Advancing Models of Privacy Decision Making

Exploring the *What* & *How* of Privacy Behaviours

Agnieszka Kitkowska

Faculty of Health, Science and Technology

Computer Science

LICENTIATE THESIS | Karlstad University Studies | 2018:51

Advancing Models of Privacy Decision Making

Exploring the *What & How* of Privacy Behaviours

Agnieszka Kitkowska

LICENTIATE THESIS | Karlstad University Studies | 2018:51

Advancing Models of Privacy Decision Making - Exploring the *What & How* of Privacy Behaviours

Agnieszka Kitkowska

LICENTIATE THESIS

Karlstad University Studies | 2018:51

urn:nbn:se:kau:diva-69974

ISSN 1403-8099

ISBN 978-91-7063-891-6 (print)

ISBN 978-91-7063-986-9 (pdf)

Distribution:
Karlstad University
Faculty of Health, Science and Technology
Department of Mathematics and Computer Science
SE-651 88 Karlstad, Sweden
+46 54 700 10 00

Print: Universitetstryckeriet, Karlstad 2018

WWW.KAU.SE

Advancing Models of Privacy Decision Making

Exploring What & How of Privacy Behaviours

Agnieszka Kitkowska

LICENTIATE THESIS | 2018:51

Advancing Models of Privacy Decision Making - Exploring What & How of Privacy Behaviours

Agnieszka Kitkowska

LICENTIATE THESIS | 2018:51

ISBN 978-91-7063-891-6 (print)

ISBN 978-91-7063-986-9 (pdf)

Distribution:
Karlstad University
Faculty of Health, Science and Technology
Department of Mathematics and Computer Science
SE-651 88 Karlstad, Sweden
+46 54 700 10 00

Print: Universitetstryckeriet, Karlstad 2018

WWW.KAU.SE

Advancing Models of Privacy Decision Making: Exploring the *What* & *How* of Privacy Behaviours

Agnieszka Kitkowska
Department of Mathematics and Computer Science
Karlstad University

Abstract

People's decisions do not happen in a vacuum; there are multiple factors that may affect them. There are external determinants, such as cost/benefit calculation of decision outcomes. There are also internal factors, such as attitudes, personality, emotions, age, and nationality. Frequently, the latter have a final say on the decision at hand, and similar determinants are triggered during the digital interaction when people make decisions about their privacy.

The current digital privacy landscape is filled with recurring security breaches and leaks of personal information collected by online service providers. Growing dependency on Internet-connected devices and increasing privacy risks prompted policy makers to protect individuals' right to privacy. In Europe, the General Data Protection Regulation requires companies to provide adequate information about their data collection and processing practices to users, to increase privacy awareness and enable better decision making. Regardless, currently there is no sufficient, usable technology, which could help people make improved privacy decisions, decreasing over-disclosure and oversharing. Hence, multidisciplinary researchers aim at developing new privacy-enhancing solutions. To define such solutions and successfully convey data provision and processing practices, potential risks, or harms resulting from information disclosure, it is crucial to understand cognitive processes underpinning privacy decisions.

In this thesis, we examine privacy decisions and define factors that influence them. We investigate the attitude-behaviour relationship and identify privacy concerns affecting perceptions of privacy. Additionally, we examine factors influencing information sharing, such as emotional arousal and personality traits. Our results demonstrate that there is a relationship between privacy concerns and behaviours, and that simplified models of behaviour are insufficient to accurately predict privacy decisions. Our findings show that internal factors, such as nationality and culture, emotional arousal, and individual characteristics, affect privacy decisions. Based on our findings, we conclude that future models of privacy should incorporate such determinants. Further, we postulate that privacy user interfaces must become more flexible and personalised than the current solutions.

Keywords: Privacy, Attitudes & Behaviour, Modelling Behaviour, HCI, UI Design.

Acknowledgements

My work is about privacy decisions, how important they are, and what factors shape them. In this section, I will tell you more about choices - my life choices that lead me to where I am today, thanks to people I met on my way.

Ever since I was a child, I dreamt of becoming an artist. I tried to follow that dream and gained a master's degree in art and met my late supervisor, Prof. Zygmunt Waźbiński. As much as my current work is not entirely related to my first degree, I must mention that it was he who taught me how important it is to seek answers and think in a scientific manner.

When I left Poland, I learned that sometimes we make the wrong choices. Living in Scotland, I was unable to proceed with a career as an art historian. However, I met people who introduced me to the field of information technology and digital design. They encouraged me to pursue a new career and study computing; for that I am grateful. My ex-supervisor and friend, now-retired Tom McEwan, supported my master's studies and built up my courage to become a researcher. He introduced me to my future friends and co-workers, whom I should also thank, because without them I would never decide to pursue a PhD.

Influenced by my friends and mentors, it was in the summer of 2016 that I moved to Sweden. Lost in a new reality, I received help from strangers who welcomed me as a friend. I would like to thank them all. My biggest gratitude goes to my PhD supervisors, Leonardo A. Martucci and Erik Wästlund, because without them I would never manage to complete this thesis. Thank you both for support, scientific advice, and for building up my confidence and aiding with my struggles. Also, I wish to thank Prof. Simone Fischer-Hübner because she was always available when I needed help. She is a true inspiration, not only as a researcher but also as a woman. Additionally, I want to thank my co-advisor, Prof. Joachim Meyer from Tel-Aviv University, and Michael Bechinie from USECON, because they both encouraged me to pursue my research ideas.

Working at Karlstad University, I have experienced nothing but a warm welcome. Whether I had personal and health issues, or I needed advice or help, everyone I met tried to support me. However, I would like to say a special "thank you" to Farzaneh, Patrick, Eva, Tobias, Lothar, and Nurul. I would like to thank all my colleagues from the Privacy&Us project, especially Yefim, who became my friend and collaborator.

Most importantly, my educational pursuit would not be possible without my family. My Mum and Dad are always there when I need them, regardless of the physical distance between us. Since I was a child, they have provided me with freedom of choice, which they hardly ever questioned. Also, my sister, Magda, my best friend, who is always available when I struggle and patiently listens to my calls. Thank you all. I wouldn't be here without you.

Karlstad University, Agnieszka Kitkowska

List of Appended Papers

I. **Agnieszka Kitkowska**, Erik Wästlund, Joachim Meyer, Leonardo A. Martucci. Is it Harmful? Re-Examining Privacy Concerns. Privacy and Identity Management. The Smart Revolution. 12th IFIP International Summer School. Ispra, Italy, September 2017.

