation to the broader community nor in relation to other individuals, who also have legal claims, and say little about whose rights weigh more.¹¹¹⁹

5.5.2 Data Protection Analysis

While data protection law aims to develop the internal European market for the free flow of personal data, it also entrenches norms associated with privacy, dignity and autonomy. The extent to which the focus has been placed on data protection, as opposed to privacy, is not without its critics. Firstly, it has been argued that data protection detracts from the notion of privacy, especially since it has been included as a separate right in the EU Charter. Rouvroy and Poullet argue that this has changed the function of data protection from being an ‘intermediate value’ and thereby a tool to be tweaked whenever necessary to protect the underlying ‘final values’ of data protection, namely, autonomy. In other words, being an intermediate value provided data protection with the ability to adapt itself to changing technologies as they appear, but this function disappeared by altering its status to that of a ‘final value’ in itself. This seemingly undesirable situation is exacerbated by what is termed ‘possessive individualism’, where giving individuals control over their personal data via the data protection regime together with data protection being viewed as a final value, leads to the situation where individuals either do not disclose their personal data on the one hand or on the other hand merely waive their rights to protection in return for commercial gain, the latter being more probable. This development deprives data protection of its ability to protect underlying values, such as autonomy.¹¹²⁰

The fact that data protection has become more constitutionally entrenched within the EU is also addressed by Lind, who argues that this development results in it becoming more difficult to balance other rights, such as freedom

1119 Brownsword and Goodwin, above n. 384, at pp. 231-232.

1120 Rouvroy and Poullet, above n. 436, at p. 50.

of speech or the right to information, against data protection, the constitutionally more entrenched right automatically taking precedence in any balancing attempt.¹¹²¹ The data protection framework, Cohen argues, is based on the rational actor model, which treats individuals as autonomous rational people who should be free to trade in personal data as they are in the best position to understand what is best for them and what will attain the highest degree of happiness, having their individual goals in mind.¹¹²² This reasoning can be traced back to the manner in which Westin noted that privacy could be achieved by ‘the claim of individuals, groups, or institutions to determine for themselves, when, how and to what extent information about them is communicated to others’.¹¹²³ What is becoming more evident, as knowledge concerning how technology can be combined with the behavioural sciences in order to manipulate people comes to the fore, is that individuals are not necessarily in the best position to make decisions, this considering the ease with which they can potentially be manipulated.

A related issue in the age of ‘possessive individualism’, is where individuals are willing to trade away ‘their’ personal data as if it were a commodity, not realizing that they are in fact also trading away the personal data of others, who possibly do not wish to disclose ‘their’ personal data.¹¹²⁴ This assertion pertains to the nature of data itself, namely, that data can rarely be associated with just a single individual. In other words, it is not uncommon that multiple parties can simultaneously hold claim to the same data. This can be viewed as a major obstacle to those who support a right to ownership in data as a solution to the challenges posed by technology.

The issue of consent is problematic for other reasons as well. An initial argument is that the provision of consent takes place in a context of a power imbalance, where the commercial actor has acquired knowledge, the existence of which is unknown to the individual, referred to as ‘invisible visibility’.¹¹²⁵ This highlights the issue of whether consent, under these circumstances, could ever be considered informed.¹¹²⁶ In addition, consent as a mechanism must be

1121 Lind, above n. 15, at p. 347.

1122 Cohen, above n. 372, at p. 1424.

1123 Westin, above n. 462, at p. 7.

1124 Rouvroy and Poullet, above n. 436, at p. 50.

1125 Hildebrandt, *Who is Profiling Who?*, above n. 237, at p. 243.

1126 Ibid.

questioned taking into account the imbalanced relationship between a commercial actor providing a service and an individual wishing to utilize that service. In many cases it boils down to a ‘take-it-or-leave-it’ situation, where consent is not only couched in lengthy terms and conditions comprising legal jargon, but where the convenience to a data subject is paramount, resulting in the terms and conditions being agreed to automatically. In addition, data subjects may be required to consent to either vague or broad purpose specifications, where withholding consent means access to the service is denied. As Cohen argues, individuals who consent to certain data processing practices receive so little information that consenting to their use can hardly be called ‘informed’.¹¹²⁷ Second, consent is ineffective as personal data may ‘belong’ to multiple data subjects simultaneously. In many instances, the nature of data and its creation is such, that personal information is created from within the bounds of a relationship.¹¹²⁸ In addition, reference is made to the example mentioned above, where Facebook has applied for a patent to an algorithm that determines the credit worthiness of an individual by monitoring the credit worthiness of his or her friends and their data. This illustrates how the data used to form an opinion of a person is out of the bounds of that person’s ability to provide consent. It is for these reasons that consent has been referred to as a ‘fairytale concept’.¹¹²⁹

As mentioned above, Article 22 deals with automatic decisions-making and profiling, in effect dealing with predictive modelling and comparable technologies. According to Article 22, the automated processing should produce legal effects or similar effects in order for Article 22 to apply. This is vague and little guidance can be attained from the GDPR. First, the legal effects being referred to are not specified, even in the recital. In addition, the reference to ‘similar effects’, denotes effects that are almost legal, but not quite. This can also cause uncertainty regarding where to draw the line between various consequences of predictive modelling and also how big the impact must be on the individual in order to engage Article 22. Article 22(1) refers to the ‘legal effects’ concerning this natural person yet goes further by referring to practices

1127 Cohen, above n. 372, at p. 1432.

1128 Solove, Daniel, J., *Conceptualizing Privacy*, 90 California Law Review, 2002, at p. 1087.

1129 Svantesson, Dan Jerker B., *The (Uncertain) Future of Online Data Privacy*, Masaryk University Journal of Law and Technology, Vol. 9, Issue 1, 2015, 129-153, at p. 148.

that ‘significantly affects him or her’. In relation to the potential harms associated with predictive modelling, some issues arise. What is meant by ‘legal effects’, or even more precisely, what is meant by ‘legal’? Is Article 22(1) applicable to harms that are not necessarily established in traditional law, but that are nevertheless a risk to society? If so, is the commercial actor obliged to make the individual, who is the object of predictive modelling, aware of all the possible potential harms as outlined above? Another challenge is to identify the boundaries of the phrase ‘significantly affects’ and from whose point of view this is to occur. Another issue regards the exception to the main rule if the profiling takes place in accordance with a national law.

Article 22(2) sets out the exceptions to the main rule of not allowing automated processing. These exceptions have the effect of considerably watering down the main rule. Recital 71, in addition, does not really add much substance to the applicability of the prohibition or the extent to which the exceptions are to be applied. According to Article 22(4), when the exceptions in Article 22(2) are applied, then Article 9(1) is engaged, in that the automatic decisions may not be based on the special categories of data specified. This may however occur, where explicit consent is obtained (Article 9(1)(a)) or where it is for reasons of ‘substantial public interest’ and proportionate to the aim (Article 9(1)(g)). In addition, automated decision making engages Articles 14 and 15 of the GDPR. Article 14 concerns the situation where the data controller is obliged to provide the data subject with information where data have not been obtained from the data subject. Where Article 22 is applicable, the data subject must be informed of the logic applied as well as the envisaged consequences for him or her (Article 14(2)(g)). Article 15 concerns the right of access of the data subject, and here too, where Article 22 is applied, the same duties attach to the data controller (Article 15(1)(h)).

Another argument questioning the applicability of the GDPR to predictive modelling or like technologies, revolves around Recital 63, dealt with above. On the topic of profiling, addressed in Article 22, Recital 63 first states that the data subject shall have access to the logic behind any decision taken concerning him or her. However, shortly after, the recital creates a far reaching limitation to this right, by stating that any rights to trade secrets or intellectual property rights shall take preference. Then the recital attempts once again to highlight that the original right still exists, be it in a dramatically watered down form, by stating that even if trade secrets or intellectual property rights prevail, the data subject should be given at least some information concerning the request for insight into the logic behind the processing and that there should not

be an outright refusal from the controller to provide the data subject with at least some knowledge of the technical process. It is argued that the right of access to the logic behind profiling technologies, granted by Recital 63, is extremely limited. First, the scope of the right to the logic of a system is clouded by the uncertainty surrounding this right. The right is granted, then to a large degree limited and then granted again, albeit in a milder form. Second, the extent to which the exception laid out in Recital 63 would not be applicable to systems using predictive modelling or similar technologies, is inconceivable. Surely most commercial actors would be able to claim successfully that the (proprietary) technology they are using to predict future outcomes is a trade secret or that the code is protected by intellectual property rights? Finally, the language regarding the return of the right to the logic of a system in Recital 63 is unclear. What is meant by ‘all information’. The controller is relieved of having to make available the logic of the system, and must provide the data subject with some information concerning how the system works, considering that there, ‘should not be a refusal to provide all information to the data subject’ (Recital 63). However, it is unclear where the border runs concerning just how much information is enough to clear the threshold of what is considered adequate information in the circumstances. To complicate matters, Recital 63 states that where the data controller possesses a large quantity of information on the data subject, the data subject must specify the information or processing activities to which the request relates. First, the phrase ‘large quantity of information’ is not specified and is characterised by the same arguments as against the use of the term ‘big data’ addressed above. The boundaries are not established and the concept of ‘large’ is a relative one, for example, relative to the size of the company holding the information. Second, how is the data subject expected to specify the processing activities to which the request applies, taking into account the complexity of the technology as well as the extent to which much of the predictive modelling process is hidden from the data subject.

The scope of Article 22 GDPR as compared with Article 15 DPD can also be considered. Above it was argued that Article 15 DPD could be interpreted to mean that a right was created, which in turn had to be enforced by the data subject, or else the right was not of much use. It can be argued that this uncertainty has been eradicated in the GDPR by stating clearly when the main rule should apply. In other words, Article 22 clarifies that the right that it confers exists irrespective of any attempts at enforcement.

On a general level, there is uncertainty over whether the data protection principles are applicable at all in certain circumstances. In the context of the DPD, given the scope and definition of personal data as well as the circumstances activating the DPD's application, it is possible to see why the DPD may not be applicable. Its binary nature is argued to cause problems in practice as it often is the case that it is difficult to determine whether data should be considered 'personal data'.¹¹³⁰ This together with the judgement in the case of *YS*, dealt with below, where the definition and scope of personal data can be argued to have been diminished. It is submitted that the same holds true in the case of the GDPR.

There are a number of ways that data can be connected to an identifiable individual. According to the Article 29 Working Party, an individual is considered identified when he or she can be identified from all other members of a group and is identified by means of 'identifiers' that have a close relationship to the individual, for example, name, identification number or physical appearance.¹¹³¹ The GDPR includes the concept 'pseudonymisation'. The use of this concept raises questions in relation to the concept of anonymity. It is argued that data can always be connected to an individual no matter what measures are taken to make it anonymous, putting into doubt whether anonymity even exists. For example, Netflix released a large batch of data, where researchers were consequently able to use the film preference data of individuals to identify them and gain insight into their political affiliations and other sensitive information.¹¹³² According to Article 4(5) GDPR, pseudonymisation occurs where data cannot be attributed to a specific data subject without the use of additional information. This information is to be kept separately and subject to necessary organizational and security measures to prevent the personal data from being attributed to a specific person. According to Recital 26, data that have undergone pseudonymisation yet which could be attributed to

1130 Schermer, Bart, *Risks of Profiling and the Limits of Data Protection Law*, above n. 651, at p. 145.

1131 Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, at p. 12.

1132 Narayanan, Arvind and Shmatikov, Vitaly, *Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset)*, University of Texas at Austin, 5 February 2008, available at https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf (last accessed on 2017-03-06). For an in-depth discussion surrounding re-identification, see Schermer, above n. 651, at p. 143.

a natural person using additional information, should be considered information relating to an identifiable natural person. However, in determining whether a natural person is identifiable, consideration must be taken of means that are ‘reasonably likely to be used’, to directly or indirectly identify the natural person. In turn, factors such as costs involved, time required and state of technology both at the time of the processing but also in relation to future developments are relevant in ascertaining the boundaries of ‘reasonably likely to be used’. It can therefore be challenging to determine where the boundary of pseudonymisation lies.

Gutwirth and De Hert argue that the use of trace data in most cases engages data protection legislation.¹¹³³ In contrast Leenes states that profiling produces digital personas that only represent the virtual individual and that these data cannot be connected to a real person at the outset. It is only after a real individual triggers the profile for some reason, that it is applied to the individual together with all the assumptions that can be inferred from the profile.¹¹³⁴ Hildebrandt agrees, stating that the DPD is not applicable in many cases of profiling, as much of the data used in the profiling process cannot be considered personal data.¹¹³⁵ Irrespective of which opinion is accepted, the uncertainty regarding the applicability of the data protection regime limits its effectiveness.

Furthermore, while autonomy is an implicit notion that is present in considerations concerning data protection, it is argued that it does not receive the attention required in order to achieve real protection. Allowing the processing of personal data to occur as long as certain procedures are followed, essentially has little to do with the protection of the interests of autonomy, dignity and freedom, ignoring the perspective of an individual’s autonomy.¹¹³⁶ Cohen argues that an autonomy-based approach is required as far as data privacy is concerned, adding that such an approach would not threaten the advantages to be gained from technological developments. Cohen further highlights that the rational actor model takes no note of how autonomy is developed, in other

1133 Gutwirth, and De Hert, above n. 1008, at p. 288.

1134 Ibid, at p. 297.

1135 Hildebrandt, *Profiling and the Identity of the European Citizen*, above n. 283, at p. 322.

1136 Prins, above n. 51, at p. 5.

words, how individuals develop the ‘capacity and facility for choice’.¹¹³⁷ The above sentiments convey the idea that the data protection regime lacks focus as far as the protection of autonomy is concerned.

Data protection relies on the notion that the individual is the champion of his or her own interests in relation to how personal data are to be processed. However, knowledge of the predictive modelling process may be lacking and it is unrealistic for the data subject to carry the burden of making all these decisions.¹¹³⁸ This engages the notion of the social benefits of privacy and not merely the individual benefits, reference being made to the collective value of privacy.¹¹³⁹ On a purely semantic level, the DPD and GDPR refer to ‘him’ and ‘her’ or the ‘data subject’, promoting the individual perspective. Also, data protection protects a plethora of interests, for example, the protection against discrimination, defamation and intellectual property breaches, however, these are bound to remain in the periphery as long as privacy is also in focus.¹¹⁴⁰ In other words, protecting multiple interests draws attention from autonomy.

There are two arguments that are on opposite sides of the same coin. On the one hand it is argued that the individual identity is extremely nuanced and cannot be represented by data no matter how many categories or groupings are created. The argument is that data cannot be regarded as ‘elements’ or ‘building blocks’ of the human personality and as a result the ‘self’.¹¹⁴¹ On the other hand, data scientists believe that this is in fact possible, Cohen stating that, ‘[d]ata processing practices are predicated on a belief that individuals are reducible to the sum of their transactions, genetic markers, and other measurable attributes, and that these attributes are good predictors of risk and reward in future dealings’.¹¹⁴² Cohen acknowledges that there is a certain truth to this view, however, she highlights that there are many things that cannot be reduced to data and predicted, human motivation being one such attribute.¹¹⁴³

1137 Cohen, above n. 372, at p. 1424.

1138 Hildebrandt, *Profiling and the Identity of the European Citizen*, above n. 283, at p. 320.

1139 Cohen, above n. 372, at p. 1435.

1140 Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*, above n. 825, at p. 120.

1141 Rouvroy and Pouillet, above n. 436, at p. 51.

1142 Cohen, above n. 372, at p. 1405.

1143 Ibid.

A criticism of the data protection regime is that its data-centric approach detracts from the fact that the human identity cannot be reduced to data. In other words, it is not data that is the problem, but rather the knowledge or insight that is gained from processing this data. What requires protection instead, is the knowledge that is attained from the predictive modelling process, where the data used to create the digital identity is not necessarily personal data, thereby making the DPD (and GDPR) redundant.¹¹⁴⁴ Hildebrandt argues that data protection is built upon the concept of personal data yet the distinction between data and personal data is no longer relevant considering that modern technology can infer sensitive information from trivial data.¹¹⁴⁵ This requires a shift in focus from the data itself to the knowledge that can be inferred from the data.¹¹⁴⁶ In other words, there should be less focus on the detailed regulation of data processing and more focus on preventing its harmful effects.

The data protection regime, besides protecting multiple interests, also has a main aim of facilitating the development of the European internal market so as to promote the flow of personal data across borders. In relation to the DPD, a Commission Communication states:

The diversity of national approaches and the lack of a system of protection at Community level are an obstacle to completion of the internal market. If the fundamental rights of data subjects, in particular their right to privacy, are not safeguarded at Community level, the cross-border flow of data might be impeded just when it is becoming essential to the activities of business enterprises and research bodies and to collaboration between Member States' authorities in the frontier-free area provided for in Article 8a of the Treaty.¹¹⁴⁷

The GDPR reiterates this objective of harnessing the power of the digital economy in Recital 7. A question that follows is whether, in the face of a conflict

1144 Hildebrandt, *Profiling and the Identity of the European Citizen*, above n. 283, at p. 320. This argument was made in relation to the DPD.

1145 Hildebrandt, *Who is Profiling Who?*, above n. 237, at pp. 239-240. It is noteworthy that this argument was made in relation to the DPD.

1146 Ibid.

1147 Commission Communication on the Protection of Individuals in Relation to the Processing of Personal Data in the Community and Information Security, COM (90) 314, final, 13 September 1990, available at <http://aei.pitt.edu/3768/1/3768.pdf> (last accessed on 2016-02-17).

between the aim of protecting the data subject and the aim of developing the internal market, which aim prevails? Is it the implicit aim of protecting autonomy via data protection, or is it the economic interests reflected by the desire for the free flow of personal data? In this regard, the Commission has stated that while both the above goals are equally important, the economic aspect takes precedence. This was acknowledged in a First Report of the Commission of the European Communities, which stated that, '[i]n legal terms, however, the existence of the Directive rests on Internal Market grounds'.¹¹⁴⁸

Schermer cites an argument provided by Zwenne, who states that a law that applies to essentially everything applies to effectively nothing.¹¹⁴⁹ In other words, a law that is so encompassing that it can be applied to everything loses its force and instead is difficult to apply to anything at all. This argument is mirrored by Svantesson, stating that the GDPR 'bites off more than it can chew', referring to the fact that its broad application cannot be matched with regards to enforceability, necessitating targeted application.¹¹⁵⁰ Here a parallel can be drawn to the implementation of the DPD into Swedish national law by means of the Personal Data Act (1998:204) that came into effect on the 24th of October 1998. Shortly after the Personal Data Act came into effect, it was amended so that many of its paragraphs were not applicable to personal data that was considered processed in unstructured material.¹¹⁵¹ This amendment came into effect on the 1st of January 2007 and was implemented by the addition of paragraph 5(a) that exempted the processing of personal data from many provisions of the Personal Data Act, provided that the terms of paragraph 5(a) were met, namely that the '... processing of personal data that do

1148 Commission of the European Communities, *First Report on the Implementation of the Data Protection Directive (95/46/EC)*, (COM (2003) 265), Brussels, 15 May 2003, at p. 3, available at <http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=COM:2003:0265:FIN:EN:PDE> (last accessed on 2016-02-17).

1149 Zwenne, G.J., *Over persoonsgegevens en IP-adressen, en de toe komst van privacywetgeving*, at p. 235 in Mommers, L., Frenken, H., Klaauw, F., van der Herik, H., van der Zwenne, G.-J., (eds.) *Het Binnenstebuiten*, Liber Amicorum Aernout Schmidt, pp. 321-341, Universiteit Leiden (2010) in Dutch, in Schermer, above n. 651, at p. 146.

1150 Svantesson, Dan Jerker B., *Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation*, *International Data Privacy Law*, Vol. 5, Issue 4, pp. 226-234, 2015, at p. 232.

1151 Personal Data Protection, Information on The Personal Data Act, Swedish Government Offices, at p. 14, <http://www.regeringen.se/content/1/c6/07/43/63/0ea2c0eb.pdf> (last accessed on 2015-02-27).

not form part of and are not intended to form part of a set of data that has been structured in order to significantly facilitate searches for or compilations of personal data specifically'.¹¹⁵² The argument here is that the Swedish legislator recognized the futility in attempting to regulate all instances of data processing considering the wide-spread use of computers within society and instead focused merely on the harmful effects of this data processing.

A final issue relating to the scope of the applicability of the data protection regime is the case of *YS* handed down by the CJEU.¹¹⁵³ Briefly the matter concerned the extent to which the Applicants could gain access to the analyses regarding the application for a residence permit to the Netherlands, alleging that the analysis was personal data. The Court determined that the analysis, though based on personal data, was not to be considered personal data:

... such a legal analysis is not information relating to the applicant for a residence permit, but at most ... is information about the assessment and application by the competent authority of that law to the applicant's situation, that situation being established inter alia by means of the personal data relating to him which that authority has available to it.¹¹⁵⁴

Korff argues that this case reduced the scope of the concept 'personal data' as well as the access to it as envisaged by the data protection regime.¹¹⁵⁵ This is significant from the predictive modelling perspective. Korff argues that it limits the right of individuals to challenge the accuracy of 'profiles' on the basis that a profile too is an abstract analysis of facts, just as in *YS*.¹¹⁵⁶ Lynskey disagrees with this analogy, stating that while access to the logic behind profiling and the algorithm compiling the profile, may be limited, access to the

1152 Öman, Sören, *Trends in Data Protection Law*, in Wahlgren, Peter (ed.), *ICT Legal Issues*, Scandinavian Studies in Law, Volume 56, Stockholm Institute for Scandinavian Law, 2010, at p. 216.

1153 *YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M and S*, Joined cases C-141/12 and C-372/12, EU:C:2014:2081.

1154 *YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M and S*, para. 40.

1155 Korff, Douwe, *The Proposed General Data Protection Regulation: Suggested Amendments to the Definition of Personal Data*, EU Law Analysis, available at <http://eula-wanalysis.blogspot.se/2014/10/the-proposed-general-data-protection.html> (last accessed on 2017-03-22).

1156 *Ibid.*

actual data and decision itself is not.¹¹⁵⁷ It is argued, that in order for any meaningful insight into the predictive modelling process to be possible, access to the logic underlying a decision is crucial. In other words, access to the data is required as well as access to the algorithm that correlated these data in calculating a decision. Failing such insight, access can only be deemed unsatisfactory.

5.6 Summary and Conclusions

This chapter set out to examine to what extent the European data privacy legal framework addresses personal autonomy and predictive modelling. While both the human right legal framework of the CoE and the data protection legal framework of the EU both address autonomy and predictive modelling, it is argued that there are many uncertainties.

The human rights framework, represented by the ECHR and the case law of the ECtHR, clearly addresses the notion of autonomy, but does not expressly address predictive modelling or like technologies. Nevertheless, the stances the ECtHR has taken in relation to the handling of data in general do have an analogous value in that they can be used to interpret modern technologies, as if they existed at the time of the drafting of the ECHR. In addition, the fact that the articles of ECHR enshrine principles that have a wide range of application makes them easier to apply in multiple situations, resulting in the ECHR being an adaptable instrument. The manner of interpreting dynamically the scope of the ECHR in relation to technology, as well as the fact that the ECtHR has clearly recognized the notion of autonomy, makes this legal regime suitable to address issues related to autonomy and predictive modelling as they arise in the future.

The data protection legal regime, while having the protection of autonomy as an implicit goal, never mentions the concept explicitly nor does it make it clear that this is its function. The DPD addresses predictive modelling-type technologies to a limited degree while the GDPR does so more clearly, albeit using the terminology ‘profiling’. However, it is argued that the main rule in the GDPR regarding profiling is accompanied by vague concepts, is watered down by a number of exceptions and has its scope of operation curbed by the

1157 Lynskey, above n. 819, at p. 123.

preference given to the right to protect trade secrets and other intellectual property rights. The data protection principles have not been updated in any real terms and seem to have been surpassed by technology. In addition, the main aim of the data protection framework is that of eradicating any obstacles in the way of the developing internal market of the EU. It is questionable therefore, considering the importance of protecting autonomy, whether a framework having multiple goals is adequate in this regard. Nevertheless, the GDPR does attempt to attain an equal level of protection in relation to data processing throughout Europe and it does raise the awareness surrounding technologies that display the same characteristics as predictive modelling. Furthermore, it does recognize the potential of using technology to enhance the awareness of the data subject, for example, by means of electronic symbols.

A final conclusion after examining the data privacy legal framework is that the frameworks provided by the CoE and EU are inherently intertwined and dependent on each other. This is reflected, if nothing else, by the manner in which the case law of these two institutions treat certain issues, for example mass surveillance.

6 A Strategy of Empowerment

6.1 Introductory Remarks

This chapter addresses the question of what regulatory strategy best protects personal autonomy in the face of the increased use of predictive modelling techniques in the commercial setting. Technology, in the form of predictive modelling, has upset the relative balance that previously existed between companies and individuals. As some of the relationships within society have become weaker, companies have resorted to other means of determining the trustworthiness of their customers concerning commercial undertakings. This is especially relevant with the advent of globalisation, where business relationships can be entered into from a distance. Companies have at their disposal the technology of predictive modelling that allows them to gauge individuals, which is beneficial before entering into a business relationship or in order to perpetuate one. The driving force is data, which in turn has unleashed the power of predictive modelling. More data fed into this technology, results in more accurate probabilities for making predictions, thereby increasing companies' ability to influence behaviour. The individuals whom are the object of this technology, have no knowledge of the predictive models nor do they have access to the same quantities of data and technical capabilities possessed by companies to convert this data to knowledge. The strategy of empowerment addresses this new power imbalance.

The challenges resulting from the development of technology vary in size and complexity. This also applies to their solutions. In certain circumstances, a single solution may suffice, while in others, multiple approaches are required. It is in this context that two arguments arise. First, predictive modelling is complex in nature and there is no single solution available. There is simply no 'silver bullet'. Instead, to minimize its harms, a myriad of tools is required. The second argument, which relates to the first, concerns the role of traditional law. An observation regarding technological developments and

their challenges, is that traditional law seldom provides the most effective solution. Traditional law may be one instrument but there are others. There are soft law instruments (legal and non-legal soft law instruments), for example, guidelines and codes. Alternatively, the instruments may take the form of education, incentives, standardization measures, ethical considerations or other technological instruments. The complex nature of predictive modelling requires a strategy, that consists of an array of tools, both legal and non-legal. It is within this context that the strategy of empowerment is introduced.

The strategy of empowerment is a multi-dimensional approach, comprising both legal and non-legal components, that can be utilized to address predictive modelling and its harms. It is a strategy to level the playing field and reach a relative equilibrium, acting as a buffer that protects autonomy and minimizes the negative effects of predictive modelling. Its aim is not to allow individuals to circumvent predictive models nor is it an attempt to stifle the innovation and public benefits that predictive modelling entails. The intention is not to prohibit a specific technology. Instead it is a compromise strategy that benefits all the parties involved, creating a symbiosis between commercial actor and individual. Publicity surrounding the existence of predictive modelling and its corresponding manipulative capabilities is a potential risk to companies, where the loss of ‘goodwill’ could occur when business practices are questioned.

The notion of an equilibrium is not unique. For example, Westin argued that, ‘[w]hen the American Republic was founded, the framers established a libertarian equilibrium among the competing values of privacy, disclosure and surveillance. This balance was based on the technological realities of eighteenth-century life’.¹¹⁵⁸ The present-day technological realities are different yet technology is one factor, amongst others, that is viewed as disruptive, especially in the privacy discourse. Poster states:

Dramatic changes in the reproduction, transmission, storage and retrieval of information profoundly affect the entire social system. Drastic changes in the means and relations of communication are making a shambles of the delicate balance in the social order that was negotiated and struggled over during the epochs of nineteenth-century industrial capitalism and twentieth-century welfare statism.¹¹⁵⁹

1158 Westin, above n. 462, at p. 67.

1159 Poster, above n. 334, at p. 71.

As early as the 1970's in the US, statements of social commentators such as Rule et al., demonstrated an awareness of the limitations to the acceptability of the inroads made by technical developments on prevailing social relationships:

At some point the powers conferred by maintenance and use of sophisticated personal-data systems must be counted excessive. Where to place that point, however, is a subtle and contentious matter. It turns on concerns which go well beyond characteristics of the data systems themselves; these include the risks of misuse of power in our society, the desirability of holding people responsible for past misdeeds, and the inherent worth of private experience ... As long as these systems grow, they can only erode privacy and autonomy ... we face social choices.¹¹⁶⁰

6.2 Empowerment Revisited

References to empowerment are not unique. Empowerment has been mentioned as a policy consideration in the legal domain, for example, within consumer protection and to a limited extent data protection. Within the EU, in the face of a lengthy period of economic uncertainty and economic crises, a remedy to this economic reality was the policy of relating to the consumer differently – not as a victim in need of protection, but rather as an active subject with a role to play in building up the European economy.¹¹⁶¹ Consumer empowerment was initially raised in the Community Consumer Policy Strategy 2002-2006, in the Commission's Consumer Strategy 2007-2013 and of late adopted in the Consumer Agenda 2014-2020.¹¹⁶² Empowerment has been applied in various forms: first, it was portrayed in terms of providing consumers

1160 Rule, McAdam, Stearns and Uglow, above n. 319, at pp. 6-8.

1161 Bakardjieva Engelbrekt, Antonina, *Consumer Empowerment in the EU: Weighing the Institutional Alternatives*, Synopsis of research report for SIEPS, 2012 (unpublished), at p. 1.

1162 Communication from the Commission to the European Parliament, Council, The Economic and Social Committee and the Committee of the Regions – Consumer Policy Strategy 2002-2006, COM (2002)0208 final, OJ C 137, 8.6.2002 in Bakardjieva Engelbrekt, *Ibid*, at p. 2.

with knowledge in two forms - knowledge about goods and services and consumer rights; second, it was portrayed in terms of transparency; third, it was portrayed in terms of political participation and fourth, it was portrayed in terms of access to fora for addressing disputes.¹¹⁶³ Regarding the first portrayal of empowerment, it has been stated that, ‘ [e]mpowered consumers need real choices, accurate information, market transparency and the confidence that comes from effective protection and solid rights’.¹¹⁶⁴ As far as the participation in policy matters is concerned, the Consumer Policy Strategy 2002-2006 had as an objective the ‘[i]nvolvement of consumer organizations in EU policies’, where it is stated that consumers must have the ability to have input into the policies that affect them, and promote their interests on an equal footing with other parties.¹¹⁶⁵ An example of the portrayal of empowerment in terms of access to institutions or fora for the resolution of disputes was the reference, in the Single Market Act, to alternative dispute resolution, where speedy resolution and easy access to institutions were key elements of empowerment.¹¹⁶⁶

Three approaches can be identified in relation to consumer empowerment. First, consumer empowerment could be realized through the market approach, where it was envisaged that the opening up of the internal market would in turn lead to the empowerment of the consumer. Second, consumer empowerment could occur through a political and legislative process approach, which in turn, had three sub-divisions, namely: information-based, full harmonization and participation in policy making. Third, consumer empowerment could be attained through the judicial and administrative process, which enshrined the notion that rights have no value if they cannot be enforced.¹¹⁶⁷

1163 Bakardjieva Engelbrekt, above n. 1161, at p. 3.

1164 Communication from the Commission to the Council, the European Parliament and the European Economic and Social Committee – EU Consumer Policy Strategy 2007-2013 – *Empowering consumers, enhancing their welfare, effectively protecting them* {SEC (2007) 321} {SEC (2007)322} {SEC (2007)323},/* COM/2007/0099 final */.

1165 Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – *Consumer Policy Strategy 2002-2006*, COM (2002)0208 final, OJ C 137, 8.6.2002.

1166 Communication from the Commission to the European Parliament, the Council, the economic and Social Committee and the Committee of the Regions, Single Market Act, *Twelve levers to boost growth and strengthen confidence*, COM (2011) 206 final.

1167 Bakardjieva Engelbrekt, above n. 1161, at p. 7.

From the legal perspective, the notion of empowerment through the judicial process is of most interest. The main idea here is that for rights to be of any value, two conditions are necessary. First, knowledge of the right or rights is required. A right is of no value if a person is not aware that the right exists. Second, easy and simple access to a forum is required, within which to enforce one's rights. The prospect of a drawn-out and expensive court battle is often a factor that can prohibit an attempt to enforce one's legal rights.

The explanatory memorandum to a proposal for a Regulation on a consumer programme 2014-2020 also put empowerment in focus:

Empowerment is not only a question of consumer rights but of building an overall environment that enables consumers to make use of those rights and benefit from them. It means building a framework wherein consumers can rely on the basic premise that safety is assured and that tools are in place to detect failings in standards and practices and to address them effectively across Europe ... Finally empowerment requires that consumers can confidently exercise their EU rights across Europe and that, when something goes wrong, they can count both on the effective enforcement of those rights and on easy access to efficient redress.¹¹⁶⁸

Considering the role of technology, it was noted that technology in fact can lead to disempowerment. For example, if technology creates the ability to access too much information, it can have the opposite effect compared to that which was anticipated. The European Consumer Association highlighted that European consumers had a tendency to make questionable decisions due mainly to 'information overload', 'the increasing complexity of markets', and the, 'overly ... complex ways in which essential information is delivered'.¹¹⁶⁹

Empowerment has also been recommended as a means of improving the position of the data subject within the data protection regime. In 2009 the Article 29 Data Protection Working Party produced a paper in response to a Consultation on the legal framework for the fundamental right to protection of personal data launched by the Commission. The paper was entitled 'The Future of Privacy' and while the main message was that the principles of data

1168 Commission Proposal for a Regulation on the European Parliament and of the Council, *On a consumer programme 2014-2020*, COM (2011) 707 final.

1169 Commission Staff Working Document, *On Knowledge-Enhancing Aspects of Consumer Empowerment 2012-2014*, at p. 5.

protection were still valid, it did suggest some changes to the DPD.¹¹⁷⁰ The Article 29 Data Protection Working Party suggested an empowerment strategy to improve the position of the data subject, in the face of new technologies such as profiling.

Here too, the main rationale was the encouragement of a more active data subject by providing more options with which to enforce rights.¹¹⁷¹ Therefore, the following measures were suggested: creating the possibility for class action procedures, providing fora for alternative dispute resolution, increasing transparency by developing new ways to inform data subjects in relation to behavioural advertising and notification of a privacy breach, utilizing consent as a mechanism of empowerment and harmonizing national laws of the Member States of the EU.¹¹⁷²

6.3 Theoretical Considerations

This section addresses two theoretical considerations. The first entails a contemplation of the role of law while the second provides a philosophical context for the strategy of empowerment.

Considering the role of the law within the subject of extraterritoriality in the area of private international law, Svantesson refers to the terms ‘bite jurisdiction’ and ‘bark jurisdiction’.¹¹⁷³ His point of departure is a reference to Hart, who states the following:

The principal functions of the law as a means of social control are not to be seen in private litigation or prosecutions, which represent vital but still ancillary provisions for the failures of the system. It is still to be seen in the diverse

1170 Article 29 Data Protection Working Party, *The Future of Privacy*, Adopted on 1 December 2009, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf (last accessed on 2016-04-06).

1171 Ibid, at p. 16.

1172 Ibid, at pp. 16-17.

1173 Svantesson, Dan Jerker B., *A Jurisprudential Justification for Extraterritoriality in (Private) International Law*, 13 Santa Clara Journal of International Law, 517, 2015 at p. 551. It can be added that the notions of ‘bark’ and ‘bite’ can be related to other laws and rules, and are not only relevant as far as jurisdiction is concerned.

ways in which the law is used to control, to guide, and to plan life out of court.¹¹⁷⁴

Svantesson highlights a theme that is present throughout Hart's work, namely the notion of the acceptance of the law even though it lacks effective sanction. Starting with the two functions of the law portrayed by Hart, namely law as a mechanism for deciding legal disputes and law as a mechanism for controlling, planning and guiding life outside of court, Svantesson identifies a third role of the law in making the distinction between 'bark' and 'bite' jurisdictions.¹¹⁷⁵ Svantesson argues that the third role of the law involves enshrining the values of society that created the law in the first place, represented by the 'bark' jurisdiction.¹¹⁷⁶ The distinction between 'bark' and 'bite' lies in the contention that, within the realm of extraterritorial claims in private and public international law, the inability to legally enforce a claim does not deprive that claim of jurisprudential legitimacy or practical utility. Svantesson points out that not all jurisdictional claims are made with the intention that they will be carried out in practice. Thus, despite lacking enforcement possibilities, there is in fact a function for 'bark' claims, in that they clarify a legal position.¹¹⁷⁷

Some possible shortcomings of the 'bark jurisdiction' notion are aired by Kuner, who questions the notion of 'bark jurisdiction' in data protection:

Despite the growing number of enforcement actions, the chance of an action being brought for a particular data protection violation is still relatively low in most cases ... There is a gap between the complexity of the rules that govern data processing, and the relatively low risk of enforcement action being taken ... In the globalized economy, all factors affecting cost (including legal compliance burdens) tend to be subject to a risk management exercise, with compliance being more likely when the risks and costs of non-compliance are higher than those of compliance. Thus, in many cases data controllers may regard data protection rules as a kind of bureaucratic nuisance rather than as

1174 Hart, H. L. A., *The Concept of Law*, third edition, 2012, at p. 40.

1175 Svantesson, *A Jurisprudential Justification for Extraterritoriality in (Private) International Law*, above n. 1173, at p. 551.

1176 *Ibid*, at p. 552.

1177 *Ibid*, at p. 556.

‘law’ in the same category as tax and other laws, mainly because of the relative lack of enforcement and the relative mildness of the possible penalties.¹¹⁷⁸

Conceding that the data protection regulatory framework is possibly not the most suitable for applying the ‘bark jurisdiction’ notion, Svantesson does continue to back it as far as other legal spheres are concerned as well as where other cultural characteristics are more accepting of the ‘bark’ notion.¹¹⁷⁹ The main argument extracted from the above reasoning is that the law does have a function despite the lack of enforceability. This rationale is relevant in the case of empowerment as well.

The ‘bark’ function of the law is reflected in various ways in regard to law-making. In this regard reference is made to laws that are goal orientated yet lack stipulations regarding enforcement or punishment. The main aim of these laws is to change the way people or society thinks. For example, in 1979 a law was promulgated in Sweden against the corporal punishment of children. The aim of this new law, according to the preparatory works, was to increase public awareness on the subject and have a pedagogical aim.¹¹⁸⁰

The second theoretical consideration contemplates which moral philosophical and political philosophical theories the strategy of empowerment resembles.¹¹⁸¹ Previously, mention was made of the three cornered triangle put forward by Brownsword and Goodwin, the corners representing utilitarianism (goal-orientated), deontology (duty based) and liberalism (rights based). Having examined the historical development of data protection, it is clear that its roots are grounded in the liberal political approach. This is apparent from the definition of privacy provided by Westin mentioned above, which stated that it was, ‘the claim of individuals, groups, or institutions to determine for themselves, when, how and to what extent information about them is communicated to others’. This notion of individual control is still a cornerstone of the data protection framework.

1178 Kuner, Christopher, *The ‘Internal Morality’ of European Data Protection Law*, November 2008, available at <https://ssrn.com/abstract=1443797> (last accessed on 2016-11-22).

1179 Svantesson, *A Jurisprudential Justification for Extraterritoriality in (Private) International Law*, above n. 1173, at p. 560.

1180 Wahlgren, Peter, *Lagstiftning: rationalitet teknik och möjligheter*, above n. 54, at p. 126. See also Prop. 1978/79:67 Förslag om lag till ändring i föräldrabalken.

1181 An in-depth examination of this topic is unfortunately not possible within the constraints of this thesis.

It is difficult to place the strategy of empowerment squarely in a pre-determined moral or political theory compartment. However, it is possible to indicate its similarities or dissimilarities with established political theories. Empowerment puts the individual in the centrum yet acknowledges the inability of this individual to always decide what is in his or her best interests. Above, reference was made to Brownsword and Goodwin, who posited that most technological developments in the Western world are regulated using the utilitarian lens. Empowerment bears similarities in that it acknowledges a point beyond which the individual cannot be empowered. For example, the argument was given previously that too much empowerment would allow individuals to bypass systems, thereby creating risks for society on the whole. Therefore, it acknowledges the need for balancing interests between individual and community. It is also utilitarian in that it recognizes the benefits of predictive modelling for society, and does not in any way attempt to outlaw it. For example, the use of a predictive model to predict who will commit a crime may seem to be beneficial for society and therefore maximize the happiness of the community. In the commercial setting, the use of predictive models by companies to identify 'desirable' customers and minimize risks will increase the economic standing of these companies, also maximizing the happiness of the community. In such circumstances, the individual is almost chanceless considering that the interests of the community will always take precedence.

Empowerment also resembles liberal political theory in that it acknowledges the benefit of providing the individual with rights. The right of access, mentioned below, is relevant in this regard. However, empowerment is also a move away from liberal political theory, as it acknowledges that individuals require assistance in determining what is in their best interests. At the same time, empowerment promotes a balance in order to not become too paternalistic in nature. Here reference is again made to the notion of 'libertarian paternalism' as put forward by Thaler and Sunstein discussed above. Considering the technical complexity of predictive modelling, combined with the time constraints on individuals, it is questionable whether the notion of individual control, reflected in the current data protection framework, is adequate. In this regard, empowerment contemplates the notion of 'collective consent' in relation to the component of collective redress, discussed hereunder. In addition, it also identifies the need for technical solutions that avoid the harms to the individual, thereby eliminating the need for the individual to reactively address the harm.

Empowerment also bears similarities with the deontological approach. This approach emphasises that irrespective of the benefits that predictive modelling has for the community, it potentially harms individuals, which cannot be tolerated. It mirrors the thinking of Kant and Rawls, requiring that the individual not be treated as a means to an end, but rather as an end in itself, accepting that individuals are different.

Finally, two submissions are made. First, taking into consideration the ‘bark’ notion, it is argued that empowerment has a role to play, even in cases where enforcement is impossible. Second, it is impossible to place empowerment in a pre-defined moral or political theory. Depending on how one views empowerment, notions of utilitarianism, liberalism and deontological ideology can all be identified within it.

6.4 The Components of Empowerment

The strategy of empowerment suggested here is made up of components that differ in nature. Some are to be considered traditional law in their nature, some are to be considered soft law in their nature, some are technical in their nature and some are difficult to label, for example, the component of knowledge. All these components play a role in regulating the risks and vulnerabilities associated with predictive modelling. Not only do they regulate these risks and vulnerabilities but they also influence each other. In addition, they need not all be applied simultaneously. The components also have a symbolic value, in that their mere existence can regulate a certain context. The role of the law as a component of empowerment is especially noteworthy. A component based on traditional law will have a direct regulatory function. For a component based on technology, traditional law still has a role in terms of regulating that technological component, but its regulatory function in this case will be indirect. The inventory of components of a strategy of empowerment provided in this thesis is not exhaustive and can be supplemented with other components depending on factors such as who is using the inventory, the technological context and the goals to be achieved. The components of the strategy of empowerment are the following: access to information and knowledge, accountability, a duty of care, a right of access, participation in the legislative process,

an independent supervisory authority, collective redress, soft law and technology. These components are discussed in the next section.