II. Majid Hatamian, **Agnieszka Kitkowska**, Jana Korunovska, Sabrina Kirrane. "It's shocking!": Analysing the Impact and Reactions to the A3: Android Apps Behaviour Analyser. Data and Applications Security and Privacy XXXII, Springer International Publishing, 2018.

III. **Agnieszka Kitkowska**, Erik Wästlund, Leonardo A. Martucci. Emotional Privacy: Explaining Privacy Behaviours with Affect and Personality Traits. Under submission.

IV. **Agnieszka Kitkowska**. Reaching Beyond Borders: Investigating Differences in Privacy Harms Concerns. Proceedings of the CHI2018 Workshop: Moving Beyond a 'One-Size Fits All' Approach: Exploring Individual Differences in Privacy, Montreal, Canada, 2018.

Comments on my Participation

Paper I I am the first author of this paper. The idea of privacy harms concerns originated from past research. I was responsible for creating the new scale, selecting other instruments that could be used in the study, data analysis, and writing. The scale development and study design were thoroughly discussed with supervisors Erik Wästlund and Leonardo Martucci. Once participants' data were collected, Joachim Meyer assisted with the data analysis. All co-authors helped write the final article, revising preliminary drafts.

Paper II The research was designed and led by my colleague from the Privacy&Us project, Majid Hatamian. I am the second author of the article, responsible for a selection of statistical methods and data analysis. Additionally, I contributed by overall content revision, proposed changes in the paper structure and co-wrote the results/discussion section.

Paper III I am the first author of this paper. The idea to investigate emotions and personality traits was acquired from the psychology and behavioural studies. It was also due to my personal interest in research on emotions. I was responsible for the overall experimental design, selection of instruments used in the research, and design of the new measuring scales. However, all of my designs were continuously discussed with supervisors, Erik Wästlund and Leonardo Martucci, who also assisted with writing and revising the article.

Paper IV I am the only author because it is a position paper - a subjective opinion on certain issues. The concepts discussed in this short paper came from past works and results from the study presented in Paper I.

Other Publications

- **Agnieszka Kitkowska**, Joachim Meyer, Erik Wästlund, Leonardo A. Martucci. Is It Harmful? Measuring People's Perceptions of Online Privacy Issues. Poster. Thirteenth Symposium on Usable Privacy and Security, 2017. Santa Clara, CA, USA.

- Molly Land, Anthony Giannoumis, **Agnieszka Kitkowska**, and Maria Mikhaylova. Article 22. In The UN Convention on the Rights of Persons with Disabilities. A commentary. Oxford University Press, 2018.

- Lothar Fritsch, Ingvar Tjøstheim, **Agnieszka Kitkowska**. I'm Not That Old Yet! The Elderly and Us in HCI and Assistive Technology. In Proceedings of the Mobile Privacy and Security for an Ageing Population workshop at the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI), 2018. Barcelona, Spain.

Contents

Acronyms

CFIP Concern for Information Privacy. 14, 29, 38, 95

EFA Exploratory Factor Analysis. 13, 33

GDPR General Data Protection Regulation. 4, 6, 17, 27, 72, 86, 88

HCI Human Computer Interaction. 5, 11, 15

IUIPC Internet Users Information Privacy Concern. 29, 38, 95

NDM Naturalistic Decision Making. 7

PCIA Privacy Concerns of Information Abuse. 14

PCIF Privacy Concerns of Information Finding. 14

PETs Privacy Enhancing Technologies. 4, 40

PHC Privacy Harms Concerns. 11, 13, 14, 16, 28, 32, 33, 38, 40

S1 System 1. 8, 9, 15

S2 System 2. 8

UI User Interface. 4, 5, 13, 14, 15, 17, 18, 72, 83, 85, 86, 87

Introductory Summary

"A man's mind may be likened to a garden, which may be intelligently cultivated or allowed to run wild; but whether cultivated or neglected, it must, and will, bring forth. If no useful seeds are put into it, then an abundance of useless weed seeds will fall therein, and will continue to produce their kind."

James Allen, "As a Man Thinketh" (1903)

1 Introduction

The concept of privacy and issues it raises have a long history. As early as in ancient Greece, philosophers made a distinction between *inner* and *outer*. They defined borders and divided public from private, society from solitude [40]. Over the centuries, the concept of privacy evolved, and the word *private* was associated with ownership and wealth, possession of ordinary physical objects.

With technological developments, privacy issues gained importance. Particularly, the advancement of photography and journalism brought to the daylight questions of what is public or private. Warren and Brandeis in *The Right to Privacy* from 1890 began an extensive discussion on the matter [72]. Not only did they define privacy beyond the previously established concept of the *right to be let alone*, they also drew a picture of why it is crucial to protect privacy, describing how "[i]nstantaneous 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 house-top'" [72]. Further, they talked about the unauthorised circulation of "private portraits" and "the evil of the invasion of privacy by newspapers." As a consequence, privacy gained attention from American lawyers and policymakers. For instance, the 20th-century courts encountered increased numbers of trials referring to the violation of privacy [40]. Despite the nonexistence of a single legal definition of privacy, and the fact that privacy has not been recognised as a liberty, privacy became an unwritten right. In Europe, privacy has been acknowledged as a human right since shortly after 1950. Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms states, "[E]veryone has the right to respect for his private and family life, his home and his correspondence", and it should not interfere with by any public authority unless it is necessary [24].

Within the second half of the 20th century and the development of computing technologies, policymakers recognised the necessity of data privacy. In 1971 in Germany, the first data protection act took effect [40]. Soon after Germany, other countries acknowledged the significance of information privacy. For instance, Sweden established the Data Protection Authority in 1973, and the United States created the Privacy Act in 1974 [40, 70]. Further technological advancements and increasing availability and use of Internet-connected devices resulted in extensive collection of digital information, such as data gathered by online service providers. The collected information varies in sensitivity and may contain a wide range of personal data, such as health, location, religion, political views, race, and behavioural data. This information gained economic value and became a target for adversaries. Currently, media frequently reports on privacy and security breaches, with personal data leaks occurring in different areas such as social networks, finances, health care, or even smart-toy companies.

This alarming privacy landscape prompted law and policy makers to fur-

ther improve the protection of digital privacy. In Europe, the General Data Protection Regulation (GDPR) came into effect in May 2018. The regulation requires online companies to comply with its requirements. The GDPR aims to ensure that people's online privacy is adequately protected. It demands online service providers to ensure that individuals understand their rights and are presented with appropriate information about data collection and processing procedures. Yet, current solutions applied by data collectors rarely fulfil the GDPR's obligations.

Hence, multidisciplinary researchers investigate the best ways to provide the data processing information in a comprehensive, accessible manner. Their work aims to improve how people manage their personal information, because at present they reveal, both knowingly and unwittingly, large amounts of their personal information [1]. People's interactions with technologies increased as they use Internet-connected devices to perform their daily routines. And almost all of the digital interactions lead to information disclosure or sharing, meaning that people continuously make decisions about their privacy. Various privacy-preserving practices and Privacy Enhancing Technologies (PETs) are subjects of research on improving the current privacy landscape. Some of such research concentrates on the enhancement of User Interface (UI). As the ambiguous, long, legal texts of consents, privacy policies, or terms and conditions add to poor privacy decisions, researchers try to identify and develop the most suitable visual displays. They try to create UIs that efficiently communicate the information collection and processing procedures, emphasising potential risks resulting from privacy decisions.

Regardless of the legal requirements and researchers' efforts, so far it remains unknown how to improve people's privacy decisions. Some statistical reports demonstrate that the awareness of privacy risks is growing, and people express their concerns about online data collection. For instance, reports showed that people worry about the secondary use of data, unauthorised access to their personal information, or unnecessary surveillance [18, 29, 75]. Despite the aforementioned concerns, people make uninformed privacy decisions and over-disclose or over-share personal information. This phenomenon, called the *privacy paradox* is the subject of an investigation of many studies. One could claim that the *privacy paradox* does not exist, that it is only the lack of sufficient technology that discourages people from making informed privacy choices. Nevertheless, there is a privacy problem, and even if it is due to the absence of appropriate technological solutions, it remains unclear how to build technologies providing people with accurate, comprehensive, and accessible information that may change behaviour, reducing risks to privacy.

1.1 Objective

The overall objective of this research is further unravelling of the *privacy paradox* by investigating factors playing a crucial role in privacy behaviours. Such knowledge is essential for future research and privacy designers because it pro-

vides insight into mental processes of privacy decision making. Also, it may be applied to the design of privacy UIs to improve the information display.

Specifically, in this work, we drew on findings from different fields such as Human Computer Interaction (HCI) and social sciences, to create and test models of privacy behaviour. The first objective of this research, addressed in Papers I, II, and IV, is to investigate the role of attitudes, such as privacy concerns, and their relation to self-reported behaviours. Examination of such privacy attitudes enables understanding of what people are concerned about and how they perceive privacy harms. The second goal of this work, discussed in Paper III, is investigation of factors beyond privacy concerns that impact the decision-making process, and identification of whether they can be used to explain privacy behaviours.

1.2 Structure

The four papers appended in this thesis are preceded with an introductory summary. The remainder of this introduction is divided into the following sections. Section 2 provides the background information for this research, explaining the essential problems and concepts that motivated it. Section 3 introduces the research question this thesis seeks to answer. Section 4 provides an overview of the research methods used in the appended articles. The research contributions are outlined in Section 5, followed by Section 6 that reviews the findings against past research. Lastly, we conclude by summarising this thesis and discussing the future work in Section 7.

2 Background

To explain our motivation and provide information necessary to understand the selection of research methods used in the study, this section presents an overview of the theoretical background that prompted our work. It explains fundamental concepts acquired from different fields, such as social sciences, law, and computer science.

2.1 Legal requirements

Various reports show that the modern online environment increases people's concerns about data protection. For instance, the European Union reports that only 15% of respondents feel they have control over personal data, and 67% are concerned about the lack of control over their online information [29]. The same source shows that the majority of people considers online information disclosure an inevitable part of contemporary life, and they think they have no choice but to trade personal data for use of online services. According to the report, almost 60% of participants think that providing personal information is a *big issue*. Similar views have been reported in the United States, where 93% of Americans think it is important to know who can get

the information about them, and 90% find it important to control what information about them is being collected [54].

Such raising of privacy concerns became a subject of interest among policymakers. In Europe, the GDPR enforced the new rules and requirements on online service providers regarding information collection and processing practices [31]. The regulation introduced extended jurisdiction, applicable beyond Europe, as long as the data-collection subjects reside within the EU borders, and it imposed high financial sanctions for lack of compliance. Furthermore, the regulation enhances end-users' rights, such as breach notifications, right to access, right to erasure, and data portability. The GDPR increases transparency, meaning that "any information and communication relating to the processing of [...] personal data be easily accessible and easy to understand, and that clear and plain language be used" [31]. Every online service provider must ensure that users are fully aware of data collection and processing practices, which demands changes in current representations of informed consent, privacy policies, or terms and conditions. Theoretically, the GDPR requirements seem to be reasonably easy to fulfil; however, the current technological solutions fail to do so.

The legal requirements are in place enhancing the protection of the individual against potential privacy violations. But their efficiency is yet unclear. So far, the technology implemented some methods to comply with legal requirements, such as presenting information as structured text, or interactive warning messages. For instance, many online services show information about data practices in the cookie banner. In such a solution, every time people use the new online service, they must agree to the data processing practices, and occasionally they have an option to manually opt out from some of the data processing. So far, there is no proof that such design is successful, or that the users actually read agreement messages or manually change their settings. Additionally, past research has demonstrated that cookie banners are not really effective [7]. Considering the existing displays of privacy information, more work has to be done to identify appropriate ways of communicating the data practices, increasing people's privacy risk awareness while fulfilling the legal requirements.

2.2 Privacy paradox

Previous research demonstrated a dichotomy between privacy attitudes and behaviours, the so-called *information privacy paradox* [58]. Regardless of broad research about this phenomenon performed by interdisciplinary teams, causes of the *privacy paradox* are unclear, and ways of diminishing its results remain undefined. However, it has been shown that the phenomenon must be thought through as an effect of cognitive processes at the time of the digital interaction [48,66,73]. Therefore, to further unravel the paradox, it is crucial to understand the basics of decision-making processes.

2.3 Decision making

There are three major trends in the decision-making research: classical economic, Naturalistic Decision Making (NDM), and psychological [35]. The first is concerned with economic tradition, such as rational calculus of judgement. This approach is often studied through the lens of theories such a utility maximization, reasoned action, cost/benefit calculus, or expectancy [51]. The second approach, NDM, concentrates on gaining an in-depth understanding of people's decisions in meaningful and familiar real-world contexts [15, 35]. Its goal is to identify novel perspectives on people's choices by focusing on more than just the decision itself - NDM includes issues of recognition and intuition. The last approach originates from psychology and focuses on simple heuristics, unconsciously or consciously used during cognitive processing. This trend concentrates on psychological constraints accompanying rational calculations. Hence, it considers factors external to the rationale, such as emotions, contexts, and social norms, as well as limitations of human cognition [35, 45].