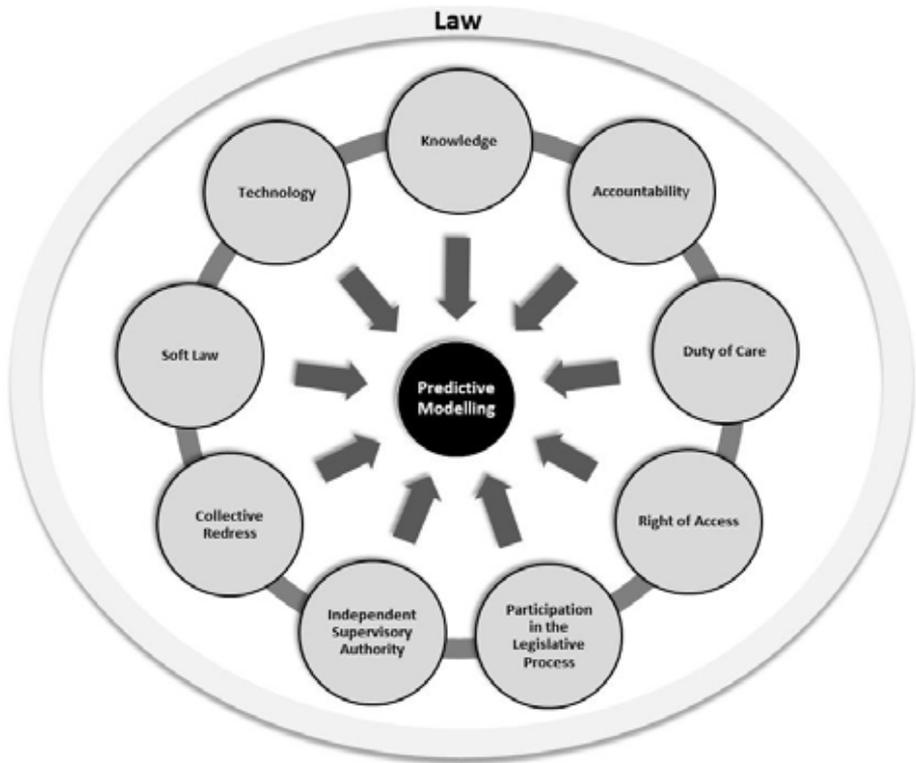


Figure 3 represents the strategy of empowerment and its various components. At the centre is predictive modelling and the resulting potential harms. Surrounding predictive modelling are the components making up the strategy of empowerment. They regulate predictive models (technology) but are also all interconnected and influence each other. Finally, the traditional law, represented by the outer ring, regulates the components making up the strategy of empowerment, having both a direct and indirect regulatory function.

6.4.1 Knowledge

Information and the accompanying knowledge that flows from it is a key component of empowerment. Only after having acquired knowledge, can the other components of empowerment be engaged. For any person to be able to address a problem, or challenge a set of circumstances, he or she first needs to know that this problem exists. For example, granting a right is meaningless in the

absence of knowledge of its existence but also in the absence of knowledge of the factual circumstances that potentially transgress this right. The main contention is that knowledge is power and that those who control the access to knowledge, also control power. The famous quotation of Bacon that ‘knowledge is power’ is relevant in this regard.¹¹⁸²

6.4.1.1 Background

Considering the focus on information and knowledge as a component of empowerment, it is necessary to distinguish between a number of concepts, namely ‘data’, ‘information’ and ‘knowledge’. Here, a general work is that of Ackoff, who in *From Data to Wisdom*, stated that the human mind can be divided into five categories, namely, data, information, knowledge, understanding and wisdom.¹¹⁸³ Data is described as ‘symbols’ with the further elaboration being that it is ‘raw and simply exists, not having any meaning in itself’. Information is described as ‘data that are processed to be useful, answering the questions “who”, “what”, “where” and “when”’, also described as ‘data that has been given meaning by way of relational connection’. Knowledge is the application of data and information, and answers the ‘how’ question also described as ‘the appropriate collection of information, such that it’s intent is to be useful’. Understanding is the ‘appreciation of why’, also being described as, ‘an interpolative and probabilistic process ... cognitive and analytical ... the process by which I can take knowledge and synthesize new knowledge from the previously held knowledge’. And finally wisdom is described as ‘evaluated understanding’, that is ‘... an extrapolative and non-deterministic, non-probabilistic process ... It calls upon all the previous levels of consciousness, and specifically upon special types of human programming (moral, ethical codes, etc.). It beckons to give us understanding about which there has previously been no understanding, and in doing so, goes far beyond

1182 García, José María Rodríguez, *Scientia Potestas Est – Knowledge is Power: Francis Bacon to Michel Foucault*, Neohelicon, Volume 28, Issue 1, January 2001, pp. 109-121, at p. 109.

1183 Ackoff, R. L., *From Data to Wisdom*, Journal of Applied Systems Analysis, Volume 16, 1989, at pp. 3-9, in Bellinger, Gene, Castro Duval and Mills, Anthony, *Data, Information, Knowledge and Wisdom*, available at <http://www.systems-thinking.org/dikw/dikw.htm> (last accessed on 2016-04-19).

understanding itself'.¹¹⁸⁴ The first three concepts, namely data, information and knowledge, are of greater interest here. Hollingsworth, describes knowledge as, 'a configurative concept which also includes information and facts ... knowledge is knowing something with a considerable degree of familiarity, while information is the communication or reception of knowledge, and facts consist of information which is perceived as having objective reality'.¹¹⁸⁵ Another categorization of data, information and knowledge treats data as the basic component, being described as, 'symbols that represent signals of any type'; information can be distinguished from data in that it is useful and can answer the questions 'what', 'who', 'where', 'when' and 'how many' and information is data that has been given meaning. Processing information further, by ordering or structuring it, creates knowledge.¹¹⁸⁶

An objective of organizations that represent certain categories of people or industries is to provide those people, whose interests they represent, with information. For example, the trade union may have various functions within the employer and employee relationship, such as organizing strikes. However, another function of the trade union is to provide its members with information. In the employer versus employee relationship, the employee is at a disadvantage as it is the employer that has access to information, for example information concerning salary. This information imbalance could be used to exploit the employee who has no information to use as the basis for gauging and negotiating a fair salary. The trade union, in taking the role of information gatherer and provider, is able to provide the employee with information concerning a reasonable salary, thereby depriving the employer of a monopoly on information and levelling the playing field by addressing the information imbalance.

Two aspects need to be taken into account. First, information is not knowledge, and access to information does not equal access to knowledge. While information may be a necessary prerequisite for knowledge, the connection is not automatic. Second, as referred to above, too much information

1184 Ibid.

1185 Hollingsworth, Rogers J., *Introduction to Part 3*, in Stehr, Nico and Weiler, Bernd (eds.), *Who Owns Knowledge?: Knowledge and the Law*, Transaction Publishers, 2008, at p. 153.

1186 Bylund, *Datadriven digitalisering*, above n. 157, at p. 36.

can be a hinder, ultimately leading to disempowerment and confusion. Information may be useful only up to a certain point, after which additional accumulated information may instead decrease knowledge.

The ‘information society’ is defined as, ‘a society in which the creation, distribution, and manipulation of information has become the most significant economic and cultural activity. An Information Society may be contrasted with societies in which the economic underpinning is primarily Industrial or Agrarian’.¹¹⁸⁷ The so-called ‘knowledge society’, on the other hand, concerns ‘... capabilities to identify, produce, process, transform, disseminate and use information to build and apply knowledge for human development. They require an empowering social vision that encompasses plurality, inclusion, solidarity and participation’.¹¹⁸⁸ In questioning how the ‘information society’ and ‘knowledge society’ are related, Hildebrandt argues that these two notions basically represent different perspectives of the same thing and that they also affect one another, in that information is required to attain knowledge while knowledge is also required to identify information.¹¹⁸⁹

Knowledge can be identified as comprising different types but also being differentiated based on perspective. For example, there is cultural knowledge, knowledge about human beings, unknown knowledge such as concerning risk and scientific knowledge. These types of knowledge are complimented by perspective, for example, an economic perspective from which knowledge is approached.¹¹⁹⁰

1187 WhatIs.com, *Information Society*, available at Wikipedia, *Information Society*, available at <http://whatis.techtarget.com/definition/Information-Society> (last accessed on 2017-03-03).

1188 Communiqué of the Ministerial Round Table, *Towards Knowledge Societies*, organized during the 32nd session of the General Conference of UNESCO, Paris, 9–10 October, 2003 (document 32 C/INF. 26, para. 3).

1189 Hildebrandt, *Profiles and Correlatable Humans*, above n. 226, at p. 266.

1190 Rogowski, Ralf, *Concluding Observations*, in Stehr, Nico and Weiler, Bernd (ed.), *Who Owns Knowledge?: Knowledge and the Law*, Transaction Publishers, 2008, at p. 307.

6.4.1.2 A New Type of Knowledge

Predictive modelling relies on data that reveals the lives of individuals. By comparing databases or by utilizing an algorithm to correlate the data, the information produced from the technological process can be considered ‘new’. Hildebrandt refers to ‘knowledge construction’, which in the age of modern technology may be sophisticated, but which is really nothing new, profiling being about creating a new type of knowledge, consisting of discovering patterns in data, which is interesting for the user of the profile.¹¹⁹¹ A differentiation is made between two situations: first, where there is knowledge of the profiling process and where the profile is incorrect and second, where the profile created is essentially correct yet where this process should be considered tainted.¹¹⁹² The notion of knowledge distinguishes these two scenarios, the argument being that no matter what the benefits and even where predictive modelling creates a correct digital identity, the process remains tainted by the lack of knowledge of the process occurring.

Mere knowledge as a remedy is an aspect of empowerment that potentially alleviates the harmful effects in relation to a technology, without the need for additional measures. The problem arises when the predictive modelling process occurs undetected and forms the basis of decisions that affect an individual’s life. Hildebrandt states that the knowledge acquired from profiling is defined by its effects, that is, it is based on correlation and probability, the probability reflecting the chance that a risk will materialise. It is in this context that a shift is suggested from the pre-occupation with data in data protection regimes to a more knowledge orientated approach. Hildebrandt coins the term ‘invisible visibility’, which refers to the knowledge that is produced from predictive modelling and that is visible only to the commercial actor producing it, while it remains invisible to individuals, producing ‘previously unknown structures of reality in flux’.¹¹⁹³

An issue that engages the component of technology, but that is also relevant in the context of knowledge, is the ability of a decision-making system to provide a reason for a particular decision. Here reference is made to the notion of interpretability mentioned above in Chapter 2. An example of this is the expert

1191 Hildebrandt, *Profiles and Correlatable Humans*, above n. 226, at pp. 269-272.

1192 Ibid, at p. 279.

1193 Hildebrandt, *Who is Profiling Who?*, above n. 237, at p. 241.

system called MYCIN, an information guidance system developed in the 1970's using artificial intelligence to assist with medical diagnoses.¹¹⁹⁴ The system comprised three main parts: the knowledge base, the data base and the rule interpreter. When a user asked the system a question, the inference engine would determine the reasoning behind the answer that was returned to the user. The system is explained as follows:

Since clinicians are not likely to accept such a system unless they can understand why the recommended therapy has been selected, the system has to do more than give dogmatic advice. It is also important to let the program explain its recommendations when queried, and to do so in terms that suggest to the physician that the program approaches problems in much the same way that he does. This permits the user to validate the program's reasoning, and to reject the advice if he feels that a crucial step in the decision process cannot be justified. It also gives the program an inherent instructional capability, allowing the physician to learn from each consultation session. Furthermore, we feel it is desirable that an expert in infectious disease therapy who notes omissions or errors in the program's reasoning should be able to augment or correct the knowledge base so that future consultations will not repeat the same mistakes.¹¹⁹⁵

The system utilized 'AND/OR trees' during the reasoning process and as a result could answer the questions 'WHY?' and 'HOW?' The 'why?' and 'how?' questions that could be asked were the following: 'why was a given fact used?', 'why was a given fact not used?', 'how was a given conclusion reached?' and 'how was it that another conclusion was not reached?'. The questions posed would be answered by leading the medical practitioner through the decision tree that the system used, thereby demonstrating the system's reasoning.¹¹⁹⁶ These two simple questions would go a far way to providing the individual, who is the object of predictive modelling or any other expert system, insight into the process and more importantly, shed light on the

1194 Marshall, Dave, *Expert Systems*, available at <http://users.cs.cf.ac.uk/Dave.Marshall/AI/mycin.html> (last accessed on 2016-02-17).

1195 Shortliffe, Edward H., Davis, Randall, Axline, Stanton G., Buchanan, Bruce G., Green, Cordell C. and Cohen, Stanley N., *Computer-Based Consultations in Clinical Therapeutics: Explanation and Rule Acquisition Capabilities of the MYCIN System*, Computers and Biomedical Research, Vol. 8, 303-320, 1975, at pp. 304-305.

1196 Marshall, above n. 1194.

basis for a certain decision being reached. For example, having been refused a loan from the bank, the individual should be able to ask and receive an answer to, first, the question as to why the loan request was denied and second, how this decision was reached, in other words upon what criteria the decision was made, and most importantly, the weight that these criteria were given in relation to each other. This is empowering to the extent that this knowledge provides access to the big picture in terms of the data used to reach a decision. This line of thought corresponds with the principle of accountability included in the GDPR, where there is a duty of accountability but also the requirement to demonstrate accountability.

Another important argument is that human freedom depends on knowledge. Freedom, in the context of the ability for humans to reflect on the choices they make, is dependent on access to the knowledge that is at the foundation of those choices. Without access to this knowledge, humans have no ability for self-reflection.¹¹⁹⁷

Knowledge also has a political dimension. The relationship and balance between public knowledge and knowledge in the private sector is fundamental to the democratic society, where the increased concentration of the media in the hands of a few, together with the fact that the recipients of this information have become more passive over time, has in fact impacted democracy.¹¹⁹⁸ The internet has changed this situation, where communication between individuals, via the social media, has led to increased democratization of society. The pendulum may be swinging back as a result of predictive modelling, where the knowledge embedded in the information in the public arena is accessible only to companies. In other words, a classification occurs, leading to the categories of the 'haves' and the 'have nots'. The problem with this type of differential treatment in relation to information, according to Gandy, is that the lowest common denominators are catered to, resulting in a general decrease in knowledge on the part of the public.¹¹⁹⁹ In other words, social categorization as a basis for differentiated levels of access to information and knowledge, decreases the general level of information and knowledge in society.

1197 Hildebrandt, *Profiling into the Future*, above n. 529, at p. 12.

1198 Hollingsworth, above n. 1185, at p. 158.

1199 Gandy, above n. 187, at p. 2.

6.4.1.3 Data Protection and Knowledge

Entrenched as a principle within the data protection regime is the duty on the data controller to provide the data subject with information regarding data processing, thereby giving the data subject a degree of influence. This obligation exists also where the data subject requests such information. Articles 10 and 11 of the DPD distinguish between circumstances where the data are collected from the data subject directly and where the data have been obtained indirectly. These obligations to provide information are retained in the GDPR, where the more extensive provision of information by the data controller is required.¹²⁰⁰ Especially significant are circumstances where an automated decision has been made, and information about the logic involved as well as information regarding the consequences and significance to the individual must be provided (Article 14(h), GDPR). Recitals 46, 48, 49 and 50 of the GDPR are also relevant and provide guidance as to how the information should be provided. Article 12(7) GDPR allows for the use of standardised icons in order to provide information on processing activities that is, ‘easily visible, intelligible and clearly legible’, and which should be machine-readable.

A result of the characteristics of data protection law is the general lack of knowledge concerning what parts of it are applicable, both as far as the data controller and data subject are concerned.¹²⁰¹ This state of confusion has been acknowledged by the European Commission, which in a report in 2003, identified the low level of knowledge of data subjects as one of the factors allowing for the low enforcement rate as far as data protection legislation was concerned.¹²⁰² In this regard, Kuner refers to a Eurobarometer survey that stated that two thirds of EU citizens were not aware of data protection laws.¹²⁰³ As stated earlier, traditional law can be empowering through the protection that it

1200 Bird and Bird, *Guide to the General Data Protection Regulation*, February 2016, available at <http://www.twobirds.com/~media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en> (last accessed on 2016-04-07), at p. 21.

1201 Kuner, *The ‘Internal Morality’ of European Data Protection Law*, above n. 1178.

1202 Report from the Commission, *First Report on the Implementation of the Data Protection Directive (95/46/EC)*, Commission document COM(2003) 265 final.

1203 Kuner, *The ‘Internal Morality’ of European Data Protection Law*, above n. 1178, at p. 12. The reference is made to Kuner in light of the link to the Eurobarometer no longer being available.

provides. However, this must be questioned in light of the fact that traditional law may be too complicated for ordinary citizens to comprehend. For example, it is argued that in order for a legal source to be constitutional, one of the many requirements it should adhere to is that of ‘understandability’.¹²⁰⁴

From the predictive modelling perspective, the information that must be provided in circumstances where profiling has occurred, is important. The data subject must be informed of the ‘existence’ of profiling and its ‘consequences’ (Recital 48, GDPR). Notwithstanding this, a number of issues remain. First, the notions of ‘existence’ and ‘consequences’ are not developed. It seems highly unlikely that a data controller will inform the data subject of the potential harms and the negative impact on autonomy. Second, data protection in general is applicable only to personal data. A question that arises concerns whether the obligation to provide information still exists when data is utilised that is not considered personal, the reference cited above where ‘friends’ data is used to judge a person. It is debatable whether this data could be considered ‘personal’ in nature. Reference is also made to the case of *YS* dealt with above in Chapter 5, which arguably reduced the scope of the concept of personal data. Third, the information requirements do not provide access to the big picture. A data subject may have access to his or her own data but not the way in which these data points have been correlated, first to each other but also to other data points that the data subject has no access to. In other words, mere access to personal data does not guarantee access to the knowledge about how the data was used and also what weight was given to the individual data points. Within the context of data protection, the distinction between data and knowledge materialises. The data protection regime concerns personal data. In the context of predictive modelling, it is not the data itself that is harmful, but rather the knowledge that is acquired from it and applied to the individual. In other words, the data subject’s personal data as correlated with the personal data of other data subjects, results in knowledge for the commercial actor. This can also be described in terms of the data subject as a member of a group scenario, alternatively referred to as group profiles, where the value of the knowledge lies not in a person’s personal data, but rather in the person’s personal data in relation to the personal data of others within a group.¹²⁰⁵

1204 Korhonen, Rauno, *The New Information Code of Finland*, in Saarenpää, Ahti and Sztobryn, Karolina, *Lawyers in the Media Society: The Legal Challenges of the Media Society*, University of Lapland, 2016, at p. 55.

1205 Hildebrandt, *Profiling into the Future*, above n. 529, at p. 13.

Another aspect for consideration is that information and knowledge is a ‘public good’. When knowledge of the individual makes its way into the hands of others, everyone benefits. An argument following this is that choices in relation only to self-interest prevent knowledge from making its way into the public sphere.¹²⁰⁶ This can be seen in relation to the tailoring of services, which are not only harmful to that individual, but stifles the dispersion of knowledge to others. In the words of Sunstein, it is not that individuals making choices based solely on self-interest may lose out by not learning about something that they are not interested in, but other individuals may lose out.¹²⁰⁷

6.4.1.4 Remarks

Knowledge in itself can be empowering, especially where the individual, receiving knowledge concerning how he or she benefits from a certain predictive modelling process, may be willing to agree to its use. For example, revealing location data may be tolerated by an individual if he or she can receive real time alerts and avoid traffic congestion. Plainly put, receiving information about the returns may be good enough. In a survey by Gigya, consumers were prepared to part with personal data if they received something in return for their data and if the conditions under which the data were used were transparent.¹²⁰⁸ Therefore, the solution to a problem may lie in the mere communication or publication of that problem. Berners-Lee, responding to a question concerning the fact that companies are logging the clickstream of internet users, stated that, ‘[i]t’s mine – you can’t have it. If you want to use it for something then you have to negotiate with me, I have to agree; I have to understand what I am getting in return’.¹²⁰⁹

The notion of the importance of information was stressed in a European Commission communication concerning collective redress. The Commission

1206 Sunstein, Cass, *Republic.com*, Princeton University Press, 2001, at p. 100.

1207 Ibid, at p. 102.

1208 Salyer, Patrick, CEO of Gigya, *Data Collection: All Consumers Want is Transparency, Relevance and Convenience*, Huffpost Tech, United Kingdom, available at http://www.huffingtonpost.co.uk/patrick-salyer/transparency-relevance-and-convenience_b_6678422.html (last accessed on 2015-01-18).

1209 Cellan-Jones, Rory, *Questions and Answers: Tim Berners-Lee*, BBC News, available at <http://news.bbc.co.uk/2/hi/technology/7300434.stm> (last accessed on 2014-04-03).

emphasised the role of information, stating that, '[e]ffective information on collective action is a vital condition for ensuring that those who could claim to have been harmed by the same or similar alleged infringement learn of the possibility to join a representative action or a group action and, thus, can make use of this means of accessing justice.'¹²¹⁰ This highlights the idea that information is a key point of departure as far as many remedies are concerned and its importance should not be underestimated.

Insight and behavioural data can have more value for companies than personal data, because of increasing value is the steps and thought processes that the person went through in arriving at the decision to buy that product, since it enables the prediction of this action in others. This has led to the notion that society is moving from the commodification of personal data to the commodification of identities and behaviour, where personal data without context is almost useless to the companies who are interested in acquiring knowledge concerning identity and behaviour.¹²¹¹

The existence of predictive modelling is starting to become public knowledge, which has been a catalyst for the establishment of organizations whose purpose is to provide information and disseminate knowledge about predictive modelling. AlgorithmWatch is an organization that helps to illuminate the fact that algorithms are playing an ever increasing role in the decision making processes that affect all human beings, and in doing so shows how behaviour is influenced, highlighting the ethical dimensions.¹²¹²

There is also the opinion that technologies, such as predictive modelling, are requiring a reconstitution of the whole concept of what knowledge actually is. An initial insight is that the knowledge or answers that the predictive models produce may be too complex for the human brain to comprehend, a consequence being that what we are now starting to witness is the generation of

1210 European Commission, Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Towards a European Horizontal Framework for Collective Redress*, available at http://ec.europa.eu/consumers/archive/redress_cons/docs/com_2013_401_en.pdf (last accessed on 2016-04-18).

1211 Prins, above n. 51, at p. 6.

1212 AlgorithmWatch, available at <http://algorithmwatch.org/mission-statement/#English> (last accessed on 2016-09-09).

knowledge without understanding.¹²¹³ This is connected to the argument addressed above, where correlations made between data by algorithms cannot be explained, in other words, where causation is inexplicable and the state of affairs simply ‘is’. As a result, in the future it may be challenging to convince individuals that the answer that a model provides is correct or even plausible, in the absence of causation, especially in situations that are seemingly ridiculous. The answer may lie in the way that society deems something to be knowledge. For example, knowledge has traditionally been thought of as, ‘a system of settled, consistent truths’, an attitude that is attributed to the medium that preserves knowledge, for example, ink and paper, where the knowledge never changes. An alternative is describing knowledge as ‘a continuous argument as it is tugged this way and that ... never fully settled, never fully written, never entirely done’.¹²¹⁴

Seipel, referring to the maximalist view towards technology, states that the modern knowledge society ought to have the ambitious goal of developing rich universal information services and that, ‘[f]or knowledge to grow, information must flow’.¹²¹⁵

6.4.2 Accountability

Traditionally, much of the responsibility for protecting the individual against the vulnerabilities resulting from technology has been placed on the individual, him or herself. The ideology of Westin is influential in this regard. However, taking into account the power of predictive modelling, a shift is required to a position where the commercial actor is held accountable for the consequences. Mayer-Schönberger and Cukier state that in this age of big data, one needs to consider whether it is even realistic to expect individuals to be able to take decisions regarding the use of their personal data. A suggested remedy is that the full responsibility of the use and re-use of data, including personal

1213 Weinberger, David, *The Machine That Would Predict the Future*, Scientific American, December 2011, at p. 36.

1214 Ibid, at p. 37.

1215 Seipel, Peter, *Access Laws in a Flux*, in Law and Information Technology: Swedish Views, Swedish Government Official Reports, SOU 2002:112, Information and Communication Technology Commission report, Stockholm, 2002 at p. 98.

data, be placed almost solely on the user of that data.¹²¹⁶ This is complemented by the attitude of companies that personal data is to be considered part of the ‘public domain’ and that individuals will either be willing or forced to provide it to third parties.¹²¹⁷ Empowering the individual requires a shift in the placement of accountability from the individual to the commercial actor.

6.4.2.1 The Development of a Principle

Accountability has been defined as, ‘an obligation or willingness to accept responsibility or to account for one’s actions’.¹²¹⁸ Another general definition, from within the data protection regime, is that it is the showing of how responsibility is exercised. Making accountability verifiable and demonstrating responsibility in turn establishes trust.¹²¹⁹ In this sense, the notion of accountability comprises two tiers. First, it entails a responsibility to adhere to and implement data protection principles, and second, it entails an ability to prove that this responsibility has been undertaken. It is not enough that, for example, legislation is followed, the ability to show that legislation has been followed is also required.

Implementing accountability requires an external body or organization that one is accountable to, which seeks answers and has the ability to impose sanctions.¹²²⁰ It is also stressed that accountability is not the same as ‘responsibility’ due to the fact that an entity can be responsible yet lack accountability.¹²²¹ For example, an individual may take on the responsibility for something of his or her own accord, without the requirement of having to prove this fact to

1216 Mayer-Schönberger and Cukier, above n. 149, at p. 173.

1217 Prins, above n. 51, at p. 5.

1218 Merriam-Webster Dictionary, *Accountability*, available at <http://www.merriam-webster.com/dictionary/accountability> (last accessed on 2016-04-07).

1219 Recommendation of the Council concerning Guidelines governing the protection of Privacy and Transborder Flows of Personal Data (Adopted 11 July 2013; (C (2013)79)).

1220 Bennett, Colin, *International Privacy Standards: Can Accountability be Adequate?*, Privacy Laws and Business International, Vol. 106, pp. 21-23, 2010, available at <http://www.colinbennett.ca/Recent%20publications/PrivacyLawsand%20BusinessAugust2010.pdf> (last accessed on 2017-04-19), at p. 3.

1221 Ibid.

anyone. Bennet therefore summarises accountability by stating that it entails an understanding of ‘who is accountable, for what and to whom’.¹²²²

Within the European data protection framework, accountability has existed for some time. It was included as a principle for data controllers to follow in the original draft of the OECD (1980) Guidelines. The Guidelines stated that, ‘[a] data controller should be accountable for complying with measures which give effect to the principles stated above’.¹²²³ When the Guidelines were updated in 2013, the accountability principle remained unchanged. Part Three of the revised Guidelines, entitled ‘Implementing Accountability’, laid out practical measures to be undertaken by the data controller in implementing the principle of accountability.¹²²⁴ The significant parts of paragraph 15(a) state that the data controller should have in place a ‘privacy management programme’ that among other things, ‘is tailored to the structure, scale, volume and sensitivity of its operations’ (15(a)(ii)), ‘provides for appropriate safeguards based on privacy risk assessment’ (15(a)(iii)), and ‘is integrated into its governance structure and establishes internal oversight mechanisms’ (15(a)(iv)). The Asia-Pacific Economic Cooperation has also produced a set of principles relating to privacy in the form of a ‘privacy framework’. One of these principles is entitled ‘accountability’ and states that, ‘[a] personal information controller should be accountable for complying with measures that give effect to the Principles stated above’.¹²²⁵

Bennett argues that what is lacking in the two above principles on accountability is the ‘to whom’ aspect.¹²²⁶ In other words, there is no independent body that has been designated to oversee the application of the accountability principle. Another document relevant in this context is the Madrid Privacy Declaration of 2009, which reaffirms international instruments for privacy

1222 Ibid.

1223 Recommendation of the Council concerning Guidelines governing the protection of Privacy and Transborder Flows of Personal Data (adopted 23 September 1980; (C (80) 58/FINAL)).

1224 Ibid.

1225 Asia-Pacific Economic Cooperation, privacy Framework, 2005, available at http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/_media/Files/Groups/ECSG/05_ecsg_privacyframework.ashx (last accessed on 2016-04-08).

1226 Bennett, above n. 1220, at p4.

protection.¹²²⁷ Here, the principle of accountability states that the responsible person shall, ‘a) take all the necessary measures to observe the principles and obligations set out in this document and in the applicable national legislation’, and ‘b) have the necessary internal mechanisms in place for demonstrating such observance both to data subjects and to the supervisory authorities in the exercise of their powers, as established in section 23’.¹²²⁸ Here, accountability requires that the adherence to this principle be demonstrated both to data subjects as well as to supervisory authorities.

The notion of accountability has also been a topic for examination by the Article 29 Data Protection Working Party. Opinion 3/2010 put forward the notion of accountability as a principle to be included in the data protection framework.¹²²⁹ The Article 29 Data Protection Working Party recommended a two-tier approach for implementing the notion of accountability, where the first tier would entail basic statutory requirements binding all controllers and ensuring a minimum level of application, with a second tier allowing for voluntary measures that would go beyond this minimum level provided by the first tier.¹²³⁰

6.4.2.2 The General Data Protection Regulation

While it has been argued that the principle of accountability has long been an essential element of the data protection ideology, this has never been explicitly stated. The DPD incorporates this notion, however, it is not lifted to the status of being a fully-fledged principle. Instead, it has been applied as parts of other principles, for example, the duty of data controllers to provide data subjects with information concerning data processing activities that concern them or

1227 The Public Voice, *Madrid Declaration*, 3 November 2009, available at <http://thepublicvoice.org/TheMadridPrivacyDeclaration.pdf> (last accessed on 2016-04-08).

1228 The Madrid Resolution, *International Standards on the Protection of Personal Data and Privacy*, International Conference of Data Protection and Privacy Commissioners, 3 November 2009, Madrid, Spain, available at http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf (last accessed on 2016-04-08).

1229 Article 29 Data Protection Working Party, *Opinion 3/2010 on the principle of accountability*, adopted on 13 July, 2010 available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf (last accessed on 2016-04-06).

1230 *Ibid*, at p. 6.

the need to put sufficient technical and organisational measures in place in order to protect privacy and security.¹²³¹ In contrast the GDPR explicitly recognizes the principle of accountability.¹²³² Article 5 expresses the underlying principles of the GDPR, where Article 5(2) states that, ‘[t]he controller shall be responsible for and be able to demonstrate compliance with paragraph 1 (“accountability”)’. This is complemented with Article 24, which states that, ‘taking into account the nature, scope, context and purposes of the processing and the associated risks, the controller shall implement appropriate technical and organisational measures to ensure and be able to demonstrate that the processing of personal data is performed in accordance with the GDPR’. Here, a duty is placed on the controller to put in place the technical means to live up to the requirements dictated by the principle of accountability, but also have in place the means with which to demonstrate the extent to which this has been done.

Accountability is now expressly an underlying principle of data protection, and there are other indicators of this as well. Blume states that the GDPR, after a reading of Articles 22 and 28 (Articles 24 and 30 respectively in the final draft), put greater accountability on the Data Controller.¹²³³ Article 24 lays down the responsibilities of the controller whereas Article 30 lays down the extent to which records shall be maintained of all the data processing activities.

An observation, picking up on the argument of Bennett above, is that the GDPR, while more clearly illuminating a principle of accountability, does not stipulate the ‘to whom’ aspect. Articles 5 and 22 require a demonstration on the part of the controller to show that the accountability procedures are met, yet nowhere is it stated to whom this should be done.

1231 Davidson, Brian, *Getting to Know the General Data Protection Regulation, Part 7 – Accountability Principles = More Paperwork*, available at <http://privacylawblog.field-fisher.com/2016/getting-to-know-the-general-data-protection-regulation-part-7-accountability-principles-more-paperwork/> (last accessed on 2016-04-08).

1232 Bird and Bird, above n. 1200, at p. 7.

1233 Blume, Peter, *An Evolving New European Framework for Data Protection*, in Svantesson, Dan Jerker B. and Greenstein, Stanley (eds.), *Nordic Yearbook of Law and Informatics 2010-2012, Internationalisation of Law in the Digital Information Society*, Ex Tuto Publishing, 2013, at p. 29.

6.4.2.3 Constituting Accountability

While the principle of accountability has been elevated, it can be more challenging to attain guidance as to how, in concrete terms, this principle can be applied in practice. Nissenbaum refers to the concept of ‘operational criteria’, stressing that it is only fair that the technology in the hands of companies be balanced against individuals. She consequently refers to operational criteria as a means of ensuring that the technology is fair in the outcomes that it produces. Her operational criteria are: first, ‘assuring non arbitrary grounds for exclusion’, second, ‘transparency of principles determining inclusion and exclusion’ and third, ‘the relevance of decision criteria to particular decisions’. She continues that these operational criteria ought to be included when companies, for example, purchase services and products.¹²³⁴ These measures can be viewed as a practical and concrete implementation of the principle of accountability. Requiring the production of operational criteria to be attached to a product or service, for example as a type of meta data, is a step that prevents companies from attempting to deny responsibility. This may be so, for example, where a product or service is sold from one company to another, thereby producing a long supply chain, such that the technology eventually loses the context from which the product or service was originally produced.

Another attempt to detail the practical implementation of accountability is provided by the Centre for Information Policy Leadership.¹²³⁵ This paper states that accountability:

... shifts the focus of privacy governance to an organisation’s ability to demonstrate its capacity to achieve specified privacy objectives. It involves setting privacy protection goals for companies based on criteria established in law, self-regulation and best practices, and vesting the organisation with both the ability and the responsibility to determine appropriate, effective measures to reach those goals. As the complexity of data collection practices, business

1234 Nissenbaum, *Privacy in Context*, above n. 230, at p. 209.

1235 The Centre for Information Policy Leadership, Hunton and Williams LLP, *Data Protection Accountability: The Essential Elements*, October 2009, available at http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf (last accessed on 2016-04-08). The document is based on the results of the Galway Project, initiated in January 2009 by an international group of experts from government, industry and academia to define the essential elements of accountability and consider how an accountability approach to information privacy protection would work in practice.

models, vendor relationships and technological applications in many cases outstrips the individual's ability to make decisions to control the use and sharing of information through active choice, accountability requires that organisations make responsible, disciplined decisions about data use even in the absence of traditional consent.¹²³⁶

This highlights the role of technology, where creative measures can convey accountability.

While there may be a legal framework in place that dictates a policy of accountability, there are other mechanisms for ensuring that a culture of accountability is cultivated and maintained. This is also voiced by the Article 29 Data Protection Working Party, which has stated that beyond the law, there are practices, such as compliance programmes or binding corporate rules, that re-inforce the notion of accountability.¹²³⁷

6.4.2.4 Transparency as an Element of Accountability

In general terms, the notion of transparency is an important element in any open and democratic society, functioning as a check on a regime's use of power.¹²³⁸ Transparency is often argued to be central in order to protect individuals from the risks and vulnerabilities of technological developments. It is also argued to be a precondition for accountability and is part of the rationale behind principles like that of open access to governmental information.¹²³⁹ However, transparency alone is no guarantee, and must sometimes be implemented with, for example, accountability. The nature of predictive modelling is such that transparency may be ineffective and even counter-productive in

1236 Ibid, at p. 3.

1237 Article 29 Data Protection Working Party, *Opinion 3/2010 on the principle of accountability*, adopted on 13 July, 2010 available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf (last accessed on 2016-04-06), at p. 7.

1238 Here reference is made to the role of journalists and the media in the Snowden revelations, as described by Glenn Greenwald. This is so both as far as the actual Snowden revelation is concerned but also in terms of the media's role as a general check on political power. Greenwald refers to the 'fourth estate', namely the political media, which ensures government transparency. Greenwald, Glenn, above n. 85, at p. 210.

1239 Brin, David, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?*, Basic Books, 1998.

that it may create the impression of empowerment while actually having the opposite effect.

There are a number of challenging aspects relating to the notion of transparency. First, for transparency to be regarded as real, the individual needs to know what to look for, in other words how to use the transparency. Granting access to a ‘black box’ need not necessarily lead to transparency. In fact it can inhibit transparency, if the core aspects of the system are not identifiable at a glance. Second, a challenge remains that many individuals will not understand what they find. It is here that the need is identified for new professions and institutions to assist with transparency. Reference has been made to a new profession called ‘algorithmists’ to shed light on the algorithms used in decision-making.¹²⁴⁰ Third, and related to the arguments above, is that real or effective transparency must not be substituted with a form of transparency that is superficial, operating as a ‘smoke screen’.¹²⁴¹ There is no doubt that this is useful, however, it should not serve as an excuse to enable a commercial actor to continue with its core business that potentially has harmful effects. Fourth, transparency as such is not necessarily a mechanism for correcting a power imbalance, as insight into an operation does not necessarily provide the power to halt that operation.

Focussing on the division between privacy and data protection, Gutwirth and De Hert refer to ‘opacity tools’ and ‘transparency tools’.¹²⁴² Privacy is protected by opacity tools that ensure non-interference with an individual’s private sphere, while data protection legislation belongs to the category of transparency tools, where transparency is the factor that compels a data controller to act in a fair and just manner in relation to the data subject.¹²⁴³ De Hert and Gutwirth assert that the transparency tools of data protection are the correct route to take in the face of profiling. A question posed is whether, given the nature of predictive modelling, this is adequate? Leenes has aired some reservations. He asserts that a different type of transparency instrument

1240 Mayer-Schönberger and Cukier, above n. 149, at p. 179.

1241 An example of a transparency initiative is the Google Transparency Report, available at <http://www.google.com/transparencyreport/?hl=en-GB> (last accessed on 2017-04-04). It is argued that while transparency reports in general may be useful, they can be abused to the extent that insight to superficial information is granted while access to important information remains hidden.

1242 Gutwirth and De Hert, above n. 1008, at p. 271

1243 Ibid.

is required, where it is not the access to the data that is at the centre but rather of the decision-making process.¹²⁴⁴

Nissenbaum refers to the concept ‘transparency paradox’. She describes it in the context of ‘notice-and-consent situations’, also referred to as informed consent or ‘transparency-and-choice’, where transparency operates together with consent.¹²⁴⁵ The notice-and-consent construction is based on two considerations: first, that the individual is in control and decides when to part with personal data, and second, that the free market prevails, in that the parties to a situation can, in the context of the free market, decide for themselves the cost of parting with personal data. A transparency-and-choice construction is characterised either by detailed, lengthy and complex privacy policies, that inhibit individuals from reading them, or by privacy policies that are so abbreviated that they lack many of the important details underlying an informed decision.¹²⁴⁶ The solution Nissenbaum proposes is a form of transparency where information is provided in a brief and clear manner that encapsulates the privacy principles of the service in a manner that ordinary people can understand.¹²⁴⁷

There is a connection between transparency and technology, where technology is an enabling tool in order to achieve transparency. In other words, technology in the hands of the ‘monitored’ has the ability to create transparency with regard to those doing the original monitoring and who are in a position of power. It is argued that human beings should by default be considered ‘watchers’, where watching other human beings places them in a position of power in relation to those being watched but also allows for humans to define themselves.¹²⁴⁸ Technology has the function of giving the less powerful in society the ability to surveil the more powerful, and in this manner create a form of transparency. For example, smart phones equipped with cameras have made

1244 Ibid, at p. 298.

1245 Nissenbaum, Helen, *A Contextual Approach to Privacy Online*, Daedalus, the Journal of the American Academy of Arts & Sciences, Vol. 140, No. 4, 2011, available at http://www.amacad.org/publications/daedalus/11_fall_nissenbaum.pdf (last accessed on 2016-04-11) at p. 34.

1246 Ibid.

1247 Ibid, at p. 36.

1248 Bennett, Haggerty, Lyon, and Steeves, above n. 330, at p. 167.

the work of the police more transparent, where instances concerning the excessive use of force are recorded and made public.¹²⁴⁹ However, technology as an enabler of transparency can also be an inhibitor. For example, Apple has patented a technology that allows the police to switch off the ability to transmit pictures and video from devices within a geographic area, all that is required is to deem a gathering ‘sensitive’ and that it needs to be ‘protected from externalities’. The technology works by sending an encoded signal to all devices within a certain geographical area, disabling all recording facilities.¹²⁵⁰ Here, technology becomes a central tool as the pendulum swings backwards and forwards in the battle for transparency.

Bennett et al. argue that while there is an increase in the use of surveillance measures by individuals, it is on a small scale, for example as they watch each other in the social media. The main difference between the surveillance performed by individuals as opposed to the surveillance performed by companies is that of scale. And while people may have access to the use of systems, for example that of face-recognition systems used by Facebook, they do not have access to the algorithms underlying the technology.¹²⁵¹

6.4.2.5 Remarks

Accountability has always been an underlying principle of data protection. The GDPR now elevates it to a fully-fledged principle. In addition, the GDPR also introduces demands that accountability can be shown to having been adhered to. Consequently, it not only requires that organizational and technical measures are in place to ensure that legislation on accountability is followed, but it places a greater emphasis and even duty on the ability to demonstrate or prove this. Also, the increased accountability placed on the data controller as far as data protection legislation is concerned, can be argued to be a recogni-

1249 Goldsmith, Andrew J., *Policing's New Visibility*, British Journal of Criminology, 50, no. 5, 2010, at pp. 914-934.

1250 Farrell, Nick, *Apple patents tech to let cops switch off iPhone video, camera and wi-fi*, TechEye, 7 August 2013, available at <http://www.techeye.net/security/apple-patents-tech-to-let-cops-switch-off-iphone-video-camera-and-wi-fi> (last accessed on 2016-04-12).

1251 Bennett, Haggerty, Lyon, and Steeves, above n. 330, at p. 7.

tion that in order for data protection to be effective, control needs to be re-assigned from the individual to controller. Mayer-Schönberger and Cukier argue that in the face of the possibilities for data-mining it is natural that accountability shift from the individual to those who will be using the data.¹²⁵² In other words, there is the realization that with the increased reliance on increasingly complex technologies, individuals have a diminishing ability to control the access to their personal data as well as how it is used. In addition, an increased focus on accountability provides an opportunity for companies to demonstrate their commitment by exhibiting mechanisms of accountability that go beyond the minimum level stipulated by the law. By demonstrating accountability, they may receive greater leeway to use the personal data of their customers or potential customers. The challenge will be to display this accountability in an easily understandable manner and possibly using new technological forms to convey the message. In addition, it is argued that the speed with which the iterative predictive models make decisions will require a central role for technology to demonstrate accountability.

Finally, the above section illustrates the methodological core of the strategy of empowerment, namely, that the components not only influence the problem at hand, but also influence each other. While traditional law entrenches the notion of accountability, it may be meaningless unless conveyed to the individual, at which point how understandable the knowledge is, becomes relevant. This section also highlights the fact that technology, while being an enabler of accountability, can also diminish it, as illustrated by the ability to suspend the recording function of smart phones. It is here that the role of traditional law as an indirect regulator comes to the fore. The manner in which the law regulates the technologies of accountability will be critical.

6.4.3 A Duty of Care

An element of the strategy of empowerment is the creation of a fiduciary type duty on those using predictive modelling. In seeking a solution to the invasive nature of technologies similar to predictive modelling, a number of authors have cited the fiduciary duty mechanism as a possible solution. This section

1252 Mayer-Schönberger and Cukier, above n. 149, at p. 173.

examines the notion of the fiduciary duty and the extent to which it is suitable as an element of an empowerment strategy.

6.4.3.1 Background

Fiduciary comes from the Latin word ‘fidere’, meaning ‘to trust’.¹²⁵³ The doctrine of fiduciary duty originates from Roman law and was developed within the English law of trusts, being a notion most prevalent within common law legal systems.¹²⁵⁴ It was consequently incorporated into precedents from the English courts.¹²⁵⁵ The courts, however, have through precedent extended the area of applicability of the fiduciary duty beyond the realm of trusts, to any relationship built on trust or confidence between two parties.¹²⁵⁶

The fiduciary duty entails the duty to act entirely in another party’s interests. The party bearing the duty is called the ‘fiduciary’ and the party to whom the duty is owed is called the ‘principal’ (or beneficiary). The main idea behind this legal instrument is that the fiduciary should not be able to profit from the relationship unless with the express consent of the principal.¹²⁵⁷ In other words, the fiduciary duty arises out of a relationship of trust and confidence between parties, where one of the parties, due to his or her position or standing, is trusted to take care of the property of the principal.¹²⁵⁸ The notion of fiduciary duty is therefore a legal mechanism, which has been created to protect the principal from abuse by the actions of the fiduciary.¹²⁵⁹ The principal, by placing a certain degree of trust and confidence in the fiduciary, is placed

1253 Merriam-Webster, *Fiduciary*, available at <http://www.merriam-webster.com/dictionary/fiduciary> (last accessed on 2016-03-22).

1254 Weinrib, Ernest J., *The Fiduciary Obligation*, University of Toronto Law Journal, Vol. 25. No. 1, 1975, pp. 1-22, at p. 3.

1255 Todd, Trevor, *Fiduciary*, Disinherited, available at <http://disinherited.com/fiduciary-relationships/> (last accessed on 2016-11-15).

1256 Ibid.

1257 Legal Information Institute, *Fiduciary Duty*, Cornell University Law School, available at https://www.law.cornell.edu/wex/fiduciary_duty (last accessed on 2016-03-22).

1258 The Free Dictionary, Legal Dictionary, *Fiduciary*, available at <http://legal-dictionary.thefreedictionary.com/fiduciary+duty> (last accessed on 2016-03-22).

1259 European Commission, *Resource Efficiency and Fiduciary Duties of Investors*, available at http://ec.europa.eu/environment/enveco/resource_efficiency/pdf/FiduciaryDuties.pdf (last accessed on 2016-03-22).

in a position of dependence in relation to the fiduciary, while the fiduciary is placed in a position of influence over the principal.¹²⁶⁰ The consequences of taking on the role of fiduciary is that the fiduciary, ‘... is held to a standard of conduct and trust above that of a stranger or of a casual business person. He/she/it must avoid “self-dealing” or “conflicts of interests” in which the potential benefit to the fiduciary is in conflict with what is best for the person who trusts him/her/it.’¹²⁶¹

Solove, in describing the notion of fiduciary, states that, ‘[t]he law of fiduciary duties creates special duties of accountability within certain relationships. A fiduciary relationship exists when one party stands in a special position of power over another person’.¹²⁶² He refers to the definition of the fiduciary duty as expressed by New York Chief Justice Benjamin Cardozo who stated that, ‘[m]any forms of conduct permissible in a workday world for those acting at arm’s length, are forbidden to those bound by fiduciary ties. A trustee is held to something stricter than the morals of the market place. Not honesty alone, but the punctilio of an honor the most sensitive, is then the standard of behavior’.¹²⁶³

The fiduciary notion is activated by relationships that are based on ‘trust’, in which conflicts of interest and duty can arise – the fiduciary is given the power to affect the principal’s interests, resulting in his or her dependency on the fiduciary.¹²⁶⁴ The need for the mechanism lies in the fact that the nature of the relationship between fiduciary and principal puts the latter at the mercy of the former, necessitating a legal device to encourage the fiduciary to use his or her power in a proper manner.¹²⁶⁵ In other words, the fiduciary relationship by its very nature is open to abuse by the fiduciary, which necessitates a legal mechanism to discourage this and protect the principal. It is argued that at the core of the fiduciary relationship is the notion of morality within the realm of

1260 The Free Dictionary, above n. 1258.

1261 Ibid.

1262 Solove, *Understanding Privacy*, above n. 535, at p. 135.

1263 *Meinhard v. Salmon* 164 N.E. 545, 546 (N.Y.1928) in Solove, *Understanding Privacy*, above n. 535, at p. 135.

1264 Kerr, Ian R., *The Legal Relationship Between Online Service Providers and Users*, Canadian Business Law Journal, Vol. 35, 2001, 419-458, at p. 447.

1265 Weinrib, above n. 1254, at p. 11.

commerce, where, in certain relationships, making a profit is frowned upon based on the nature of that relationship.¹²⁶⁶

The fiduciary mechanism therefore has two parts: first is the fact that the fiduciary has a certain scope within which to exercise his or her discretion and second, this discretion must be capable of affecting the legal position of the principal. Weinrib summarises the concept stating that, ‘the leeway afforded to the fiduciary to affect the legal position of the principal in effect puts the latter at the mercy of the former, and necessitates the existence of a legal device which will induce the fiduciary to use his power beneficially’.¹²⁶⁷ Breach of the fiduciary duty requires that the principal be placed in the position that he or she would have been in had the breach not occurred, with damages also available.¹²⁶⁸

6.4.3.2 Status-Based versus Fact-Based Fiduciary Relationships

There are two types of fiduciary relationships, namely, the status-based and fact-based fiduciary relationship. The status-based fiduciary relationship recognises a certain category of professional relationships that are accorded the characteristic of being a fiduciary relationship, for example, trustee/beneficiary, lawyer/client, principal/agent, doctor/patient and employer/employee.¹²⁶⁹ Once a relationship falls within one of these categories, it is automatically considered a fiduciary relationship, without any further evidence required to this effect. A characteristic of the fiduciary relationship is that there is a disclosure of information from principal to fiduciary (for example the seeking of advice), which in turn puts the fiduciary in a position of power, thereby providing the fiduciary with the ability to affect the principal’s interests.¹²⁷⁰

The above list of fiduciary relationships is not all-inclusive. Kerr notes that the Courts in Canada have come to recognize other relationships as fiduciary based relationships even though they do not fall within the category of status-

1266 Ibid, at p. 3.

1267 Ibid, at pp. 4-5.

1268 Todd, above n. 1255.

1269 Kerr, above n. 1264, at p. 449.

1270 Ibid.

based fiduciary relationships, thereby requiring that the courts actively undertake to recognize fact-based fiduciary relationships.¹²⁷¹ These fiduciary relationships are considered fact-based fiduciary relationships as they are not part of the traditionally accepted list of status-based relationships. The test for recognizing fact-based fiduciary relationships in ‘new relationships’ was devised by Wilson J in the case of *Frame v. Smith* and comprises three elements: first, the fiduciary has scope for the exercise of some discretion of power, second, the fiduciary can unilaterally exercise that power or discretion so as to affect the beneficiary’s legal or political interests and third, the beneficiary is particularly vulnerable to or at the mercy of the fiduciary holding the discretion or power.¹²⁷² Therefore, in determining the existence of a fiduciary relationship, a number of requirements are necessary. It must be determined first, whether the fiduciary was in a position to exercise power and affect the principal’s legal interests, resulting in a degree of dependency and second, whether there was a degree of dependency, in other words that the principal was entitled to expect that the fiduciary would act in his or her interests based on their relationship.¹²⁷³ It is noteworthy that the extension of the reach of the fiduciary relationship reflects the court’s willingness to develop the common law so as to make it more ‘socially responsive and acceptable to the community’.¹²⁷⁴

6.4.3.3 Hedley Byrne

A well-known case within English law is that of *Hedley Byrne and Co Ltd v. Heller and Partners Ltd*.¹²⁷⁵ The Applicant, an advertisement agency (Hedley Byrne), approached the bank of their client for clarification regarding the credit worthiness of this individual. The information provided by the bank was favourable but came with the proviso that it was provided without responsibility on the part of the bank. The client subsequently went bankrupt, and Hedley Byrne was unable to recoup certain losses for advertising purchased

1271 Ibid, at p. 450.

1272 *Frame v. Smith* (1987), 42 D.L.R. (4th) 81, at pp. 998-99 in Kerr, above n. 1143, at p. 451.

1273 Kerr, above n. 1264, at p. 454.

1274 Todd, above n. 1255.

1275 *Hedley Byrne & Company Limited v. Heller & Partners Limited* [1964] AC 465 (HL).

by their client. Instead, Hedley Byrne claimed damages from the bank due to relying on the information provided by it. The main question that the case examined was, ‘whether and in what circumstances a person can recover damages for loss suffered by reason of his having relied on an innocent but negligent misrepresentation’.¹²⁷⁶

The Court found that the disclaimer provided by the bank prevented any claim against it. However, the significance of this case is that the duty of care, which previously existed only in fiduciary relationships and as a result of contractual relationships, was extended to other relationships. The effect of Hedley Byrne was to increase the ambit of the duty of care to situations where one party relied on information provided by another party and where there was a special relationship. In other words, it was argued that, ‘a duty of care to make non-negligent statements is imposed whenever a special relationship exists and responsibility is not expressly disclaimed’.¹²⁷⁷ In the judgement, Lord Reid refers to the case of *Robinson v. National Bank of Scotland*, where Lord Haldane remarked that the duty of care should not be limited to relationships of a fiduciary character, referring to other ‘special relationships’. Lord Reid thereupon remarked:

... I can see no logical stopping place short of all those relationships where it is plain that the party seeking information or advice was trusting the other to exercise such a degree of care as the circumstances required, where it was reasonable for him to do that, and where the other gave the information or advice when he knew or ought to have known that the enquirer was relying on him’.¹²⁷⁸

Subsequent cases have both limited and extended the reach of the principle of a duty of care established in Hedley Byrne. Despite these swings in its scope of application, it remains an established principle in the common law.

1276 Ibid, at p. 1.

1277 Stevens, Robert, *Hedley Byrne v. Heller: Judicial Creativity and Doctrinal Possibility*, *The Modern Law Review*, Vol. 27, No. 2, March 1964, at p. 122.

1278 *Hedley Byrne*, at p. 5.

6.4.3.4 Remarks

The concept of fiduciary duty is essentially a common law legal instrument regulating certain legal relationships and hence may not be entrenched to the same extent from one country to another. Considering the characteristics of the fiduciary mechanism, a question worth investigating is whether the relationship between the individual as an object of predictive modelling and the commercial actor using predictive modelling ought to be considered fiduciary in nature?

An initial observation is that the relationship between commercial actor and individual does not fall within any preconceived list of fiduciary based relationship based upon status. The next step is to determine whether the above relationship can be considered to fall within the fiduciary mechanism, in other words, whether it could be considered a fiduciary relationship based on fact. Applying *Frame v. Smith*, such an inquiry requires the examination of whether the relationship involves the exercise of some type of discretion or power, where this discretion or power can be exercised unilaterally so as to affect the individual's legal or practical interests and the individual is at the mercy of the fiduciary. Applying this test, it is argued that a commercial actor does exercise power over an individual, this power is unilateral and can affect the individual's legal or practical interests and finally, the individual is vulnerable in the face of the commercial entity's power. Subsequent Canadian case law, however, has stated that in order for there to be a fiduciary relationship, there must be, 'evidence of a mutual understanding that one party has relinquished its own self-interest and agreed to act solely on behalf of the other party', and that the three criteria mentioned above in *Frame v. Smith* were only a guide as to the existence of a fiduciary relationship and not an exact determination.¹²⁷⁹ In other words, in addition to one party being in a position of vulnerability in relation to the other, an expectation (on the part of the principal) that the fiduciary would act in the principal's best interests is also required. This essentially means that just because one party is in a vulnerable relationship with another party, does not automatically signal that the fiduciary notion is applicable. The law requires the expectation on the part of the principal that the fiduciary has his or her best interests at heart.

1279 La Forest J, in *Hodgkinson v. Simms* (1984), 117 D.L.R. (4th) 161, reported [1994] 3 S.C.R. 377, in Kerr, Ian R., *The Legal Relationship Between Online Service Providers and Users*, Canadian Business Law Journal, Vol. 35, 2001, at p. 452.

The Hedley Byrne case took the duty of care notion, originally associated with the fiduciary mechanism, and extended it to relationships outside of the fiduciary relationship, more specifically ‘special relationships’. While the notion of the fiduciary duty is not automatically applicable just because the individual is in a position of vulnerability due to the predictive modelling operations of a commercial actor, the scope of the duty of care, that has developed from the fiduciary duty, has been extended.

In as far as the relationship between commercial actor and individual can be characterised as of a fiduciary nature is highly debateable. There may be an agreement between commercial actor and individual, where the latter relinquishes self interest in favour of the former, which in turn agrees to act solely on behalf of that individual. It may even be able to be assumed from the facts of a certain circumstance. However, even if a fiduciary relationship does not exist, a duty of care can be argued to be applicable based on a ‘special relationship’. Much will depend on the manner in which the term ‘special relationship’ is interpreted. Schneier refers to the fiduciary duty and argues that it could be the foundation of a regime to which commercial actors, that hold large amounts of data, could apply to become a member of. In doing so, they would agree to certain legal restrictions and protections in relation to the held data and the people that the data concerns.¹²⁸⁰

The fiduciary duty is a common law system mechanism and therefore it is easier for the courts to adapt to modern day scenarios and extend its applicability as well as its principles, such as the duty of care, to prevailing social conditions. In this manner, it is possible to argue for and extend the fiduciary duty to the relationship between commercial actor and individual, in the form of the duty of care. Taking into account the power of companies, coupled with the fact that this power can be used to affect the individual’s interests, leaving him or her in a position of vulnerability, inspiration can be drawn from this mechanism, irrespective of which legal system is applied.

6.4.4 A Right of Access

A component of the empowerment strategy includes the creation of a right of access to an individual’s digital identity, referred to as a ‘right to know’ in

1280 Schneier, above n. 152, at pp. 204-205.

other contexts. This right would allow the individual to gain access to his or her digital identity in order to determine what factors formed the basis for a decision. The establishment of a right is a legal measure ensuring access to the digital identity, thereby facilitating empowerment. As argued hereunder, a legal basis for such a right, although not expressly stated, can be argued to have support in the case law of the ECtHR, where an individual's right to access information held by another party, can be claimed. This section examines the attempts to establish what can be considered a right of access to one's digital identity as well as the implications thereof.

6.4.4.1 A Right to Know

It has been suggested that one method of attaining insight into how technologies, such as predictive modelling, are being used to monitor, predict and influence behaviour, is by the creation of a right of access to the digital identity. Branscomb advances such a right, calling it 'the right to know', stating that this right can be complex and also can take on various forms. In other words, the enforcer of the right can be a different protagonist depending on the circumstances. For example, it could be a right for an individual to know his or her origins or it may be the right of the public to know the basis for decisions of a public nature.¹²⁸¹ This right to know has been interpreted to include the right to know about oneself and the right to know about one's environment, including the risks and opportunities one faces and the qualities of the goods and services one might acquire.¹²⁸² Considering that the digital identity contains information about the individual, for example his or her characteristics, personality attributes, mannerisms, habits etcetera, it is not inconceivable that the human being, whose data is used to produce digital identities, has a right to know what information they include and how they were arrived at. It is further submitted that, given the nature of the data making up the digital identity, it is not inconceivable that the basis for a right to know is arguable from within the human rights legal regime. What follows is an examination of an

1281 Branscomb, Anne Wells, *Property Rights in Information*, in *Information Technologies and Social Transformation*, Guile, Bruce R. (ed.), National Academy Press, 1985, at p. 86.

1282 Gandy, above n. 187, at p. 190.

attempt to create a right of access to one's digital identity that occurred in the US legislative process.

6.4.4.2 The s3418 United States Senate Bill

In the US, the right of access to one's profile was submitted in a Bill to Congress in the 1960's that in essence would have allowed an individual access to his or her digital identity. Parallels can be drawn even though it must be acknowledged that the level of technology during the 1960's can in no way be compared to present developments, including the types and magnitude of data that constitute the modern digital identity.

As the extent of information collection by companies during the late 1960's became public knowledge, together with the publicity that was attained by the Watergate scandal, the issue of privacy received more attention from the public sphere.¹²⁸³ In reaction, a number of Bills were introduced in the US Congress, in both the House and Senate.

One of the Bills introduced in the Senate was Bill s3418, dealing with the issue of privacy.¹²⁸⁴ The Bill was far-reaching in that it governed both manual and automatic files held by the Federal government, local government as well as private companies, proposing the following: the creation of an independent body, the Federal Privacy Board, that would be endowed with substantial powers, including the power to enter premises and compel the production of information (upon subpoena), the power to hold hearings as well as compel the cessation of certain practices, and giving individuals the right to view their files, make amendments to these files and also be notified when the information in these files had been forwarded to other entities. It also included its own code of fair information practices.¹²⁸⁵

At the same time in the House, another privacy Bill was being debated. This privacy Bill was not as substantial and far-reaching as Bill s3418, for example, only covering the operations of federal authorities. What is of interest are the deliberations that took place within Congress in connection with

1283 Regan, above n. 527, at p. 77.

1284 Ibid.

1285 United States Congress Senate committee on Government Operations, *Legislative History of the Privacy Act of 1974 S.3418*, available at http://www.loc.gov/rr/frd/Military_Law/pdf/LH_privacy_act-1974.pdf (last accessed on 2017-04-04), at p. 6.

these two Bills, reflecting the attitudes to privacy, both within government and also within the private sector. For example, both the public and private sectors were against the fact that one Bill covered both these sectors, that is, under the umbrella of one piece of legislation. In addition, the private sector argued that there was no evidence of any abuse having taken place from within the private sector as regards the processing of personal information in addition to the fact that the above measures would be excessively costly.¹²⁸⁶ One of the proposals within the House Bill was the establishment of an oversight body, which would have certain investigatory powers, but this proposal ultimately was rejected by the House.¹²⁸⁷ In the Senate there were suggestions for the introduction of an information ‘ombudsman’ and a ‘regulatory Commission’ with full powers to oversee the collection, use and dissemination of personal information’.¹²⁸⁸ Similar arguments against the creation of a board of oversight were expressed in discussions taking place in the Senate in connection with Bill s3418, where federal institutions claimed that they were able to monitor their own practices while private companies stated that the establishment of fair information practices alone would be sufficient to protect individual privacy.¹²⁸⁹ In contrast to the House, within the Senate, the creation of an oversight agency for federal agencies was agreed to, which would have had the power to monitor and inspect federal information systems, investigate and hold hearings on violations, develop guidelines and study both state and private information systems.¹²⁹⁰ As Regan notes, two themes emerged during the deliberations within both the House and Senate: first, that privacy was an individual concern and second, that the individual should be provided with legal remedies with which to protect his or her privacy.¹²⁹¹

On the 21st of November 1974, the Senate and the House passed their respective versions of the Privacy Act. The differences between the two related to the inclusion of the Privacy Protection Commission in the Senate version, as well as its tougher stance on the use of information and finally the extension

1286 Regan, above n. 527, at p. 78.

1287 Ibid, at p. 79.

1288 United States Congress Senate committee on Government Operations, above n. 1285, at p. 119.

1289 Regan, above n. 527, at p. 79.

1290 Ibid.

1291 Ibid, at p. 80.

of its applicability to certain law enforcement files. After a compromise agreement between these two versions of the Privacy Bill, the version that prevailed was most similar to the version that had passed the House. In other words, it covered only federal agencies and there was no reference to an independent agency to oversee information practices. The Privacy Act of 1974 signed into law on the 1st of January 1975 reflected this weaker stance on privacy in relation to information processing systems.¹²⁹² A report in connection to the drafting of the Senate Bill refers to a Professor Miller who stated that, ‘[i]n the past, dictatorships always have come with hobnailed boots and tanks and machineguns, but a dictatorship of dossiers, a dictatorship of data banks can be just as repressive just as chilling and just as debilitating on our constitutional protections’.¹²⁹³

The version of the Privacy Bill put before the Senate was more empowering than the Privacy Act that finally came into being. S3418 was described as an, “Information Bill of Rights” for citizens and a “Code of Fair Information Practices” for departments and agencies of the executive branch’.¹²⁹⁴ A unique aspect of s3418 was the creation of a ‘right of access and challenge’. This right presupposed an active citizen – active to the extent that he or she would oversee the government as far as the protection of his or her own privacy was concerned. S3418 encompassed a right for individuals, who were the subject of a government file, to have access to it and review its accuracy. This right was seen as extremely important and as a result, exceptions were to be rejected as far as possible, being allowed only in circumstances relating to national defence, foreign policy and law enforcement. This strong stance followed a recommendation from a report from the HEW Secretary’s Advisory Committee on Automated Personal Data Systems:

No exemption from or qualification of the right of data subjects to have full access to their records should be granted unless there is a clearly paramount and strongly justified societal interest in such exemption or qualification ...

1292 Campbell, Colton C. and Stack Jr., John F (eds.), *Congress and the Politics of Emerging Rights*, Rowman and Littlefield, 2001, at p. 50.

1293 Report accompanying s3418 submitted by Mr. Erwin from the Committee on Government Operations, available at <http://babel.hathitrust.org/cgi/pt?id=mdp.39015077945395;view=1up;seq=25> (last accessed on 2016-04-21), at p. 25.

1294 Ibid, at p. 23.

The instances in which it can be convincingly demonstrated that there is a paramount society interest in depriving an individual of access to data about himself would seem to be rare.¹²⁹⁵

The main ideas behind the right of access and challenge were to reinforce the principle of government accountability and to reinforce the public's sense of social justice, recognized in a report by the Project SEARCH group to the Department of Justice. The report stated that the above rights of access and challenge were important for the following reasons:

First an important cause of fear and distrust of computerized data systems has been the feelings of powerlessness they provoke in many citizens. The computer has come to symbolize the unresponsiveness and insensitivity of modern life. Whatever may be thought of these reactions, it is at least clear that genuine rights of access and challenge would do much to disarm this hostility. Second, such rights promise to be the most viable of all the possible methods to guarantee the accuracy of data systems. Unlike more complex internal mechanisms, they are triggered by the most powerful and consistent of motives, individual self-interest. Finally, it should now be plain that if any future system is to win public acceptance, it must offer persuasive evidence that it is quite seriously concerned with the rights and interests of those whose lives it will record. The committee can imagine no more effective evidence than authentic rights of access and challenge.¹²⁹⁶

While the technology of that time cannot be compared to predictive modelling, what still holds true is that for predictive modelling to gain public acceptance, companies will be required to persuade individuals that their rights and interests are being taken seriously.

1295 HEW Secretary's Advisory Committee on Automated Personal Data Systems at p. 61 in Report accompanying s3418 submitted by Mr. Erwin from the Committee on Government Operations, available at <http://babel.hathitrust.org/cgi/pt?id=mdp.39015077945395;view=1up;seq=25> (last accessed on 2016-04-21), at p. 38.

1296 Project SEARCH, Committee on Security and Privacy, Technical Report No. 2, July 1970, p. 28 in Report accompanying s3418 submitted by Mr. Erwin from the Committee on Government Operations, available at <http://babel.hathitrust.org/cgi/pt?id=mdp.39015077945395;view=1up;seq=25> (last accessed on 2016-04-21), at p. 39.

6.4.4.3 The Right to Know Act

The s3418 Bill has not been the only attempt to legislate an access right for individuals to their digital identities. A more modern attempt has been the introduction of a Bill in 2013 in the US State of California, according to which consumers would have the right to gain access to their personal profiles created by online data brokers.¹²⁹⁷ Eventually, and after pressure from computer companies in Silicon Valley, the Bill (AB 1291), which would have become the Right to Know Act, was put on hold. The aim of the Bill was to, ‘... make internet companies, upon request, share with Californians personal information they have collected—including buying habits, physical location and sexual orientation—and what they have passed on to third parties such as marketing companies, app makers and other companies that collect and sell data’. Section 2(b) of the Bill reads:

For free market forces to have a role in shaping the privacy practices of California businesses and for ‘opt-in’ and ‘opt-out’ remedies to be effective, Californians must be more than vaguely informed that a business might share personal information with third parties. Consumers must, for these reasons and pursuant to Section 1 of Article 1 of the California Constitution, be better informed about what kinds of personal information are purchased by businesses for direct marketing purposes. With these specifics, consumers can knowledgeably choose to opt-in or opt-out or choose among businesses that disclose information to third parties for direct marketing purposes on the basis of how protective the business is of consumers’ privacy.¹²⁹⁸

Here, the emphasis is not solely on the access to data held by the companies, but also on how this data has been treated, and more especially, whether it has been forwarded on to third party data brokers.

Bygrave, referring to cases in the US, indicates that even where such a Bill were to be passed and become law, it could still face challenges. He refers to

1297 Guynn, J and Lifschier, Mark, *Silicon Valley Uses Growing Clout to Kill a Digital Privacy Bill*, Los Angeles Times, 3 May 2013, available at <http://articles.latimes.com/print/2013/may/03/business/la-fi-digital-privacy-20130503> (last accessed on 2016-02-09).

1298 California Legislative Information, *AB-1291 Privacy: Right to Know Act of 2013: disclosure of a customer’s personal information*, available at http://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB1291 (last accessed on 2016-03-22).

cases where similar laws have been declared unconstitutional because they breach the US Constitution's First Amendment on free speech. He also cites the case of *Sorrell v. IMS Health, Inc*, where the right of marketers to use pharmacy records was seen in light of the First amendment, such that the State was not allowed to pass legislation encroaching on this right.¹²⁹⁹

6.4.4.4 Remarks

A legal component of the strategy of empowerment is the creation of a right of access for an individual to his or her digital identity as created or held by a commercial actor. Above, reference was made to two initiatives incorporating a so-called 'right to know', which would have provided individuals with access to the digital identity that is the basis for decisions taken about him or her.

In the case of s3418, technology was at its infancy and cannot be compared to the current state of technical complexity. Providing an individual access to his or her files would probably have been less problematic as he or she would more likely have been able to make sense of an assembled profile, something made more difficult in the context of predictive modelling. Such access to a digital identity would be almost meaningless today, if the 'black box' remains intact. However, there is a principled value in this right of access. It is in this regard that reference is made to the third role of the law put forward by Svantesson, namely the 'bark jurisdiction', where the role of creating such a right would clarify and cement a legal position and communicate the values of society. In addition, just because individuals cannot make sense of the profile now does not mean that this will always be the case. In this regard, Mayer-Schönberger and Cukier predict the rise of the profession of algorithmist, stating that, '[t]hey would evaluate the selection of data sources, the choice of analytical and predictive tools, including algorithms and models, and the interpretation of results. In the event of a dispute, they would have access to the algorithms, statistical approaches, and datasets that produces a given decision'.¹³⁰⁰

The effective implementation of a right to know with respect to an individual's digital profile, requires that its existence and scope be clearly expressed.

1299 Bygrave, *Data Privacy Law*, above n. 69, at p. 111.

1300 Mayer-Schönberger and Cukier, above n. 149, at p. 180.

Article 15 of the DPD illustrates this point, where, as argued above, the nature of that right was susceptible to alternative interpretations, and uncertainty as to its ambit watered down its usefulness.¹³⁰¹ Without once again entering into a material discussion of this point, what is significant from the point of view of creating any right, for example a right to know, is that the scope of the right must be unambiguous, with no space for confusion or discussion concerning the powers it bestows on the individual as well as the circumstances under which it becomes activated.

In addition, after examining human rights law and, more specifically, a number of cases from the ECtHR, it seems that there is some latitude with the claim that access to the digital identity should be considered a human right within the ambit of Article 8 ECHR:

Article 8 protects the individual's private life. At the core of that protection lies the right of every person to have the more intimate segments of his being excluded from public inquisitiveness and scrutiny. There are reserved zones in our person and in our spirit which the Convention requires should remain locked. It is illegitimate to probe for, store, classify or divulge data which refer to those innermost spheres of activity, orientation or conviction, sheltered behind the walls of confidentiality.¹³⁰²

This sentiment can also be seen in light of the diminishing distinction between so-called private and public life. There have been a number of judgements from the ECtHR where the activities of a professional or business nature are deemed to have fallen within the private sphere. Added to this is the applicability of human rights law on the commercial actor in lieu of the horizontal effect of human rights law.

A potential challenge is that a commercial actor could claim a 'trade secret' with regard to any attempts to gain access to the digital identities they hold. This stance is to a large degree supported by the GDPR in Recital 63, which can be interpreted as creating a type of right to access to the digital identity. However, after referring to this access right, the same Recital allows for an

1301 Article 15 of the DPD was discussed above due to its material relevance and applicability with regard to predictive modelling. Here, however, what is of more interest is not its material scope and ambit of applicability, but rather its effectiveness and applicability from a legislative technique point of view.

1302 *Rotaru v. Romania*, partly consenting opinion of Judge Bonello, para. 2.

exception to the extent that this right of access not interfere with the rights and freedoms of others, specifically mentioning trade secrets and intellectual property rights. Arguably, a large portion of the predictive modelling process could be deemed to fall under the trade secret notion, thereby nullifying the utility of this right of access. In addition, the problem tainting the GDPR generally remains the fact that a right of access pertains only to personal data concerning the data subject. This is not adequate, considering that in many circumstances, the data of ‘others’ is used to form an image of the individual and the big picture still remains outside the boundaries of this right of access.

6.4.5 Participation in the Legislative Process

Another component of the empowerment strategy takes the form of greater access to the legislative process. Different jurisdictions have different legislative processes as far as the promulgation of legislation is concerned. However, this does not prohibit the empowerment of individuals by providing them access to the legislative process. This element of empowerment is suggested with extreme caution, due to the adverse effects that populism can have on any society. It is therefore suggested that any access to the legislative process is limited and incorporated with checks and balances so as to prevent its utilization for the furthering of populist ideas. Nevertheless, as referred to above, an element of consumer protection empowerment entailed greater access to the policy making process. In this regard, legislating by means of crowd sourcing is relevant, where technology plays a role in empowering people by providing them with a greater say in the law making process.

6.4.5.1 Crowdsourcing Legislation

Crowdsourcing is the idea of achieving something by engaging people to contribute via the internet, the concept originating from the words ‘crowd’ and ‘outsource’.¹³⁰³ The term is associated with other instances of getting the as-

1303 Daily Crowdsourceme, *What is Crowdsourcing*, available at <http://dailycrowdsourcing.com/training/crowdsourcing/what-is-crowdsourcing> (last accessed on 2016-04-13).

sistance of the masses in order to achieve a goal. For example, ‘crowdfunding’, entails receiving small financial contributions from many people in order to finance a project and ‘crowdsourcing design’ entails the input of the masses in order to assist with a design task.¹³⁰⁴ A definition of crowdsourcing states that it is ‘the practice of obtaining needed services, ideas, or content by soliciting contributions from a large group of people and especially from the online community rather than from traditional employees or suppliers’.¹³⁰⁵ The idea of using technology platforms in order to engage the masses in the legislative process is in its infancy, yet there are potential benefits. One such benefit is increasing participation in the legislating process, thereby making an eventual law more representative, and empowering citizens by giving them a say. In Finland, crowdsourcing is being used for the purpose of eliciting contributions to the legislating process.

6.4.5.2 Crowdsourcing the Legislative Process

The Open Ministry Crowdsourcing Initiative is a European initiative established in Finland. It is an example of using technology, in order to initiate crowdsourcing methods, and increase participation in the legislation making process and ultimately increase democracy. Open Ministry is a non-profit organization founded in 2012 that has no political ties and that helps individuals make recommendations regarding legislative suggestions, in the face of a growing dissatisfaction with the traditional legislative process, dominated by lobby groups and the automatic passing by Parliament of legislation drawn up by civil-servants. In the Finnish context, once the threshold of 50 000 signatures of citizens of voting age is attained, a proposal in the form of a law or a general suggestion to be taken up by the legislator can be put forward. The effect is that the traditional legislator no longer holds the monopoly over the legislative process and the citizens set the law making agenda. The process therefore involves access to the Finnish Parliament and the traditional law making approach.¹³⁰⁶

1304 Ibid.

1305 Merriam-Webster Dictionary, ‘*Crowdsourcing*’ available at <http://www.merriam-webster.com/dictionary/crowdsourcing> (last accessed on 2016-04-13).

1306 The Open Ministry, available at <http://openministry.info/> (last accessed on 2016-04-13).

The initiative is not without criticism. For example, Parliament has been criticised for procrastinating about hearing the Open Ministry suggestions for legislation. Parliament has cited technological difficulties as the main reason for this. In addition, of the 266 published initiatives, only six applications thus far have made it through the Parliamentary Committees to the floor of the Parliament.¹³⁰⁷ The six issues that did make it to the floor of Parliament have concerned the following: tightening penalties for drunken driving, changes to the energy certification law, gender-neutral marriage, making Swedish instruction optional in schools, copyright reform and opposition to the closure of birth centres.¹³⁰⁸

Another legislative initiative via crowdsourcing occurred in Estonia in connection with a political scandal at the end of 2012. The political scandal surrounded the financing of political parties. It was anticipated that the Estonian Parliament was not the most appropriate institution to deal with this problem, and a crowdsourcing initiative was used to put forward appropriate legislation on the matter. The People's Assembly (Rahvakogu) was established as a result.¹³⁰⁹ The People's Assembly is an online forum, using the Your Priorities eDemocracy platform to bring active citizens together.¹³¹⁰ On this occasion, the Your Priorities web interface was changed slightly and the Estonian Identity card was linked to the system. Six thousand proposals were submitted with 18 being selected for submission to the Deliberation Day Assembly, where 320 elected Estonian citizens voted on the contributions, with 15 of these finally being submitted to the Estonian Parliament for a vote. Three of these were implemented and became law.¹³¹¹

Crowdsourcing has also caught on in the US states of California and New York. In the first instance, a Bill concerned a probate law, which allowed a

1307 News, *All six citizen's initiatives have failed – activists accuse Parliament of intentionally slowing the process*, available at http://yle.fi/uutiset/all_six_citizens_initiatives_have_failed_activists_accuse_parliament_of_intentionally_slowing_the_process/7525779 (last accessed on 2016-04-13).

1308 Ibid.

1309 Grimsson, Gunnar, Razgute, Giedre and Hinsberg, Hille, *Rahvakogu - How the people changed the laws of Estonia*, available at https://docs.google.com/document/d/1lhoyZfRsgftOkcSppu3L78_Uz_IugUkzMycN2xg3MPo/edit?pref=2&pli=1 (last accessed on 2016-04-14).

1310 Your Priorities, available at <https://yrpri.org/home/world> (last accessed on 2016-04-14).

1311 Grimsson, Razgute, and Hinsberg, above n. 1309.

court to designate a person to take care of a deceased person's pet. The initiative used the technological platform of Wikispaces and all people who had a connection to the internet were able to participate. The main purpose was to facilitate future efforts concerning more important types of legislation. Another initiative has been created in New York, where a number of Bills are open for comment and even editing using the technology GitHub. In addition, other states are showing an interest in legislative initiatives based on crowdsourcing.¹³¹² Also in the US, Representative Issa and Senator Wyden put forward the OPEN (Online Protection and ENforcement of Digital Trade) Act, with the ideas for this Act being crowdsourced via the platform, KeepTheWebOPEN.com. Six of the ideas incorporated into the final draft had originated from the crowdsourced initiative.¹³¹³

6.4.5.3 Other Societal Initiatives

An initiative not necessarily related to the legislative process but nevertheless representing the crowdsourcing potential of allowing citizens to influence their immediate surroundings, in relation to their elected officials, is Better Rejkjavik. It is an initiative in Iceland run by Citizens Foundation, a non-profit organization established in 2008 with the aim of using crowdsourcing to get ideas on how to improve society.¹³¹⁴ Citizens Foundation uses and maintains the Your Priorities eDemocracy platform, which is a web application that allows people to participate in public life by airing their opinions, mentioned above in the Estonian example. One of the projects concerned the city of Rejkjavik. A website was opened in 2010, just before municipal elections, with all the political parties given space to crowdsource ideas for their campaigns. Subsequently, considering the success of the initiative, the platform was maintained in order to receive input from citizens on how the city of Rejkjavik could be improved. As a result of the initiative, the Rejkjavik City Council

1312 Brian, Heaton, *Is Crowdsourcing the Future for Legislation?*, Government Technology, available at <http://www.govtech.com/internet/Experts-Predict-More-Legislation-Will-Be-Crowdsourced.html> (last accessed on 2016-04-14).

1313 DeMoss, *Dustin*, *Can Crowdsourced Government Happen in the U.S.?*, StackStreet, available at <https://stackstreet.com/can-crowdsourced-government-happen-u-s/> (last accessed on 2016-04-14).

1314 Citizens Foundation, available at <http://www.citizens.is/> (last accessed on 2016-04-14).

votes on ten to fifteen matters each month. Seventy thousand people (out of a population of 120 000) have participated in the project thus far, 3300 ideas have been submitted (including 5500 opinions for and against these ideas), 257 ideas have been formally reviewed and 165 accepted since 2011.¹³¹⁵

6.4.5.4 Remarks

Participation in the legislative process is empowering and participation can be facilitated by technology. In other instances where empowerment has been viewed as a desired measure, for example within consumer protection, an increased participation in the legislative process has been suggested. Most legislative processes are rather closed to the public. The process is dominated by politicians, all wishing to drive through the will of their political parties, as well as by lobby groups, all wanting to influence the process to the advantage of the groups they represent. However, using technology combined with the ideology of crowdsourcing in the legislation process can change this situation and in turn empower people.

There are both advantages and disadvantages with crowdsourcing the legislative process. Advantages include the creation of value through access to the expertise and knowledge of large distributed crowds and allow for, ‘inclusiveness, transparency, accountability, deliberation and civic empowerment in policymaking’.¹³¹⁶ However, a number of factors influence the creation of value, for example, large-scale participation, a diversity in participation and an automation of the process in order that all the input is taken into consideration.¹³¹⁷ In addition, there are a number of obstacles: first, leadership is required so as to prevent opportunistic incentives that amount to, ‘the coincidental alignment of forces’, second, there is as yet no real understanding of

1315 Citizens Foundation, available at <http://www.citizens.is/portfolio/better-reykjavik-connects-citizens-and-administration-all-year-round/> (last accessed on 2016-04-14).

1316 Aitamurto, Tanja and Chen, Kaiping, *The value of crowdsourcing in public policy-making: epistemic, democratic and economic value* in Ranchordás Sofia and Voermans, Wim (eds.), *Crowdsourcing Legislation: New Ways of Engaging the Public, The Theory and Practice of Legislation*, Special Issue Vol. 5, Issue 1, 2017, at p. 71.

1317 Ibid.

the role of public participation in democratic institutions and third, many of the initiatives taken thus far have been trivial in nature.¹³¹⁸

Being based on technology, crowdsourcing the legislative process makes participation easier, which can increase participation. This may be beneficial for democracy, as the legislative system is more open to input from the public or the citizen. In addition, it allows the formation of a general view of what is important to the citizen, as opposed to what is important to the politician. It also attracts the attention of the politicians, as a popular idea finding support with the masses is hard to ignore. Also, as seen in the Estonian example above, there are certain matters that are best left out of the hands of the political realm, where a conflict of interest could arise

As referred to above, the crowdsourcing of the legislative process is not without its pitfalls. Lobby groups could ‘highjack’ the legislative crowdsourcing initiative, which could result in a view that is skewed and not really representative of the people. Another danger is that an idea is not necessarily better for society just because it has popular support. There may be situations where an inherently bad idea, for example based on racial discrimination, receives popular support out of a frustration of the people of a country or as a vote of no confidence in the establishment. Finally, considering that the phenomenon of legislating by means of crowdsourcing is in its infancy, there is little known about the relationship democratic legitimacy and online participation.¹³¹⁹ Therefore, while using crowdsourcing in the legislative process is empowering, it must be implemented cautiously, with certain checks and balances in place to prevent an unintended result.

1318 Fung, Archon, *Putting the Public Back into Governance: The Challenges of Citizen Participation and Its Future*, *Public Administration Review*, Vol. 75, Issue 4, 2015, at pp. 520-521.

1319 Ranchordás, Sofia, *Digital agoras: democratic legitimacy, online participation and the case of Uber-petitions*, in Ranchordás Sofia and Voermans, Wim (eds.), *Crowdsourcing Legislation: New Ways of Engaging the Public*, *The Theory and Practice of Legislation*, Special Issue Vol. 5, Issue 1, 2017, at p. 54. For further reading on the issue of crowdsourcing, see Pečarič, Mirko, *Can a group of people be smarter than experts?* and Souza, Carlos Affonso, Steibel, Fabro and Lemos, Ronaldo, *Notes on the creation and impacts of Brazil’s Internet Bill of Rights*, in Ranchordás Sofia and Voermans, Wim (eds.), *Crowdsourcing Legislation: New Ways of Engaging the Public*, *The Theory and Practice of Legislation*, Special Issue Vol. 5, Issue 1, 2017, at p. 5.

6.4.6 An Independent Supervisory Authority

Empowerment also entails the establishment of an institution overseeing the use of predictive modelling by industry, which is necessary considering the hidden nature of predictive modelling and its effects. While the data protection framework has been built around the existence of the notion of the Data Protection Authority, an authority with insight into data processing practices, it is argued that the existence of an independent institution is important also from a human rights perspective. This line of thought provides the impetus for this component of empowerment.

6.4.6.1 The European Court of Human Rights Case Law

The notion that there is an organization or body that oversees a potentially harmful procedure as far as an individual is concerned, has been lifted by the ECtHR in the context of human rights case law. The ECtHR has concluded that reconciling Article 8 ECHR with the use of personal information by government authorities requires that Article 8, ‘should be interpreted in an open-minded manner, with an eye for the actual circumstances and requirements of the society’.¹³²⁰ The cases that have come before the ECtHR essentially concern the balancing of two rights, namely, the right of the authorities to resort to surveillance measures on the one hand and on the other hand, the rights of the individuals concerned and who are affected by these surveillance measures. De Hert and Gutwirth in their analysis of case law arising from the ECtHR state that, ‘... the ECtHR has insisted on the need for an independent supervisory authority as a mechanism for the protection of the rule of law and to prevent the abuse of power, especially in regard to secret surveillance systems’.¹³²¹ In other words, in a democratic society characterised by the notion of the rule of law, a necessary requirement is the existence of an independent authority that monitors a certain activity in order to ensure that the boundaries put in place by the law are not over-stepped. In other words, it is a counter-measure in the face of excessive power and hence a form of empowerment.

1320 Brouwer, above n. 833, at p. 172.

1321 Gutwirth and De Hert, above n. 896, at p. 19.

The case of *Klass v. Germany*, while relating to surveillance in the context of the state versus individual relationship, is of relevance to the commercial setting. The Court stated that, where there are proceedings to which the individual cannot take part or in any way review, due to the lack of knowledge of their existence, it is essential that his or her rights are upheld in order for there to be compliance with Article 8 of the ECHR.¹³²² The Court referred to judicial control as the best alternative in the circumstances.¹³²³ In the above matter, there was a form of oversight, however, this was carried out by an ‘official qualified for judicial office’. The Court also further highlighted that where the potential harms are so serious, control could not be given to any other person than a judge.¹³²⁴ Here the notion is lifted of a particular proceeding possibly having such severe consequences that only a person of certain stature and qualification is deemed adequate to oversee the administration of justice. The importance of an independent authority lay in the fact that the individual would most probably have no knowledge of the surveillance being performed and therefore not be able to have any recourse of a retroactive nature.¹³²⁵

In the case of *Leander v. Sweden*, the ECtHR took particular note of all the institutions that were in place in Sweden, to look after the individual’s interests, namely Parliamentarians on the National Police Board, The Parliamentary Committee on Justice, the Chancellor of Justice and the Parliamentary Ombudsman. The existence of these bodies and their powers of oversight had the effect that a breach of Article 8(2) ECHR did not occur.¹³²⁶ The case of *Rotaru v. Romania* echoed the above reasoning, once again referring to the fact that there must be sufficient safeguards in place in order that the surveillance that was used to protect society in fact does not destroy democracy. The Court referred to the fact that in situations, such as those characterized by the above case, it is the judiciary that affords the best guarantees due to their independence and impartiality.¹³²⁷ In *Gaskin v. the United Kingdom*, the Court stated that the existence of rules relating to the confidentiality of contributors to files was not in contravention of Article 8 ECHR and the right to private

1322 *Klass v. Germany*, para. 55.