In this thesis we investigate privacy attitudes and their role in decision making. Section 2.3.1 provides a brief overview of attitude-behaviour models defined in past research. The explanation of decision-making with a sole economic approach has been proven insufficient, and this work builds on concepts acquired from psychology [43, 67]. Hence, in section 2.3.2 we present the most common approaches used to examine overall decision making, as well as privacy decision making, and in section 2.3.3 we illustrate the role of psychological biases and heuristics in cognitive processes.

2.3.1 Attitudes and behaviours; Relationships and models

To build a model of behaviour and attempt an understanding of cognitive processes accompanying decision making, one must consider the relationship between attitude and behaviour. Various models of this relationship were created, such as the Fishbein-Ajzen models, looking at the indirect impacts of attitudes on behaviour [5]; roles of different antecedents of behaviour such as previous experiences; or models considering the causal influence of attitude on behaviour [9]. In the past, models of behaviour, such as the one proposed by Bentler and Speckart, claimed a causal relationship between attitude and behaviour [10]. Initially, attitudes were considered to be direct influencers of behaviour, while modern psychology recognised that this relationship is less straightforward [5]. The modern approaches to decision making explain it as a matter of routinised choice. Additionally, contemporary research applied factors such as emotions and stress into the models of decision making [12,50,53]. This resulted in more complex models, such as Triandis's incorporating factors such as habit, facilitating conditions, and intentions [19].

2.3.2 Decision making and Privacy

One of the most common approaches used to explain privacy decision-making processes has roots in economics; it has been fundamental for many researchers [2, 11, 58]. The majority of studies using the economic approach focused on information disclosure, emphasising transactional dimensions of online behaviours. This concept was applied in studies about the monetary value of information protection [36], or even price-tagging of different types of information [17]. Similarly, privacy calculus studies have aimed to explain that responsibility for privacy decisions lies in the calculation of expected benefits and losses of information disclosure, implying that users' decisions result from estimated privacy trade-off. The privacy calculus models have been developed to improve understanding of privacy concerns and their potential implications for behaviour [28]. Additionally, privacy calculus was fundamental in studies related to risk/benefit analysis [27, 37]. Some such research applied utility maximisation expectation theory [74] and expectancy value theory [28, 55]. The research demonstrated that rational decision models and the cost/benefit calculus on their own, cannot adequately account for privacy decisions [2, 4]. There are other factors that must be included in the models of privacy behaviour, such as different psychological aspects crucial during judgement and decision making.

2.3.3 Psychological distortions, biases and affect heuristics

The rational decisions are often influenced by cognitive biases and heuristics [36, 43]. Some studies demonstrated how the *optimism bias* affects risky decisions [6, 20]. Users tend to perceive themselves as less vulnerable than others when confronted with risky decisions. This frequently results in underprotected privacy behaviours. In addition to the *optimism bias*, people seem to be overconfident about their knowledge and skills [42]. This may result in disclosure of more data and increased risk exposure. Similarly, the *control paradox* affects people's decisions. Previous research had indicated that paradoxically, people perceiving more control over limited aspects of privacy reveal more information, making themselves more vulnerable; people with lower perceived control disclose less, even when the risks associated with disclosure are lower [13].

Affect heuristics add to the complexity of privacy decision-making research. In short, according to affect heuristics, during the judgement process people are looking for mental short-cuts, allowing for quick decision making. Sometimes such quick decisions are based on the affect [47]. Studies showed that affect heuristics influences people's judgements of risks and benefits, creating an inverse relationship between the two [33]. This may confirm Zajonc's theory claiming that people's choices rely on emotions and *likes* (i.e., people buy a product because they like it) [76]. Similarly, Epstein and Mower demonstrated that affect is fundamental for behaviour motivation, and Damasio's study demonstrated a crucial role of feelings, resulting from people's mental images somatically marked with positive or negative emotions [62].

One possible way to understand this is to assume the existence of two systems responsible for cognitive operations: System 1 (S1) and System 2 (S2) [69]. S1 is automatic, effortless, intuitive, and perception based, while S2 is analytic, effortful, and consciously controlled. The affect heuristic is one of the outcomes of S1 [44]. Psychological studies not only demonstrated the existence of both systems but also provided evidence that S1 can dominate decision making [26], even when people are aware of the irrationality of their decisions. Thus, it can be concluded that affect heuristics are responsive to people's preferences both conscious and unconscious, and that they can be independent of cognition [62].

3 Research Question

Motivated by the legal requirements, studies of privacy decision making and the existence of the *privacy paradox*, we recognised the demand for better understanding of people's privacy perceptions and improved models of privacy behaviour. Hence, this thesis focuses on the relationship between attitude and behaviour, and on factors that influence this relationship. Therefore, the overall research question the thesis attempts to answer is:

How can we improve models of privacy decision making to advance the understanding of people's behaviours and enhance privacy designs?

To address the research question, this work concentrated on three aspects of privacy decision making. First, it aimed to investigate the attitudes. Hence, in Papers I and II we looked at the function of privacy concerns. We examined whether privacy concerns relate to people's privacy expectations, and we investigated the relationship between privacy harms concerns and behaviours. Second, in Papers I, III, and IV we investigated and discussed how demographic characteristics influence privacy decisions. Lastly, in Paper III we examined emotions and personality characteristics to identify their effect on disclosure and sharing behaviours.

4 Research Methods

To answer the research question, this work applied empirical quantitative methods. We chose quantitative methods because they are the most appropriate to investigate both attitudes and behaviours. Such methods enabled the collection of numerical data that can be statistically analysed and generalised to explain phenomena across larger samples.

The methods used in the study target correlations and causal relationships between dependent and independent variables in question. The overview of the conceptual design for this work is presented in Figure 1. It illustrates, at the high level, which variables and relationships were examined in the appended papers.