1323 *Ibid.*

1324 *Ibid*, para. 56.

1325 *Ibid*, para. 57.

1326 *Leander v. Sweden*, paras. 65-67.

1327 *Rotaru v. Romania*, paras. 59-60.

and family life. However, the Court did deem unacceptable and a breach of Article 8 ECHR the fact that there was no system to allow the individual access to these files when the contributor was no longer available or where the contributor improperly refused to consent to the information being given out. The Court added that such a system was proportional only when there existed an independent authority to determine whether access to files should be granted.¹³²⁸ This case is of interest in that it does not revolve around the issue of whether it is appropriate for a public authority to collect, store and disseminate information concerning an individual, but rather concerns whether an individual has the right to access certain information about himself, taking into account the interests of the community or other persons.

In *Odièvre v. France*, the dissenting opinion referred to an independent authority being required where there is a situation of competing interests, in other words to strike a fair balance. In this regard, the Court referred to *Gaskin* as well as *M.G. v. the United Kingdom*, where the applicant wished to gain access to social service records held by the local authority. In *Odièvre*, the Court stated:

If the system of anonymous births is to be retained, an independent authority of that type ... whether or not to grant access to the information; such access may in appropriate cases be made conditional, or subject to compliance with a set procedure ... in the absence of any machinery enabling the applicant's right to find out her origins to be balanced against competing rights and interests, blind preference was inevitably given to the sole interests of the mother. The applicant's request for information was totally and definitively refused, without any balancing of the competing interests or prospect of a remedy.¹³²⁹

Once again, the Court referred to an independent authority to balance the interests involved in the application of Article 8 of ECHR. Brouwer identifies two grounds, elaborated by the ECtHR, for the need of an independent authority of supervision in circumstances where personal information is used by public authorities. First, is the issue of the rule of law and the need for control measures to be in place, especially taking into account that the affected individual will most probably not have any say in the surveillance procedure. Here, the effect of the surveillance measures on democracy is central. Second,

1328 *Gaskin v. the United Kingdom*, para. 49.

1329 *Odièvre v. France*, para. 18.

the existence of an independent supervisory authority is necessary in order to balance various interests at stake, as amplified by the *Gaskin* case.¹³³⁰ The role of the independent supervisory authority, therefore, is to uphold the rule of law and democracy in situations where surveillance technology threatens to transgress the border of acceptability as well as to balance interests between interested parties, taking into account notions such as proportionality.

In *Gaskin* and *Leander*, it is noteworthy that the Court did not require the independent supervisory authority to be a judicial one. This differed from *Klass* and *Rotaru*, where it was stated that the highest level of protection would be from the judiciary, in other words, a judge.

6.4.6.2 Remarks

The notion behind an independent authority is that in circumstances when a balancing of interests is required, there will be a party that will potentially be in a position to objectively determine where the border of acceptability lies as far as the effects of a certain technology are concerned. This may have a reassuring effect but also be pivotal in respect to the degree to which the use of a technology is to be considered legal, as demonstrated by the ECtHR.

Such a supervisory authority could have additional functions. For example, algorithms used to make important decisions could require certification with the supervisory authority.¹³³¹ This would allow professionals who have a deep understanding of how machine learning works, to provide insight into whether the technology is benign or whether its objective is harmful to such an extent that its use should be regulated. The establishment of an independent body to oversee the process of predictive modelling should not necessarily be viewed as purely negative from the point of view of companies. Providing individuals with an instrument, in the form of an oversight body, may encourage them to part with their data. Also, companies, would potentially be able to use the large repositories of data at their disposal without fear of tarnishing their commercial renommé. Finally, a certification process would result in a distinction between those companies who have a good intent from those who do not necessarily take the interests of the individual to heart in making business decisions.

1330 Brouwer, above n. 833, at p. 175.

1331 Mayer-Schönberger and Cukier, above n. 149, at p. 176.

6.4.7 Collective Redress

Collective redress is similar to the institution of the class action, which has come to the fore predominantly in the US. Termed collective redress in the EU context, it is a suggested empowerment component. It has found support within consumer protection law and as will be highlighted, it has previously received attention within the data protection framework. This section examines the notion of collective redress, its development within the EU context and its importance as an instrument implementing empowerment.

6.4.7.1 Development

Collective redress has its origins in the notion of the class action, established within the US legal system. The class action has advantages and disadvantages depending on which party's perspective is taken. For example, from the perspective of the individual, it allows for bringing an action in circumstances where that individual otherwise would not have had redress for the harm caused. On the other hand, from the perspective of a commercial actor, a disadvantage is the potential of having to defend an increased number of drawn-out law suits. It is within this context that the arguments of advocates for and opponents against collective redress should be perceived.

The class action is a means to hold companies accountable for their actions that are potentially harmful to individuals. It allows claims to be brought even in cases where the damage caused to each individual is not extremely high in monetary terms. In many cases, the damages that could potentially be awarded are too small to warrant a lengthy court action, and the costs involved do not justify a judicial procedure. In this regard, it is noteworthy that while the financial damage for each individual is low, the profits for the commercial actor of certain actions may be high.¹³³² For example, the Federal Trade Commission has estimated that in one year there were approximately 25 million cases of fraud against individuals, the median claim was \$220 per person, but the

1332 Alexander, Janet C., *An Introduction to Class Action Procedure*, available at <https://www.law.duke.edu/grouplit/papers/classactionalexander.pdf> (last accessed on 2016-04-15), at p. 1.

total amounted to millions of dollars.¹³³³ Another advantage is that without a class action, the prospect of a small claim may not be able to attract legal representation. Here, the class action serves as a market-orientated solution, where the state may not have instituted sufficient protections and where lawyers, that specialize in class action cases use this tool as an entrepreneurial incentive.¹³³⁴ A class action also allows for combining resources, making the legal system more accessible to those who lack the necessary resources to file a suit.¹³³⁵ Class action suits are also a means of determining whether wrongful conduct has actually taken place.¹³³⁶ In this manner, it is a way of attaining information and knowledge, in that an individual is made aware that a harm has allegedly been committed, of which he or she has been a victim. The class action is also argued to be an effective method for complementing other initiatives that are aimed at protecting individuals, for example, those initiated by Government.¹³³⁷ The class action performs a preventative function, as commercial actors fear the idea of becoming embroiled in a class action.¹³³⁸ In other words, the notion of the class action is synonymous with a costly and drawn out process, which is risky from the commercial actor perspective. Potentially being a lengthy process can also work to the individual's advantage, if a case is repeatedly brought up in the media, thereby damaging the reputation of a commercial actor and encouraging good commercial conduct.¹³³⁹

The class action also has disadvantages. One such disadvantage is the potential for conflicts of interest. For example, no single person within the class may have a large enough justification to bring the law suit in their own right. Also, the lawyers leading the class action can have different preferences than

1333 PublicCitizen, *Class Actions Empower Consumers, Help Them to Hold Wrongdoers Accountable*, available at <https://www.citizen.org/documents/Concepcion-and-consumers10282010.pdf> (last accessed on 2016-04-15).

1334 Alexander, above n. 1332, at p.2.

1335 Ibid.

1336 PublicCitizen, above n. 1333. It can be argued that this is the goal in almost all regular legal cases.

1337 Ibid.

1338 PublicCitizen, above n. 1333.

1339 Hawthorn, Nigel, *10 things you need to know about the new EU data protection regulation*, ComputerworldUK, available at <http://www.computerworlduk.com/security/10-things-you-need-know-about-new-eu-data-protection-regulation-3610851/> (last accessed on 2016-04-15).

the individuals in going to trial. This could lead to a conflict of interests where it is in the interests of the lawyer that a long trial be held, while a settlement before the trial begins is potentially more beneficial to the individuals concerned. The opposite might also be true, where a lawyer prefers to settle pre-trial in situations where this is not in the interests of the individuals in the class action. Second, there is the risk that class actions are brought where there is no real ground for the action. Also, in the US, the class action can be brought in almost every state simultaneously, with the consequence that the defendant must defend the action in multiple jurisdictions. In addition, the existence of the class action as a legal mechanism can affect the substantive law, which may be altered to facilitate the bringing of class actions.¹³⁴⁰ Therefore, while there are many advantages to the class action, it is open to criticism for being driven by economic and profit considerations, thereby leading to frivolous claims that need to be addressed by companies, possibly in multiple legal jurisdictions. In the US, the Supreme Court has started to limit the class action due to the potential for abuse from an economic as well as legal stand point.¹³⁴¹

6.4.7.2 The European Union

The class action has been suggested as a mechanism for placing individuals in a stronger position, in certain areas of law, as far as the European legal framework is concerned. The idea of the class action, has found support, under the banner ‘collective redress’, albeit in a different form compared to the class action of the US. The notion of collective redress has been available in the European context for some time, especially in consumer law and competition law, with the Commission producing a Green Paper on anti-trusts damages action in 2005 and a White Paper in 2008.¹³⁴²

1340 Alexander, above n. 1332, at p. 21.

1341 European Commission, Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Towards a European Horizontal Framework for Collective Redress*, above n. 1210, at p.8.

1342 European Commission, Commission Staff Working Document Public Consultation, *Towards a Coherent European Approach to Collective Redress*, Brussels, 4 February 2011 SEC (2011)173 final, available at http://ec.europa.eu/justice/news/consulting_public/0054/ConsultationpaperCollectiveredress4February2011.pdf (last accessed on 2016-04-19), at p. 5.

As far as data protection is concerned, in December 2009 the notion of the class action was raised by the Article 29 Data Protection Working Party. In a document setting forth the results from an inquiry into the state of data protection rules in the face of new technologies, the notion of the class action was put forward as a mechanism for providing the individual with control.¹³⁴³ In 2011 the Commission investigated the notion of collective redress, examining what the common principles were and how these related to the European legal system. The document entitled *Towards a Coherent European Approach to Collective Redress* states:

EU citizens and businesses should be able to take action when harmed by a breach of any EU legislation creating substantive rights. When citizens and businesses are victims of the same breach committed by the same company, bundling of their claims in a single collective redress procedure, or allowing such a claim to be brought by a representative entity or body acting in the public interest, could simplify the process and reduce costs. ‘Collective redress’ is a broad concept encompassing any mechanism that may accomplish the cessation or prevention of unlawful business practices which affect a multitude of claimants or the compensation for the harm caused by such practices.¹³⁴⁴

Two main forms of collective redress are referred to: injunctive relief, where claimants seek to stop the continuation of illegal behaviour and compensatory relief, where damages for the harm caused are sought. The forms of collective redress include, ‘out-of-court mechanisms for dispute resolution or the entrustment of public or other representative entities with the enforcement of collective claims’.¹³⁴⁵

Collective redress therefore allows for the pursuit of multiple claims in one single action, in order to reduce costs and increase the ease with which an action can be brought by individuals. The above citation also refers to the breadth of the notion, so as to include different procedural mechanisms and options for claiming relief. The Commission also showed an awareness of the

1343 Article 29 Data Protection Working Party, *The Future of Privacy*, Adopted on 1 December 2009, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf (last accessed on 2016-04-06), at p. 16.

1344 European Commission, *Towards a Coherent European Approach to Collective Redress*, above n. 1342, at p. 3.

1345 Ibid.

problems with the US-style class action, characterised by large economic incentives, the availability of punitive damages, the fact that almost anyone had standing to bring a class action, the availability of contingency fees as well as the rules regarding the discovery of evidence.¹³⁴⁶

In response to the above Commission investigation, the European Parliament adopted a Resolution on collective redress.¹³⁴⁷ The Parliament was receptive to the notion of collective address, especially in a form that avoided the potential abuses associated with the US-style class action and highlighted the need for harmonization as many Member States had differing systems in place as far as collective redress was concerned. On the 11th of June 2013, the European Commission published a Recommendation that Member States allow for collective redress by consumers.¹³⁴⁸ Collective redress here is described as a procedural mechanism, which allows, for reasons of procedural economy and/or efficiency of enforcement, many single claims (relating to the same case) to be bundled into a single court action.¹³⁴⁹ The Recommendation's main aim was to ensure horizontal application of the notion of collective redress without the need for harmonizing Member States' systems, and included a set of common but non-binding principles in order that individuals (and companies) be able to enforce their rights in the area of consumer protection, competition law, environmental protection and financial services.¹³⁵⁰ In other words, at the national level there should be collective redress systems in the above areas. It was also stated that there should be collective redress procedural measures in place to prevent abuse of the system.¹³⁵¹ Explaining the reasons for turning to collective redress, the EU's Justice Minister Reding stated

1346 Ibid, at p. 9.

1347 Ibid.

1348 European Commission, *Towards a European Horizontal Framework for Collective Redress*, above n. 1210.

1349 European Commission, *Commission recommends Member States to have collective redress mechanisms in place to ensure effective access to justice*, Press Release, 11 June 2013, available at http://europa.eu/rapid/press-release_IP-13-524_en.htm (last accessed on 2016-04-15), at p. 3.

1350 European Commission, *Daily News*, 11th June 2013, available at http://europa.eu/rapid/press-release_MEX-13-0611_en.htm (last accessed on 2016-04-15).

1351 European Commission, *Towards a European Horizontal Framework for Collective Redress*, above n. 1210, at p. 1.

that, '[t]his Recommendation is a balanced approach to improve access to justice for citizens while avoiding a US-style system of class actions and the risk of frivolous claims and abusive litigation'.¹³⁵² One of the reasons for the Communication from the Commission was that whereas collective redress had been established in the domain of consumer law, there were differences regarding the national laws in the areas of competition law, financial markets, environmental protection and other areas of law.¹³⁵³ Vice President Almunia, referring to the context of competition law, stated:

When they are victims of infringements of competition rules, citizens and businesses – particularly SMEs – often face strong obstacles in obtaining effective compensation. To overcome these difficulties, we have proposed a Directive on antitrust damages actions. Since the harm may be shared by many injured parties, collective actions mechanisms should also be in place. This Recommendation is therefore a useful complement, sending a clear message to Member States.¹³⁵⁴

The word 'complement' highlights an important advantage with the collective redress system, in that it operates as a complement where law is not adequate in regulating certain activities. This problem was highlighted in the Commission consultation, *Towards a Coherent European Approach to Collective Redress*, where a problem highlighted was the growing territory of the EU and the accompanying problem that this required a more decentralized application of the law, for example, by means of private enforcement by individuals in addition to public enforcement of the law.¹³⁵⁵

1352 European Commission, *Commission recommends Member States to have collective redress mechanisms in place to ensure effective access to justice*, above n. 1349.

1353 European Commission, *Commission recommends Member States to have collective redress mechanisms in place to ensure effective access to justice*, *Ibid*, at p. 3.

1354 European Commission, *Commission recommends Member States to have collective redress mechanisms in place to ensure effective access to justice*, *Ibid*.

1355 European Commission, *Towards a Coherent European Approach to Collective Redress*, above n. 1342, at p. 2.

6.4.7.3 The Principles of Collective Redress

The Commission Recommendation referred to above set out a number of principles that the Member States should adhere to: Member States should have a system for collective redress in order to attain injunctive relief as well as the ability to claim damages, where a large number of individuals are harmed by the same practice; the collective redress system should be fair, equitable, timely and not expensive; any collective redress system should be based on an ‘opt-in’ principle; procedural safeguards to prevent abuse of the collective redress system should be included (for example by allowing a system of contingency fees, demanding that the organization representing the individuals is a non-profit organization and prohibiting punitive damages); the claim should be presided over by a judge and a system of alternative dispute resolution should be offered to the parties.¹³⁵⁶

An aspect that the Commission highlighted was the relationship between public enforcement and collective redress, which is a form of private enforcement, as these two recourses have different objectives. The main objective of public enforcement is to apply EU law, punish those who breach the law and see to it that the law remains a preventive instrument, that prevents people from breaking the law. The objective of private enforcement, on the other hand, is to provide people with access to justice and damages.¹³⁵⁷ Another point that was brought by the Commission was that of legal standing, namely, that collective redress actions should be brought by a representative entity on behalf of the individuals concerned, and that they should have the best interests of the group at heart. The representative entity could be a public authority or have stringent rules for qualification as a representative body, or a judge.¹³⁵⁸ Finally, whereas in the US the rule is that all class actions are ‘opt-out’, the Commission recommended an ‘opt-in’ system, where individuals were by de-

1356 European Commission, *Commission recommends Member States to have collective redress mechanisms in place to ensure effective access to justice*, above n. 1349, at p. 2.

1357 European Commission, *Towards a European Horizontal Framework for Collective Redress*, above n. 1210, at p. 10.

1358 Ibid.

fault not part of the collective redress action and must make a conscious decision and elect to become part of one. The Commission preferred an opt-in system because it better preserved autonomy.¹³⁵⁹

In Germany, the Ministry for Justice and Consumer Protection approved a draft law strengthening the position of consumers, in relation to data protection, by allowing for the class action in the areas of ‘advertising and market and opinion research, the creation of personality or usage profiles, address or data bank brokering and similar commercial uses’.¹³⁶⁰ Associated with this class action option was the provision of powers to associations to bring an action on behalf of the individuals that they represent (in this case the consumer). The notion of the class action law suit has also found favour in the United Kingdom. In 2015 the English High Court in London approved a Group Litigation Order (GLO) by the employees of a supermarket chain, for data breach, where a former employee stole and published the salary and other details of 100 000 of the supermarket’s employees.¹³⁶¹ In France too, the class action notion is gaining momentum. On the 26th of January 2016, the French National Assembly adopted the ‘Digital Republic’ Bill, which has as its aim the regulation of the digital sphere in French society. The Bill allows for a class action, empowering certain consumer organizations to bring a class action relating to data protection, including associations that protect privacy and personal data, consumer protection associations, trade unions where the processing of data affects employees and finally, any association that has been formed with the intention of pursuing class actions.¹³⁶²

The notion of collective redress has also found favour in the GDPR, where Article 80 allows for the bringing of a collective redress action, where a data subject can appoint a non-profit body, organization or association to exercise

1359 Ibid, at p. 11.

1360 Kuschewsky, Monika, *Germany Wants to Introduce Class Actions for Privacy Violations*, Inside Privacy, available at <https://www.insideprivacy.com/international/ger-many-wants-to-introduce-class-actions-for-privacy-violations/> (last accessed on 2016-04-16).

1361 Ball, Jonathan, Navetta, David, and Kleiner, Kris, *British supermarket chain faces group litigation action in the UK based on data breach*, available at <http://www.dataprotectionreport.com/2016/03/british-supermarket-chain-faces-group-litigation-action-in-the-uk-based-on-data-breach/> (last accessed on 2016-14-15).

1362 Nadege, Martin and Coulouvrat, Geoffroy, *French National Assembly adopts ‘Digital Republic’ bill*, Norton Rose Fulbright, Data Protection Report, available at <http://www.dataprotectionreport.com> (last accessed on 2016-04-15).

his or her rights referred to in Articles 77, 78 and 79 as well as the right to compensation provided for in Article 82 (Article 80(1)). Article 80(2) also caters to circumstances where one of the organizations mentioned in Article 80(1) can lodge a complaint with a supervisory body independently of a data subject's mandate, where the data subject's rights, protected under the GDPR have been infringed.

6.4.7.4 In the Context of Consent

The notion of acting as a collective is beneficial to the individual in relation to the notion of consent. Sweden was the first country to introduce national data protection legislation in the form of the Data Act of 1973, which opted for the licensing model, where companies that held mainframe computers with large databases were required to apply to the Data Inspection Board for permission to process data. As personal computers became more popular and affordable, it was realized that a new legislative regime was required for all of Europe. This resulted in the creation of the DPD, which was implemented in Sweden by means of the Personal Data Act of 1998 (1998:204).¹³⁶³ The DPD and consequently the Personal Data Act went from a system of licensing, where the data subject had no say in the matter and which has been described as paternalistic in nature, to a situation where the data subject had full autonomy to decide whether his or her personal data could be processed. This autonomy was enshrined in the notion of consent, which was, '... based on the opinions of enlightened data subjects, who partly receive information from the controller, and partly collect information on the basis of their statutory access rights'.¹³⁶⁴ In other words, the power to consent was transferred from the Data Inspection Board (which consented on behalf of the subject) to the individual, and was based on personal autonomy and freedom to enter into agreements. One identified problem with this type of construction is defined as 'autonomy fatigue', where multiple requests for consent from the individual, especially

1363 Öman, Sören, *Implementing Data Protection in Law*, in Wahlgren, Peter (ed.), *IT Law, Scandinavian Studies in Law*, Volume 47, Stockholm Institute for Scandinavian Law, 2004, at p. 390.

1364 Wiese Schartum, Dag, *Data Protection: Between Paternalism and Autonomy* in *Festschrift till Peter Seipel*, Norstedts Juridik, 2006, at p. 559.

in trivial circumstances, eventually leads to a situation where it becomes difficult to exert control.¹³⁶⁵ It is within this context that the notion of overexposure to something has the opposite effect than that which was initially intended. For example, the notion of consent has as its aim the empowerment of the individual as data subject. However, overexposure by being required to provide this consent in multiple instances, especially of a trivial nature, can lead to disempowerment.

It is in this scenario that the notion of ‘collective consent’ has been suggested, where an individual enters into a collective arrangement where his or her consent is given to another institution or organization to use on his or her behalf. Here two types of arrangements are envisaged: first, that of ‘broad individual consent’, an example being where the consent is given to an NGO to use certain types of data for certain purposes and second, ‘consent by authorization’, where an organization, such as a bank, is given authority to process data where such processing is in the individual’s best interests. In these cases, a certain amount of personal autonomy is retained since the individual has the ability to withdraw consent at any given time.¹³⁶⁶

6.4.7.5 Remarks

Collective redress can be a powerful tool for individuals, especially considering that it is generally disliked by companies.¹³⁶⁷ This indicates its effectiveness, both as a preventive measure but also as an instrument in correcting the harms caused by irresponsible behaviour. For example, an Israeli judge approved a collective redress action in the amount of 400 million dollars in an Israeli court against Facebook. The court ruled that a clause in Facebook’s terms and conditions, stating that all disputes be heard in California, was invalid. The Applicant argued that Facebook’s use of its users’ content, without their consent, to determine what advertisements they be shown, invaded privacy. The judge did admit that usually the court stipulated in the terms and conditions, takes precedence, but continued by stating that, ‘[p]erhaps the time has come to examine the issue from a different angle, from the customer’s

1365 Ibid, at p. 560.

1366 Ibid, at p. 562.

1367 European Commission, *Towards a European Horizontal Framework for Collective Redress*, above n. 1210, at p. 7.

standpoint, especially when he's the customer of huge international companies that deal with customers all over the world'.¹³⁶⁸

6.4.8 Soft Law

Soft law is the eighth component of empowerment. It arguably derives its applicability and popularity from its specific nature of enshrining general principles rather than stipulating enforceable rules. This is especially relevant in situations where a large schism may exist between parties and more informal mechanisms are required in order to cultivate trust and bridge differences. It is in this role that soft law can be more effective than traditional law. Due to its nature, soft law is an important component of empowerment. This section examines a soft law initiative that is relevant to empowerment. The initiative examined is the Guiding Principles on Business and Human Rights ('Guidelines') developed by Ruggie, and endorsed in 2006 by the UN Human Rights Council.¹³⁶⁹ This illustration is especially relevant for two reasons. First, it was a solution to a problem that bears many similarities to the issue at hand and as a result can be regarded as a blueprint for inspiration and second, an analysis of the Guidelines provides insight into how implementation could occur on an operational level, for example, within the confines of companies.

6.4.8.1 Background

The human rights legal regime for the most part consists of treaties that are adopted and ratified by states. This is done on a voluntary basis, and despite the existence of committees to oversee the adherence to these treaties, they may not be enforced as their pronouncements are not considered a source of

1368 Oded, Yaron, *Israeli Judge Approves \$400 Million Class Action Against Facebook for Violating Privacy*, available at <http://www.haaretz.com/israel-news/business/1.725512> (last accessed on 2016-06-16).

1369 United Nations Human Rights Office of the High Commissioner, *Guiding Principles on Business and Human Rights*, available at http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf (last accessed on 2016-09-21).

law. The situation becomes more complicated where multi-national companies are suspected of human rights law breaches. International human rights law as such places no duties on companies, who are only required to follow the laws in their host state or in the state that they originate from. An effect of this is that human rights law is applied differently depending on which country a commercial actor is operating in. The human rights situation prior to his initiative is best described by Ruggie himself:

... a deeply divided arena of discourse and contestation lacking shared knowledge, clear standards and boundaries; fragmentary and often weak governance systems concerning business and human rights in states and companies alike; civil society raising awareness through campaigning against companies, and sometimes also collaborating against companies, and sometimes also collaborating with the most willing among them to improve their social performance; and occasional law suits against companies brought mainly through the innovative use of legal provisions that were originally intended for different purposes.¹³⁷⁰

The human rights situation was characterised by a division between the multinational companies on the one hand, who preferred self-regulation in the form of corporate social responsibility measures, and human rights activists on the other, that insisted on the protection of human rights taking the form of a treaty, that is enshrined in the form of traditional hard law. The voluntary path in the form of corporate social responsibility had been criticised by human rights activists for allowing a commercial actor to improve its image without altering its behaviour. A formal treaty, on the other hand, was also not considered effective, due to the length of time it would take to enact and because, ‘the foundations were lacking, the issues too complex, and states too conflicted ...’¹³⁷¹

The situation was therefore characterised by the conflict between a mandatory approach on the one hand and a voluntary one on the other. Ruggie’s idea was the creation of an instrument that would combine the public governance system (traditional law) with the private one (corporate social responsibility), and using a method of ‘polycentric governance’, create:

1370 Ruggie, John, *Just Business: Multinational Corporations and Human Rights*, W. W. Norton and Company Ltd., 2013, at p. xxxiv.

1371 Ibid, at pp. 67-68.

a new regulatory dynamic and under which public and private governance systems – corporate as well as civil – each come to add distinct value, compensate for one another’s weaknesses, and play mutually reinforcing roles – out of which a more comprehensive and effective global regime might evolve, including specific legal measures.¹³⁷²

The aim of Ruggie, in other words, was the creation of a ‘politically authoritative, not a legally binding instrument’.¹³⁷³ Consequently, the solution was a soft law one in the form of the Guidelines.

6.4.8.2 The Solution

The solution to the above challenge, according to Ruggie, was the use of soft law in the form of the Guidelines, which according to him had the following attributes:

It does not by itself create legally binding obligations. It derives its normative force through recognition of social expectations by states and other key actors. States may turn to soft law for several reasons: to chart possible future directions for, and fill gaps in, the international legal order when they are not yet able or willing to take firmer measures; where they conclude that legally binding mechanisms are not the best tool to address a particular issue; or to avoid having more binding measures gain political momentum.¹³⁷⁴

It is here that the advantages of soft law come to the fore, namely, as a solution that entails fewer risks compared to committing to a legally binding instrument, and an instrument that is useful for laying out the principles and norms that are expected to be followed. The Guidelines are described by Ruggie himself as combining both traditional law (the responsibility of states to enact laws and provide remedies) and soft law elements (corporate binding rules) that establish a normative platform for the protection of human rights, incorporating companies in the human rights protection regime.¹³⁷⁵

1372 Ibid, at p. 78.

1373 Ibid, at p. xlvi.

1374 Ibid, at pp. 45-46.

1375 Ibid, at pp. 124-125.

6.4.8.3 The Scope of the Guidelines

The Guidelines highlight a state's duty to protect against human rights abuse within their territory, preventing and punishing any abuses, mainly by making certain that there are laws in place that prevent such abuse. This includes a duty on states to provide best practices advice and even advise on how to perform a human rights due diligence check.¹³⁷⁶ In addition, the Guidelines include a section (Section II) on corporate responsibility to protect human rights. Accordingly, companies should respect human rights, avoid infringing them and address adverse human rights impacts that they are involved in. In this regard, reference is made to the International Bill of Human Rights and the International Labour Organization's Declaration on Fundamental Principles and Rights at Work, in that these documents represent the minimum standard to adhere to as far as the protection of human rights is concerned.¹³⁷⁷ It is also expected that companies have a policy regarding human rights, which also includes a due diligence process to identify, prevent, mitigate and account for how they address the impact of their activities on human rights. Principle 17 of the Guidelines stipulates the nature of the due diligence procedure, where business should assess actual and potential human rights impacts, integrate and act upon these findings, track the responses and communicate how the impacts have been addressed via an iterative process.

The commentary to Principle 17 states that this due diligence assessment must, in addition, be incorporated in a broader risk management system, that goes beyond identifying only the material risks to the commercial actor and must also be initiated at the earliest point in time possible, for example in the development of a new activity. Companies are held responsible for complicity in human rights abuses, where the standard to be upheld in determining complicity is that of aiding and abetting as established by international criminal law. Principle 18 stipulates that in addition to assessing potential human rights abuses, a commercial actor is required to consult with potentially affected groups, or other representatives, for example, expert resources from civil society. Principles 19 through 21 state how the findings from a human rights risk

1376 United Nations Human Rights Office of the High Commissioner, *Guiding Principles on Business and Human Rights*, above n. 1369, at pp. 1-12.

1377 *Ibid*, at p. 13.

assessment should be incorporated into company functions and processes. Finally, Principle 22 concerns remediation, and states that businesses are required to provide legitimate processes for the remediation of any human rights abuses, with the commentary to this Principle referring to ‘operational-level grievance mechanisms’.

6.4.8.4 Remarks

The ambit of soft law is wide and it includes many mechanisms. This study of soft law as a component of empowerment focussed on guidelines in the form of the Guiding Principles on Business and Human Rights. However, soft law is also characterised by extra-judicial norm formation and self-regulation.¹³⁷⁸ Examples of resulting mechanisms can include codes of professional ethics and tribunals for settling disputes.¹³⁷⁹ For example, the legal profession in most countries is usually represented by a law society that has developed an internal code of conduct. These reflect the norms and ethical guidelines that should be adhered to in the profession that they represent.¹³⁸⁰ The Swedish Bar Association is that body that oversees the adherence to the Code of Judicial Procedure and a special disciplinary board with the Bar Association hears matters where the Code has been allegedly contravened, having the power to warn members, fine them, reprimand them and in serious cases, exclude them from the Bar Association.¹³⁸¹

The example of the Guidelines is useful for their insight into the advantages associated with soft law mechanisms and to the extent that the Guidelines can be combined with traditional law. The example is also of particular interest due to the similarities it bears with the commercial setting regarding predictive modelling. Both instances are characterised by the following: first, companies

1378 Bernitz, Ulf, *Commercial Norms and Soft Law*, in Wahlgren, Peter (ed.), *Soft Law*, Scandinavian Studies in Law, Volume 58, Stockholm Institute for Scandinavian Law, 2013, at p. 34.

1379 Ibid.

1380 Sveriges Advokatsamfundet, *Code of Conduct of the Swedish Bar Association*, available at <https://www.advokatsamfundet.se/Advokatsamfundet-engelska/Rules-and-regulations/Code-of-Conduct/> (last accessed on 2017-04-04).

1381 Bernitz, above n. 1378, at p. 34.

are performing actions that are potentially harmful to individuals, second, there is a certain scepticism on the part of companies with respect to the enactment of traditional law that is burdensome and third, there is a need for an instrument to bridge the gap between commercial actor and individual. To the extent that the GDPR is relevant to predictive modelling, it must be conceded that a more traditional law approach has been adopted by the data protection regime in regulating the problem.

6.4.9 Technology

Technology is the final suggested component of empowerment. It is the dual nature of technology that, while part of the cause of the problem, it is also an integral part of the solution. It is technology that has partially upset a relative power balance between individuals and companies, yet, it remains part of the solution and therefore a component of empowerment. Considering the pace at which technology is developing and the extent to which personal autonomy is shrinking, it is argued that a solution to this challenge will rely to an ever-increasing extent on the role of technology.

Investigating technology as a component of empowerment is undertaken with some broader themes in mind. First, as was addressed above, misdirected technology, for example in the form of information overload, can become a hindrance instead of a solution and consequently disempowering. Second, using technology as a tool for empowerment requires a certain level of technical competence. Accepting that most individuals lack the technical competence to empower themselves, technology as a tool of empowerment will require creating solutions by third parties that either are simple to use or that are used by others on behalf of the individual for the purposes of empowerment. Third, despite the harms associated with predictive modelling, technology-based decision-making systems have benefits compared with human decisions, which are seldom objective or impartial and are open to influence. Predictive models may be discriminatory, however access to the computer code at least makes this bias identifiable.

6.4.9.1 Cases in Point

The disempowering effect of technology is illustrated in the following example regarding the supply of energy, where two smart city initiatives were examined in order to determine the social effects resulting from these initiatives. Consumers were provided with the technical functionality to control their consumption of energy, the aim being to achieve lower costs. Using an interface for visualization in order to understand energy consumption required that users of the system had the technological competence to read and interpret the information delivered by the system of visualization and interpret the energy consumption patterns produced by the smart system. Individuals who failed to learn how the technology worked as well as how to interpret the results from the system became marginalized and were even put at a disadvantage.¹³⁸² The inability to understand the technology resulted in consumers using energy when the price was highest, the effect opposite to that which was intended with the implementation of the system.

An example of technology that empowers the individual is the application called Compricer.¹³⁸³ Compricer compares the prices of goods and services on-line, thereby providing the consumer with a list of available goods and services and their price in relation to each other. This service does away with the need for the consumer to have a technical background in that another entity performs this function on his or her behalf. It therefore also functions as a portal for knowledge.¹³⁸⁴

The Swedish banking sector is facing challenges from technologically empowered clients and consumers. The company Sigmastocks has produced a product whereby programme software automatically provides individuals with advice on which stocks to buy.¹³⁸⁵ A popular scenario, when saving for

1382 Bylund, Markus and Cakici, Baki, *Smart IKT för att bo och arbete i Norra Djurgårdsstaden: Social Concerns in Information Systems for Sustainability*, SICS, 2012, at p. 7.

1383 Compricer, available at <https://www.compricer.se/press/om-compricer/> (last accessed on 2016-02-21).

1384 To complicate matters, consideration must also be taken of the extent to which the developers of any system created to assist the consumer/individual also has an agenda that is hidden from the consumer and may be manipulative.

1385 Sigmastocks, available at <https://sigmastocks.com/> (last accessed on 2016-06-17).

one's pension, is through the purchase of stocks or shares.¹³⁸⁶ Usually, an individual will approach his or her bank for advice on which stocks to purchase. This situation can be complicated as the bank not only provides investment advice to their clients, but also sells products that the client can invest in, making a profit on these products and calling into question the appropriateness of the situation, considering the potential conflict of interests. A computer programme providing this type of advice is empowering in many respects. In the case of Sigmastocks, the client is no longer required to pay a percentage of the capital investment, but can instead pay a lower, fixed price.¹³⁸⁷ In addition, the above conflict of interests is resolved, as the advice provided by the computer programme could be more objective than the advice from the bank, eliminating the conflict of interests. Other programmes are also available that examine a person's stock portfolio.¹³⁸⁸ These applications examine the stocks one has purchased and provide information concerning their performance, providing clients with alternative suggestions for the purchase of stocks that could possibly perform better.¹³⁸⁹ A final point is the positive attitude to these products by Finansinspektionen, the public authority in Sweden given the task by government of monitoring and analysing trends in the financial market, as these products can eliminate the conflict of interests mentioned above.¹³⁹⁰

6.4.9.2 The Notion of Resistance

Within sociology and surveillance studies, a notion that is well established is that of the 'resistance' to surveillance. In the face of technologies considered intrusive, individuals do not merely sit back, capitulate and accept the surveillance if they consider it unwarranted. Lyon refers to sociological studies where

1386 Eriksson, Hasse, *Råd från robotar utmanar banker*, available at <http://www.dn.se/ekonomi/rad-fran-robotar-utmanar-banker/> (last accessed on 2016-06-17).

1387 Ibid.

1388 For example, see Opti, available at <https://www.opti.se/om-oss> (last accessed on 2016-06-17).

1389 Eriksson, above n. 1386.

1390 Ibid. More information about the public authority and what it does can be found at <http://www.fi.se/Folder-EN/Startpage/About-FI/What-we-do/> (last accessed on 2016-16-17).

individuals are far from passive when in disagreement with new forms of surveillance and will resist the surveillance method if they feel unfairly challenged by it.¹³⁹¹ Marx puts forward a taxonomy of eleven mechanisms that are used to evade surveillance, namely, discovery moves, avoidance moves, piggybacking moves, switching moves, distorting moves, blocking moves, masking moves, breaking moves, refusal moves, cooperative moves and counter-surveillance moves.¹³⁹² These methods assume knowledge of the surveillance, which is a pre-condition for the resistance. An awareness of the extent to which predictive modelling enables surveillance is more difficult.

One method of resistance is turning the tables on the technology of surveillance. In this regard, the example of Farecast is illustrative of how technology can be used to the advantage of the individual. Predictive technologies are used by airline companies to discriminate between passengers based on their personal circumstances, for example, where two seats placed next to each other can attract a different price depending on the circumstances of the individual buying them.¹³⁹³ Given enough data about the price of plane tickets over time, the Farecast software could predict whether the ticket price that the consumer was considering buying, was likely to increase or decrease in the future. This in turn would allow the consumer to wait before purchasing the ticket if the model predicted that the price was likely to decrease or suggest the purchase of the ticket immediately, if it was going to increase according to system predictions. The programme was based on big data and essentially utilized the same technology as was being utilized by airline companies. The technology analysed ticket sales for a specified route using the prices paid in relation to date of departure, and provided a prediction with a seventy five percent success rate.¹³⁹⁴ Of significance is that no knowledge of the airlines' predictive modelling was required and all that was necessary was enough data.¹³⁹⁵

1391 David Lyon, *Surveillance Studies*, above n. 64, at p. 167.

1392 Marx, Gary T., *A Tack in the Shoe: Neutralizing and Resisting the New Surveillance*, *Journal of Social Issues*, Vol. 59 No.2, 2003, pp. 369- 390.

1393 Borenstein, Severin and Rose, Nancy L., *Competition and Price Dispersion in the U.S. Airline Industry*, *Journal of Political Economy*, Vol. 102, No. 4, 1994, available at <http://faculty.haas.berkeley.edu/borenste/download/JPE94AirPrice.pdf> (last accessed on 2016-03-24).

1394 Ibid.

1395 Ibid.

Another method of resistance is evasion. An example of technology involving evasion is Tor.¹³⁹⁶ Tor is a group of volunteer-operated servers that connect to each other by means of virtual tunnels instead of doing so by means of direct connections. This technical setup allows individuals and organizations to communicate with each other, using public networks, while keeping their identities and communications private. Tor provides the ability to both connect to web sites and instant messenger services as well as publish material without the person involved being located. It also provides the ability to bypass ISP's that block access to certain content, for example by repressive regimes.¹³⁹⁷ With such tools, opponents of totalitarian regimes are able to both access information and publish it without fear of being detected, governments wishing to find out more about other governments or groupings can do so without being accused of 'snooping around' and individuals can make their way around in the digital environment without being detected and surveilled.¹³⁹⁸ One of the modes of surveillance that Tor protects against is 'network traffic analysis'.¹³⁹⁹ A Tor communication will typically go through three Tor nodes before being sent on to the destination computer. The packets hop between the Tor nodes that compose the circuit, the essential element being that a packet hopping between two nodes has information only concerning that hop in the circuit, encryption also an essential element of Tor.¹⁴⁰⁰

6.4.9.3 Embedding Legal Rules in Technology

The notion of embedding legal rules in technology is not new. Lessig alludes to the fact that code is law and that those who write the code also are the de

1396 Tor, available at <https://www.torproject.org/download/download-easy.html.en> (last accessed on 2017-02-21).

1397 Ibid.

1398 Ibid.

1399 Techopedia, *Network Traffic Analysis*, available at <https://www.techopedia.com/definition/29976/network-traffic-analysis> (last accessed on 2016-05-26).

1400 Thoreson, Anders, *Kom igång med Tor!*, IIS, Internetguider, available at https://www.iis.se/docs/kom_igang_med-tor.pdf (last accessed on 2016-05-25).

facto legislators.¹⁴⁰¹ The notion of privacy-by-design is an example of embedding law in technology that is included in the GDPR. In the context of a strategy of empowerment, privacy-by-design is an indispensable element.

6.4.9.3.1 *Privacy by Design*

Cavoukian is credited with coining the notion ‘privacy-by-design’, which is briefly described as, ‘... an approach to protecting privacy by embedding it into the design specifications of technologies, business practices, and physical infrastructures. That means building in privacy up front – right into the design specifications and architecture of new systems and processes’.¹⁴⁰² Privacy by design consists of seven principles:

- 1) Proactive not Reactive — Preventative not Remedial,
- 2) Privacy as the Default Setting,
- 3) Privacy Embedded into Design,
- 4) Full Functionality — Positive-Sum, not Zero-Sum,
- 5) End-to-End Security — Full Lifecycle Protection,
- 6) Visibility and Transparency — Keep it Open and
- 7) Respect for User Privacy — Keep it User-Centric.¹⁴⁰³

Also, it is a stated objective of the notion of privacy by design, that it should afford individuals a greater degree of control, while at the same time providing a competitive advantage to those commercial actors that apply it.¹⁴⁰⁴

The fourth principle is relevant from the empowerment perspective. Its aim is to allow for competing interests to be satisfied in its application, being referred to as a ‘win-win’ scenario.¹⁴⁰⁵ This reinforces the idea that the attainment of privacy need not be viewed in terms of a struggle between parties, but

1401 Lessig, Lawrence, *Code is Law: On Liberty in Cyberspace*, Harvard Magazine, 2000, available at <http://harvardmagazine.com/2000/01/code-is-law-html> (last accessed on 2016-03-24).

1402 Information and Privacy Commissioner of Ontario, *Introduction to PbD*, available at <https://www.ipc.on.ca/english/privacy/introduction-to-pbd/> (last accessed on 2016-03-24).

1403 Cavoukian, Ann, *Privacy by Design: The 7 Foundational Principles*, available at <https://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf> (last accessed on 2016-03-24).

1404 Ibid.

1405 Ibid.

rather as a mechanism for cooperation and mutual gain. It is possibly this rationale that has resulted in privacy-by-design being included in the GDPR, as examined below.

Article 23 of the GDPR deals with privacy by design. It is entitled ‘Data protection by design and by default’ and states that, taking into account the level and nature of the data processing, as well as the risks thereof, the appropriate technical and organizational measures must be put in place to achieve the data protection principles. Article 23 also states that data protection should be by default. Currently new users of an application would have the default settings set to most open, with for example the user’s profile being open to all. In contrast, Article 23 of the GDPR requires that the default settings be set to their strongest from the start, with the user later being able to relax the degree of protection by changing the application’s settings. Initiatives exist where protection is implemented by default, providing an increased level of protection as the technical measure is in place right from the outset and is not dependent on any technical expertise.

Organizations also provide information and software that can help individuals evade surveillance. The Electronic Frontier Foundation (EFF) is a non-profit organization established in 1990 to protect civil liberties in the digital environment, promoting privacy and freedom of expression.¹⁴⁰⁶ The EFF published the ‘Surveillance Self-Defence’ guide, which is a source of information on how to evade surveillance in the digital environment as well as a source for the relevant technological means of achieving this goal, an example being the Tor browser bundle.¹⁴⁰⁷

In addition to providing information on how to become empowered, solutions that are empowering can also be embedded into the actual technology. For example, the initiative called ‘Do Not Track’ provides both policy but also technical tools in order for people to evade being tracked by behavioural advertisers while on-line.¹⁴⁰⁸ When accessing a web page, the computer browser requesting access to a web page sends an initial message called a ‘header’ to the web page server. The header includes various types of information, for

1406 Electronic Frontier Foundation, *About EFF*, available at <https://www.eff.org/about> (last accessed on 2016-04-14).

1407 Electronic Frontier Foundation, *Surveillance Self-Defence*, available at <https://ssd.eff.org/en/about-surveillance-self-defence> (last accessed on 2016-04-16).

1408 Electronic Frontier Foundation, *Do Not Track*, available at <https://www.eff.org/issues/do-not-track> (last accessed on 2017-04-04).

example, what browser is being used. Do Not Track is a machine-readable header that indicates that a person does not want to be tracked. In 2011, the browsers Firefox and Safari provided features supporting Do Not Track while Internet Explorer came with a similar built-in feature. However, advertising companies for the most part have disregarded the Do Not Track feature and attempts to achieve a broad consensus within the advertising industry have for the most part failed.¹⁴⁰⁹ Despite these setbacks, efforts are continually being made to develop new tools that are user-friendly and that allow individuals to evade being monitored by advertisers. For example, the World Wide Web Consortium (W3C) has developed two standards to curtail tracking (Tracking Preferences Expression (TPE) and Tracking Compliance and Scope (TCS)).¹⁴¹⁰

Another example of empowerment using technology has occurred in the context of SPAM, which can be described as, 'unsolicited usually commercial e-mail sent to a large number of addresses'.¹⁴¹¹ A problem from the legal point of view is that SPAM is not legally defined.¹⁴¹² Nevertheless, attempts have been made to legally regulate it. For example, at the EU level, the ePrivacy Directive attempts to regulate unsolicited email. However, as conceded by the Commission, '[I]aws, however, are not always enough'.¹⁴¹³ Consequently, the Commission also refers to other measure to be taken, including technical ones. In Communication on unsolicited commercials or 'SPAM', the Commission referred to the technology of filtering and encouraged the use of technology in that companies, 'offer filtering facilities or services to their customers as an option available on request, as well as information on third party products.'¹⁴¹⁴ In addition, the Commission referred to the Safer Internet Programme, wherein it was stated that, [t]he programme provides funding for

1409 Ibid.

1410 Ibid. See also World Wide Web Consortium (W3C), available at <http://www.w3.org/Consortium/> (last accessed on 2017-04-04).

1411 Merriam-Webster, *SPAM*, available at <https://www.merriam-webster.com/dictionary/spam> (last accessed on 2017-04-04).

1412 Magnusson Sjöberg, Cecilia (red.), *Rättsinformatik*, second edition, Studentlitteratur, 2016, at p. 294.

1413 European Commission, *Protection Privacy and Fighting Spam*, Information, Society and Media Fact Sheet, available at http://ec.europa.eu/information_society/doc/fact-sheets/024-privacy-and-spam-en.pdf (last accessed on 2017-04-04).

1414 European Commission, Communication from the Commission of 22 January 2004 on unsolicited commercial communications or 'spam' [COM(2004) 28 final.

technological measures which enable users to limit the amount of unwanted and harmful content, and manage the spam they receive ... assessing the effectiveness of available filtering technology ... contributing to the accessibility of filter technology, notably in languages not adequately covered by the market.¹⁴¹⁵ Consequently, the above illustrates that despite the existence of laws for combatting SPAM there is a heavy reliance on technology in order to attain the goal of eradicating SPAM and empowering the individual through technology.

6.4.9.3.2 *Coding Accountability*

Considering the wide application of predictive models and the influence they exert on individuals, initiatives are taking place within computer science to make the decisions produced by technology both accountable and governable, according to legal and policy considerations.¹⁴¹⁶ The main contention is that current accountability mechanisms were developed to oversee human decision making processes and are therefore not adequate for present day technological phenomena.¹⁴¹⁷ The goal therefore, as far as automatic decisions are concerned, is to allow for the verification and demonstration of the compliance with legal fairness. To this end, demanding transparency in order to attain accountability is not considered an adequate solution considering an environment where automated decisions are based on machine learning, where a decision cannot be explained, the underlying software may be protected as a trade secret and explaining how a decision was arrived at usually requires the access to the underlying data, which could be protected by secrecy demands.¹⁴¹⁸

1415 European Commission, *Safer Internet Programme 2005-2008* (Safer Internet Plus), Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks.

1416 Kroll, Huey, Barocas, Felten, Reidenberg, Robinson, and Yu, above n. 14, at p. 4.

1417 Citron, Danielle Keats, *Technological Due Process*, U of Maryland Legal Studies Research Paper No. 2007-26; Washington University Law Review, Vol. 85, pp. 1249-1313, 2007, available at SSRN: <https://ssrn.com/abstract=1012360> (last accessed 2016-11-22).

1418 Ibid, at p. 6.

In examining the notion of building accountability into decision-making systems, two issues become apparent. The first issue concerns procedural regularity, that is, ensuring that every automated decision was made following the exact same procedure, while the second issue concerns the extent to which automated decision systems adhered to legal or policy standards when a decision was arrived at. Regarding these two issues, Kroll et al. make some observations about systems design that are relevant. First, there are static and dynamic methods for testing systems, both with their respective advantages and disadvantages. Second, an inherent characteristic of systems development is randomness, which is necessary in order to prevent strategic behaviour, to protect secret information and to allow the system to operate in changing environments. The challenges in determining procedural regularity can be addressed by technical methods, such as cryptographic commitments, zero-knowledge proofs and fair random choices.¹⁴¹⁹ These technologies can ensure that the same policy rule was used for all decisions, that a decision policy was specified before decisions were taken, that each decision can be reproduced and that random inputs to a system cannot be controlled by any person. These technologies must be taken into account already at the early design stages of a decision-making system.¹⁴²⁰ Third, ensuring procedural regularity is less complicated than ensuring that a certain policy was adhered to, for example, where laws about fairness or the balancing of interests are difficult to reproduce in the technical context.¹⁴²¹

Ensuring a certain policy was adhered to can be facilitated by zero-knowledge proofs, which is a technical phenomenon developed within computer science, best described by Kroll et al.:

In the context of cryptographic commitments, zero-knowledge proofs allow the committer to prove that the hidden value inside a commitment has a certain property, but without having to exhibit that value directly or explain how that property is known. For example, if a decision maker commits separately to a specific policy, the inputs to a particular decision based on the policy, and the application of the policy to those inputs for an outcome, a non-interactive zero-knowledge proof can prove that these values correspond to each other, namely

1419 Kroll, Huey, Barocas, Felten, Reidenberg, Robinson and Yu, above n. 14, at pp. 27-36. For an in-depth study of these technologies, see the above reference.

1420 Ibid, at p. 15.

1421 Ibid, at p. 30.

that the outcome of applying the committed-to policy to the committed-to input data is the committed-to outcome.¹⁴²²

There are a number of advantages with zero-knowledge proofs. The entity making a decision can produce logs verifying that a certain policy was adhered to, without having to reveal the actual decision or the data that was either used as input or that was produced in the form of an output. Should a dispute arise, the decision-making entity could reveal the policy that was included as well as the input and output data, to a court of law or any other forum of expertise, thereby validating the correctness of the initial statement.¹⁴²³ Another advantage is that the algorithm used to make a decision can be verified by an ‘examining algorithm’, with the accompanying assertion that if the examining algorithm were to be run on the decision algorithm, it would verify that a policy rule was adhered to as stated. Finally, zero-knowledge proofs can be used as a mechanism of compliance, proving that a system behaved as it was alleged that it would.¹⁴²⁴

6.4.9.3.3 *Incorporating Interpretability*

As mentioned previously, some types of predictive models are more interpretable than others, depending on the technology used. As technology itself progresses, so too are the technological means of ensuring interpretability. An example of this is ‘conformal prediction’, which entails the provision of a guarantee that a predictive model is working as envisaged to a certain degree. Put another way, ‘[t]he predictions these algorithms make are often imperfect, but they improve over time, and they are *hedged*: they incorporate a valid indication of their own accuracy and reliability’.¹⁴²⁵ Continuing with the notion that predictive models assign labels, Vouk states:

1422 Ibid, at p. 21.

1423 Ibid, at p. 22.

1424 Ibid, at pp. 44-45.

1425 Vouk, Vladimir, *Preface*, in Vouk, Vladimir, Gammernan, Alex, and Shafer, Glenn, *Algorithmic learning in a random world*, Springer, 2005, emphasis in the original citation.

When we use this method, we predict that a new object will have a label that makes it similar to the old examples in some specified way, and we use the degree to which the specified type of similarity holds within the old examples to estimate our confidence in the prediction. Our conformal predictors are, in other words, ‘confidence predictors’.¹⁴²⁶

Put differently, ‘[c]onformal prediction uses past experience to determine precise levels of confidence in new predictions’.¹⁴²⁷ The main development as far as conformal prediction is concerned is that while the accuracy of predictive models in general can be assessed, conformal predictions allow for the assessment of each and every prediction made.¹⁴²⁸ In addition, instead of a predictive model producing an output in the form of a single label, the output consists of varying labels, each with a probability of accuracy, the result being that only those labels with a certain accuracy can be used in the decision-making process.¹⁴²⁹

6.4.9.3.4 *Blockchain Technology*

A relatively new technology is the ‘blockchain’ technology. This technology was originally developed in conjunction with the Bitcoin digital currency.¹⁴³⁰ Blockchain is described as, ‘a shared public ledger on which the entire Bitcoin network relies’, with all transactions included in the blockchain and where the integrity of the data and the chronology of the transactions are maintained through the use of cryptography.¹⁴³¹ The ledger grows continuously, with all transaction being joined to the chain in a linear fashion, a copy of the ledger

1426 Ibid, at p. 7.

1427 Shafer, Glenn and Vovk, Vladimir, *A Tutorial on Conformal Prediction*, Journal of Machine Learning Research, 9. 2008, 371-421, at p. 371.

1428 Johansson, Ulf, Boström, Henrik and Löfström, Tuve, *Conformal Prediction Using Decision Trees*, 2013 IEEE 13th International Conference on Data Mining, Dallas, TX, pp. 330-339, available at <http://ieeexplore.ieee.org/document/6729517/> (last accessed on 2017-01-30), at p. 330.

1429 Ibid.

1430 Bitcoin, *How does Bitcoin work?* available at <https://bitcoin.org/en/how-it-works> (last accessed on 2017-04-04).

1431 Ibid.

downloaded to each device connecting to Bitcoin.¹⁴³² Once a transaction has been added to the public ledger, it cannot be altered. In addition, the ledger resides on multiples nodes (computers) that are continuously synchronizing this data with other nodes.¹⁴³³ The system is decentralized, making it robust and not susceptible to becoming unavailable. Augur aptly describes the technology:

A block generally contains four pieces of information: a reference to the previous block, a summary of included transaction, a time stamp, and Proof of Work that went into creating the secure block. The blocks are strung together into a chain - a fluid chain that does not allow for any inconsistencies ... and transactions entered are necessarily valid and can be processed. By checking the blockchain and confirming transactions, the entire system is effectively self-regulated and fully secure ... Once it's in the blockchain, it's there forever.¹⁴³⁴

Blockchain technology does away with the need for a trusted third party, such as a bank. In facilitating a Bitcoin transaction, for example, the network performs a number of steps. The ledger is inspected to see if the Bitcoin exists. If so, the nodes called 'miners' assemble the proposed transaction into a new block on the blockchain and a hash function ensures the integrity of the data. Any change in the data will be reflected in the hash sum. Once confirmed, the hash of the new header becomes that blocks identifying string and it becomes part of the entire ledger.¹⁴³⁵

The main point by referring to this technology is to highlight that there are mechanisms becoming available that ensure the integrity of data in an open and transparent manner, and which is updated in real time. In other words it ensures the integrity of the data coupled with insight into this integrity, which

1432 Blockchain, available at <http://www.investopedia.com/terms/b/blockchain.asp> (last accessed on 2017-04-04).

1433 Augur, Hannah, *WTF is a Blockchain? A Guide for Total Beginners*, Dataconomy, available at <http://dataconomy.com/2015/10/wtf-is-the-blockchain-a-guide-for-total-beginners/> (last accessed on 2017-04.04).

1434 Ibid.

1435 Blockchains, *The great chain of being sure about things*, The Economist, available at <http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable> (last accessed on 2017-04-24).

is an empowering tool if it is in the interests of an individual that data has not been altered.

6.4.9.4 Remarks

Of all the components of the strategy of empowerment, the utilization of technology is probably the component that will continue to gain in importance as the technical nature of both the digital environment and technologies such as predictive modelling become more ambient and complex. It is within this context that the effectiveness of human intervention must be questioned. While technology is generally empowering, there are a number of factors that need to be taken into account. First, taking a strategy of empowerment through technology too far can result in disempowerment. Second, empowerment through technology poses a potential threat in that overstepping the point at which the desired balance is achieved can in itself pose risks and vulnerabilities, where the ability to by-pass certain systems would not be beneficial to society. It could allow for decision systems ensuring economic stability to be by-passed or allow for a commercial actor's competitor to gain access to classified system code.

The notion of privacy by design was introduced in the 1990's and is still relevant, especially considering its inclusion in the GDPR. This, it is argued, is a confirmation that the principles that privacy-by-design enshrine confirm the role that technology is to play in the future data protection legal regime. However, a number of points require clarification. Article 25 refers to the adherence to data protection principles as the aim or goal of privacy by design, yet, exactly which principles are being referred to remains unclear. Is it only the data protection principles as explicitly expressed in the GDPR or does it include those principles that are implicitly protected as well. If only the former, then the extent to which autonomy as a notion will be afforded protection remains dubious. Article 25 also refers to 'pseudonymisation' as an example of a privacy by design technique. It is debatable whether anonymity as a notion can be said to exist within the realm of modern technology. Multiple examples illustrate the problems associated with attempting to make data anonymous where the reality of technology in many cases puts in question the ability to attain this goal. It is also questionable whether Article 25 adheres to the privacy by design principle number 6 referred to above. This principle requires that the privacy by design technology be kept open 'to users and providers

alike'.¹⁴³⁶ Recital number 63 to the GDPR states that trade secrets and intellectual property rights should remain out of the scope of the transparency afforded in connection with profiling, restricting the applicability of principle number 6.

In relying on technology to keep technology in check, some aspects need to be stressed. First, there is the need for proactivity in systems design, identifying what technologies will be employed to ascertain accountability. Also, transparency cannot be equated with accountability, the risk being that transparency to 'insignificant' parts of a decision-making system will be used to deflect 'real' access. The GDPR has a built-in contradiction to the extent that access to the logic of decision-making systems is granted, while at the same time this access is limited by trade secrets and intellectual property rights. It is here that technologies such as zero-knowledge proofs can come to the rescue of the GDPR. Assuming that this technology can be applied without revealing trade secrets, certain data and other intellectual property rights, it may be a useful mechanism for allowing appropriate access to the logic of decision systems.

6.5 The 'Washington, D.C. Example' Revisited

The 'Washington, D.C. example' referred to in the introduction is briefly revisited in order to determine what difference the strategy of empowerment potentially would have made to SW. In the first place, the strategy of empowerment would have required that SW be notified that a predictive model had been used to make a decision about her performance as a teacher and that the output from the predictive model had laid the basis for the decision to fire her. A strategy of empowerment would also have placed the accountability on the education authorities to adhere to the notion of accountability but also be in a position to demonstrate this accountability. In addition, the education authorities could also have demanded that the developers of the predictive model build accountability into the model and be in a position to demonstrate this in an easily understood manner. Constructing a system in a manner that allowed

1436 Cavoukian, Ann, *Privacy by Design*, above n. 1403.

for the provision of answers to the questions, ‘why?’ and ‘what?’ would have provided SW with the insight needed to take the matter further if need be and would have prevented both the system developers and education authorities from hiding behind the mathematical complexities of the ‘black box’ system. Demanding interpretability and ensuring a certain level of accuracy would have made the results explainable and would have ensured a higher level of accuracy. So too would increased supervision, possibly with multiple iterations, have ensured that the system had been tested and the results verified. Placing not only the duty of accountability but also the duty to demonstrate accountability on the entity using the predictive model would also have made for a more transparent process.

One can also argue that a duty of care placed on the developers and education authorities would have forced those relying on the decisions made by the system to verify them and not merely take them at face value. In other words, taking into account the nature of the decisions being relied on in this case and the potentially devastating ramifications for the individual’s involved, steps should have been taken to ensure that the system worked as was intended and was not open to fraudulent behaviour at any stage of the process. Also, providing the victim with a right of access to the image that the system compiled on her and the ability to contradict that image may have resulted in a different outcome. In addition, providing space for alternative narratives, for example references from SW’s at the time current principal, would also have provided a truer image of SW.

This example is also characterised by the emotional state of helplessness experienced by SW. Having a representative organization to turn to in order to object to a system-based decision, would have alleviated this. While in the area of labour relations, trade unions can play a role, what is also required are institutions that would have had the power of oversight and most importantly knowledge of the technology, which could also have functioned as a forum within which the victim could have aired her concerns and suspicions, quite simply giving her the ability to tell her side of the story. In total 206 teachers were negatively affected by the computer system and a simple and accessible collective redress system would have allowed for the group of disenfranchised teachers to take their claim forward in a court of law. In the end, the damage to SW was minimised by the fact that she soon found alternative employment. In such circumstances, the motivation to pursue a suit in a court of law may not be that enticing. However, the option of collective redress could be a factor encouraging redress even where the gains are not expected to be substantial.

Finally, the technology was constructed in a manner that was open to bias and gaming. It was intentionally a 'black box' with only the developers having any idea of the mathematics behind the algorithm. The code making up the system was designed to be a 'black box' and there was no public pressure demanding otherwise. This should be seen in contrast to technologies such as the blockchain technology mentioned above. Had blockchain technology been available at the time and used in the predictive model, it would have provided the system with characteristics essential in the circumstances. It would have prevented that the data on which the predictive model operated, had been secretly altered without detection and it would also have allowed for the scrutiny of the system by the public at large, the functioning of the system essentially an open record.

6.6 Summary and Conclusions

Considering that human interaction with the digital environment is to an increasing extent being controlled by predictive models, the space available within which a person is able to exert his or her personal autonomy or agency is diminishing. Expressed in more practical terms, a problem arises where a human is unknowingly subjected to a decision-making system, such as a predictive model, of which little is known and from which there is no or very little redress. The harm is especially serious where the result of the decision-making system is disadvantageous to the individual. Nevertheless, even when an individual benefits from a decision made by a model, a certain degree of harm ensues merely by virtue of the fact that the process occurs clandestinely and camouflaged by the 'black box'. An approach to address this problem is to cultivate an environment that allows for the expression of human autonomy while at the same time allowing for innovation that is to be gleaned from the use of predictive models.

To this end the strategy of empowerment is suggested. The term empowerment has been used in various contexts to remedy past injustices or improve the situation of a specific class of individuals and has been associated with the aim of encouraging a more active individual. However, the difference in the commercial setting that forms the backdrop of this study is the disruptive role

played by technology, in turn creating the need for a particular type of empowerment. Whereas the previous use of the term empowerment has had as its aim the promotion of a more active individual, the above strategy of empowerment, while enabling a more active individual, simultaneously identifies an individual in need of assistance. In other words, it steps away from the thinking of Westin, where the solution to the risks from computing was to assign more control to the individual, and advocates a scenario where the individual is identified as not always being in the best position to determine his or own best needs, the term 'libertarian paternalism' relevant in this regard. This becomes particularly relevant in the relationship between commercial actor and individual.

Empowerment is a strategy comprising an inventory of a number of components, which regulate a problem but which also are interrelated and influence each other. The extent to which one component or multiple components are required to address a problem depends on the complexity and nature of that problem. In some cases a single component, for example knowledge, will be sufficient, while in others, the complexity of the technology may inhibit the effectiveness of a single component. In such cases, multiple components may be required to rectify the imbalance that arises from predictive modelling, thereby levelling the playing field and cultivating a respect for personal autonomy on the part of companies. To this extent, a strategy of empowerment is not intended as a 'zero-sum' solution, but rather a 'positive-sum' solution, benefitting both commercial actors and individuals.

A strategy of empowerment is also intended to have a proactive function. In other words, it is not intended to function only as a reactive instrument after the damage is done, but also have a pre-emptory function in preventing the harms before they occur. It is once again in this respect that empowerment has a 'bark' function that not only provides individuals with multiple courses of action, thereby dissuading commercial actors from harmful practices, but also lays out the acceptable norms and practices that society should strive after.

Becoming more apparent, also, is the leading role technology will play in the future. The nature and complexities of the digital environment are such that the scope for human intervention is decreasing. So, while technology, in the form of predictive modelling is the cause of the risks and vulnerabilities that have presented themselves, it remains a substantial part of the solution. It is in this regard that there is limited insight into the pace at which technology may provide the solution, or parts thereof. Here mention must be made of the

blockchain technology that is relatively new and which holds untold potential as far as the practical applications in can be put to.

A crucial consideration, in the light of the above strategy of empowerment, is what the present and future role of the law will be. The law, both traditional and soft, directly addresses the risks and vulnerabilities caused by predictive modelling. The component entitled ‘duty of care’ is an example of this. However, the law encircles all the components of the strategy of empowerment and to this extent, operates indirectly, regulating the components that is in turn regulating the problem. In this regard, the component of technology is relevant, especially in light of technologies such as blockchain. While the blockchain technology provides innumerable applications, its use has already been identified as potentially creating issues in relation to personal integrity. It is in this regard that the law in its current form will always have a function.

7 Conclusion

7.1 Introduction

Technology is constantly developing and the phenomenon of predictive modelling is typical of the situation where new technologies, or even the novel application of established technologies, challenge society. They challenge the established way of working, they challenge existing notions of ethics and morality and they challenge existing legal frameworks. The manner in which predictive modelling challenges the law is relevant to the extent that it is a function of the law to protect society from the risks associated with new technologies.

As illustrated in the preceding chapters, predictive models are increasingly being used by commercial actors to manage their relationships with their clients and potential clients that they interact with in the digital environment. It is undisputed that the use of predictive models generally is extremely beneficial to society. However, for all the benefits to society associated with this technology, and taking the individual's perspective into account, there are potential harms that can be inflicted on the individual as a result of the use of this technology in the commercial setting. Predictive models, incorporating sophisticated algorithms to analyse data, not only have the ability to predict human behaviour, but combined with knowledge from the social sciences, life sciences and behavioural sciences, can also provide insight into how human behaviour can be manipulated. The commercial actors have the resources to access and apply this technology, allowing them to acquire knowledge from big data that is invisible to the human eye. This situation is compounded by a lack of awareness on the part of individuals, resulting from the fact that this technology is almost invisible to human beings. And if visible, it is for all intents and purposes inaccessible, due to its complexity. It is essentially a 'black box'. The result is a playing field that is not level, something that this thesis seeks to address.

This thesis began with an examination of how technology has progressed to the extent that this was relevant in relation to predictive modelling. Thereafter, it laid out a theoretical base for the notion of surveillance and discussed the concepts of autonomy and identity. Thereafter an inventory was made of some of the potential harms that can be attributed to predictive modelling. Working on the hypothesis that most new technologies, for all their benefits, usually also entail risks and vulnerabilities, this thesis examined the extent to which the data privacy legal framework addressed predictive modelling and its harmful effects to personal autonomy. Finally, a strategy of empowerment was introduced, comprising components of a traditional legal, soft law and technological nature, and suggesting alternative remedies to existing traditional legal frameworks.

This summary is divided into three main parts. First, a summary of the general findings of this thesis in relation to the research questions set at the start is provided. Second, based on the findings presented throughout this thesis, some general opinions are provided. Third, looking to the future, some suggestions are provided as to what trends and developments will most likely be of interest taking into account the subject matter covered by this thesis.

7.2 Summary of Findings

Chapter 1 of this thesis provided the background to this thesis and explained the importance of conducting research on this subject. It laid out the research questions and provided a methodological basis. Chapter 2 of this thesis provided a historical background concerning the technological developments deemed relevant in relation to predictive modelling. It examined what big data is and also the technology of predictive modelling, highlighting technical notions relevant to the study of predictive modelling as well as notable trends in relation to this technology. It also highlighted the power that could be harnessed arising from the combination of the technology of predictive modelling with the knowledge from other scientific disciplines, for example, the behavioural sciences. As far as the technology is concerned, two main developments are noteworthy. The first concerns the manner in which data is handled. While previously the focus had been on the possibilities of storing all available data in structured databases, while still relevant, the modern approach is rather to exploit the data for the knowledge that it contains, thereafter discarding it,

retaining only the knowledge that these data held and incorporating this knowledge into models. The second development is somewhat linked to the first and concerns the shift in the nature of big data itself. While its nature in the past has been characterised by it being more static and rigid, systematically being stored in a structured format in databases in anticipation of the uses it can be put to, big data has become more fluid, dynamic and streaming in nature, essentially residing all over the digital environment.

Chapter 3 of this thesis provided a theoretical framework. First, it examined some theories behind the reasons for surveillance. While many of these theories have the state versus individual relationship in mind, they are no less relevant in the commercial setting. They highlight the power aspect associated with surveillance as well as the role played by technology. These theories of surveillance are indicative of the shift from a centralised method of surveillance, confined by physical limitations, to a situation characterised by decentralised surveillance, facilitated by technologies of the digital environment. This chapter then proceeded to investigate the notions of autonomy and identity. The notion of autonomy is especially relevant as it underpins most of the potential harms associated with predictive modelling and serves as a common denominator. In addition, the notion of identity in the digital era was investigated, with the ‘digital identity’ proposed as a concept that better describes the digital representation of humans in the on-line environment and its use as a proxy in place of them.

Chapter 4 of this study provided an inventory of the potential harms identified in relation to predictive modelling. This list was not intended to be exhaustive. The purpose of the inventory was twofold: first, to create an awareness of the types of harms that can arise as a result of predictive modelling and second, to illustrate the extent to which these harms are addressed by traditional law. A finding was that some of the harms examined were more recognized in traditional law while others were recognized to a lesser extent. The inventory comprised the following potential harms: privacy, reputation, discrimination, self-censorship, deindividualization, loss of agency, stereotyping, manipulation, lost human dignity and lost human identity.

Chapter 5 of this work examined the extent to which the European data privacy legal framework addressed the notions of autonomy and predictive modelling. In doing so, two legal frameworks were examined. These were the CoE’s ECHR as adjudicated by the ECtHR as well as the EU’s data protection legal framework, more specifically the principles of data protection as en-

trenched in the DPD and GDPR. First, considering its human rights legal regime, the CoE explicitly addressed autonomy, stating what it is comprised of and that it was a value in need of protection. A finding was that the ECtHR as an institution is more flexible to the challenges posed by predictive modelling. While not addressing the phenomenon of predictive modelling explicitly, it displays a certain flexibility in that its dynamic interpretation policy enables it to address new technologies and bring them within the confines of the principles as entrenched within the articles of the ECHR. Second, the data protection regime expressly mentions ‘profiling’, which as defined in the GDPR, displays some of the attributes associated with predictive modelling. In addition, while both the DPD and GDPR are argued to have the protection of autonomy as an implicit goal, this goal seems to get lost in the complexities of applying the DPD and GDPR. In addition, considering the dated nature of the principles of data protection as well as the nature of modern technologies such as predictive modelling, concerns must be raised relating to the extent to which the GDPR will be able to respond to the demands of regulating technologies as complex as predictive modelling.

Chapter 6 of this thesis provided an alternative regulatory strategy in the form of ‘empowerment’. It is envisaged that for any regulatory mechanism to deal satisfactorily with complex technologies like predictive modelling, it will need to be flexible and responsive. To this end, empowerment is a strategy that includes an inventory of components that have a traditional legal, soft law or technical dimension. The following components made up the strategy of empowerment: knowledge, accountability, duty of care, a right of access, participation in the legislative process, an independent supervisory authority, collective redress, soft law and technology. Not all components need necessarily be resorted to in every situation. In addition, all components are interrelated to the extent that they influence each other. For example, technology can be used in innovative ways to increase awareness and enhance knowledge. In addition, this chapter considered the future function of traditional law in the light of the strategy of empowerment. It concluded by theorising as to how the components of a strategy of empowerment could work to alleviate the potential harms of predictive modelling in a practical example.

7.3 General Opinions

7.3.1 The European Legal Terrain

The European legal terrain is rather complex and encompasses a number of actors that have overlapping coverage as far as certain issues are concerned, data privacy being one of them. In this regard, the extent to which the issues addressed by the CoE and EU overlap is no exception. While the CoE was initially more concerned with fundamental rights, it has expanded into the realm of data protection. At the same time, the EU, having the main aim of encouraging peace via the commercial integration of its Member States, has taken on the role of protector of human rights. While in practice the integration of these two legal systems is substantial, they remain separated. Opinion 2/13 of the CJEU scuttled the attempt to allow the EU to accede to the ECHR, thereby confirming that the ECHR is not a legal instrument formally incorporated into EU law until accession occurs.¹⁴³⁷

In addition, it is argued that the basis of the existence of the EU, namely its founding goal of ensuring peace by integrating the markets of its Member States, is a complicating factor when addressing its ability to regulate the effects of a certain technology. As was highlighted above, the data protection regime does not prohibit data processing. In fact, it allows it to continue on the understanding that certain protections are put in place and that there is a certain degree of transparency. It is a regime based on pragmatism, where the processing and transfer of data is deemed essential for the internal market and that this should be allowed to continue under controlled conditions and with protections in place. The problem arises where data protection is viewed as protecting a number of subsidiary rights, for example autonomy, in addition to the main goal of economic integration. The argument is that the commercial perspective is at the core of the EU data protection legal regime and as such, the extent to which it adequately addresses notions such as autonomy must be questioned. While the protection of autonomy remains an implicit goal of data protection, it will always remain subsidiary in relation to the commercial goal.

¹⁴³⁷ Opinion 2/13 of 18 December 2014, EU:C:2014:2454.

Another point of consideration, in assessing the ability of the institutions of the CoE and EU to address the potential harms of predictive modelling, is the possibility for action by the ECtHR and CJEU. Considering the subject matter that this thesis covered, especially with regard to the interaction between the CoE and EU, one cannot but help consider the following citation:

The countries that have introduced a systemic and comprehensive law on data privacy have done so through legislation, and this is true both in relation to Civil [L]aw and Common Law countries. At the same time, it is undeniable that major steps in the protection of data privacy have been taken through court decisions ... there will be no doubt that case law will continue to play a central role in the development of data privacy law.¹⁴³⁸

The ECtHR has the goal of implementing the ECHR, which incorporates broad principles concerning fundamental rights as enshrined in the different articles of the ECHR. Accordingly, the ECtHR has the rather specific role of determining whether a fundamental right has been transgressed. To this end, it has a relatively wide discretion in determining which concrete instances fall within the ambit of the principles as enshrined in the articles of the ECHR. Furthermore, it has the capacity to interpret technology in a flexible manner so as to allow for the applicability of the ECHR. Within the area of EU data protection law, the CJEU on the other hand has a different role. It has a number of functions, one of which is to ensure that EU law is applied in the same manner in all EU Member States.¹⁴³⁹ Consequently, while the temptation exists to compare the suitability of the ECtHR and the CJEU to address questions related to technology and its effects, this would be unfair as the scope of the CJEU to achieve this is limited. Put in other terms, the ECtHR has a greater capacity to make law, while this is not the case as far as the CJEU is concerned. Returning to the above citation, considering the wide scope of the ECtHR, both as far as its discretion to hear matters and to interpret new technologies is concerned, its role is more in line with that of a traditional common law court. And if one agrees with the argumentation in the citation, then it can

1438 Svantesson, Dan Jerker B., *Extraterritoriality in Data Privacy Law*, Ex Tuto Publishing, 2013, at pp. 39-40.

1439 European Union, *Court of Justice of the European Union*, available at https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_en (last accessed on 2017-04-15).

be argued that the ECtHR should be better equipped to deal with future matters that concern autonomy and predictive modelling as they arise.

7.3.2 Relevance of Human Rights

In the context of this thesis, an advantage with the human rights legal framework as represented by the CoE is that it explicitly mentions ‘autonomy’ and views it as a fundamental right that is in need of protection, within the boundaries of Article 8 ECHR. Autonomy is not treated as an implicit value, but instead is clearly expressed as falling within the right to private life encapsulated in Article 8 ECHR. This recognition of the value of autonomy must be viewed in light of the ECtHR’s willingness to interpret dynamically new technologies as falling within the scope of the ECHR, thereby displaying a willingness to proactively meet the demands resulting from new technologies.

It is argued that the formal incorporation of fundamental human rights into the EU constitutional legal framework would have enhanced their legal status. However, the fact that the ECHR is formally not binding law within the EU does not make it redundant. There remains good reason to refer to principles, even if they have no binding legal force. Here, reference is made to the notions of ‘bite jurisdictions’ and ‘bark jurisdictions’ discussed above. The function of the ‘bark jurisdiction’ as a reflection of a society’s principles has a certain value. First, it can function as a yardstick against which actions are measured. For example, a commercial actor failing to adhere to human rights law, while possibly not legally obligated to do so, can still be singled out for not following the norms as reflected in various human rights legal instruments. This is especially true in cultures where reputation (and consequently commercial reputation) carries weight. Second, the ability to influence behaviour is not always dependent on enforceability. For example, laws may be promulgated solely to mark a certain behaviour as unacceptable, without that law having any real enforcement capabilities or intentions behind it. Consequently, the human rights legal regime, despite its shortcomings as noted above, does have a role to play in the protection of human rights in the light of new technologies.

Brownsword and Goodwin refer to the ‘dualism’ of human rights, namely that it comprises both legal rights enshrined within legal instruments as well as moral claims that exist outside the positive law. This allows the moral

claims aspect of human rights to ‘outrun’ the legally established aspect of human rights, in turn allowing human rights law to adapt and making it in effect limitless.¹⁴⁴⁰ It is in this context that Brownsword and Goodwin refer to future human rights, where one such right is the right to a unique identity.¹⁴⁴¹ This is of relevance in the context of predictive modelling. In addition, the potential harms of predictive modelling may necessitate the establishment of additional new rights. Without speculating as to what these could be, it is argued that the dualism of human rights puts it in a position to recognize such rights.

7.3.3 Relevance of the Data Protection Framework

It is argued that for the most part the data protection principles have remained unchanged over some time now, and the GDPR incorporates these very same principles. Reflection is required as to whether these principles, dating back to the 1970’s when the technology landscape was very different, are still adequate to deal with the challenges posed today by technologies such as predictive modelling and in the era of big data.

Questions relating to whether the principles on which the data protection regime is built are still relevant and realistic, have existed for some time now. For example, such questions were contemplated already in connection with the enactment of the DPD.¹⁴⁴² It is in this context that the distinction between the ‘processing model’ and ‘misuse model’ was addressed. In broad terms, the former model regulates every step in the processing of data, specifying a number of data processing principles that must be adhered to under all circumstances. The misuse model, on the other hand, softens up the processing model by concentrating, in certain circumstances, only on the prevention of abuse, disregarding circumstances where abuse does not occur.¹⁴⁴³ The DPD was implemented into Swedish law via the Personal Data Act (1998:204) and initially

1440 Brownsword and Goodwin, above n. 384, at p. 230.

1441 Ibid.

1442 Öman, Sören, *Protection of Personal Data – But How?*, in *Law and Information Technology: Swedish Views*, Seipel, Peter (ed.), Swedish Government Official Reports, SOU 2002:112, Information and Communication Technology Commission Report, Stockholm, 2002, at pp. 179-180.

1443 Ibid, at p. 182.

implemented the processing model. However, it soon became apparent that it was an unrealistic approach considering the advances regarding the widespread access to computers by individuals and word-processing capabilities available generally. Therefore, shortly after implementation, preparations were put in place to change significantly the Personal Data Act.¹⁴⁴⁴ In this regard, Sweden, together with Great Britain, Austria and Finland, also put forward suggestions to the EU Commission on how the application of the DPD could be made less cumbersome.¹⁴⁴⁵ Ultimately, the Personal Data Act was extensively amended, incorporating the misuse model to the extent that it did not contravene the DPD. This was made possible by distinguishing between personal data that was structured and unstructured material.¹⁴⁴⁶

The aims of the European data protection framework are noble and there is a point in ensuring that all the EU Member States uphold a minimum level of protection when considering the personal integrity of Europeans. However, at least for the time being, there seems to be the impression that commercial actors are currently flouting the data protection principles. As the modern method for attaining knowledge has progressed to a data-driven approach, commercial actors are similarly implementing business models based on technologies that support and employ this approach. The effect is that data protection principles are perceived as a hindrance. For example, some businesses find the data protection principle against re-purposing data to be completely at odds with how the businesses want to use the data they have collected or bought. This perspective is reinforced by the Swedish Government Report, the Privacy Committee's interim report (SOU 2016:41), which notes current trends that go against the principles of data protection. The Government Report provides the following examples of this: databases having multiple purposes, data being collected and retained because it may be useful in the future, the technical ability and low cost of retaining data, data mining, gathering personal data from all situations and personal data becoming a commodity.¹⁴⁴⁷ It is argued that instead of enquiring why the data protection regime lacks legit-

1444 Översyn av personuppgiftslagen, Regerings proposition 2005/06:173.

1445 Ibid, at p. 14.

1446 For an in-depth analysis of the process from 'processing model' to 'misuse model', see also Öman, *Implementing Data Protection in Law*, above n. 1363, at p. 389 and Öman, *Trends in Data Protection Law*, above n. 1152, at p. 209.

1447 Swedish Government Official Reports, SOU 2016: 41, above n. 11, at p. 117.

imacy, the EU has decided to raise the stakes in the GDPR, by markedly increasing the penalties for breaching the data protection principles. Speculating that the heavier penalties in the GDPR for breach of the data protection principles will result in an increased observance of these principles, it is argued that this will not be so because the GDPR enjoys greater legitimacy, but rather because the risks attached to not adhering to the GDPR will be too great.

Another limitation of the data protection framework is related to the manner it views technology, more specifically, data. The GDPR, as with the DPD, distinguishes between different types of data. For example, there are data that are to be considered ‘personal data’ and there are data that are to be considered ‘sensitive personal data’. It is argued that any classification of data is not realistic when taking into account modern technology. All data, however insignificant, is potentially sensitive to the extent that it can be correlated with other data. For example, data of a seemingly ‘innocuous’ character, combined with data of a sensitive nature, itself becomes sensitive by association. The ability of mathematical algorithms to identify seemingly non-existent connections between data requires that one think in new terms when contemplating the classification of data.

It can be argued that the data protection framework has taken into account the power of technology and the difficulty associated with its control. A development is that the GDPR refers to ‘pseudonymisation’ as opposed to anonymisation, which can be interpreted as an acceptance that the notion of anonymisation no longer exists in the digital environment. In addition, preamble 26 refers to the fact that data that have undergone pseudonymisation, yet which could be attributed to a natural person using additional information, should be considered information relating to an identifiable natural person. However, in determining whether a natural person is identifiable, consideration must be taken of means that are ‘reasonably likely to be used’, to directly or indirectly identify the natural person. In order to ascertain the boundaries of what is ‘reasonably likely to be used’, consideration should be taken of the costs involved, the time required and the state of technology both at the time of the processing but also with future developments. This can be interpreted as implying that if reasonable steps are taken to pseudonymise data, it will be considered non-identifiable data. Exactly what steps, both technical and operational, will be considered adequate has been left open by the GDPR. This in turn provides an opportunity for academia and industry to come up with solutions that will be judged adequate.

7.3.4 Technology

As mentioned above, while it is technology that is under the spotlight due to it being disruptive and having potentially harmful effects, it is technology that will also be part of the solution. It is in this context that some core themes regarding technology are highlighted.

There is no doubt that technological applications have increased and continue to increase at a phenomenal pace. However, this must be viewed in relation to the fact that much of the fundamentals upon which these technological applications are based, in fact have not changed that dramatically over time. This holds true in relation to predictive modelling. While the availability of data has increased, thereby multiplying the uses to which predictive modelling can be put, its core remains the practical application of statistics and mathematics, the results of which are used to gain insight into human behaviour. What has changed, however, is the practical application of the insights gained from these technologies in conjunction with knowledge from other disciplines, for example, the behavioural sciences and life sciences. This has markedly increased the manipulative capabilities of new technologies.

Another point worth illuminating, is that no technology is neutral and, moreover, no physical environment is neutral. The physical architecture of the cafeteria exerts an influence, whether intentional or not. All digital environments have been built from a perspective and with a goal in mind. These environments also exert an influence, be it intentional or unintentional. In a digital environment, the controllers of the code determine how individuals are able to navigate that space, in order to achieve the goals of a system. It is with this in mind that the controllers of the code of the digital environment have the ability to code the degree of transparency into these systems. They have a choice as to whether the 'black box' will remain just that or whether it will become more transparent. Continuing from the point above, the 'black box' is constructed by people. These people can determine the extent to which insight is granted in to the 'black box'. It is possible, if not probable, that the 'black box' is such, not because systems developers are evil, but rather because there has previously been no demand placed on them to make the systems more transparent or interpretable. It is in this vein that the efforts to make predictive models more interpretable as well as guaranteeing that their outputs are correct to a certain minimum level, can diminish the potential harms associated with them.

Finally, the following example of a technological development reflects the capacity of technology to empower individuals, and is illustrative of a number of themes addressed throughout this thesis. It concerns an application in the form of a chatbot lawyer called DoNotPay.¹⁴⁴⁸ This application uses artificial intelligence and provides a free service that assists individuals, who have received a parking fine, to appeal that parking fine via a user-friendly interface. Having received a parking fine, the individual accesses the chatbot lawyer and is prompted in an interactive manner to provide certain details surrounding the circumstances under which the fine was received. Thereafter the chatbot lawyer seeks a legal bases upon which to file an appeal against the fine. For example, it could be that there were no signs reflecting that it was illegal to park in a particular manner. Having provided the necessary information, the user merely presses a button and the appeal is automatically sent off to the authorities. Thus far, DoNotPay is available in London and New York and over a period of 21 months, 250 000 appeals have been submitted of which 160 000 have been successful, reflecting a success rate of 64%. The developer of this chatbot lawyer intends to expand its application to other areas, for example, to help people apply for compensation after experiencing a flight delay, to help HIV sufferers understand their legal rights and to allow foreign refugees to understand their rights according to a new legal system.¹⁴⁴⁹ This example illustrates how far technologies implementing artificial intelligence have progressed. Also, it is an example of how technology can assist the individual by providing knowledge and also by streamlining and automating a certain process. Without such a system, people would probably not realize that there were

1448 Chatbots are defined as, ‘computer programs that mimic conversation with people using artificial intelligence. They can transform the way you interact with the internet from a series of self-initiated tasks to a quasi-conversation’, Wong, Julia Carrie, *What is a chat bot, and how should I be using one?*, The Guardian, available at <https://www.theguardian.com/technology/2016/apr/06/what-is-chat-bot-kik-bot-shop-messaging-platform> (last accessed on 2017-04-24). In Sweden, for example, chatbots are used by IKEA, The Swedish National Tax Board, The Swedish Customs, The Swedish Social Insurance Agency and Scandinavian Airlines, to mention but a few example, see Chatbots.org, *Virtual Agents/Chatbots: In Sweden*, available at <https://www.chatbots.org/country/se> (last accessed on 2017-04-24).