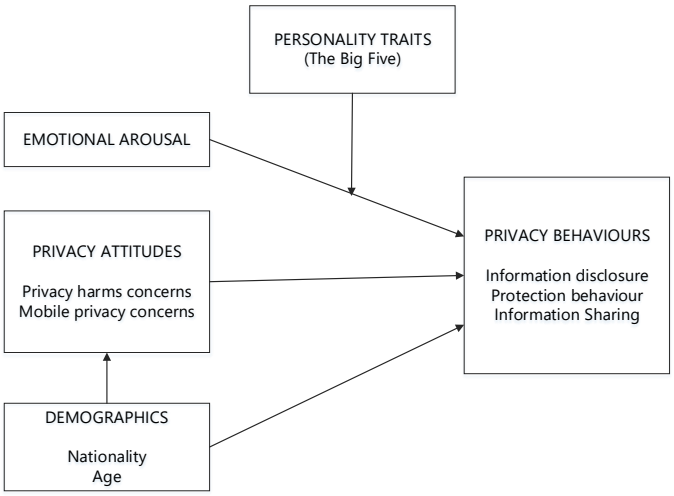

Figure 1: Conceptual design of the relationships investigated in this thesis.

When possible, we used prestructured research instruments acquired from the past work. This adds to the validity and reliability of our findings. The use of pretested questionnaires increases confidence that the instrument works and measures the concept of interest [41].

In the majority of studies on which this research is based, we applied detailed null hypotheses (stating that there is no difference between groups) containing dependent and independent variables. Hypotheses were suitable because they aim to resolve a precise problem statement with an empirical investigation. Compared to a research question, a hypothesis is narrower and can be examined in a single study or experiment [49].

Overall, the methods used in this thesis can be divided according to the study designs: nonexperimental, quasiexperimental and experimental.

4.1 Nonexperimental design

To investigate attitudes, we used the nonexperimental design. Such design enables identification of correlations between variables and leads to the presumed identification of cause and effect [21]. However, due to the lack of structural elements of real experiments, it cannot be used to establish the cause-effect relation. Often nonexperimental design can be used in cross-sectional studies when all data are measured at the same time, and the researcher has no control over variables.

In this research, the nonexperimental design enabled establishment of correlational relationships between the variables in question. Additionally, as we

sampled the data from different demographics (Paper I and Paper III), we were able to unravel attitudinal patterns and trends in the population samples.

Online survey

To measure attitudes and self-reported behaviours, we used an online survey. An online survey is a convenient method of gathering opinions from large samples in an efficient and cost-effective manner. The purpose of a survey is to produce statistics, or quantitative or numerical descriptions, about the sampled population [34].

When designing the survey, it is important to ensure that the variables of interest are measured with appropriate instruments. Hence, when possible (Papers I and III) we used the instruments validated in previous research. In instances when we wanted to measure a new concept (such as Privacy Harms Concerns (PHC)) or created new measuring scales, we ensured instruments' validity and reliability (Papers I, II and III) [16]. Additionally, when the new psychometric was created, we used pilot studies or expert reviews to ensure that the items correctly assessed the desired concept.

4.2 Quasiexperimental design

We applied quasiexperimental methods when seeking to establish a potential cause-effect relationship (Paper II). Quasiexperiments are similar to experiments in the sense that they also look at causal relations, and they may include control groups or pretest-posttest designs [21]. However, quasiexperiments lack a control group, and that makes it cumbersome to rule out alternative explanations for the phenomena in question.

User study

In Paper II, we used a within-group design. Such a design requires a smaller sample size than between-group design. The approach is beneficial for HCI studies, reducing the costs of experiment and enabling recruitment of qualified participants [49].

The pretest-posttest design used in Paper II aimed to measure whether the tool displaying privacy information is capable of changing participants' attitudes. In general, the pretest-posttest method consists of three steps. First, the pretest measures the level of the dependent variable. Second, the treatment (in Paper II: Use of the tool) is applied. Third, the same dependent variable is measured. As a result, it is possible to compare the differences in this variable, which are attributed to the experimental treatment [25].

4.3 Experimental design

We used an experimental design to investigate causal relationships between variables (Paper III). It is common that experiments contain the treatment variable controlled by the researcher [21]. In this work, we used a randomised

experiment, in which subjects were randomly assigned to one of the three groups exposed to different emotion-eliciting stimuli: positive, negative, and neutral (control).

Online experiment

To reach the desired sample and enable greater generalisation of the results, we created an online experiment (Paper III). We used a between-group design with clearly predefined null hypotheses. To create groups, we manipulated the independent variable with three conditions. The manipulation was later checked statistically. To decrease potential errors, we applied questionnaires and used the emotion-elicitation stimuli validated in past research.

The online experiment was built as a factorial design, with two independent variables and two dependent variables. We adopted a between-group design (applied also in Paper I), which is suitable to examine larger samples. Additionally, the between-group design is cleaner, prevents the effects of learning, and it reduces confounding effects such as tiredness [49].

Ethical review

The experiment from Paper III aimed to elicit emotional arousal. According to the Swedish Ethical Review Act, any research that "is performed according to a method with the purpose of affecting a research person physically or mentally" must apply for an ethical approval [68]. Because in Paper III we elicited emotional states and used a minor form of deception regarding the collection of personal sensitive information, we applied for ethical approval. In May 2018 our application received approval from the Swedish Regional Ethical Review Board in Uppsala.

4.4 Participants

In all studies, participants were gathered online. In Papers I and III we used online crowd-sourcing platforms, such as Microworkers, mTurk, and Clickworkers. When possible, to enhance data quality we hired respondents with high worker ratings. The main reason for using the crowd-sourcing platforms was the interest in demographical differences, such as different age groups and countries of origin, factors we wanted to add to the statistical models. Additionally, we aimed to collect data from a large sample in a time-efficient manner. Hence, the crowd-sourcing platforms seemed to be the most suitable.

In Paper II, participants were gathered online over social networks. This snowballing method was used because it was suitable for the design in which participants are required to meet the researcher in charge and install the application on their own devices. The downside of snowballing was that there was a large amount of time (over two months) spent on gathering the small sample of respondents.

4.5 Analysis methods

The data collected in the three studies forming this thesis were analysed statistically, with the use of methods ranging from descriptive statistics to more complex statistical models. We used significance testing that allowed us to determine whether the observed data were truly different, with α threshold $p < .05$.

The statistical method selection depended on the study design and types of variables. Apart from using descriptive statistics, we employed correlation analyses to investigate attitudes. To investigate causal relationships between different factors and privacy behaviours, we applied statistics such as nonparametric Wilcoxon tests or parametric tests such as means comparison (ANOVA) and general linear models (ANCOVA).

Additionally, to create the PHC scale, we applied Exploratory Factor Analysis (EFA), following the best practices defined in the literature to develop a new measurement scale [23, 32, 34]. The scale was built on the theoretical concept acquired from legal literature [64]. We created the scale to examine whether there is a relation between the legally defined privacy harms and people's perceptions.

5 Contribution

The contribution of this thesis is two-fold: privacy research and privacy design.