1449 Gibbs, Samuel, *Chatbot Lawyer Overturns 160 000 Parking Tickets in London and New York*, The Guardian, available at <https://www.theguardian.com/technology/2016/jun/28/chatbot-ai-lawyer-donotpay-parking-tickets-london-new-york> (last accessed on 2017-04-22). See also DoNotPay, available at <http://www.donotpay.co.uk/signup.php> (last accessed on 2017-04-22).

legal grounds upon which to contest a decision and make a claim for compensation. In addition, many individuals would probably be put off making a claim for compensation considering the length of time this could take and the effort required. This technology makes the law more accessible and is the epitome of empowerment.

7.3.5 The Law

It is not unreasonable, taking into account the findings of this study, to question the role of law in the face of predictive modelling and like technologies as well as theorise on the form that the law should take. What has become apparent is that the solution to the challenges posed to personal autonomy by technologies such as predictive modelling does not lie only in traditional law. Soft law mechanisms also have a role to play in bringing opposing parties together, and embedding law into technology is also a manner by which to increase the law's effectiveness as a mechanism of control. In certain instances, there may be a role for the direct application of traditional law, that is the black-letter law. In other instances, soft law may be more appropriate, and in certain cases technology may be the solution. It is in this vein that it becomes necessary to recognize the law as a flexible instrument. In some cases, the traditional law will be required to regulate a potential harm, while in other cases, technology will provide the solution, in which case the traditional law will have an indirect role, by regulating the technology that regulates the problem. Consequently, it is argued that there will always be a role for the law to play. What may be challenging initially is the extent to which regulatory instruments, for example technology, soft law or ethics, will also be recognized as law.

Distinguishing between traditional and non-traditional law, challenging the idea that traditional law will always have a role to play in technology regulation is the forecast that society is progressing into the era of autonomic computing, where computer systems will have the following characteristics: self-awareness, self-configuring, self-optimizing, self-healing, self-protecting,

context aware, open and anticipatory.¹⁴⁵⁰ In other words, smart and independent predictive computer systems will be able to predict people's needs and cater to these, working unseen in the background. Here there would be only one regulator, namely, the systems developer, discarding the need for traditional law or even non-traditional law. Contradicting this argument, however, is the fact that we really do not know how the future will be constituted as far as technology is concerned. Reference is made to the fact that the 'hype' surrounding profiling and predictive modelling can be compared with the 'techno-hype' surrounding artificial intelligence (which started in technology circles and was picked up by the media) that never really materialized.¹⁴⁵¹ Considering the uncertainty regarding the speed and direction of technological developments, there remains a role for law in the form of both direct and indirect regulation. In other words, there is no certainty as to how the technology of the future will be constituted. As a result, it is almost impossible to make an exact prognosis as to what the role of the traditional law will be.

There also remains a role for the traditional law to play in terms of making technology accountable. As witnessed above, the GDPR has introduced the new principle of accountability, including the duty to be able to demonstrate accountability. It is argued that there is a regulatory role for the traditional law as far as demanding accountability is concerned. It is in this context that the distinction between different types of predictive models is referred to. Some are more interpretable while others are more independent and less controllable. A possible role of the law is to differentiate between different types of technologies based on different functions that they perform. For example, in determining whether a bank loan will be granted, it could be stipulated that only highly interpretable predictive models be used in order that the outputs can be explained. This is not to outlaw less supervised algorithms for other purposes. However, the law can demand a certain degree of transparency or

1450 Hildebrandt, Mirielle, *Introduction: a Multi Focal View of Human Agency in the Era of Autonomic Computing*, in Hildebrandt, Mirille and Rouvroy, Antoinette, *Law, Human Agency and Autonomic Computing: The Philosophy of Law Meets the Philosophy of Technology*, Routledge, 2011, at pp. 3-5.

1451 Ihde, Don, *Smart? Amsterdam Urinals and Autonomic Computing*, in Hildebrandt, Mirille and Rouvroy, Antoinette, *Law, Human Agency and Autonomic Computing: The Philosophy of Law Meets the Philosophy of Technology*, Routledge, 2011, at pp. 15-16.

supervision in relation to predictive models where the decisions have a large impact on the individual.

7.4 Looking Ahead

Taking a moment to contemplate the future, two aspects are illuminated. First, certain areas are highlighted that are expected to be of interest as far as future research is concerned. Second, some general observations concerning future developments are made taking into account the subject matter of this thesis.

7.4.1 Future Research

In contemplating the relevance of the data protection framework above, reference was made to the notion of pseudonymisation and the fact that this concept will require more precise definition in the future. There are already indications that the research community, in consultation with industry, is initiating research projects in order to determine where the boundaries of pseudonymisation are as anticipated by the GDPR.¹⁴⁵²

Another area within which research is and will continue to be conducted, is in relation to driverless cars. Many of the solutions incorporate algorithms and predictive models, and research, current but also future, will be required to ascertain a number of legal issues in this regard. For example, how will this technology relate to legal notions, such as responsibility, and also incorporate ethical considerations.¹⁴⁵³

Finally, on the technology front, a topic of continued research will be that of the blockchain technology.¹⁴⁵⁴ The blockchain research front is particularly

1452 This is based on the author's own experience.

1453 In this regard, reference is made to initiatives taking place both at a national level in Sweden and on the EU level. For example, see Regeringskansliet, *Stärkt samarbete om självkörande bilar*, available at <http://www.regeringen.se/artiklar/2017/02/starkt-samarbete-om-sjalvkorande-bilar/> (last accessed on 2017-04-15).

1454 SICS, *Rise*, available at <https://www.sics.se/groups/blockchain-innovation-centre> (last accessed on 2017-04-15).

interesting considering all the concrete applications of this technology as well as considering all the academic disciplines that are activated, the law being just one of them.

7.4.2 General Observations

In looking ahead to the future, one cannot resist the temptation of contemplating the effect that the GDPR will have, generally and in the context of predictive modelling. Considering the extent to which the data protection principles as enshrined in the data protection regime have to a large degree been left unchanged, it will be interesting to see how the GDPR is applied to modern digital technologies. Also interesting will be the effect that an increase in fines for not complying with the GDPR (20 000 000 EUR or 4% of global turnover (Art. 83)) will have and how this will alter compliance. In addition, having left the interpretation of certain concepts open to the commercial sector for determination, it will be interesting to view the technical and organizational mechanisms that are developed as well as see how these will be received by the industry.

It is also anticipated that as the publicity surrounding predictive modelling and similar technologies increases, so too will the awareness of its potential harms to individuals. Already now, ideological movements are springing up that have the goal of creating an awareness of the dangers with technologies that are for all intents and purposes ‘black box’ systems. For example, ‘AI Now’ is a multi-disciplinary research initiative that aims to understand the social implications associated with the use of artificial intelligence.¹⁴⁵⁵ As the social implications of these technologies become known, it is quite likely that a backlash from society in general will ensue.¹⁴⁵⁶ This may in turn elicit a

1455 AI Now Initiative, available at <https://artificialintelligencenow.com/> (last accessed on 2017-03-22).

1456 For example, Crawford refers to the scenario where computer scientists at Carnegie Mellon University found that women are less likely to be shown advertisements on Google for higher paid jobs. This in turn begs the question of how a woman would ever know to apply for a job if she never got to see the advertisement? See Crawford, Kate, *Artificial Intelligence’s White Guy Problem*, 25 June, 2016, available at https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html?_r=0 (last accessed on 2016-04-16). See also Spice, Byron, *Questioning the Fairness of Targetting Ads Online*, Carnegie Mellon University, available

response from the political establishment and ultimately the legislator, attempting to diminish the harms from these technologies. Much, however, will depend on the attitude of those developing these ‘black box’ systems in the interim and how they go about addressing public concerns.

A theme throughout this thesis has been the dual nature of technology. Technology has disrupted the relative balance with respect to societal relationships, and technology is and will be part of the solution. It is probably a rather banal observation that the pace at which technology is progressing is not going to slow down. The manner in which technology will be combined with the behavioural sciences in order to provide insight into human behaviour will only become more intrusive. In this regard, reference is made to concepts such as ‘deep learning’, which is a cognitive technology that allows computers to learn by mimicking the processes of the human brain, a technology that is already being applied in mobile phone technologies for the purpose of voice-recognition.¹⁴⁵⁷ At the same time, speculating on the proliferation of ‘black box’ systems in the future, one cannot but realize that technology will also be a major part of any solution.

Future developments are also going to force society to not only re-define many concepts but also be open to new associations between concepts. For example, as the norms regarding the function of identity change, so too will the legal definition of identity be required to adapt. In addition, the interaction between identity and other seemingly unrelated notions will need to be accepted. Bodstrom and Sandberg make the connection between identity and medicine or personalized health. Personalized health in the form of eating healthily is an expression of identity in the same way that enhancement medicine must be seen in terms of the expression of identity. In addition, the fact that medicine is resulting in people living longer will result in people identifying differently with certain age groups.¹⁴⁵⁸ Also, the notion of privacy will change as brain-scanning techniques develop, and the fear of people in this

at <http://www.cmu.edu/news/stories/archives/2015/july/online-ads-research.html> (last accessed on 2017-04-16).

1457 Rubin, Eliran, *Forget About Big Data: Teaching Computers to Think Just Like Humans is the New Big Thing*, Haaretz, restricted source, available at <http://www.haaretz.com/israel-news/business/.premium-1.712140?=&ts=1490874436018> (last accessed on 2017-03-30).

1458 Bodstrom and Sandberg, above n. 474, at p. 5.

regard will result in new conceptions of privacy, for example the notion of ‘neural privacy’.¹⁴⁵⁹

Just as the notion of privacy has been challenged, so too will the notion of identity. It is argued that the digital environment has not only provided people with a platform from which to experiment with identity, but it has also been a catalyst that has resulted in people thinking differently about identity. For example, technology has resulted in people laying more emphasis on external appearances in determining identity, the ‘selfie’ being a typical illustration of this.¹⁴⁶⁰ Another issue is how future technologies are going to influence how we see ourselves. For example, presently technologies such as armbands measure a person’s physical activity, which says something about that person and is relevant in so far as the portrayal of health is an outward manifestation of a person’s identity. It is argued that technologies of the future may measure a human from inside, for example, morally, intellectually and ethically.¹⁴⁶¹ This in turn will surely also influence the manner in which we see ourselves as well as the manner in which we outwardly portray ourselves.

7.5 Final Thoughts

A final consideration contemplates why it is worthwhile to read the approximately 500 pages of this thesis. In other words, what is the point? As mentioned at the beginning of this thesis, the general goal was to find a balance, on the one hand, between embracing the innovation associated with technology, and on the other hand, guarding against the risks that it entails for society. In this regard, this thesis is directed towards individuals as members of society, towards computer scientists and towards lawyers. Individual members of society will be required to attain a certain level of awareness of the existence of certain digital technologies and their accompanying dangers. No solution will be attained without public pressure and no public pressure will materialize without a public awareness of the risks. Computer scientists will also have to become familiar with addressing ethical and legal considerations and not just take the attitude that, ‘if it can be done, then do it!’. Finally, lawyers will have

1459 Ibid.

1460 Gärdenfors, Peter, *Den svåra konsten att se sig själv*, Natur och Kultur, 2017, at p. 9.

1461 Ibid, at p. 153.

to realize that technological phenomena of a digital nature are going to seep into all areas of law. This will place demands on lawyers to have technical skills but also require them to think differently regarding the function of the law.

We are at a crossroads and as society's reliance on decision-making systems increases, we are going to be required to consider what type of society we want. This thesis is a 'shot across the bow'. It is a warning to take heed of the dangers associated with technology before it is too late.

Swedish Summary

Tekniken prediktiv modellering är ett kraftfullt verktyg som företag alltmer använder för att identifiera risker och möjligheter. Men det kan också orsaka skador för individer, särskilt relaterade till deras personliga autonomi. Prediktiv modellering bygger på statistik, matematik, maskininlärning och artificiell intelligens. Algoritmer identifierar mönster i data som människor inte kan se. Den kunskapen infogas sedan i datoriserade modeller och tillämpas i nya situationer och sammanhang. Modellerna känner igen och förutsäger människors agerande, och öppnar därmed för möjligheten att påverka mänskligt beteende.

Ett centralt begrepp i sammanhanget är "big data" som betecknar de datamängder som blir tillgängliga genom att enskilda användare tillbringar en allt större del av sin tid uppkopplade mot nätet, till exempel för att använda sociala medier. Källorna som skapar "big data" är heterogena, och data kan vara statistisk och strukturerad eller dynamisk och flyktig. Ju mer data som finns tillgängligt, desto större är träffsäkerheten i prediktionerna. Detta har lett till att kommersiella aktörer samlar in data om och övervakar enskilda personer i tilltagande omfattning. Enskild användning av uppkopplad teknik lämnar digitala spår. Detta genererar vad som kan kallas en "digital identitet", en databaserad representation som kan användas som substitut för individen.

Prediktiva modeller förs i ökande grad in i beslutssystem för att påverka överväganden och beslut. De kan bland annat föreslå musikval, presentera urval av nyhetsflöden och individualisera sökresultat. De kan exempelvis också föreslå passande partner och indikera arbeten som är lämpliga att söka eller utfärda kreditvärdighetsomdömen och sjukdomsdiagnoser, allt baserat på analys av ackumulerade datasamlingar.

Att använda prediktiva modeller för att hitta affärsmässiga risker kan orsaka skador på olika nivåer för individer. Avhandlingen analyserar ett urval av sådana potentiella skador för att ge en översikt av skadornas karaktär, särskilt i en digital miljö. Vissa av dessa skador är välkända och behandlas i befintlig lagstiftning, medan andra inte har reglerats eller uppmärksamats tidigare. De potentiella skador som tas upp i avhandlingen är integritetskränkning,

förlust av anseende och värdighet, diskriminering, självzensur, avindividualisering, stereotypisering, förlust av rättshandlingsförmåga och förlust av identitet. En gemensam nämnare är skadornas negativa effekter för personlig autonomi.

Avhandlingen undersöker vidare i vilken omfattning den europeiska dataskyddslagstiftningen kan relateras till personlig autonomi och prediktiv modellering. Prediktiva modeller granskas utifrån deras förenlighet med de mänskliga rättigheterna, som dessa är reglerade i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (EKMR) och genom avgöranden av Europadomstolen för mänskliga rättigheter (Europadomstolen).

Genomgången av de befintliga regelverken visar att prediktiv modellering som teknik är oreglerad och att regelverket för dataskydd vilar på principer som inte är samstämmiga med dagens tekniklösningar. Europadomstolen använder visserligen begreppet personlig autonomi och tillämpar en tolkningsmodell som tillåter reglering av tekniker som ännu inte utvecklats då regelverket trädde i kraft, och några av Europadomstolens avgöranden kan även analogt tillämpas på prediktiv modellering. Men slutsatsen är att de befintliga juridiska instrumenten överlag uppvisar avsevärda tillkortakommanden, inte minst vad gäller materialets komplexitet och vaghet.

Avhandlingens avslutande del presenterar en strategi för att stärka individers kontrollmöjligheter ("empowerment"). Den inkluderar befintlig och traditionell lagstiftning, soft law, tekniska lösningar och en rad andra mekanismer som kan användas för att hantera frågor om ansvar, kunskapsspridning, datahantering, informationsbalans och transparens. Finns det ett sätt att stärka det mänskliga värdet samtidigt som prediktiv modellering fortsätter att utvecklas?

Table of Cases

European Court of Human Rights (ECtHR)

- Amann v. Switzerland (2000) 30 EHRR 843.
- Bensaid v. United Kingdom, (2001) 33 EHRR 205.
- Copland v. United Kingdom (2007) 45 EHRR 37.
- Gaskin v. United Kingdom (1990) 12 EHRR 36.
- Guerra v. Italy (1998) 26 EHRR 357.
- Halford v. United Kingdom, (1997) 24 EHRR 523.
- Handyside v. United Kingdom (1979-80) 1 EHRR 737.
- Kahn v. United Kingdom (2000) 31 EHRR 1016.
- Klass v. Germany (1979-80) 2 EHRR 214.
- Konstantin Markin v. Russia, (Application No. 30078/06), 7 October 2010.
- Kopp v. Switzerland (1998) 27 EHRR 93.
- Leander v. Sweden (1987) 9 EHRR 433.
- Malone v. United Kingdom (1985) 7 EHRR 14.
- Marckx v. Belgium (1979-80) 2 EHRR 330.
- Niemietz v. Germany (1992) 16 EHRR 97.
- Odièvre v. France, (2004) 38 EHRR 871.
- PG and JH v. United Kingdom (2008) 46 EHRR 51.
- Peck v. United Kingdom (2003) 36 EHRR 41.
- Perry v. United Kingdom (2004) 39 EHRR 3.
- Pretty v. United Kingdom (2002) 35 EHRR 1.
- Rees v. United Kingdom, (1987) 9 EHRR 56.
- Roman Zakharov v. Russia, (App. 47143/06), 4 December 2015.
- Rotaru v. Romania, (App. No. 28341/95) (unreported), 4 May, 2000.
- S and Marper v. United Kingdom (2009) 48 EHRR 50.

Silver and Others v. United Kingdom (1983) 5 EHRR 347.
Segerstedt-Wiberg v. Sweden (2007) 44 EHRR 2.
Von Hannover v. Germany (2005) 40 EHRR 1.
Von Hannover v. Germany (No. 2) (2012) 55 EHRR 15.
X v. Iceland (Application no. 6825/74), Commission Decision, 18 May 1976.
Weber and Saravia v. Germany (2008) 46 EHRR SE5.
Young, James and Webster v. United Kingdom (1982) 4 EHRR 38.
Z v. Finland (1998) 25 EHRR 371.

Court of Justice of the European Union (CJEU)

Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, joined cases C-293/12 and C-594/12, EU:C:2014:238.
Erich Stauder v. Stadt of Ulm, Sozialamt, Case 29/69, EU:C:1969:57.
Flaminio Costa v. E.N.E.L, case 6/64, EU:C:1964:66.
Internationale Handelsgesellschaft mbH v. Einfuhr- und Vorratsstelle für Getreide und Futtermittel, Case 11/70, EU:C:1970:114.
Maximilian Schrems v. Data Protection Commissioner, C-362/14, EU:C:2015:650.
National Panasonic v. Commission of the European Communities, Case 136/79, EU:C:1980:169.
NV Algemene Transport- en Expeditie Onderneming van Gend & Loos v. Netherlands Inland Revenue Administration, Case 26/62, EU:C:1963:1.
Nold KG v. Commission, Case 4/73, EU:C:1974:51.
Productores de Música de España (Promusicae) v. Telefónica de España, C-275/06, EU:C:2008:54.
Roland Rutili v. Ministre de l'intérieur, Case 36/75, EU:C:1975:137.
Rechnungshof v. Österreichischer Rundfunk and Others, Joint Affairs C-465/00, C-138/01 and C-139/01.
Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others, Joined cases, C-203/15 and C698/15, EU:C:2016:970.
YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M and S, Joined cases C-141/12 and C-372/12, EU:C:2014:2081.
Åklagaren v. Hans Åkerberg Fransson, Case C-617/10, EU:C:2013:280.

Österreichischer Rundfunk and Others, C-465/00, Joined cases C-465/00, C-138/01 and C-139/01, EU:C:2003:294.

United States

Katz v. United States 389 US 347 (1967) 389 US 347 (1967).

Griswold v. Connecticut, 281 US 479, 493 (1965).

Meinhard v. Salmon 164 N.E. 545, 546 (N.Y.1928).

Price Waterhouse v. Hopkins, 490 U.S. 228 (1989).

Roper v. Simmons 543 US 551 (2005).

Slack v. Havens, 522, F.2d 1091, 1091-93 (9th Cir. 1975).

Sorrell v. IMS Health Inc., 564 U.S. 552 (2011).

Canada

Frame v. Smith (1987), 42 D.L.R. (4th) 81.

Hodgkinson v. Simms (1984), 117 D.L.R. (4th) 161.

United Kingdom

Hedley Byrne & Company Limited v. Heller & Partners Limited [1964] AC 465 (HL).

Netherlands

Coeriel and Aurik v. the Netherlands, Communication No. 453/1991, U.N. Doc. CCPR/C/52/D/453/1991 (1994).

Table of Statutes, Conventions and Preparatory Works

European Union

Directive 95/46 of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995, L 281/31.

Charter of Fundamental Rights of the European Union, 18 December 2000, OJ C 364/01 and [2010] OJ C83/389.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201/37.

Directive 2006/24/EC of the European Parliament and the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of public available electronic communications services or of public communication networks and amending Directive 2002/58/EC, OJ L 105/54-63.

Directive 98/44/EC of the European Parliament and of the Council of 6 July 1998 on the Legal Protection of Biotechnological Inventions, OJ L 213, 30.7.1998.

Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive').

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016.

Consolidated version of the Treaty on European Union, 26 October 2012, 2012 OJ C 326.

Consolidated version of the Treaty on the Functioning of the European Union, 26 October 2012, 2012 OJ C 326.

Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, OJ L 180, 19.7.2000.

Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast), OJ L 204, 26.7.2006.

Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services, OJ L 373, 21.12.2004.

Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation. OJ L 303, 2.12.2000.

Opinion 2/13 of 18 December 2014, EU:C:2014:2454.

Council of Europe

European Convention for the Protection of Human Rights and Fundamental Freedoms, adopted 4 November 1950 as amended by Protocols No. 11, CETS 005.

Convention for the Protection of Individuals with Regard to Automatic Processing of personal Data, 28 January 1981, CETS No. 108.

Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows (open for signature 8 November 2001, in force 1 July 2004, ETS 181).

Council of Europe, Committee of Ministers, Recommendation R (87) 15 of the Committee of Ministers to Member States Regulating the Use of Personal Data in the Police Sector.

Council of Europe, Consultative Committee of the Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, Guidelines on the Protection of Individuals With Regard to the Processing of Personal Data in a World of Big Data, Strasbourg, 23 January, 2017.

Recommendation of the Council concerning Guidelines governing the protection of Privacy and Transborder Flows of Personal Data (adopted 23 September 1980; (C(80) 58/FINAL).

Recommendation of the Council concerning Guidelines governing the protection of Privacy and Transborder Flows of Personal Data (Adopted 11 July 2013; (C(2013)79).

Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, Adopted by the Committee of Ministers on 23 November, 2010, available at <https://wcd.coe.int/View-Doc.jsp?id=1710949> (last accessed on 2016-03-04).

United Nations

Universal Declaration of Human Rights, G.A. Res. 217A, at 58, U.N. GAOR, 3rd Sess., 1st plen. Mtg., U.N. Doc A/810 (12 December 1948).

International Covenant on Civil and Political Rights, G.A. Res. 2200 (XXI) A, 21 U.N. Doc. A/6316 at 52 (16 December 1966).

International Covenant on Economic, Social and Cultural Rights, G.A. Res. 2200 (XXI) A, 21 UnN. Doc. A/6316 at 49 (16 December 1966).

Communiqué of the Ministerial Round Table, *Towards Knowledge Societies*, organized during the 32nd session of the General Conference of UNESCO, Paris, 9–10 October 2003 (document 32 C/INF. 26, para. 3).

World Summit on the Information Society Declaration of Principles, 12 December, 2003, available at <http://www.itu.int/net/wsis/docs/geneva/official/dop.html> (last accessed on 2016-10-05).

United Nations Human Rights Office of the High Commissioner, *Guiding Principles on Business and Human Rights*, available at http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf (last accessed on 2016-09-21).

OECD

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980).

Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (adopted 23 September 1980; (C (80)58/FINAL as amended on 11 July 2013 by C (2013)79).

OECD Report, Participative Web: User-created Content, DSTI/ICCP/IE(2006)7/FINAL, 12th April 2007 at page 4 available at <http://www.oecd.org/sti/38393115.pdf> (last accessed 2015-01-01).

OECD (2011), *OECD Guidelines for Multinational Enterprises*, OECD Publishing, available at <http://dx.doi.org/10.1787/9789264115415-en> (last accessed on 2016-09-20).

Seoul Declaration for the Future of the Internet Economy (18 June 2008; C (2008)99).

United States

US Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Persona; Data Systems, *Records, Computers, and the Rights of Citizens* (Washington D.C.: Government Printing Office, 1993).

HEW Secretary's Advisory Committee on Automated Personal Data Systems at p. 61 in Report accompanying s3418 submitted by Mr. Erwin from the Committee on Government Operations, available at <http://babel.hathitrust.org/cgi/pt?id=mdp.39015077945395;view=1up;seq=25> (last accessed on 2016-04-21) at p. 38.

Project SEARCH, Committee on Security and Privacy, Technical Report No. 2, July 1970, p. 28 in Report accompanying s3418 submitted by Mr. Erwin from the Committee on Government Operations, available at <http://babel.hathitrust.org/cgi/pt?id=mdp.39015077945395;view=1up;seq=25> (last accessed on 2016-04-21).

California Legislative Information, *AB-1291 Privacy: Right to Know Act of 2013: disclosure of a customer's personal information*, available at http://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB1291 (last accessed on 2016-03-22).

United States Congress Senate committee on Gogernment Operations, *Legislative History of the Privacy Act of 1974 S.3418*, available at http://www.loc.gov/frd/Military_Law/pdf/LH_privacy_act-1974.pdf (last accessed on 2017-04-04).

United Kingdom

Younger Committee, Report of the Committee on Privacy, Home Office, London: HMSO, 1973 available at <http://hansard.millbanksystems.com/lords/1973/jun/06/privacy-younger-committees-report> (last accessed 2017-03-05).

Germany

BVerfGE 45, 187, 229 (1997).

Sweden

Datalagen (1973:289) (Swedish Data Act 1973:289).

Personuppgiftslag (1998:204) (Personal Data Act (1998:204)).

Lag (15:218) om avtal och andra rättshandlingar på förmögenhetsrättens område (The Contracts Act).

Prop. 1978/79:67 Förslag om lag till ändring i föräldrabalken.

Swedish Government Official Reports, SOU 2002:112, *Law and Information Technology: Swedish Views*, Peter Seipel (ed.), Information and Communication Technology Commission Report, Stockholm, 2002.

Swedish Government Official Reports, SOU 2016:41, *Hur står det till med den personliga integriteten? – en kartläggning av Integritetskommittén*, Delbetänkande av Integritetskommittén, Stockholm, 2016.

Översyn av personuppgiftslagen, Regerings proposition 2005/06:173.

Temarapport 2016:1 från Digitaliseringskommissionen (N2012:04), *Det datadrivna samhället*, Stockholm, 2014.

Australia

Australian Law Reform Commission, *For Your Information, Australian Privacy Law and Practice (ALCR Report 108)*, at <http://www.alrc.gov.au/publications/your-information-australian-privacy-law-and-practice-alrc-report-108/terms-reference>, Chapter 67, *Children, Young People and Attitudes Towards Privacy*, available at <http://www.alrc.gov.au/publications/67.%20Children%2C%20Young%20People%20and%20%20Attitudes%20to%20Privacy/online-social-networking>

European Commission

- European Commission, Commission Staff Working Document Public Consultation, *Towards a Coherent European Approach to Collective Redress*, Brussels, 4 February 2011
- European Commission, *Daily News*, 11th June 2013, available at http://europa.eu/rapid/press-release_MEX-13-0611_en.htm (last accessed on 2016-04-15).
- European Commission, *Commission recommends Member States to have collective redress mechanisms in place to ensure effective access to justice*, Press Release, 11 June 2013, available at http://europa.eu/rapid/press-release_IP-13-524_en.htm (last accessed on 2016-04-15).
- European Commission, *Commission Staff Working Document Public Consultation, Towards a Coherent European Approach to Collective Redress*, Brussels, 4th February, 2011, SEC(2011)173 final, available at http://ec.europa.eu/justice/news/consulting_public/0054/ConsultationpaperCollectiveredress4February2011.pdf (last accessed on 2016-04-19).
- European Commission, Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Towards a European Horizontal Framework for Collective Redress*, available at http://ec.europa.eu/consumers/archive/redress_cons/docs/com_2013_401_en.pdf (last accessed on 2016-04-18).
- European Parliament, Directorate-General for External Policies, Policy Department, Workshop, *Dual Use Export Controls*, 2015, available at [http://www.europarl.europa.eu/RegData/etudes/STUD/2015/535000/EXPO_STU\(2015\)535000_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2015/535000/EXPO_STU(2015)535000_EN.pdf) (last accessed 2016-03-18).
- European Commission, *Unfair Commercial Practices Directive*, available at http://ec.europa.eu/consumers/consumer_rights/unfair-trade/unfair-practices/index_en.htm (last accessed on 2016-01-13).
- European Commission, Resource Efficiency and Fiduciary Duties of Investors, available at http://ec.europa.eu/environment/enveco/resource_efficiency/pdf/FiduciaryDuties.pdf (last accessed on 2016-03-22).
- European Commission, *Public Consultation on Building the European Data Economy*, available at <https://ec.europa.eu/digital-single-market/en/news/public-consultation-building-european-data-economy> (last accessed on 2017-03-30).
- European Commission, *Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*, {COM(2017) final}, Brussels, 10.1.2017, SWD(2017) 2 final, available at <https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy> (last accessed on 2017-03-30).

- European Commission, *Protection Privacy and Fighting Spam*, Information, Society and Media Fact Sheet, available at http://ec.europa.eu/information_society/doc/factsheets/024-privacy-and-spam-en.pdf (last accessed on 2017-04-04).
- European Commission, Communication from the Commission of 22 January 2004 on unsolicited commercial communications or 'spam' [COM(2004) 28 final.
- European Commission, *Safer Internet Programme 2005-2008* (Safer Internet Plus), Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks.
- European Commission, Commission Communication on the Protection of Individuals in Relation to the Processing of Personal Data in the Community and Information Security, COM (90) 314, final, 13 September 1990, available at <http://aei.pitt.edu/3768/1/3768.pdf> (last accessed on 2016-02-17).
- Commission of the European Communities, *First Report on the Implementation of the Data Protection Directive (95/46/EC)*, (COM (2003) 265), Brussels, 15 May 2003, at p. 3, available at <http://eur-lex.europa.eu/LexUriServ/LexUriSrvdo?uri=COM:2003:0265:FIN:EN:PDF> (last accessed on 2016-02-17).
- Communication from the Commission to the European Parliament, Council, The Economic and Social Committee and the Committee of the Regions – Consumer Policy Strategy 2002-2006, COM (2002)0208 final, OJ C 137, 8.6.2002.
- Communication from the Commission to the Council, the European Parliament and the European Economic and Social Committee – EU Consumer Policy Strategy 2007-2013 – *Empowering consumers, enhancing their welfare, effectively protecting them* {SEC (2007) 321} {SEC (2007)322} {SEC (2007)323},/* COM/2007/0099 final */.
- Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – *Consumer Policy Strategy 2002-2006*, COM (2002)0208 final, OJ C 137, 8.6.2002.
- Communication from the Commission to the European Parliament, the Council, the economic and Social Committee and the Committee of the Regions, Single Market Act, *Twelve levers to boost growth and strengthen confidence*, COM (2011) 206 final.
- Report from the Commission, *First Report on the Implementation of the Data Protection Directive (95/46/EC)*, Commission document COM(2003) 265 final.

Article 29 Working Party Documents

European Commission, *Article 29 Working Party*, available at http://ec.europa.eu/justice/data-protection/article-29/index_en.htm (last accessed on 2016-05-30).

Article 29 Data Protection Working Party, *Opinion 3/2010 on the principle of accountability*, adopted on 13 July, 2010 available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf (last accessed on 2016-04-06).

Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, Adopted on 20th June.

Article 29 Data Protection Working Party, *The Future of Privacy*, Adopted on 1 December 2009, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf (last accessed on 2016-04-06).

Other

Asia-Pacific Economic Cooperation, *privacy Framework*, 2005, available at http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx (last accessed on 2016-04-08).

European Parliament Resolution of 2 February 2012, *Towards a Coherent European Approach to Collective Redress*, available at <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2012-0021+0+DOC+XML+V0//EN> (last accessed on 2016-04-19).

The Madrid Resolution, *International Standards on the Protection of Personal Data and Privacy*, International Conference of Data Protection and Privacy Commissioners, 3 November 2009, Madrid, Spain, available at http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf (last accessed on 2016-04-08).

Office of the Privacy Commissioner of Canada, *The Age of Predictive Analytics: From Patterns to Predictions*, Report Prepared by the Research Group of The Office of the Privacy Commissioner of Canada, August 2012.

Court of Justice of the European Union, Press Release No. 117/15, Luxembourg, October, 2015, available at <http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf> (last accessed on 2017-03-08).

Bibliography

Books

- Aarts, E., and Marzano, S., (eds.), *The New Everyday. Views on Ambient Intelligence*, 010 Publishers, 2003.
- Altman, Irvin, *The Environment and Social Behavior: Privacy, Personal Space, Territory and Crowding*, CA:Brooks/Cole Pub. Co., Inc, 1975.
- Andersson, Helene, *Dawn Raids under Challenge: A Study of the European Commission's Dawn Raid Practices in Competition Cases from a Fundamental Rights Perspective*, Doctoral Thesis in European Law at Stockholm University, Sweden, 2017, available at <http://su.diva-portal.org/smash/rec-ord.jsf?pid=diva2%3A1051228&dswid=-805> (last accessed on 2017-04-07).
- Barrat, James, *Our Final Invention: Artificial Intelligence and the End of the Human Era*, Thomas Dunne Books, 2013.
- Bari, Anasse, Chaouchi, Mohamed and Jung, Tommy, *Predictive Analytics for Dummies*, John Wiley and Sons Inc., 2014.
- Belley, Jean-Guy, *The Protection of Human Dignity in Contemporary Legal Pluralism*, Springer Science and Business Media, 2013.
- Bennett, Colin J., Haggerty, Kevin D., Lyon, David and Steeves, Valerie, *Transparent Lives: Surveillance in Canada*, Athabasca University Press, 2014.
- Bentham, Jeremy, *An Introduction to the Principles of Morals and Legislation*, Hafner Publishing Company, Darien Conn. 1970 (first printed in 1780 and first published in 1789. A new edition corrected by the author was published in 1823, Oxford at the Clarendon Press).
- Black, Edwin, *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation*, Crown Books, 2001.
- Brand, A. Wiley, *Predictive Analytics for Dummies*, John Wiley and Sons, Inc., 2014.
- Brenner, Susan W., *Law in an Era of "Smart" Technology*, Oxford Scholarship Online, 2007.
- Brin, David, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom*, Basic Books, 1998.

- Bring, Ove, Mahmoudi, Said and Wrangé, Pål, *Sverige och folkrätten*, fourth edition, Norstedts, Juridik, 2011.
- Brouwer, Evelien, *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*, Martinus Nijhoff Publishers, 2008.
- Brownlie, Ian, *Principles of Public International Law*, seventh edition, Oxford University Press, 2008.
- Brownsword, Roger and Goodwin, Morag, *Law and the Technologies of the Twenty-First Century*, Cambridge University Press, 2012.
- Bygrave, Lee, A., *Data Privacy Law: An International Perspective*, Oxford University Press, 2014.
- Bygrave, Lee, A., *Data Protection Law: Approaching Its Rationale, Logic and Limits*, Kluwer Law International, 2002.
- Bylund, Markus, *Personlig integritet på nätet*, första upplaga, Fores, 2013.
- Cahn, Steven M. and Markie, Peter, *Ethics: History, Theory and Contemporary Issues*, sixth edition, Oxford University Press, 2016.
- Calhoun, Craig, *Critical Social Theory: Culture, History, and the Challenge of Difference*, Blackwell, 1995.
- Campbell, Colton C. and Stack Jr., John F (eds.), *Congress and the Politics of Emerging Rights*, Rowman and Littlefield, 2001.
- Chaiken, Shelly and Trope, Yaacov (eds.), *Preface in Dual-Process Theories in Social Psychology*, The Guilford Press, 1999.
- Chruchill, Winston S., *The Second World War, Volume V, Closing the Ring*, Cassell & Co, 1952.
- Clapham, Andrew, *Human Rights Obligations of Non-State Actors*, Oxford University Press, 2006.
- Cohen, Julie E., *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*, Yale University Press, 2012.
- Cover, Rob, *Digital Identities: Creating and Communicating the Online Self*, Elsevier, 2016.
- Custers, Bart, Calders, Toon, Schermer, Bart and Zarsky, Tal (eds.), *Discrimination and Privacy in the Information Society – Data Mining and Profiling in Large Databases*, Springer, 2013.
- Dahlin, Moa Kindström, *Psykiatrirätt: Intressen, rättigheter och principer*, Jure, 2014.
- Danielsen, Andreas, *Hederskriget: hur Österrike-Ungern startade första världskriget*, Atlantis, 2014.
- DeLanda, Manuel, *War in the Age of Intelligent Machines*, Swerve Editions, 1991.

- De Latil, Pierre, *Thinking by Machine: A Study of Cybernetics*, Houghton Mifflin Company Boston, (translated by Golla, Y. M.), 1957.
- Dick, Philip K., *Minority Report*, Gollancz, 2012.
- Dixon, Martin, *Textbook on International Law*, sixth edition, Oxford University Press, 2007.
- Duhigg, Charles, *Habit: Why We Do What We Do in Life and Business*, Random House Trade Paperback Edition, 2012.
- Dworkin, G., *The Theory and Practice of Autonomy*, first edition, Cambridge, Cambridge University Press, 1988.
- Edvardsson, Tobias, Frydinger, David, *Molntjänster – Juridik, Affär och säkerhet*, Norstedts Juridik, 2013.
- Ericson, Richard V., and Haggerty, Kevin D., *Policing the Risk Society*, Oxford University Press, 1997.
- European Union Agency for Fundamental Rights, Council of Europe, *Handbook on European Data Protection Law*, 2014.
- Finkelstein, Michael O., and Levin, Bruce, *Statistics for Lawyers*, Springer-Verlag, 1990.
- Finlay, Steven, *Predictive Analytics, Data Mining, and Big Data: Myths, Misconceptions and Methods*, Palgrave Macmillan, 2014.
- Foucault, Michel, *Discipline and Punish: The Birth of the Prison* (Alan Sheridan trans.), Peregrine Books, 1977, reprinted in Penguin Books, 1991.
- Gandy, Oscar H., Jr., *The Panoptic Sort: A Political Economy of Personal Information*, Westview Press, 1993.
- Greenstein, Stanley (ed.), *Vem reglerar informationssamhället?*, Nordic Yearbook of Law and Informatics, 2006-2008, Jure, 2010.
- Greenwald, Glenn, *No Place to Hide*, Picador, 2014.
- Greer, Steven, *Europe*, in Moeckli, Daniel, Shah, Sangeeta and Sivakumaran, Sandesh (eds.), *International Human Rights*, Oxford University Press, 2014.
- Gutwirth, Serge, Pouillet, Yves, De Hert, Paul, de Terwangne Cecile and Nouwt, Sjaak, (eds.), *Reinventing Data Protection?*, Springer Science and Media, 2009.
- Gärdenfors, Peter, *Den svåra konsten att se sig själv*, Natur och Kultur, 2017.
- Hart, H. L. A., *The Concept of Law*, third edition., Oxford University Press, 2012.
- Hellstadius, Åsa, *A Quest for Clarity – Reconstructing Standards for the Patent Law Morality Exclusion*, Doctoral Thesis in Civil Law at Stockholm University, Sweden, 2015, available at <http://su.diva-portal.org/smash/rec-ord.jsf?pid=diva2%3A805837&dsid=-6231> (last accessed on 2017-04-07).
- Henrichsen, C., Rytter, J. and Rønsholdt, S., (eds), *Ret, Informatik og Samfund*, DJØF, 2010.

- Hildebrandt, Mireille and Gutwirth, Serge (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer Science and Media, 2008.
- Hildebrandt, Mirille and Rouvroy, Antoinette, *Law, Human Agency and Autonomic Computing: The Philosophy of Law Meets the Philosophy of Technology*, Routledge, 2011.
- Kafka, Franz, *The Trial*, Dover Publications Inc., 2009 (originally published in German, *Der Process*, Verlag Die Schmiede, 1925).
- Kant, Immanuel, *The Metaphysics of Morals*, translated and edited Mary Gregor, Cambridge University Press, 1996 (originally published in German, *Die Metaphysik der Sitten*, 1797).
- Klamberg, Mark, *Evidence in International Criminal Trials: Confronting Legal Gaps and the Reconstruction of Disputed Events*, Martinus Nijhoff Publishers, 2013.
- Klamberg, Mark, *Power and Law in International Society: International Relations as the Sociology of International Law*, Routledge, 2015.
- Klang, Mathias, *Disruptive Technology – Effects of Technology Regulation on Democracy*, Gothenburg Studies in Informatics, Report 36, October, 2006.
- Klausen, Jytte, *The Cartoons that Shook the World*, Yale University Press, 2009.
- Lash, Scott, *Critique of Information*, Sage Publications, 2002.
- Lessig, L., *Code 2.0*, Basic Books, 2006.
- Lenaerts, Koen and Gutiérrez-Fons, José Antonio, *The Place of the Charter in the EU Constitutional Edifice*, in Peers et al. (eds.), *The EU Charter of Fundamental Rights: A Commentary*, Hart Publishing, 2014.
- Lind, Anna-Sara, Reichel, Jane and Österdahl, Inger (eds.), *Information and Law in Transition – Freedom of Speech, the Internet, Privacy and Democracy in the 21st Century*, Liber, 2015.
- Locke, John L., *Eavesdropping: An Intimate History*, Oxford University Press, 2010.
- Lynskey, Orla, *The Foundations of EU Data Protection Law*, Oxford University Press, 2015.
- Lyon, David, *The Electronic Eye: The Rise of Surveillance Society*, Polity press, 1994.
- Lyon, David, *Surveillance Studies: An Overview*, Polity Press, 2007.
- Lyon, David, and Zureik, Elia, *Computers, Surveillance and Privacy*, University of Minnesota Press, 1996.
- Mascalzoni, Deborah (ed.), *Ethics, Law and Governance of Biobanking*, The International Library of Ethics, Law and Technology, Vol. 14, Springer, 2015.
- Magnusson Sjöberg, Cecilia, *Legal Management of Information Systems – Incorporating Law in E-solutions*, Studentlitteratur, 2005.

- Magnusson Sjöberg, Cecilia (red.), *Rättsinformatik*, second edition, Studentlitteratur, 2016.
- Magnusson Sjöberg, Cecilia and Wahlgren, Peter (eds.), *Festskrift till Peter Seipel*, Norstedts Juridik, 2006.
- Manovich, Lev, *The Language of New Media*, MIT Press, 2001.
- Mayer-Schönberger, Viktor and Cukier, Kenneth, *Big Data: A Revolution That Will Transform How We Live, Work and Think*, Mifflin Harcourt Publishing Company, 2013.
- McLuhan, Marshall, *The Gutenberg Galaxy*, University of Toronto Press, 1962.
- Mead, George, H., *Mind, Self and Society from the Standpoint of a Social Behaviourist*, Edited by C. W. Morris, The University of Chicago Press, 1934.
- Meyrowitz, Joshua, *No Sense of Place: The Impact of the Electronic Media on Social Behaviour*, Oxford University Press, 1985.
- Milton, John, *Areopagitica*, Project Gutenberg, 2006, retrieved May 4, 2008, from the website temoa: Open Educational Resources (OER) Portal at <http://www.temoa.info/node/799> (last accessed on 2015-12-10).
- Mill, John Stuart, *On Liberty*, fourth edition, London: Longman, Roberts & Green, 1869; Bartleby.com, 1999. (Originally published in 1859, John W. Parker and Son). Available at www.bartleby.com/130/ (last accessed on 2015-12-10).
- Mitchell, Melanie, *An Introduction to Genetic Algorithms*, Massachusetts Institute of Technology, 1996.
- Moeckli, Daniel, Shah, Sangeeta and Sivakumaran, Sandesh (eds.), *International Human Rights*, second edition, Oxford University Press, 2014.
- Nissenbaum, Helen, *Privacy in Context: Technology, Policy and the Integrity of Social Life*, Stanford University Press, 2009.
- Nørretranders, Tor, *Märk världen: En bok om vetenskap och intuition*, Bonnier Alba, translation by Wahlén, 1991.
- Nussbaum, Martha C., *Creating Capabilities*, The Bellknap Press, 2013.
- O’Neil Cathy, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Crown, 2016.
- Orwell, George, *Nineteen Eighty-Four*, Penguin Books Ltd., 2008.
- Ovey Clare and White, Robin, Jacobs and White, *The European Convention on Human Rights*, Fourth Edition, Oxford University Press, 2006.
- Packard, Vance, *The Naked Society*, IG Publishing, 1964.
- Palfrey, John and Gasser, Urs, *Born Digital. Understanding the First Generation of Digital Natives*, Basic Books, 2008.
- Peers, Steve, Hervey, Tamara, Kenner, Jeff and Ward, Angela (eds.), *The EU Charter of Fundamental Rights: A Commentary*, Hart Publishing, 2014.

- Poster, Mark, *The Mode of Information: Poststructuralism and Social Context*, Polity Press, 1990.
- Postman, Neil, *Technopoly: The Surrender of Culture to Technology*, Vintage Books, 1993.
- Provost, Foster and Fawcett, Tom, *Data Science for Business: What you Need to Know About Data Mining and Data-Analytic Thinking*, O'Reilly Media, 2013.
- Purtova, Nadezhda, *Property Rights in Personal Data: A European Perspective*, Wolters Kluwer, 2012.
- Rannenbergh, Kai, Royer, Denis, Deuker, André (eds.), *The Future of Identity in the Information Society: Challenges and Opportunities*, Springer, 2009.
- Rasmussen, Terje, *Social Theory and Communication Technology*, Ashgate, 2000.
- Raz, Joseph, *The Morality of Freedom*, Oxford Scholarship Online 2003, first publication, 1998.
- Regan, Priscilla M. *Legislating Privacy: Technology, Social Values, and Public Policy*, Chapel Hill, University of North Carolina Press, 1995.
- Ricoeur, Paul, *Oneself As Another*, translated by Blamey K, The University of Chicago Press, 1992 (originally published in French, *Soi-même comme un autre*, Editions du Sueil, 1990).
- Roosendaal, Arnold, *Digital Personae and Profiles in Law – Protecting Individuals' Rights in Online Contexts*, Wolf Legal Publishers, 2013.
- Alfredsson, Gudmundur, Grimheden, Jonas, Ramcharan, Bertrand G. and de Zayas, Alfred (eds.), *International Human Rights Monitoring Mechanisms: Essays in Honour of Jacob Th. Möller*, Brill Academic Publishers, 2009.
- Ruggie, John, *Just Business: Multinational Corporations and Human Rights*, W. W. Norton and Company Ltd., 2013.
- Rule, James B., *Private Lives and Public Surveillance*, Allen Lane, 1973.
- Rule, James B., McAdam Douglas, Stearns Linda and Uglow, David, *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies*, Elsevier, 1980.
- Saarenpää, Ahti and Sztobryn, Karolina, *Lawyers in the Media Society: The Legal Challenges of the Media Society*, University of Lapland, 2016.
- Saldeen, Åke, *Divorce Damages: A Study in the Field of Sociology of Law and Jurimetrics (Skadestånd vid äktenskapsskilnad: En rättssociologisk och jurimetrisk studie)*, Almqvist and Wiksell, 1973.
- Schartum, Dag Wiese (ed.), *Overvåkning i en rettsstat*, Fagbokforlaget, 2010.
- Schauer, Fredrick, *Free Speech*, Cambridge University Press, 1982.
- Schauer, Fredrick, *Profiles, Probabilities and Stereotypes*, Harvard University Press, 2003.

- Schneier, Bruce, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, Norton, 2015.
- Schwartz, Seth J., Luyckx, Koen and Vignoles, Vivian L., (eds.), *Handbook of Identity Theory and Resrearch*, Springer, 2011.
- Schwartz, Barry, *The Paradox of Choice: Why More is Less*, Ecco Press, 2016.
- Schütze, Robert, *European Union Law*, Cambridge University Press, 2015.
- Seipel, Peter, *Juridik och IT*, Norstedts Juridik, 2001.
- Sellers, Mortimer (ed.), *Autonomy in the Law*, Springer, 2008.
- Siegel, Eric, *Predictive Analytics – The Power to Predict Who Will Click, Buy, Lie or Die*, John Wiley and Sons, 2013.
- Simmonds, N.E., *Central Issues in Jurisprudence- Justice, Law and Rights*, Sweet and Maxwell, 2008.
- Slokenberga, Santa, *European Legal Perspectives on Health-Related Direct-to-Consumer Genetic Testing*, Jure, 2016.
- Smith, Rhona K. M., *Textbook on International Human Rights*, sixth edition, Oxford University Press, 2014.
- Solove, Daniel J., *The Future of Reputation – Gossip, Rumor, and Privacy on the Internet*, Yale University Press, 2007.
- Solove, Daniel J., *The Digital Person*, New York University Press, 2004.
- Solove, Daniel J., *Understanding Privacy*, Harvard University Press, 2008.
- Solove, Daniel J. and Schwartz, Paul M., *Information Privacy Law*, Wolters Kluwer, 2011.
- Spaak, Torben, *Guidance and Constraint: The Action-Guiding Capacity of Theories of Legal Reasoning*, Iustus Förlag, 2007.
- Stehr, Nico and Weiler, Bernd (eds.), *Who Owns Knowledge?: Knowledge and the Law*, Transaction Publishers, 2008.
- Sunstein, Cass R. (ed.), *Behavioural Law and Economics*, Cambridge Uniiversity Press, 2000.
- Sunstein, Cass R., *Republic.com*, Princeton University Press, 2001.
- Sunstein, Cass R., *The Ethics of Influence: Government in the Age of Behavioural Science*, Cambridge University Press, 2016.
- Svantesson, Dan Jerker B., *Extraterritoriality in Data Privacy Law*, Ex Tuto Publishing, 2013.
- Svantesson, Dan Jerker B. and Greenstein, Stanley (eds.), *Internationalisation of Law in the Digital Information Society*, Nordic Yearbook of Law and Informatics 2010-2012, Ex Tuto Publishing, 2013.
- Svensk Samhällsvetenskaplig Datatjänst, SSD, *Svenska Databaser I*, Svensk Samhällsvetenskaplig Datatjänst, 1982.

- Thaler, Richard H. and Sunstein, Cass R., *Nudge: Improving Decisions about Health, Wealth and Happiness*, Penguin Books, 2009.
- Trzaskowski, Jan, Savin, Andrej, Lundqvist, Björn and Lindsoug, Patrik, *Introduction to EU Internet Law*, Ex Tuto Publishing, 2015.
- Vouk, Vladimir, Gammerman, Alex, and Shafer, Glenn, *Algorithmic learning in a random world*, Springer, 2005.
- Wahlgren, Peter (ed.), *IT Law*, Scandinavian Studies in Law, Volume 47, Stockholm Institute for Scandinavian Law, 2004.
- Wahlgren, Peter (ed.), *A Proactive Approach*, Scandinavian Studies in Law, Volume 49, Stockholm Institute for Scandinavian Law, 2006.
- Wahlgren, Peter (ed.), *ICT Legal Issues*, Scandinavian Studies in Law, Volume 56, Stockholm Institute for Scandinavian Law, 2010.
- Wahlgren, Peter (ed.), *Soft Law*, Scandinavian Studies in Law, Volume 58, Stockholm Institute for Scandinavian Law, 2013.
- Wahlgren, Peter, *Lagstiftning: rationalitet, teknik, möjligheter*, Jure, 2014.
- Wahlgren, Peter, Warnling-Nerep, Wiweka and Wränge, Pål, *Juridisk skrivguide*, fourth edition, Jure, 2014.
- Wasserstrom, Richard, A., *The Judicial Decision: Toward a Theory of Legal Justification*, Stanford University Press, 1961.
- Westin, Alan F., *Privacy and Freedom*, Atheneum, 1967.
- Wiener, Norbert, *Cybernetics: Or Control and Communication in the Animal and the Machine*, (Hermann & Cie) & Camb. Mass., MIT Press, 1948.
- Williams, Raymond, *Televisions, Technology and Cultural Form*, Fontana, 1974.
- Witten, Ian H., and Frank, Eibe, *Data Mining: Practical Machine Learning Tools and Techniques*, Elsevier, 2005.

Journals and Articles

- Aitamurto, Tanja and Chen, Kaiping, *The value of crowdsourcing in public policy-making: epistemic, democratic and economic value* in Ranchordás Sofia and Voermans, Wim (eds.), *Crowdsourcing Legislation: New Ways of Engaging the Public*, The Theory and Practice of Legislation, Special Issue Vol. 5, Issue 1, 2017.
- Akandji-Kombe, Jean-Francois, *Positive Obligations under the European Convention of Human Rights: A Guide to the Implementation of the European Convention on Human Rights*, Human Rights Handbook, No. 7, Council of Europe, 2007.

- Asp, Petter, *Om relationalistik metod eller spridda anteckningar i jämförande rättsvetenskap*, in *Konsterna att rättsvetenskap - den tysta kunskapen i juridisk forskning*, Asp, Petter och Nuotio, Kimmo (red.), Iustus, 2004.
- Bakardjieva Engelbrekt, Antonina, *Consumer Empowerment in the EU: Weighing the Institutional Alternatives*, Synopsis of research report for SIEPS, 2012, (unpublished).
- Baruch, Jordan J., *Comments*, to Branscomb, Anne Wells, Property Rights in Information, in *Information Technologies and Social Transformation*, Guile, Bruce R. (ed.), National Academy Press, 1985.
- Belley, Jean-Guy, *The Protection of Human Dignity in Contemporary Legal Pluralism*, Springer Science and Business Media, 2013.
- Bennett, Colin, *International Privacy Standards: Can Accountability be Adequate?*, *Privacy Laws and Business International*, Vol. 106, August 2010.
- Blume, Peter, *An Evolving New European Framework for Data Protection*, in Svantesson, Dan Jerker B. and Greenstein, Stanley (eds.), *Internationalisation of Law in the Digital Information Society*, *Nordic Yearbook of Law and Informatics 2010-2012*, Ex Tuto Publishing, 2013.
- Branscomb, Anne Wells, *Property Rights in Information*, in *Information Technologies and Social Transformation*, Guile, Bruce R. (ed.), National Academy Press, 1985.
- Briefing, *Telecoms and Society*, *The Economist*, 28 February, 2015.
- Boehm, Franziska and De Hert, Paul, *Notification, an important safeguard against the improper use of surveillance - finally recognized in case law and EU law*, *European Journal of Law and Technology*, Vol. 3, No. 2, 2012.
- Borenstein, Severin and Rose, Nancy L., *Competition and Price Dispersion in the U.S. Airline Industry*, *Journal of Political Economy*, Vol. 102, No. 4, 1994, available at <http://faculty.haas.berkeley.edu/borenste/download/JPE94Air-Price.pdf> (last accessed on 2016-03-24).
- boyd, danah and Marwick, Alice, *Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies*, Microsoft Research, available at <http://ssrn.com/abstract=1925128> (last accessed on 2014-04-08).
- boyd, danah and Crawford, Kate, *Critical Questions for Big Data*, *Information, Communication and Society*, Vol. 15, Issue 5, 2012, pp. 662-679.
- Boyle, A. E., *Some Reflections on the Relationship of Treaties and Soft Law*, *International and Comparative Law Quarterly*, Vol. 48, 1999 at pp. 901-901.
- Brownsword, Roger, *Red Lights and Rogues: Regulating Human Genetics*, in Somesen, Han (ed.), *The Regulatory Challenge of Biotechnology: Human Genetics, Food and Patents*, Edward Elgar, 2007.
- Brownsword, Roger, *Friends, Romans and Countrymen: Is there a Universal Right to Identity?*, *Law, Innovation and Technology*, 1(2) (2009), 223.

- Bygrave, Lee, *Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, Computer Law and Security Report, Volume 17, 2001, pp. 17-24.
- Bygrave, Lee, *Privacy Protection in a Global Context*, in Wahlgren, Peter (ed.), *IT Law*, Scandinavian Studies in Law, Volume 47, Stockholm Institute for Scandinavian Law, 2004.
- Bygrave, Lee, *Privacy and Data Protection in an International Perspective*, in Wahlgren, Peter (ed.), *ICT Legal Issues*, Scandinavian Studies in Law, Volume 56, Stockholm Institute for Scandinavian Law, 2010.
- Bylund, Markus and Cakici, Baki, *Smart IKT för att bo och arbete i Norra Djurgårdsstaden: Social Concerns in Information Systems for Sustainability*, SICS, 2012, available at <http://smartict.swedishict.se/public/deliverables/Iteration%201.%20May%202012/Social%20Concerns%20in%20Information%20Systems%20for%20Sustainability,%202012-05-14.pdf> (last accessed on 2017-01-14).
- Bylund, Markus, *Datadriven digitalisering – översikt och strukturering*, in Temarapport 2016:1 från Digitaliseringskommissionen (N2012:04), Det datadrivna samhället, Stockholm, 2014.
- Calders, Toon and Zliobaite, Indre, *Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures*, in Custers, Bart et al. (eds.), *Discrimination and Privacy in the Information Society – Data Mining and Profiling in Large Databases*, Springer, 2013.
- Cellan-Jones, Rory, *Questions and Answers: Tim Berners-Lee*, BBC News, available at <http://news.bbc.co.uk/2/hi/technology/7300434.stm> (last accessed on 2014-04-03).
- Chin, Josh, *China's New Tool for Social Control: A Credit Rating for Everything*, The Wall Street Journal, available at <https://www.wsj.com/articles/chinas-new-tool-for-social-control-a-credit-rating-for-everything-1480351590> (last accessed on 2017-02-07).
- Chinkin, C. M., *The Challenge of Soft Law: Development and Change in International Law*, International and Comparative Law Quarterly, Vol. 38, 1989.
- Chinkin, Christine, *Sources* in Moeckli, Daniel, Shah, Sangeeta and Sivakumaran Sandesh (eds.), *International Human Rights*, second edition, 2014.
- Citron, Danielle Keats, *Technological Due Process*, U of Maryland Legal Studies Research Paper No. 2007-26; Washington University Law Review, Vol. 85, pp. 1249-1313, 2007.
- Clark, Roger, *What's Privacy?*, Prepared for a workshop at the Australian Law Reform Commission on 28 July 2006, at <http://www.privacy.org.au/Re-sources/PLawsIntl.html> (last accessed on 2014-05-21).
- Clarke, Roger, *Information Technology and Dataveillance*, November 1987, available at <http://www.rogerclarke.com/DV/CACM88.html> (last accessed on 2016-09-28).

- Centre for Information Policy Leadership, Hunton and Williams LLP, *Data Protection Accountability: The Essential Elements*, October 2009, available at http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf (last accessed on 2016-04-08).
- Cohen Julie E., *What is Privacy For*, Harvard Law Review, volume 126, p. 1904, 2013.
- Cohen, Julie E., *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stanford Law Review, 1373, 1425, 2000.
- Custers, Bart and Calders, Toon, *What is Data Mining and How Does it Work?*, in Custers, Bart et al. (eds.), *Discrimination and Privacy in the Information Society – Data Mining and Profiling in Large Databases*, Springer, 2013.
- Custers, Bart, *Data Dilemmas in the Information Society: Introduction and Overview*, in Custers, Bart et al. (eds.), *Discrimination and Privacy in the Information Society – Data Mining and Profiling in Large Databases*, Springer, 2013.
- Davidov, Dmitry, Tsur, Oren and Rappoport, Ari, *Semi-Supervised Recognition of Sarcastic Sentences in Twitter and Amazon*, Proceedings of the Fourteenth Conference on Computational Natural Language Learning, pages 107–116, Uppsala, Sweden, 15-16 July 2010. © 2010 Association for Computational Linguistics, available at <http://www.aclweb.org/anthology/W10-2914> (last accessed on 2015-05-06).
- De Hert, Paul, *A Right to Identity to Face the Internet of Things?*, available at http://portal.unesco.org/ci/fr/files/25857/12021328273de_Hert-Paul.pdf/de%2BHert-Paul.pdf (last accessed on 2016-03-04).
- De Hert, Paul and Gutwirth, Serge, *Privacy, Data Protection and law enforcement. Opacity of the individuals and transparency of the power*, in *Privacy and the Criminal Law*, Claes, E., et al. (eds.) Interscientia, Antwerpen-Oxford, 2006, p.74 in Rouvroy, Antoinette and Pouillet, Yves, *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy in Gutwirth, S., et al. (eds.), Reinventing Data Protection*, Springer Science and Business Media, 2009.
- De Mulder, Richard V., Van Noortwijk, Kees and Kleve, Pieter, *Knowledge Management for Lawyers: A New School Approach in Vem reglerar informationssamhället?*, in Greenstein, Stanley (ed.), *Nordisk Årsbok i rättsinformatik 2006-2008*, Jure, 2010.
- De Mulder, Richard, Van Noortwijk, Kees and Combrink-Kuiters, Lia, *Jurimetrics Please!*, in Paliwala, Abdul (ed.), *A History of Legal Informatics*, LEFIS Series 9, Prensas Universitarias de Zaragoza, 2010.
- Dent, Chris, and Kenyon, Andrew T., *Defamation Law's Chilling Effect: A Comparative Content Analysis of Australian and US Newspapers*, *Media and Arts Law Review*, Vol. 9, No. 2, pp. 89-112.
- Dauenhauer, Bernard, *Paul Ricoeur*, Stanford Encyclopedia of Philosophy, available at <http://plato.stanford.edu/entries/ricoeur/> (last accessed on 2015-05-29).

- De Mul, Jos, and Van den Berg, Bibi, *Remote Control: Human Autonomy in the Age of Computer-Mediated Agency*, in Hildebrandt, Mirille and Rouvroy, Antoinette, *Law, Human Agency and Autonomic Computing: The Philosophy of Law Meets the Philosophy of Technology*, Routledge, 2011.
- Dworkin, Gerald, *The Younger Committee Report on Privacy*, *The Modern Law Review*, Vol. 36, No. 4, July 1973, pp. 399-406.
- Eckes, Christina, *EU Accession to the ECHR: Between Autonomy and Adaptation*, *The Modern Law Review*, Vol. 76, No. 2, 2013.
- Ellul, Jacques, *The 'autonomy' of the technological phenomenon*, 2003, in Scharff, RC and Dusek V., (eds), *Philosophy of Technology: The Technological Condition*, Malden, Blackwell Publishing Ltd, pp. 386-397.
- Eriksson, Bengt, *Maintaining Information Quality – Experiences from the Swedish Parliament- Sveriges Riksdag*, in Magnusson Sjöberg, Cecilia (ed.), *Legal Management of Information Systems: Incorporating Law in e-Solutions*, Studentlitteratur, 2005.
- Fayyad, Usama, Piatetsky-Shapiro, Gregory and Smythe, Padhraic, *From Data Mining to Knowledge Discovery in Databases*, in American Association for Artificial Intelligence, Fall, 1996, at p. 37, available at <http://www.kdnuggets.com/gpspubs/aimag-kdd-overview-1996-Fayyad.pdf> (last accessed on 2016-09-08).
- Feinberg, Joel, *Autonomy*, in *The Inner Citadel, Essays on Individual Autonomy*, Christman, John (ed.), Oxford University Press, 1989.
- Foresight, Government Office for Science, *Future Identities – Changing Identities in the UK: the Next Ten Years*, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/273968/13-524-future-identities-changing-identities-summary.pdf (last accessed on 2014-09-17).
- Franko Aas, Katja, *From Narrative to Database: Technological Change and Penal Culture*, *Punishment and Society*, Vol. 6 Issue 4, 2004, Sage Journals, available at <http://pun.sagepub.com/content/6/4/379.abstract> (last accessed on 2015-06-02).
- Fung, Archon, *Putting the Public Back into Governance: The Challenges of Citizen Participation and Its Future*, *Public Administration Review*, Vol. 75, Issue 4, 2015.
- Gandy, Oscar H., *Exploring Identity and Identification in Cyberspace*, *Notre Dame Journal of Law, Ethics and Public Policy*, Vol. 14, 2000.
- García, José María Rodríguez, *Scientia Potestas Est – Knowledge is Power: Francis Bacon to Michel Foucault*, *Neohelicon*, Volume 28, Issue 1, January 2001, pp. 109-121.
- Gavison, Ruth, *Privacy and the Limits of the Law*, *Yale Law Journal*, Vol. 89, No. 3, 1980, pp. 421-471.
- Gellert, Raphaël, de Vries, Katja, de Hert, Paul and Gutwirth, Serge, *A Comparative Analysis of Anti-Discrimination and Data Protection Legislation*, in Custers,

- Bart et al. (eds.), *Discrimination and Privacy in the Information Society – Data Mining and Profiling in Large Databases*, Springer, 2013.
- Gertz, Nolen, *Autonomy online: Jacques Ellul and the Facebook emotional manipulation study*, *Research Ethics*, Vol. 12, Issue 1, pp. 55-61 at p. 56.
- Gillum, Jack and Bello, Marisol, *When standardized test scores soared in D. C., were the gains real?* USA Today, March 30, 2011, available at http://usatoday30.usatoday.com/news/education/2011-03-28-1Aschooltesting28_CV_N.htm (last accessed on 2017-02-27).
- Ginner, Viktor and Olsson, Mattias, *Smart teknik vet vad du vill köpa*, Mitt i Nacka, tisdag 13 december, 2011.
- Goldsmith, Andrew J., *Policing's New Visibility*, *British Journal of Criminology*, 50, no. 5, 914-934, 2010.
- Gomez-Arostegui, Tomas, *Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations*, *California Western International Law Journal*, Vol. 35. Number 2, 2005.
- Gordon, Diana, *The Electronic Panopticon: A Case Study of the Development of the National Criminal Records System*, *Politics and Society*, 15(4): 483-511.
- Grauers, Karl, *Gigantisk database hjälpte Trump vinna*, Dagens Etc, 16th December 2016.
- Greenleaf, Graham, *'Modernising' Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?*, *Computer Law and Security Review*, Vol. 29, Issue 4, 2013.
- Gutwirth, Serge and De Hert, Paul, *Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action*, in Gutwirth, Serge et al. (eds.) *Reinventing Data Protection?*, Springer Science and Business Media, 2009.
- Gutwirth, Serge and De Hert, Paul, *Regulating Profiling in a Democratic Constitutional State*, in Hildebrandt, Mireille and Gutwirth, Serge (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer Science and Media, 2008.
- Haggerty, Kevin D., Ericson, Richard V., *The Surveillant Assemblage*, *British Journal of Sociology*, Vol. No. 51, Issue No. 4, December 2000, pp. 605-622.
- Heimer, Carol, A., *Solving the Problem of Trust*, in *Trust in Society*, p. 40, available at https://www.researchgate.net/publication/261707664_Solving_the_Problem_of_Trust (last accessed on 2016-09-28).
- Herz, Zachary R., *Price's Progress: Sex Stereotyping and Its Potential for Antidiscrimination Law*, *The Yale Law Journal*, available at http://www.yalelawjournal.org/pdf/c.396.Herz.446_eou7btj2.pdf (last accessed on 2016-01-21).
- Hildebrandt, Mireille, *Defining Profiling: A New Type of Knowledge*, in Hildebrandt, Mireille and Gutwirth, Serge (eds.), *Profiling the European Citizen*, Springer, 2008.

- Hildebrandt, Mireille, *Profiling and the Identity of the European Citizen*, in Hildebrandt, Mireille and Gutwirth, Serge (eds.), *Profiling the European Citizen*, Springer, 2008.
- Hildebrandt, Mireille, *Who is Profiling Who? Invisible Visibility*, in Gutwirth, S., Poullet, S., de Terwangne C., Nouwt, S., (eds.), *Reinventing Data Protection*, Springer, 2009.
- Hildebrandt, Mireille, *Slaves to Big Data. Or Are We?*, IDP. REVISTA DE INTERNET, DERECHO Y POLÍTICA, Issue 17, October 2013, available at: http://works.bepress.com/mireille_hildebrandt/52 (last accessed on 2017-04-14)
- Hildebrandt, Mireille, *Profiles and Correlatable Humans*, in Stehr, Nico and Weiler, Bernd (ed.), *Who Owns Knowledge?: Knowledge and the Law*, Transaction Publishers, 2008.
- Hildebrandt, Mireille, *Profiling and AmI*, in Rannenber, Kai, Royer, Denis and Deuker, André (eds.), *The Future of Identity in the Information Society – Challenges and Opportunities*, Introduction, Springer, 2009.
- Hildebrandt, Mireille, *Profiling into the Future: An Assessment of Profiling Technologies in the Context of Ambient Intelligence*, in Bus, Jacques et al. (eds.), *Digital Enlightenment Yearbook 2012*, IOS Press, 2012.
- Hollingsworth, Rogers J., *Introduction to Part 3*, in Stehr, Nico and Weiler, Bernd (ed.), *Who Owns Knowledge?: Knowledge and the Law*, Transaction Publishers, 2008 at p. 153.
- Hood, Leroy, *Systems Biology: Integrating Technology, Biology and Computation*, *Mechanisms of Ageing and Development*, 124, 2003, pp. 9-16.
- Hunter, David and Evans, Nicholas, *Facebook Emotional Contagion Experiment Controversy*, *Research Ethics*, vol. 12(1) 2-3, 2016.
- Johansson, Ulf, Boström Henrik and Löfström, Tuve, *Conformal Prediction Using Decision Trees*, 2013 IEEE 13th International Conference on Data Mining, Dallas, TX, pp. 330-339, available at <http://ieeexplore.ieee.org/document/6729517/> (last accessed on 2017-01-30).
- Karlgren, Jussi, *Legal Information Retrieval*, in Magnusson Sjöberg, Cecilia (ed.), *Legal Management of Information Systems – Incorporating Law in E-solutions*, Studentlitteratur, 2005.
- Kerr, Ian R., *The Legal Relationship Between Online Service Providers and Users*, *Canadian Business Law Journal*, Vol. 35, 2001.
- Kilkelly, Ursula, *The Right to Respect for Private and Family Life: A Guide to the Implementation of Article 8 of the European Convention on Human Rights*, *Human Rights Handbook No. 1*, Council of Europe, 2001.
- Kirby, Michael, *The History, Achievement and Future of the 1980 OECD Guidelines on Privacy*, *International Data Privacy Law*, Volume 1, Number 1, February 2011.

- Kranenborg, Herke, *Article 8*, in Peers, Steve, Hervey, Tamara, Kenner, Jeff and Ward, Angela (eds.), *The EU Charter of Fundamental Rights: A Commentary*, Hart Publishing, 2014.
- Kranzberg, Melvin, *Technology and History: 'Kranzberg's Laws'*, *Bull. Sci. Tech. Soc.*, Vol. 15, No. 1, pp 5-13, 1995.
- Klamberg, Mark, *FRA and the European Convention on Human Rights*, in *Overvågning i en rettsstat*, Schartum, Dag Wiese (ed.), Fagbokforlaget, 2010, at p. 96.
- Korhonen, Rauno, *The New Information Code of Finland*, in Saarenpää, Ahti and Sztobryn, Karolina, *Lawyers in the Media Society: The Legal Challenges of the Media Society*, University of Lapland, 2016.
- Krishnamurthy, Balachander and Wills, Craig E., *Privacy Leakage in Mobile Online Social Networks*, *Proceedings of the 3rd Wonference on Online Social Networks*, 2010.
- Kroll, Joshua A., Huey, Joanna, Barocas, Solon, Felten, Edward W., Reidenberg, Joel R., Robinson, David G., and Yu, Harlan, *Accountable Algorithms*, Vol. 165, Issue 3, *University of Pennsylvania Law Review*, p. 633, 2017, available at: http://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3 (last accessed on 2017-04-13).
- Kuner, Christopher, *The 'Internal Morality' of European Data Protection Law*, November 2008, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1443797 (last accessed on 2016-11-22).
- Kuner, Christopher, Cate, Fred H., Millard Christopher and Svantesson, Dan Jerker B., *Editorial*, *International Data Privacy Law*, 2011, Vol. 1, No. 1 at page 1.
- Lessig, Lawrence, *Code is Law: On Liberty in Cyberspace*, *Harvard Magazine*, 2000, available at <http://harvardmagazine.com/2000/01/code-is-law-html> (last accessed on 2016-03-24).
- Leaders, *Planet of the Phones*, *The Economist*, 28 February 2015.
- Lind, Anna-Sara, *LifeGene – a Closed Case?* in Lind, Anna-Sara, Reichel, Jane and Österdahl, Inger (eds.), *Information and Law in Transition – Freedom of Speech, the Internet, Privacy and Democracy in the 21st Century*, Liber, 2015.
- Loevinger, Lee, *Jurimetrics the Next Step Forward*, *Minnesota Law Review*, Vol. 33, No. 5, 1949, at p. 455.
- Lundberg, Johanna, *Användarvillkoren som ingen läser*, *Stiftelsen för internetinfrastruktur*, .SE:s Internetguide nr 35.
- Lundblad, Nicklas, *Privacy in the Noise Society*, in Wahlgren, Peter (ed.), *IT Law, Scandinavian Studies in Law*, Volume 47, *Stockholm Institute for Scandinavian Law*, 2004.
- Marx, Gary T., *A Tack in the Shoe: Neutralizing and Resisting the New Surveillance*, *Journal of Social Issues*, Vol. 59 No.2, 2003, pp. 369- 390.

- Manzerolle, Vincent and Smeltzer, Sandra, *Consumer Databases and the Commercial Mediation of Identity: A Medium Theory Analysis*, Surveillance and Society, 2011, Vol. 8, No. 3, pp. 323-337, at pp. 325-326, available at <http://www.surveillance-and-society.org> (last accessed on 2015-05-13).
- McAdams, Dan P., *The Psychology of Life Stories*, Review of General Psychology, Vol. 5, No. 2, 2001.
- McAdams, Dan P., *Narrative Identity*, in Schwartz, Seth J., Luyckx, Koen and Vignoles, Vivian L., (eds.), *Handbook of Identity Theory and Research*, Springer, 2011.
- Nabeth, Thierry, *Identity of Identity*, in Rannenber, Kai, Royer Denis and Deuker André (eds.), *The Future of Identity in the Information Society – Challenges and Opportunities*, Introduction, Springer, 2009.
- Narayanan, Arvind and Shmatikov, Vitaly, *Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset)*, The University of Texas at Austin, February 5, 2008.
- Neal, David T., Wood, Wendy and Quinn, Jeffrey M., *Habits- A Repeat Performance*, Current Directions in Psychological Science, August 2006, Vol. 15 no. 4, pp 198-202, at p. 198, available at <http://cdp.sagepub.com/content/15/4/198.abstract> (last accessed on 2016-11-25).
- Nissenbaum, Helen, *Privacy as Contextual Integrity*, Washington Law Review, 2004 available at <https://crypto.stanford.edu/portia/papers/Revnissenbaum-DTP31.pdf> (last accessed on 2016-01-19).
- Nissenbaum, Helen, *A Contextual Approach to Privacy Online*, Daedalus, the Journal of the American Academy of Arts & Sciences, 140 (4), 2011, available at http://www.amacad.org/publications/daedalus/11_fall_nissenbaum.pdf (last accessed on 2016-04-11).
- Odlyzko, Andrew, *Privacy, Economics and Price Discrimination on the Internet*, <http://www.dtc.umn.edu/~odlyzko/doc/privacy.economics.pdf>, (last accessed 2013-10-08).
- Ottsjö, Peter, *Kedjan förstärker internet*, Ny Teknik, 30 March, 2017, at p. 4.
- Palen, Leysia, Starbird, Kate, Vieweg, Sarah and Hughes, Amanda, *Twitter-Based Information Distribution During the 2009 Red River Valley Flood Threat*, Bulletin of the American Society for Information Science and Technology, Vol. 36, No. 5, available at <https://pdfs.semanticscholar.org/29aa/e3480fb3b1563d83d600787487e7d8427535.pdf> (last accessed on 2017-03-31).
- Pečarič, Mirko, *Can a group of people be smarter than experts?* in Ranchordás Sofia and Voermans, Wim (eds.), *Crowdsourcing Legislation: New Ways of Engaging the Public*, The Theory and Practice of Legislation, Special Issue Vol. 5, Issue 1, 2017.
- Peczenik, Alexander, *A Theory of Legal Doctrine*, Ratio Juris, Vol. 14, No. 1, March 2001.

- Post, Robert C., *The Social Foundations of Defamation Law: Reputation and the Constitution*, 74 California Law Review, 691, 1986, pp. 691-742.
- Poster, Mark, *Databases as Discourses; or, Electronic Interpellations*, in Lyon, David, and Zureik, Elia, *Computers, Surveillance and Privacy*, University of Minnesota Press, 1996.
- Prins, J. E. J., *The Propertization of Personal Data and Identities*, *Electronic Journal of Comparative Law*, Vol. 8(3), October 2004, available at <http://www.ejcl.org/83/abs83-1.html> (last accessed on 2016-04-26).
- Kaye, Jane, *The Tension between Data Sharing and the Protection of Privacy in Genomics Research*, in Mascalcioni, Deborah (ed.), *Ethics, Law and Governance of Biobanking*, The International Library of Ethics, Law and Technology, Vol. 14, Springer, 2015.
- Ranchordás, Sofia, *Digital agoras: democratic legitimacy, online participation and the case of Uber-petitions*, in Ranchordás Sofia and Voermans, Wim (eds.), *Crowdsourcing Legislation: New Ways of Engaging the Public, The Theory and Practice of Legislation*, Special Issue Vol. 5, Issue 1, 2017.
- Reiman, Jeffery H., *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future*, *Santa Clara High Technology Law Journal*, Volume 11, Issue 1, Article 5, 1995, available at <http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1174&context=chtlj> (last accessed on 2016-04-20).
- Ricoeur, Paul, *Narrative Identity*, *Philosophy Today*, 35:1, Springer, 1991.
- Robins, Kevin and Webster, Frank, *Cybernetic Capitalism: Information, Technology, Everyday life*, in Mosco, Vincent and Wasko, Janet, *The Political Economy of Information*, The University of Wisconsin Press, 1988.
- Rogowski, Ralf, *Concluding Observations*, in Stehr, Nico and Weiler, Bernd (ed.), *Who Owns Knowledge?: Knowledge and the Law*, Transaction Publishers, 2008.
- Rosas, Allan, *Fundamental Rights in the EU, with Special Emphasis on the Case-law of the European Court of Justice (Luxembourg)*, in Alfredsson, Gudmundur, Grimheden, Jonas, Ramcharan, Bertrand G. and de Zayas, Alfred (eds.), *International Human Rights Monitoring Mechanisms: Essays in Honour of Jacob Th. Möller*, Brill Academic Publishers, 2009.
- Rouvroy, Antoinette and Pouillet, Yves, *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy* in Gutwirth, S., et al. (eds.), *Reinventing Data Protection?*, Springer Science and Business Media, 2009.
- Schauer, Frederick, *Fear Risk and the First Amendment: Unravelling the 'Chilling Effect'*, 58, *Boston University Law Review*, 685, 693 (1978).
- Schwartz, Paul, M., *Privacy and Democracy in Cyberspace*, 52 *Vanderbilt Law Review*, 1607, 1999, available at <http://scholarship.law.berkeley.edu/fac-pubs/1162> last accessed on 2017-04-14).

- Seipel, Peter, *Law and ICT. The Whole and its Parts*, in Swedish Government Official Reports, SOU 2002:112, Law and Information Technology: Swedish Views, Information and Communication Technology Commission Report, Stockholm, 2002.
- Seipel, Peter, *Access Laws in a Flux*, in Swedish Government Official Reports, SOU 2002:112, Law and Information Technology: Swedish Views, Information and Communication Technology Commission Report, Stockholm, 2002.
- Seipel, Peter, *IT Law in the Framework of Legal Informatics*, in Wahlgren, Peter (ed.), *IT Law*, Scandinavian Studies in Law, Vol. 47, Stockholm Institute for Scandinavian Law, 2004.
- Seipel, Peter, *Legal Informatics Broad and Narrow*, in Magnusson Sjöberg, Cecilia, (ed.), *Legal Management of Information Systems: Incorporating Law in e-solutions*, Studentlitteratur, 2005.
- Seipel, Peter, *Nordic School of Proactive Law Conference, June 2005 Closing Comments*, in Wahlgren, Peter (ed.), *A Proactive Approach*, Scandinavian Studies in Law, Volume 49, Stockholm Institute for Scandinavian Law, 2006.
- Shafer, Glenn and Vovk, Vladimir, *A Tutorial on Conformal Prediction*, *Journal of Machine Learning Research*, 9. 2008, 371-421.
- Simon, Bart, *The return of Panopticism: Supervision, Subjection and the New Surveillance*, *Surveillance and Society* 3(1): 1-20, 2005.
- Shermer, B., *Risks of Profiling and the Limits of Data Protection Law*, in Custers, Bart et al. (eds.), *Discrimination and Privacy in the Information Society – Data Mining and Profiling in Large Databases*, Springer, 2013.
- Shortliffe, Edward H., Davis, Randall, Axline, Stanton G., Buchanan, Bruce G., Green, Cordell C. and Cohen, Stanley N., *Computer-Based Consultations in Clinical Therapeutics: Explanation and Rule Acquisition Capabilities of the MYCIN System*, *Computers and Biomedical Research*, Vol. 8, 303-320, 1975, at pp. 304-305.
- Solve, Daniel, J., *Conceptualizing Privacy*, 90 *California Law Review*, 2002, p. 1087.
- Souza, Carlos Affonso, Steibel, Fabro and Lemos, Ronaldo, *Notes on the creation and impacts of Brazil's Internet Bill of Rights*, in Ranchordás Sofia and Voermans, Wim (eds.), *Crowdsourcing Legislation: New Ways of Engaging the Public*, *The Theory and Practice of Legislation*, Special Issue Vol. 5, Issue 1, 2017.
- Stevens, Robert, *Hedley Byrne v. Heller: Judicial Creativity and Doctrinal Possibility*, *The Modern Law Review*, Vol. 27, No. 2, March 1964, at p. 121.
- Sumner, Chris, Byers, Alison, Boochever, Rachel, Park, Gregory. J., *Predicting Dark Triad Personality Traits from Twitter usage and a Linguistic Analysis of Tweets*, *Proceeding, ICMLA '12 Proceedings of the 2012 11th International Conference on Machine Learning and Applications - Volume 02*, pages 386-393.

- Svantesson, Dan Jerker B., *A Legal Method for Solving Issues of Internet Regulation*, International Journal of Law and Information Technology, Vol. 19, No. 3, Oxford University Press, 2011.
- Svantesson, Dan Jerker B., *A Jurisprudential Justification for Extraterritoriality in (Private) International Law*, 13 Santa Clara Journal of International Law, 2015.
- Svantesson, Dan Jerker B., *Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation*, International Data Privacy Law, Vol. 5, Issue 4, November 2015.
- Svantesson, Dan Jerker B., *The (Uncertain) Future of Online Data Privacy*, Masaryk University Journal of Law and Technology, Vol. 9, Issue 1, 2015, 129-153.
- Scott R. Peppet, *Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security and Consent*, Texas Law Review, (Vol.93:85), 2014, also available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2409074&download=yes (last accessed on 2015-05-06).
- Timmer, Alexandra, *Toward an Anti-Stereotyping Approach for the European Court of Human Rights*, Human Rights Law Review, 11:4, pp. 707-738, Oxford University Press, 2011.
- Trzaskowski, Jan, *EU Law and the Internet*, in Trzaskowski, Jan, Savin, Andrej, Lundqvist Björn and Lindsoug, Patrik, Introduction to EU Internet Law, Ex Tuto Publishing, 2015.
- Van der Sluijs, Jessika, *Soft Law – an International Concept in a National Context*, in Wahlgren, Peter (ed.), Soft Law, Scandinavian Studies in Law, Volume 58, Stockholm Institute for Scandinavian Law, 2013.
- Van der Sloot, Bart, *From Data Minimization to Data Minimummization*, in Custers, Bart et al. (eds.), Discrimination and Privacy in the Information Society – Data Mining and Profiling in Large Databases, Springer, Heidelberg, 2013.
- Vedder, Anton, *KDD: The Challenge to Individualism*, Ethics and Information Technology, 1: 275-281, Kluwer Academic Publishers, Netherlands, 1999.
- Vermeulen, Mathias, *Regulating profiling in the European Data Protection Regulation: An Interim Insight into the Drafting of Article 20*, EMSOC Working Paper, 2013, SSRN, available at <https://ssrn.com/abstract=2382787> or <http://dx.doi.org/10.2139/ssrn.2382787> (last accessed on 2017-03-30).
- Vignoles, Vivian L., Schwartz, Seth J., and Luyckx, Koen, *Introduction: Toward an Integrated View of Identity*, in Schwartz, Seth J., et al. (eds.), Handbook of Identity Theory and Resresearch, Springer, 2011.
- Vlahos, James, *The Department of Pre-Crime*, Scientific American, January, 2012.
- Wahlgren, Peter., *Manipulation: Lagstiftningsteknik eller integritetskränkning?*, in Henrichsen, C., Rytter, J. and Rønsholdt, S., (eds.), *Ret, Informatik og Samfund*, DJØF, 2010.

- Wahlgren, Peter, *Inbyggda lagar*, in Magnusson Sjöberg, Cecilia and Wahlgren, Peter (eds.), *Festskrift till Peter Seipel*, Norstedts Juridik, 2006.
- Warren, Samuel D., Brandeis, Louis D., *The Right to Privacy*, Harvard Law Review, Vol. 4, Number 5, December 1890.
- Wells, Helen and Wills, David, *Individualism and Identity: Resistance to Speed Cameras in the UK*, *Surveillance and Society*, 6(3): 259-274, at p. 259, available at <http://www.surveillance-and-society.org> (last accessed on 2015-05-25).
- Weinberger, David, *The Machine That Would Predict the Future*, Scientific American, December 2011.
- Weinrib, Ernest J., *The Fiduciary Obligation*, University of Toronto Law Journal, Vol. 25. No. 1, 1975. pp. 1-22.
- Wiese Schartum, Dag, *Data Protection: Between Paternalism and Autonomy* in *Festskrift till Peter Seipel*, Norstedts Juridik, Stockholm, 2006.
- Wu, Xiaolin and Xi, Zhang, *Automated Inference on Criminality using Face Images*, 2016, available at <https://arxiv.org/abs/1611.04135> and <https://arxiv.org/pdf/1611.04135.pdf> (last accessed on 2017-03-21).
- Zarsky, Tal Z., 'Mine Your Own Business!': *Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion*, Yale Journal of Law and Technology, 2002-2003.
- Öman, Sören, *Implementing Data Protection in Law*, in Wahlgren, Peter (ed.), *IT Law*, Scandinavian Studies in Law, Volume 47, Stockholm Institute for Scandinavian Law, 2004.
- Öman, Sören, *Trends in Data Protection Law*, in Wahlgren, Peter (ed.), *ICT Legal Issues*, Scandinavian Studies in Law, Volume 56, Stockholm Institute for Scandinavian Law, 2010.
- Öman, Sören, *Protection of Personal Data – But How?*, in *Law and Information Technology: Swedish Views*, Seipel, Peter (ed.), Swedish Government Official Reports, SOU 2002:112, Information and Communication Technology Commission Report, Stockholm, 2002.