Contributions to the research on privacy

Firstly, we propose the new instrument measuring privacy concerns, the *Privacy Harms Concerns* (Paper I). Our work demonstrates that people are concerned about seven dimensions of privacy harms. They do not consider harms at the individual level defined in Solove's framework [64]. Instead, people have simplified and generic harms perceptions, perhaps because it is easier for cognitive processing. The PHC scale can be used in future research to measure concerns. Because the scale is universal in form, its items can be modified according to the research question.

Secondly, our findings confirm that there is a relationship between privacy attitudes and behaviours. Also, we demonstrate correlations between trust, concerns and privacy behaviours. These findings add to the body of knowledge on privacy decisions.

Lastly, we identify causal relationships between factors such as emotional arousal and personality, information disclosure, and sharing. We postulate that these factors should be incorporated into future models of privacy behaviour, to enable better prediction of decision outcomes. Additionally, our findings add to enhanced understanding of mental processes underlying privacy decisions.

Contributions to the privacy design

This research findings can be used by privacy UI designers and developers. We show that it is possible to change people's privacy attitudes by providing them with certain privacy information (in the context of a mobile environment). On the other hand, we demonstrate that influencing emotions and accounting for individual characteristics has the potential to change behaviour. Such knowledge might be incorporated in the UI designs, for instance, to develop new, affective ways of nudging people toward better privacy decisions. Further, our findings can help online companies fulfil the legal requirement of transparency, ensuring that people are provided with necessary information that is easy to comprehend.

Our results show that privacy behaviour differ among demographically diverse people. This suggests that the privacy UI should be dynamic and flexible, taking into account individual characteristics, such as age, nationality, or culture. Our results imply that designers should not try to develop one-size-fits-all privacy solutions. On the contrary, it seems that privacy notions differ among groups and should become personalised.

6 Related Work

The detailed description of the related work can be found in each appended paper. This section provides a very brief overview of the main findings of this thesis and briefly discusses them compared to past work.

6.1 Scales measuring privacy concerns

The past research established quite a few scales measuring privacy concerns. It produced scales determining Concern for Information Privacy (CFIP), where concerns are measured as a latent variable emerging from other worries about personal information, mostly in the organisational context [63]. Other scales are more specific, investigating concerns raising from certain privacy-invasive practices [60]. Some researchers focus on the individual items that may construct privacy concerns, while others address the issues from the perspective of a person, such as someone finding out information about themselves (Privacy Concerns of Information Finding (PCIF)) or someone abusing the information about others (Privacy Concerns of Information Abuse (PCIA)) [14, 27].

As much as all of these scales are valid and applied in the research, most of them were created in the context of an e-commerce consumer or organisation. Also, instruments seem to be outdated, and they do not consider today's extensive data collection and increased privacy awareness. When developing the PHC scale, we aimed to include modern risks related to data collection and processing. Additionally, as per recommendation from the past literature, the scale's goal is to investigate concerns about the diversity of privacy harms [48]. Our research examines whether people's mental models of privacy harms align with harms defined from court cases, the real-life examples

of digital privacy breaches.

6.2 Emotional arousal and personality

Past privacy research did not dedicate a lot of attention to the role of emotions and personality. Some researchers show that the S1 overrides the assessment of privacy concern, enabling heuristic-based decisions [59, 71]. This leads to the *privacy paradox* because rational behaviour such as cost/benefit calculus is blurred, and it is not used to assess potential risks. On the other hand, some research demonstrates that the pre-existing moods or emotional experiences that are unrelated to the decision at hand influence privacy-related risks [46]. Affective states may trigger sharing or privacy attitudes, depending on the type of emotion experienced by the user [22]. The claims that the emotional state is a strong influencer of decision making are supported by the research on changes of risk perception that result from the affective representation of information and the cognitive evaluations mediated by affective responses [62]. Unfortunately, sometimes affective states were placed in a negative light, as a factor leading to uninformed decisions and resulting in a greater *privacy paradox* [1].

Because the past research is inconsistent in regard to the role of emotions in privacy decision making, in this thesis we focus on a model acquired from the field of decision making [50]. Unlike the majority of past research, we do not investigate moods or discrete emotions. Instead, we examine *immediate emotions*, specifically various levels of emotional arousal. Following the conceptual model of Loewenstein and Lerner, we incorporate individual characteristics such as personality traits, to demonstrate their causal effects on information sharing.

Our results show that the level of emotional arousal, together with personality, are important factors shaping privacy decisions. Following the findings from psychology and HCI, we postulate that the affective design applied in the privacy UIs has a potential to improve privacy awareness and people's decisions [3, 38, 39, 52, 57].

6.3 Geographical differences

The inclusion of factors such as demographic characteristics in studies of privacy decisions is difficult. This is mainly due to the fact that such research should include samples representative to whole nations. And as much as it is true, the fact is that some studies performed on multiple occasions on smaller samples consistently demonstrated that nationality indeed affects privacy attitudes [8, 56, 61, 65]. Additionally, some of the national and international surveys confirm such differences - for instance, the EU barometers about data protection or data security [29, 30].

This thesis adds to the previous research, showing national differences in privacy concerns and information disclosure. According to our results, the most prominent differences are among participants from Northern Europe,

the United States, and the UK. What makes our results more valuable is the fact that we identified similar differences across two studies (discussed in three papers: I, III, and IV). Therefore, we postulate that the cultural and geographical factors must be considered when building models of privacy behaviour. Similarly, individual differences should be incorporated into design of privacy UI to provide better-suited solutions.

Paper I – Is it Harmful? Re-Examining Privacy Concerns

This research aimed to examine the relationship between privacy attitudes and self-reported behaviour. To assess the attitudes, we developed a new instrument measuring privacy harms concerns.

The novelty of this work was the use of a legal framework acquired from Daniel Solove. We aimed to check whether people's perceptions of privacy correspond to the individual privacy harms identified in court cases. Solove's framework is based on user-centered information flow. To simplify, the information is first disclosed by the data subject, and next it is collected and disseminated by online service providers, eventually returning to the user. Within such an information cycle, Solove recognised 16 individual privacy harms, and those underpinned the development of the PHC scale.

The results of this study showed that people do not consider privacy harms at the individual level. Instead, they perceive them as more generic and simplified concepts. Additionally, the results demonstrated correlations between the identified dimensions of privacy concerns and self-reported protection behaviours. Further, the study identified potential demographic differences, emphasising the need to consider characteristics such as age, culture, or nationality when designing privacy.