Electronic Sources and web pages

- Alexander, Janet C., *An Introduction to Class Action Procedure*, available at <https://www.law.duke.edu/grouplit/papers/classactionalexander.pdf> (last accessed on 2016-04-15).

- AlgorithmWatch, available at <http://algorithmwatch.org/mission-statement/#English> (last accessed on 2016-09-09).
- Andersson, Katarina, *Vad säger våra digitala fotspår?*, Aftonbladet, 2016-04-08, available at <http://www.aftonbladet.se/partnerstudio/digitalalivet/article22525851.ab> (last accessed on 2016-09-08).
- Anderson, Chris, *The End of Theory: The Data Deluge Makes the Scientific Method Obsolete*, Wired, available at <https://www.wired.com/2008/06/pb-theory/> (last accessed on 2017-04-05).
- Angwin, Julian and Valentino-Devries, Jennifer, *Google's iPhone Tracking*, Wall Street Journal, 17 February, 2012, available at <http://online.wsj.com/news/articles/SB10001424052970204880404577225380456599176> (last accessed on 2014-10-01).
- Angwin, Julia, Larson Jeff, Mattu Surya and Kirchner, Lauren, *Machine Bias*, ProPublica, available at <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> (last accessed on 2016-09-09).
- Augur, Hannah, *WTF is a Blockchain? A Guide for Total Beginners*, Dataconomy, available at <http://dataconomy.com/2015/10/wtf-is-the-blockchain-a-guide-for-total-beginners/> (last accessed on 2017-04-04).
- Australian Law Reform Commission, *For Your Information, Australian Privacy Law and Practice (ALCR Report 108)*, at <http://www.alrc.gov.au/publications/your-information-australian-privacy-law-and-practice-alrc-report-108/terms-reference>, Chapter 67, *Children, Young People and Attitudes Towards Privacy*, available at <http://www.alrc.gov.au/publications/67.%20Children%2C%20Young%20People%20and%20%20Attitudes%20to%20Privacy/online-social-networking>, (last accessed on 2017-04-14).
- Ball, Jonathan, Navetta, David and Kleiner, Kris, *British supermarket chain faces group litigation action in the UK based on data breach*, available at <http://www.dataprotectionreport.com/2016/03/british-supermarket-chain-faces-group-litigation-action-in-the-uk-based-on-data-breach/> (last accessed on 2016-14-15).
- BBC, *French parliament adopts DNA bill*, available at <http://news.bbc.co.uk/2/hi/europe/7059186.stm> (last accessed on 2016-02-15).
- BDI, The German Business Representation, *Breakthrough on EU general data protection regulation*, available at <http://english.bdi.eu/article/news/breakthrough-on-eu-general-data-protection-regulation/> (last accessed on 2016-04-18).
- Bellinger, Gene, Castro Duval and Mills, Anthony, *Data, Information, Knowledge and Wisdom*, available at <http://www.systems-thinking.org/dikw/dikw.htm> (last accessed on 2016-04-19).
- Berkow, Ira, *Rower With Muslim Name Is an All-American Suspect*, The New York Times, available at <http://www.nytimes.com/2003/02/21/sports/other-sports/21ROWW.html> (last accessed on 2015-12-03).

- Biddle, Sam, *Troubling Study Says Artificial Intelligence Can Predict Who Will Be Criminals Based on Facial Features*, The Intercept, 18th November 2016, available at <https://theintercept.com/2016/11/18/troubling-study-says-artificial-intelligence-can-predict-who-will-be-criminals-based-on-facial-features/> (last accessed on 2017-03-22).
- Bird and Bird, *Guide to the General Data Protection Regulation*, February 2016, available at <http://www.twobirds.com/~media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en> (last accessed on 2016-04-07).
- Bitcoin, *How does Bitcoin work?* available at <https://bitcoin.org/en/how-it-works> (last accessed on 2017-04-04).
- Bklockchains, *The great chain of being sure about things*, The Economist, available at <http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable> (last accessed on 2017-04-24).
- Blockchain, available at <http://www.investopedia.com/terms/b/blockchain.asp> (last accessed on 2017-04-04).
- Bodstrom, Nick and Sandberg, Anders, *The Future of Identity*, Report Commissioned by the UK's Government Office for Science, 2011, available at <http://www.nickbodstrom.com/views/identity.pdf> (last accessed on 2017-03-27).
- Bonchek, Mark, HBR Blog Network, *Little Data Makes Big Data More Powerful*, 3 May 2013, available at <http://blogs.hbr.org/2013/05/little-data-makes-big-data-mor/> (last accessed on 2017-04-14).
- Brian, Heaton, *Is Crowdsourcing the Future for Legislation?*, Government Technology, available at <http://www.govtech.com/internet/Experts-Predict-More-Legislation-Will-Be-Crowdsourced.html> (last accessed on 2016-04-14).
- Bridle, James, *The algorithm method: how internet dating became everyone's route to a perfect love match*, The Guardian, available at <https://www.theguardian.com/lifeandstyle/2014/feb/09/match-charmony-algorithm-internet-dating> (last accessed on 2016-10-20).
- BRÅ, *The Swedish National Council for Crime Prevention*, available at <http://www.bra.se/bra/bra-in-english/home.html> (last accessed on 2017-01-18).
- Business and Human Rights Resource Centre, *UN Guiding Principles*, available at <https://business-humanrights.org/en/un-guiding-principles> (last accessed on 2016-09-21).
- Cambridge Dictionaries Online, available at <http://dictionary.cambridge.org/dictionary/english/self-censorship> (last accessed on 2015-12-04).
- Cavoukian, Ann, *Privacy by Design: The 7 Foundational Principles*, available at <https://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf> (last accessed on 2016-03-24).

- Cavoukian, Ann, *Privacy by Design*, available at <https://www.ipc.on.ca/images/resources/privacybydesign.pdf> (last accessed on 2016-03-24).
- Centre for Information Policy Leadership, Hunton and Williams LLP, *Data Protection Accountability: The Essential Elements*, October 2009, available at http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf (last accessed on 2016-04-08).
- Chatbots.org, *Virtual Agents/Chatbots: In Sweden*, available at <https://www.chatbots.org/country/se> (last accessed on 2017-04-24).
- Chi, Kelly Rae, *Why are Habits So Hard to Break?*, DukeToday, available at <https://today.duke.edu/2016/01/habits> (last accessed on 2016-11-25).
- Citizens Foundation, available at <http://www.citizens.is/> (last accessed on 2016-04-14).
- Citizens Foundation, available at <http://www.citizens.is/portfolio/better-reykjavik-connects-citizens-and-administration-all-year-round/> (last accessed on 2016-04-14).
- Civic Consulting, *Country-Report Sweden*, available at http://ec.europa.eu/consumers/archive/redress_cons/sv-country-report-final.pdf (last accessed on 2016-04-18).
- Clover, Julian, *Telia-Facebook Move Sparks Swedish Net Neutrality Row*, Broadband TV News, available at <http://www.broadbandtvnews.com/2016/05/03/telia-facebook-move-sparks-swedish-net-neutrality-row/> (last accessed on 2016-05-23).
- Coleman, S., *The Minnesota Income Tax Compliance Experiment State Tax Results*, Minnesota Department of Revenue, 1996, available at http://www.revenue.state.mn.us/research_stats/research_reports/19xx/research_reports_content_complnce.pdf (last accessed on 2015-04-08).
- Compricer, available at <https://www.compricer.se/press/om-compricer/> (last accessed on 2016-02-21).
- Consortium of European Social Science Data Archives (Cessda), available at <https://cessda.net>, (last accessed on 2017-03-31).
- Cook, Philip and Heilmann, Conrad, *Censorship and Two Types of Self-Censorship*, March 20, 2010, SSRN, available at <http://ssrn.com/abstract=1575662> or <http://dx.doi.org/10.2139/ssrn.1575662> (last accessed 2015-12-12).
- Crawford, Kate, *Artificial Intelligence's White Guy Problem*, 25 June, 2016, available at https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html?_r=0 (last accessed on 2016-04-16).
- Custers, Bart, *Effects of Unreliable Group profiling by means of Data Mining*, available at <http://www.wis.win.tue.nl/~tcalders/dadm/data/media/ds-03-custers.pdf> (last accessed on 2016-05-26).
- Daily Crowdsource, *What is Crowdsourcing*, available at <http://dailycrowdsource.com/training/crowdsourcing/what-is-crowdsourcing> (last accessed on 2016-04-13).

- Data and Society, available at <http://datasociety.net/> (last accessed on 2016-09-09).
- Davidson, Brian, *Getting to Know the General Data Protection Regulation, Part 7 – Accountability Principles = More Paperwork*, available at <http://privacylaw.blog.fieldfisher.com/2016/getting-to-know-the-general-data-protection-regulation-part-7-accountability-principles-more-paperwork/> (last accessed on 2016-04-08).
- De Hert, Paul and Cristobal Bocos, Pedro, *Case of Roman Zakharov v. Russia: The Strasbourg follow up to the Luxembourg Court's Schrems judgment*, available at <https://strasbourgobservers.com/2015/12/23/case-of-roman-zakharov-v-russia-the-strasbourg-follow-up-to-the-luxembourg-courts-schrems-judgment/> (last accessed on 2017-03-07).
- DeMoss, Dustin, *Can Crowdsourced Government Happen in the U.S.?*, StackStreet, available at <https://stackstreet.com/can-crowdsourced-government-happen-us/> (last accessed on 2016-04-14).
- Discovery, *DQ-Track Helps Measure Your Driving Ability*, available at <https://www.discovery.co.za/portal/individual/insure-measure-driving> (last accessed on 2016-01-20).
- DoNotPay, available at <http://www.donotpay.co.uk/signup.php> (last accessed on 2017-04-22).
- Doty, Jeffrey S., *What is a Public?*, available at <http://project.makingpublics.org/research/what-do-you-mean/> (last accessed on 2014-04-08).
- Duhigg, Charles, *How Companies Learn Your Secrets*, New York Times, <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?page-wanted=all> (last accessed on 2017-04-14).
- Economist, *Keeping Watch: Digital advertisers battle over online privacy*, 5 November 2016, available at <http://www.economist.com/node/21709584/print> (last accessed on 2016-11-07).
- Edelman, David and Singer, Marc, *The new consumer decision journey*, available at <http://www.mckinsey.com/business-functions/marketing-and-sales/our-insights/the-new-consumer-decision-journey> (last accessed on 2016-05-19).
- Edwards, L., *Study Suggests Reliance on GPS May Reduce Hippocampus Function As We Age*, PhysOrg.Com, available at <http://phys.org/news/2010-11-reliance-gps-hippocampus-function-age.html> (last accessed on 2015-03-20).
- Electronic Frontier Foundation, *About EFF*, available at <https://www.eff.org/about> (last accessed on 2016-04-14).
- Electronic Frontier Foundation, *Surveillance Self-Defence*, available at <https://ssd.eff.org/en/about-surveillance-self-defense> (last accessed on 2016-04-16).
- Electronic Frontier Foundation, *CAPPS II: Government Surveillance via Passenger Profiling*, <https://w2.eff.org/Privacy/cappsii/background.php> (last accessed on 2017-04-14).

- Electronic Frontier Foundation, *Surveillance Self-Defence*, available at <https://ssd EFF.org/en/about-surveillance-self-defense> (last accessed on 2016-04-16).
- Encyclopaedia Britannica, available at <http://global.britannica.com/EB-checked/topic/477822/Procrustes> (last accessed on 2017-04-14).
- Encyclopaedia Britannica, *Categorical Imperative*, available at <https://global.britannica.com/topic/categorical-imperative> (last accessed on 2016-10-05).
- English Oxford Living Dictionaries, *Algorithm*, available at <https://en.oxforddictionaries.com/definition/algorithm> (last accessed on 2017-03-19).
- English Oxford Living Dictionaries, *Predict*, available at <https://en.oxforddictionaries.com/definition/predict> (last accessed on 2017-01-27).
- English Oxford Living Dictionaries, *Sensor*, available at <https://en.oxforddictionaries.com/definition/sensor> (last accessed on 2017-03-19).
- English Oxford Living Dictionaries, *SPAM*, available at <https://en.oxforddictionaries.com/definition/spam> (last accessed on 2017-01-26).
- Eriksson, Hasse, *Råd från robotar utmanar banker*, available at <http://www.dn.se/ekonomi/rad-fran-robotar-utmanar-banker/> (last accessed on 2016-06-17).
- European Union, *Court of Justice of the European Union*, available at https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_en (last accessed on 2017-04-15).
- Eurostat, *Overview*, available at <http://ec.europa.eu/eurostat/about/overview> (last accessed on 2017-03-30).
- Faception, available at <http://www.faception.com/our-technology> , <http://www.faception.com/about-us> and <http://www.faception.com/copy-of-financial-services> (last accessed on 2017-03-22).
- Facility Labs, *Facility Labs och den personliga integriteten*, available at <http://www.facilitylabs.com/> (last accessed on 2017-04-14).
- Farrell, Nick, *Apple patents tech to let cops switch off iPhone video, camera and wi-fi*, TechEye, 7 August 2013, available at <http://www.techeye.net/security/apple-patents-tech-to-let-cops-switch-off-iphone-video-camera-and-wi-fi> (last accessed on 2016-04-12).
- Free Dictionary, Legal Dictionary, *Fiduciary*, available at <http://legal-dictionary.thefreedictionary.com/fiduciary+duty> (last accessed on 2016-03-22).
- Free Snowden, available at <https://edwardsnowden.com/> (last accessed on 2017-03-26).
- Friends Online Report 2016, available at <https://friends-brandmanualswede.netdna-ssl.com/wp-content/uploads/2016/03/Friends-natrapport-2016-eng.pdf> (last accessed on 2017-02-07).

- Fung, Brian, *What to Expect Now That Internet Providers Can Collect and Sell Your Web Browser History*, The Washington Post, available at https://www.washingtonpost.com/news/the-switch/wp/2017/03/29/what-to-expect-now-that-internet-providers-can-collect-and-sell-your-web-browser-history/?hpid=hp_hp-more-top-stories_switch-internet606m%3Ahomepage%2Fstory&utm_term=.d8cc4a3b6a81 (last accessed on 2017-03-30).
- Gavagai, available at <https://www.gavagai.se/solutions/> (last accessed on 2017-04-07).
- Gibbs, Samuel, *Chatbot Lawyer Overturns 160 000 Parking Tickets in London and New York*, The Guardian, available at <https://www.theguardian.com/technology/2016/jun/28/chatbot-ai-lawyer-donotpay-parking-tickets-london-new-york> (last accessed on 2017-04-22).
- Gilbert, Eric and Karahalios, Karrie, *Widespread Worry and the Stock Market*, Association for The Advancement of Artificial Intelligence, available at <https://www.aaai.org/ocs/index.php/ICWSM/ICWSM10/paper/view-File/1513/1833> (last accessed on 2017-04-14).
- Garmin, available at <http://www8.garmin.com/aboutGPS/> (last accessed on 2017-01-26).
- Gartner, IT Glossary, *Location-based Services*, available at <http://www.gartner.com/it-glossary/lbs-location-based-services/> (last accessed on 2017-01-26).
- Gartner, IT Glossary, *Predictive Modelling*, available at <http://www.gartner.com/it-glossary/predictive-modeling> (last accessed on 2017-04-14).
- Gartner IT Glossary, *Big data* available at <http://www.gartner.com/it-glossary/big-data> (last accessed on 2017-03-01).
- Gartner IT Glossary, *Neural Net or Neural Network*, available at <http://www.gartner.com/it-glossary/neural-net-or-neural-network/> (last accessed on 2017-01-31).
- Gould, Jeff, *Courts docs show how Google slices users into “millions of buckets”*, available at <https://medium.com/@jeffgould/courts-docs-show-how-google-slices-users-into-millions-of-buckets-ec9c768b6ae9#.2gqyhep6g> (last accessed on 2017-04-14).
- Google, Transparency Report, available at <https://www.google.com/transparencyreport/> (last accessed on 2016-05-23).
- Grimsson, Gunnar, Razgute, Giedre and Hinsberg, Hille, *Rahvakogu - How the people changed the laws of Estonia*, available at https://docs.google.com/document/d/1lhoyZfRsgfhQkcSppu3L78_Uz_Iu-gUkzMycN2xg3MPo/edit?pref=2&pli=1 (last accessed on 2016-04-14).
- Guynn, J, and Lifschier, Mark, *Silicon Valley Uses Growing Clout to Kill a Digital Privacy Bill*, Los Angeles Times, 3 May 2013, available at <http://articles.latimes.com/print/2013/may/03/business/la-fi-digital-privacy-20130503> (last accessed on 2016-02-09).

- Hardy, Quentin, *Big Data Done Cheap*, The New York Times, available at http://bits.blogs.nytimes.com/2013/03/04/big-data-done-cheap/?_r=0 (last accessed on 2017-04-14).
- Hawthorn, Nigel, *10 things you need to know about the new EU data protection regulation*, ComputerworldUK, available at <http://www.computerworlduk.com/security/10-things-you-need-know-about-new-eu-data-protection-regulation-3610851/> (last accessed on 2016-04-15).
- Hunt, Elle, *New algorithm-driven Instagram feed rolled out to the dismay of users*, available at <https://www.theguardian.com/technology/2016/jun/07/new-algorithm-driven-instagram-feed-rolled-out-to-the-dismay-of-users> (last accessed on 2017-02-05).
- IBM, *First-of-a-Kind Technology to Help Doctors Care for Premature Babies*, available at <https://www-03.ibm.com/press/us/en/pressrelease/24694.wss> (last accessed on 2017-01-18).
- Information and Privacy Commissioner of Ontario, *Introduction to Pbd*, available at <https://www.ipc.on.ca/english/privacy/introduction-to-pbd/> (last accessed on 2016-03-24).
- Information Commissioners Office (ICO), United kingdom, available at <https://ico.org.uk/for-organisations/guide-to-pecr/location-data/> (last accessed on 2015-05-06).
- Information Commissioners Office (ICO), United kingdom, *Rights related to automated decision making and profiling*, available at <https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/rights-related-to-automated-decision-making-and-profiling/> (last accessed on 2016-09-23).
- Institute for Legal Reform, US Chamber of Commerce, *European Union*, available at <http://www.instituteforlegalreform.com/global/european-union> (last accessed on 2016-04-15).
- Institute for Legal Reform, US Chamber of Commerce, *The EU's Data Protection proposals open the door to abusive mass Litigation*, September 2015, available at <http://www.instituteforlegalreform.com/uploads/sites/1/a. EU Data Protection Regulation Proposal Handout with Annex 1 and 2.pdf> (last accessed on 2016-04-18).
- Institute for Aerospace Technology, *IAT Academic discusses airport scheduling at Heathrow on BBC series*, available at <https://www.nottingham.ac.uk/aerospace/news/iat-academic-discusses-airport-scheduling-at-heathrow-on-bbc-series.aspx> (last accessed on 2017-02-27).
- International Press Institute and Media Legal Defence Institute, *Freedom of Expression, Media Law and Defamation*, available at http://www.freemedia.at/fileadmin/user_upload/FoE_MediaLaw_Defamation_ENG.pdf (last accessed on 2016-01-22).
- International Telecommunication Union, *Big Data – Cloud Computing Based Requirements and Capabilities*, Recommendation Y.3600, available at

- <http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12584&lang=en> (last accessed on 2017-03-30).
- Intel, available at <http://www.intel.com/content/www/us/en/silicon-innovations/moores-law-technology.html> (last accessed on 2015-05-07).
- Internet Society, *Your Digital Footprint Matters*, available at <https://www.internetsociety.org/your-digital-footprint-matters> (last accessed on 2017-03-23).
- Klout, available at <https://klout.com/home> (last accessed on 2017-02-07).
- Korff, Douwe, *The Proposed General Data Protection Regulation: Suggested Amendments to the Definition of Personal Data*, EU Law Analysis, available at <http://eulawanalysis.blogspot.se/2014/10/the-proposed-general-data-protection.html> (last accessed on 2017-03-22).
- KPMG, *The Path to Purchase Journey*, available at <https://home.kpmg.com/xx/en/home/insights/2017/01/the-path-to-purchase-journey.html> (last accessed on 2017-03-19).
- Kravets, David, *U.N. Report Declares Internet Access a Human Right*, Wired, available at <http://www.wired.com/2011/06/internet-a-human-right/> (last accessed on 2017-04-14).
- Kumagai, Jean, Cherry, Steven, *Sensors and Sensibility*, IEEE Spectrum, available at <http://spectrum.ieee.org/computing/networks/sensors-and-sensibility> (last accessed on 2015-05-11).
- Kuschewsky, Monika, *Germany Wants to Introduce Class Actions for Privacy Violations*, Inside Privacy, available at <https://www.insideprivacy.com/international/germany-wants-to-introduce-class-actions-for-privacy-violations/> (last accessed on 2016-04-16).
- Kwow, Leslie, *Facebook Profiles Found to Predict Job Performance*, Wall Street Journal, available at <http://www.wsj.com/articles/SB10001424052970204909104577235474086304212> (last accessed on 2015-05-05).
- Lam, Bourree, *For More Workplace Diversity, Should Algorithms Make Hiring Decisions?*, available at <http://www.theatlantic.com/business/archive/2015/06/algorithm-hiring-diversity-HR/396374/> (last accessed on 2016-10-20).
- Legal Information Institute, *The Fourth Amendment*, available at https://www.law.cornell.edu/constitution/fourth_amendment (last accessed on 2015-12-21).
- Legal Information Institute, *The Eighth Amendment*, available at https://www.law.cornell.edu/constitution/eighth_amendment (last accessed on 2015-12-21).
- Legal Information Institute, *Fiduciary Duty*, Cornell University Law School, available at https://www.law.cornell.edu/wex/fiduciary_duty (last accessed on 2016-03-22).

- Living Internet, *Marshall McLuhan Predicts the Global Village*, available at http://www.livinginternet.com/i/ii_mcluhan.htm (last accessed on 2016-10-07).
- Lohr, Steve, *The Age of Big Data*, New York Times, available at http://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html?_r=0 (last accessed on 2015-05-13).
- Lohr, Steve, *Unblinking Eyes Track Employees*, New York times, available at http://www.nytimes.com/2014/06/22/technology/workplace-surveillance-sees-good-and-bad.html?_r=0 (last accessed on 2016-02-15).
- Leonard, Andrew, *How Netflix is Turning Viewers into Puppets*, February 2013, available at http://www.salon.com/2013/02/01/how_netflix_is_turning_viewers_into_puppets/ (last accessed on 2016-06-01).
- Livejournal, available at <http://www.livejournal.com/> (last accessed on 2017-03-01).
- Living Internet, *Marshall McLuhan Predicts the Global Village*, available at http://www.livinginternet.com/i/ii_mcluhan.htm (last accessed on 2016-10-07).
- Marshall, Dave, *Expert Systems*, available at <http://users.cs.cf.ac.uk/Dave.Marshall/AI1/mycin.html> (last accessed on 2016-02-17).
- Matlis, Jan, *Predictive Analytics*, Computer World, available at <http://www.computerworld.com/article/2554079/business-intelligence/predictive-analytics.html?page=2> (last accessed on 2015-05-11).
- Mattmar, Ulf, Eriksson, Hedvig, *Grävande journalist blev måltavla för proryska troll (Investigative Journalist Targeted by Pro-Russian Trolls)*, published on 2016-03-13, available at <http://www.svt.se/nyheter/utrikes/gravande-journalist-blev-maltavla-for-proryska-troll> (last accessed on 2017-02-08).
- Maycotte, Higinio, *The Evolution of Big Data, And Where We're Headed*, Wired, available at <https://www.wired.com/insights/2014/03/evolution-big-data-headed/> (last accessed on 2017-04-05).
- McCormick, Matt, *Immanuel Kant: Metaphysics*, Internet Encyclopedia of Philosophy, available at <http://www.iep.utm.edu/kantmeta/#H9> (last accessed on 2017-02-28).
- McCarthy, Erin, *Profiling Versus Modeling Versus Segmentation*, available at <http://www.sourcelink.com/blog/guest-author-series/2013/03/06/profiling-versus-modeling-versus-segmentation> (last accessed on 2015-11-24).
- Merriam-webster Dictionary, *Discrimination*, available at <http://www.merriam-webster.com/dictionary/discrimination> (last accessed on 2017-02-07).
- Merriam-Webster, *Deindividualize*, <http://www.merriam-webster.com/dictionary/deindividualize> (last accessed 2015-12-03).
- Merriam-Webster Dictionary, *Profiling*, available at <https://www.merriam-webster.com/dictionary/profiling> (last accessed on 2017-01-24).

- Merriam-Webster Dictionary, *Cybernetics*, available at <https://www.merriam-webster.com/dictionary/cybernetics> (last accessed on 2017-01-19).
- Merriam-Webster Dictionary, *Autonomy*, available at <http://www.merriam-webster.com/dictionary/autonomy> (last accessed on 2015-12-15).
- Merriam-Webster Dictionary, *Accountability*, available at <http://www.merriam-webster.com/dictionary/accountability> (last accessed on 2016-04-07).
- Merriam-Webster Dictionary, *Censorship*, available at <http://www.merriam-webster.com/dictionary/censorship> (last accessed on 2015-12-04).
- Merriam-Webster Dictionary, *Reasonable person*, available at <https://www.merriam-webster.com/legal/reasonable%20person> (last accessed on 2017-01-18).
- Merriam-Webster on-line dictionary, *Identity*, available at <http://www.merriam-webster.com/dictionary/identity> (last accessed on 2015-02-05).
- Merriam-Webster, *Reputation*, available at <http://www.merriam-webster.com/dictionary/reputation> (last accessed on 24-01-2014).
- Merriam-Webster Dictionary, *Crowdsourcing*, available at <http://www.merriam-webster.com/dictionary/crowdsourcing> (last accessed on 2016-04-13).
- Merriam-Webster, *SPAM*, available at <https://www.merriam-webster.com/dictionary/spam> (last accessed on 2017-04-04).
- Mitchell, Bradley, *What is an IP Address?*, Lifewire, available at <https://www.lifewire.com/what-is-an-ip-address-818393> (last accessed on 2017-02-07).
- Memorial Sloan Kettering Cancer Center, *Memorial Sloan Kettering Trains IBM Watson to Help Doctors Make Better Cancer Treatment Choices*, available at <https://www.mskcc.org/blog/msk-trains-ibm-watson-help-doctors-make-better-treatment-choices> (last accessed on 2017-01-18).
- Meyer, Robinson, *Could a Bank Deny Your Loan Based on Your Facebook Friends?*, The Atlantic, September 25th, 2015, available at <http://www.theatlantic.com/technology/archive/2015/09/facebooks-new-patent-and-digital-redlining/407287/> (last accessed on 2015-11-30).
- Mill, John Stuart, *On Liberty*, fourth edition, London: Longman, Roberts & Green, 1869; Bartleby.com, 1999. www.bartleby.com/130/ (last accessed on 2015-12-10).
- Milton, John. (2006). *Areopagitica* by John Milton, Project Gutenberg. Retrieved at May 4, 2008, from the website temoa : Open Educational Resources (OER) Portal, available at <http://www.temoa.info/node/799> (last accessed on 2015-12-10).
- Morgan, Jacob, *A Simple Explanation of 'The Internet of Things'*, Forbes, available at <http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/> (last accessed on 2015-05-08).
- Moore's Law, available at <http://www.moorelaw.org/> (last accessed on 2017-03-21).

- Moss, Simon, *Big Data: New Oil or Snake Oil?*, Wired, available at <http://www.wired.com/2014/10/big-data-new-oil-or-snake-oil/> (last accessed on 2015-05-22).
- Mystar, available at <http://www.mystarsanofi.com/web/products/glucometers/ibgstar> (last accessed on 2017-01-26).
- Narayanan, Arvind and Shmatikov, Vitaly, *Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset)*, University of Texas at Austin, February 5, 2008, available at https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf (last accessed on 2017-03-06).
- Nadege, Martin, Coulouvat, Geoffroy, *French National Assembly adopts 'Digital Republic' bill*, Norton Rose Fulbright, Data Protection Report, available at <http://www.dataprotectionreport.com> (last accessed on 2016-04-15).
- Netflix, available at <https://signup.netflix.com/> (last accessed on 2013-11-25).
- Netflix Tech Blog, <http://techblog.netflix.com/2012/04/netflix-recommendations-beyond-5-stars.html> (last accessed 2017-04-14).
- Nike at https://secure-nikeplus.nike.com/plus/what_is_fuel/ (last accessed on 2017-01-26).
- News, *All six citizen's initiatives have failed – activists accuse Parliament of intentionally slowing the process*, available at http://yle.fi/uutiset/all_six_citizens_initiatives_have_failed_activists_accuse_parliament_of_intentionally_slowing_the_process/7525779 (last accessed on 2016-04-13).
- Oded, Yaron, *Israeli Judge Approves \$400 Million Class Action Against Facebook for Violating Privacy*, available at <http://www.haaretz.com/israel-news/business/1.725512> (last accessed on 2016-06-16).
- OECD, *Data-Driven Innovation for Growth and Well-being*, available at <http://www.oecd.org/sti/ieconomy/data-driven-innovation.htm> (last accessed on 2017-01-18).
- OECD, *Data-Driven Innovation*, available at <http://www.oecd.org/sti/data-driven-innovation-9789264229358-en.htm> (last accessed on 2016-09-09).
- OECD Report, *Participative Web: User-created Content*, STI/ICCP/IE(2006)7/FINAL, 12 April 2007, available at <http://www.oecd.org/sti/38393115.pdf> (last accessed on 2015-01-01).
- Olson, Parmy, *Algorithm Aims to Predict Crime By Tracking Mobile Phones*, Forbes Tech, available at <http://www.forbes.com/sites/parmyolson/2012/08/06/algorithm-aims-to-predict-crime-by-tracking-mobile-phones/> (last accessed on 2015-05-06).
- Olofsson, Johanna, *Datainspektionen granskar mobilkartläggningen i Västerås*, SVT Nyheter, available at <http://www.svt.se/nyheter/regionalt/varmland/datainspektionen-utredar-mobilkartlaggningen-i-vasteras-city> (last accessed on 2015-05-06).
- Open Ministry, available at <http://openministry.info/> (last accessed on 2016-04-13).

- Oremus, Will, *Who Controls Your Facebook Feed?*, available at http://www.slate.com/articles/technology/cover_story/2016/01/how_facebook_news_feed_algorithm_works.html (last accessed on 2016-10-20).
- Opti, available at <https://www.opti.se/om-oss> (last accessed on 2017-03-06).
- Parks, Michael, *Blank Spaces in S. Africa Papers Protest Censorship*, Los Angeles Times, available at http://articles.latimes.com/1986-06-18/news/mn-11057_1_winnie-mandela (last accessed on 2016-08-23).
- Pangaro, Paul, “Getting Started” *Guide to Cybernetics*, available at <http://www.pangaro.com/definition-cybernetics.html> (last accessed on 2017-01-19).
- Pangaro, Paul, *What is Cybernetics?*, available at <https://vimeo.com/41776276> (last accessed on 2017-01-19).
- Pariser, Eli, *Beware Online “Filter Bubbles”*, TED, 2011, available at https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles/transcript (last accessed on 2016-05-12).
- PEN American Center, *Chilling Effects: NSA Surveillance Drives Writers to Self-Censorship*, November 2013, available at <http://www.pen-international.org/read-pen-american-centres-report-chilling-effects-nsa-surveillance-drives-writers-to-self-censor/> (last accessed on 2017-02-24).
- Personal Data Protection, Information on The Personal Data Act, Swedish Government Offices, available at <http://www.regeringen.se/content/1/c6/07/43/63/0ea2c0eb.pdf> (last accessed on 2015-02-25).
- PTS, The Swedish Post and Telecom Authority (PTS), *Q&A About Cookies*, available at <http://www.pts.se/en-GB/Industry/Regulations/Legislation/Electronic-Communications-Act/FAQ-about-cookies/> (last accessed on 2015-11-24).
- Peekyou, available at <http://www.peakyou.com/> (last accessed on 2017-02-07).
- PR Web, *PeekYou Launches First Digital Footprint Ranking System for Individuals; PeekScore Gauges One's Relevance and Reach on the Web*, available at <http://www.prweb.com/releases/peakyou/peekscore/prweb4148084.htm> (last accessed on 2017-02-07).
- Proust, Oliver, *Getting to know the GDPR, Part 5: Your big data analytics and profiling activities may be seriously curtailed*, fieldfisher, available at <http://privacylawblog.fieldfisher.com/2015/getting-to-know-the-gdpr-part-5-your-big-data-analytics-and-profiling-activities-may-be-seriously-curtailed/> (last accessed on 2016-09-26).
- Paul, Ian, *Girls Around Me App Voluntarily Pulled After Privacy Backlash*, PC World, available at http://www.pcworld.com/article/252996/girls_around_me_app_voluntarily_pulled_after_privacy_backlash.html (last accessed on 2016-01-12).
- Pocket-Lint, *What's the Point of Snapchat and How Does it Work?*, available at <http://www.pocket-lint.com/news/131313-what-s-the-point-of-snapchat-and-how-does-it-work> (last accessed on 2015-11-25).

- PublicCitizen, *Class Actions Empower Consumers, Help Them to Hold Wrongdoers Accountable*, available at <https://www.citizen.org/documents/Concepcion-and-consumers10282010.pdf> (last accessed on 2016-04-15).
- Quartz, *The magic that makes Spotify's Discover Weekly playlists so damn good*, available at <http://qz.com/571007/the-magic-that-makes-spotifys-discover-weekly-playlists-so-damn-good/> (last accessed on 2016-10-20).
- Regeringskansliet, *Stärkt samarbete om självkörande bilar*, available at <http://www.regeringen.se/artiklar/2017/02/starkt-samarbete-om-sjalvkorande-bilar/> (last accessed on 2017-04-15).
- Reitman, Rainey, *New California "Right to Know" Act Would Let Consumers Find Out Who Has Their Personal Data -- And Get a Copy of It*, 2 April 2013, available at <https://www.eff.org/deeplinks/2013/04/new-california-right-know-act-would-let-consumers-find-out-who-has-their-personal> (last accessed on 2016-02-09).
- Rossi, Ben, *Is big data dead? The rise of smart data*, Information Age, available at <http://www.information-age.com/technology/information-management/123458486/big-data-dead-rise-smart-data#> (last accessed on 2016-08-16).
- Rondeaux, C., *An Optical Illusion Might Slow Drivers*, The Washington Post, 2006, available at <http://www.washingtonpost.com/wp-dyn/content/article/2006/05/03/AR2006050302306.html> (last accessed on 2015-04-08).
- Rotella, Perry, *Is Data the New Oil?*, Forbes, available at <http://www.forbes.com/sites/perryrotella/2012/04/02/is-data-the-new-oil/> (last accessed on 2015-05-22).
- Rubin, Eliran, *Forget About Big Data: Teaching Computers to Think Just Like Humans is the New Big Thing*, Haaretz, restricted source, available at <http://www.haaretz.com/israel-news/business/.premium-1.712140?=&ts=1490874436018> (last accessed on 2017-03-30).
- Salyer, Patrick, CEO of Gigya, *Data Collection: All Consumers Want is Transparency, Relevance and Convenience*, Huffpost Tech, United Kingdom, available at http://www.huffingtonpost.co.uk/patrick-salyer/transparency-relevance-and-convenience_b_6678422.html (last accessed 2015-01-18).
- Scandau, available at <https://www.scanadu.com/blog/a-week-in-the-life-of-a-young-medical-consumer-company> (last accessed on 2017-01-26).
- Schlicht, Matt, *How the Personalized Newspaper Can Save Journalism*, Business Insider, available at <http://www.businessinsider.com/how-to-save-journalism-with-personalization-2011-3?IR=T> (last accessed on 2015-05-20).
- SICS, *Rise*, available at <https://www.sics.se/groups/blockchain-innovation-centre> (last accessed on 2017-04-15).
- Sigmastocks, available at <https://sigmastocks.com/> (last accessed on 2016-06-17).
- Simonite, Tom, *What Facebook Knows*, MIT Technology Review, available at <http://www.technologyreview.com/featuredstory/428150/what-facebook-knows/> (last accessed 2015-05-13).

- Sofia University, *Transpersonal Pioneers: Carl Jung*, available at <http://www.sofia.edu/about/history/transpersonal-pioneers-carl-jung/> (last accessed on 2015-02-03).
- Solon, Olivia, *Study: Twitter analysis can be used to detect psychopathy*, Wired.co.uk, available at <http://www.wired.co.uk/news/archive/2012-07/23/twitter-psychopaths> (last accessed on 2015-05-06).
- Solon, Olivia, *Artificial Intelligence is Ripe for Abuse, Tech Researcher Warns: 'a Fascist's Dream'*, The Guardian, available at <https://www.theguardian.com/technology/2017/mar/13/artificial-intelligence-ai-abuses-fascism-donald-trump> (last accessed on 2017-03-22).
- Spice, Byron, *Questioning the Fairness of Targetting Ads Online*, Carnegie Mellon University, available at <http://www.cmu.edu/news/stories/archives/2015/july/online-ads-research.html> (last accessed on 2017-04-16).
- Strauss, Valerie, *Firing of D.C. teacher reveals flaws in value-added evaluation*, March 7, 2012, available at https://www.washingtonpost.com/blogs/answer-sheet/post/firing-of-dc-teacher-reveals-flaws-in-value-added-evaluation/2012/03/07/gIQAtmlGxR_blog.html?utm_term=.6e40150898f2 (last accessed on 2017-02-27).
- Stanford Encyclopedia of Philosophy, *Autonomy in Moral and Political Philosophy*, available at <http://plato.stanford.edu/entries/autonomy-moral/> (last accessed on 2016-05-17).
- Stanford Encyclopedia of Philosophy, *Kant's Moral Philosophy*, available at <http://plato.stanford.edu/entries/kant-moral/> (last accessed on 2016-10-05).
- Stiftelsen för rättsinformation, available at <https://rattsinfo.se/> (last accessed on 2017-04-07).
- Sundberg, Sam, *Trumps nya lag öppnar för helt ny nivå av propaganda*, Svenska Dagbladet, available at <https://www.svd.se/trumps-nya-lag-oppnar-for-helt-ny-niva-av-propaganda> (last accessed on 2017-03-30).
- Sveriges Advokatsamfundet, *Code of Conduct of the Swedish Bar Association*, available at <https://www.advokatsamfundet.se/Advokatsamfundet-engelska/Rules-and-regulations/Code-of-Conduct/> (last accessed on 2017-04-04).
- Swedish National Data Service (Svensk Nationell Datatjänst, SND), available at <https://snd.gu.se/sv> (last accessed on 2017-03-31).
- TMF, *Can an Algorithm Diagnose Better than a Doctor?*, available at <http://medicalfuturist.com/can-an-algorithm-diagnose-better-than-a-doctor/> (last accessed on 2016-10-20).
- Techopedia, *Network Traffic Analysis*, available at <https://www.techopedia.com/definition/29976/network-traffic-analysis> (last accessed on 2016-05-26).
- Thomson, Iain, *Microsoft Seeks Patent on Employee Spy System*, The Register, http://www.theregister.co.uk/2011/11/18/microsoft_patent_employee_monitoring/ (last accessed on 2016-02-15).

- Thoreson, Anders, *Kom igång med Tor!*, IIS, Internetguider, available at https://www.iis.se/docs/kom_igang_med-tor.pdf (last accessed on 2016-05-25).
- Todd, Trevor, *Fiduciary*, Disinherited, available at <http://disinherited.com/fiduciary-relationships/> (last accessed on 2016-11-15).
- Turque, Bill, 'Creative ... motivating' and fired, The Washington Post, March 6, 2012, available at https://www.washingtonpost.com/local/education/creative-motivating-and-fired/2012/02/04/gIQAwzZpvR_story.html?utm_term=.c00363531ed5 (last accessed on 2017-02-27).
- Target, available at <http://intl.target.com/> (last accessed on 2016-12-20).
- Techopedia, *Internet of Things (IoT)*, available at <http://www.techopedia.com/definition/28247/internet-of-things-iot> (last accessed on 2015-05-08).
- Tor, *Tor: Overview*, available at <https://www.torproject.org/about/overview.html.en> (last accessed on 2016-05-25).
- US Equal Employment Opportunity Commission, *Laws Enforced by EEOC*, available at <http://www.eeoc.gov/laws/statutes/> (last accessed on 2016-01-21).
- United Nations Global Pulse, available at <http://www.unglobalpulse.org/about-new> (last accessed 2015-05-07).
- United Nations Treaty Collection, available at https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtmsg_no=IV-4&chapter=4&clang=_en (last accessed on 2017-03-28).
- US Legal Definitions, *Psychological Manipulation Law and Legal Definition*, available at <http://definitions.uslegal.com/p/psychological-manipulation%20/> (last accessed on 2015-12-14).
- Valentino-Devries, Jennifer and Singer-Vine, *They Know What You're Shopping For*, Wall Street Journal, available at <http://online.wsj.com/news/articles/SB10001424127887324784404578143144132736214> (last accessed on 2014-10-06, subsequently a restricted site).
- Valentino-Devries, Jennifer, Singer-Vine, Jeremy and Soltani, Ashkan, *Websites Vary Prices, Deals Based on Users' Information*, Wall Street Journal, 24 December, 2012, available at <http://online.wsj.com/news/articles/SB1000142412788732377204578189391813881534> (last accessed 2014-10-01, subsequently a restricted site).
- Vauhini, Vara and Fowler, Geoffrey A., *New Online-Data Bill Sets Up Privacy Fight*, The Wall Street Journal, available at <http://www.wsj.com/articles/SB10001424127887323916304578402912554668102> (last accessed on 2016-03-22).
- Viadeo Group, available at <http://corporate.viadeo.com/en/> (last accessed on 2017-03-05).
- Wikipedia, *Shop at Home Network*, available at https://en.wikipedia.org/wiki/Shop_at_Home_Network (last accessed on 2016-06-15).

- Yougov, available at <https://yougov.com/> (last accessed on 2017-03-05).
- Your Priorities, available at <https://yrpri.org/home/world> (last accessed on 2016-04-14).
- Your Dictionary, *Self-censorship*, available at <http://www.yourdictionary.com/self-censorship> (last accessed on 2015-12-04).
- Whatis.com, *Digital Footprint*, available at <http://whatis.techtarget.com/definition/digital-footprint> (last accessed on 2015-05-06).
- World Summit on the Information Society Declaration of Principles, 12 December, 2003, available at <http://www.itu.int/net/wsis/docs/geneva/official/dop.html> (last accessed on 2016-10-05).
- World Wide Web Consortium (W3C), available at <http://www.w3.org/Consortium/> (last accessed on 2017-04-04).
- Wired, *What your Klout Score Really Means*, available at https://www.wired.com/2012/04/ff_klout/ (last accessed on 2017-02-07).
- Wong, Julia Carrie, *What is a chat bot, and how should I be using one?*, The Guardian, available at <https://www.theguardian.com/technology/2016/apr/06/what-is-chat-bot-kik-bot-shop-messaging-platform> (last accessed on 2017-04-24).
- Åkerblom, Tobias Andersson, *Så blir du en kinesisk mönstermedborgare*, available at <https://kit.se/2015/09/25/11823/sa-blir-du-en-kinesisk-monstermedborgare/> (last accessed on 2015-12-01).
- Örstadius, Kristoffer, *Websidor avslöjar ditt besök för Google*, Dagens Nyheter, Thursday 27 September, 2012, available at <http://www.dn.se/ekonomi/webbsidor-avslojar-ditt-besok-for-google/>, (last accessed on 2017-04-14).