Paper II – "It's shocking!": Analysing the Impact and Reactions to the A3: Android Apps Behaviour Analyser

The study aimed to identify whether it is possible to increase privacy risk awareness and change participants' privacy concerns, measured before and after using the tool analysing Android apps behaviour. The user study was applied to investigate the tool's effectiveness and examine how people react to the information about mobile apps accessing phone resources.

First, our results showed that the A3 tool successfully detects the privacy-violating activities of smartphone apps. Additionally, we found that the information provided to 52 participants in the user study affected their privacy concerns and has the potential to change privacy awareness.

Paper III – Emotional Privacy: Explaining Privacy Behaviours with Affect and Personality Traits

The main goal of this work was to establish whether additional factors, such as affect and individual characteristics, could be applied in models of privacy behaviour. An online experiment was created to investigate a possible causal

relationship between emotional arousal, personality traits, and information disclosure and sharing.

The results gathered from the sample of 483 participants confirmed that the above-mentioned factors indeed influence privacy behaviours. Further, our study confirmed differences in information disclosure among people from different geographic areas. We postulate that our findings should be implemented in the future models of privacy behaviour. Additionally, such results can be applied in the design of privacy UIs.

Paper IV – Reaching Beyond Borders: Investigating Differences in Privacy Harms Concerns

This paper is a workshop position paper, which is not based on the new empirical research. Hence, it is established on the findings presented in Paper I and the knowledge acquired from the past research on privacy attitudes and behaviours.

The main purpose of this paper was to discuss the issues of individual characteristics, culture, and demographic differences as factors impacting an individual's privacy decisions. The paper aimed to begin a workshop discussion about the role of such factors in privacy design, emphasising the need for flexibility and personalisation of privacy that are missing in the current solutions.

7 Conclusion and future work

The modern ecosystems of Internet-connected devices increase data collection and processing. Taking a historical view over privacy, we can only expect that with development in technology, preservation of privacy might become even more important than it is today. Currently, legal directives such as the European GDPR restrain how online service providers deal with personal information. The strictly defined requirements oblige online companies to provide the user with comprehensive but easy-to-understand information about data collection and practices. However, the current solutions, such as long privacy policies, terms and conditions, or cookie banners seem to be ineffective. Hence, the multidisciplinary researchers attempt to improve designs of privacy UIs, to make them compliant with legal requirements, and ensure that people are fully aware of privacy risks and harms, which may result from digital interactions.

To develop sufficient solutions such as appropriate privacy UIs, it is necessary to gain in-depth knowledge about mental processes accompanying privacy decisions, to understand *what* and *how* people think about privacy. Without knowledge about privacy concerns or worries, it is impossible to produce interfaces diminishing the *privacy paradox*. Researchers and designers must determine factors that influence people's online decisions, such as disclosing or sharing personal and sensitive information. To acquire such knowledge,

in this thesis we investigate the relationships between privacy attitudes and behaviours.

First, we identify that people's attitudes toward privacy harms do not differ from their self-reported behaviour. Our findings imply that privacy harms concerns are suitable determinants of information disclosure and privacy protection practices and could be adopted in UIs (i.e., information on harms emphasised at the points of interaction) to diminish the effects of the *privacy paradox*. Second, we show that privacy perceptions differ cross-culturally. Yet, we demonstrate that regardless of such differences, emotions and personal characteristics have a strong influence on privacy decisions. The results indicate that privacy decision making is influenced by *immediate emotions* and individual characteristics. Thus, the modern models of decision making, considering factors beyond classical economics such as cost/benefit analysis, should be applied to predictive models of privacy behaviour. In addition, our findings suggest that people's privacy behaviours might change if privacy UIs become flexible, personalised, or trigger emotional arousal.

In the next phase of our work, we plan to use findings from this thesis to design, develop, and empirically evaluate what we call *affective nudges*. We aim to build privacy UI elements that trigger emotional responses and draw users' attention toward issues of privacy, and make them stop and reflect before disclosing their personal information. The goal is to examine usability and effectiveness of such *affective nudges* in different conditions, for instance in the lab and in online experiments with international participants. We believe that applying the results from this thesis to visual designs will help us to develop the new nudges, and to change behaviour, to decrease risks to privacy.

References

[1] A. Acquisti, L. Brandimarte, and G. Loewenstein. Privacy and Human Behavior in the Age of Information. *Science*, 347(6221):509–514, 2015.

[2] A. Acquisti and J. Grossklags. Privacy and Rationality in Individual Decision Making. *IEEE Security & Privacy*, 3(1):26–33, 2005.

[3] A. Acquisti, M. Sleeper, Y. Wang, S. Wilson, I. Adjerid, R. Balebako, L. Brandimarte, L. F. Cranor, S. Komanduri, P. G. Leon, N. Sadeh, and F. Schaub. Nudges for Privacy and Security. *ACM Computing Surveys*, 50(3):1–41, 2017.

[4] A. Acquisti, C. Taylor, and L. Wagman. The economics of privacy. *Journal of Economic Literature*, 54(2):442–492, 2016.

[5] I. Ajzen and M. Fishbein. Attitudes and the Attitude-Behavior Relation: Reasoned and Automatic Processes. *European Review of Social Psychology*, 11(1):1–33, 2000.

[6] Y. M. Baek. Solving the privacy paradox: A counter-argument experimental approach. *Computers in Human Behavior*, 38:33–42, 2014.

[7] R. V. Bavel and N. Rodriguez-Priego. Testing the Effect of the Cookie Banners on Behaviour, 2016.

[8] S. Bellman, E. J. Johnson, S. J. Kobrin, and G. L. Lohse. International differences in information privacy concerns: A global survey of consumers. *Information Society*, 20(5):313–324, 2004.

[9] P. M. Bentler and G. Speckart. Models of attitude–behavior relations. *Psychological review*, 86(5):452, 1979.

[10] P. M. Bentler and G. Speckart. Attitudes "cause" behaviors: A structural equation analysis. *Journal of Personality and Social Psychology*, 40(2):226, 1981.

[11] A. R. Beresford, D. Kübler, and S. Preibusch. Unwillingness to pay for privacy: A field experiment. *Economics Letters*, 117:25–27, 2012.

[12] T. Betsch, S. Haberstroh, and C. Höhle. Explaining routinized decision making. a review of theories and models. *Theory & Psychology*, 12(4):453–488, 2002.

[13] L. Brandimarte, A. Acquisti, and G. Loewenstein. Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science*, 4(3):340–347, 2013.

[14] T. Buchanan, C. Paine, A. N. Joinson, and U. D. Reips. Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology*, 58(2):154–165, 2007.

[15] M. Canelas and K. Feigh. Toward Simple Representative Mathematical Models of Naturalistic Decision Making Through Fast-and-Frugal Heuristic. *Journal of Cognitive Engineering and Decision Making*, 10(3):255–267, 2016.

[16] E. G. Carmines and R. A. Zeller. *Reliability and validity assessment*. Sage publications, 1979.

[17] J. Carrascal and C. Riederer. Your browsing behavior for a big mac: Economics of personal information online. *Proceedings of the 22nd international conference on World Wide Web*, pages 189–200, 2013.

[18] Centre of International Governance Innovation & Ipsos. CIGI-ipsos global survey on internet security and trust, 2018. Accessed: 2018-10-02.

[19] W. Cheung, M. K. Chang, and V. S. Lai. Prediction of Internet and World Wide Web usage at work: A test of an extended Triandis model. *Decision Support Systems*, 30(1):83–100, 2000.

[20] H. Cho. Determinants of Behavioral Responses to Online Privacy: The Effects of Concern, Risk Beliefs, Self-Efficacy, and Communication Sources on Self-Protection Strategies. *Journal of Information Privacy & Security*, 6(1):3–27, 2010.

[21] T. D. Cook and D. T. Campbell. The design and conduct of true experiments and quasi-experiments in field settings. In M. D. Dunnette, editor, *Handbook of Industrial and Organizational Psychology*, pages 223–326. 1976.

[22] K. P. Coopamootoo and T. Groß. Why Privacy Is All But Forgotten. *Proceedings on Privacy Enhancing Technologies*, 2017(4):97–118, 2017.

[23] A. B. Costello and J. W. Osbourne. Best practices in exploratory factor analysis: Four recommendations for getting the most from your analysis. *Practical Assessment, Research & Evaluation*, 10(7):1–9, 2005.

[24] Council of Europe. Convention for the Protection of Human Rights and Fundamental Freedoms, 1950.

[25] J. W. Creswell. *Research design. Qualitative, Quantitative and Mixed Methods Approaches*. Thousand Oaks: SagePublications, 2003.

[26] V. Denes-Raj and S. Epstein. Conflict Between Intuitive and Rational Processing: When People Behave Against Their Better Judgment. *Journal of Personality and Social Psychology*, 66(5):819–829, 1994.

[27] T. Dinev and P. Hart. Internet privacy concerns and their antecedents - measurement validity and a regression model. *Behaviour & Information Technology*, 23(6):413–422, 2004.

[28] T. Dinev and P. Hart. An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, 17(1):61–80, 2006.

[29] European Commission. Special Eurobarometer 431: Data Protection, 2015.

[30] European Commission. Special Eurobarometer 432: Europeans' Attitudes Towards Security. (April):108, 2015.

[31] European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, 2016.

[32] L. Fabrigar, R. McCallum, D. Wgener, and E. Strahan. Evaluating the use of exploratory factor analysis in psychological research. *Psychological Methods*, 4(3):272–299, 1999.

[33] M. L. Finucane, A. Alhakami, P. Slovic, and S. M. Johnson. The affect heuristic in judgments of risks and benefits. *Journal of Behavioral Decision Making*, 13(1):1, 2000.

[34] F. J. Fowler Jr. *Survey research methods*. Sage publications, 2013.

[35] C. Gonzalez and J. Meyer. Integrating Trends in Decision-Making Research. *Journal of Cognitive Engineering and Decision Making*, 10(2):120–122, 2016.

[36] J. Grossklags, S. Hall, and A. Acquisti. When 25 Cents is too much : An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information. *Information Security*, pages 7–8, 2007.

[37] I.-H. Hann, K.-L. Hui, S.-Y. T. Lee, and I. P. Png. Overcoming Online Information Privacy Concerns: An Information Processing Theory Approach. *Journal of Management Information Systems*, 24(2):13–42, 2014.

[38] M. Hassenzahl, S. Diefenbach, and A. Göritz. Needs, affect, and interactive products - Facets of user experience. *Interacting with Computers*, 22(5):353–362, 2010.

[39] M. Hibbeln, J. L. Jenkins, C. Schneider, J. S. Valacich, and M. Weinmann. How Is Your User Feeling? Inferring Emotion Through Human-Computer Interaction Devices. *MIS Quarterly*, 41(1):1–21, 2017.

[40] J. Holvast. History of Privacy. In *The Future of Identity in the Information Society*, pages 13–42. 2009.

[41] L. Hyman, J. Lamb, and M. Bulmer. The Use of Pre-Existing Survey Questions : Implications for Data Quality. In *European Conference on Quality in Survey Statistics*, 2006.

[42] C. Jensen, C. Potts, and C. Jensen. Privacy practices of Internet users: Self-reports versus observed behavior. *International Journal of Human Computer Studies*, 63(1-2):203–227, 2005.

[43] D. Kahneman. *Thinking, fast and slow*. Farrar, Straus and Giroux, 2011.

[44] D. Kahneman and S. Frederick. Representativeness revisited: Attribute substitution in intuitive judgment. *Heuristics and biases: The psychology of intuitive judgment*, 49, 2002.

[45] D. Kahneman and G. Klein. Conditions for Intuitive Expertise: A Failure to Disagree. *American Psychologist*, 64(6):515–526, 2009.

[46] F. Kehr, T. Kowatsch, D. Wentzel, and E. Fleisch. Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, 25(6):607–635, 2015.

[47] F. Kehr, D. Wentzel, T. Kowatsch, and E. Fleisch. Rethinking Privacy Decisions: Pre-Existing Attitudes, Pre-Existing Emotional States, and a Situational Privacy Calculus. *ECIS 2015 Completed Research Papers*, 2015.

[48] S. Kokolakis. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 7(2):1–29, 2015.

[49] J. Lazar, J. H. Feng, and H. Hochheiser. *Research methods in human-computer interaction*. Morgan Kaufmann, 2017.

[50] J. S. Lerner, Y. Li, P. Valdesolo, and K. S. Kassam. Emotion and Decision Making. *Annual Review of Psychology*, 66:799–823, 2015.

[51] Y. Li. Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, 54(1):471–481, 2012.

[52] S. Lichtenstain and P. Slovic. *The Construction of Preference*. Cambridge University Press, 2006.

[53] G. Loewenstein and J. S. Lerner. The role of affect in decision making. In *Handbook of affective science*, pages 619–642. 2003.

[54] M. Madden and L. Rainie. Americans' attitudes about privacy, security and surveillance. Technical report, 2015.

[55] N. K. Malhotra, S. S. Kim, and J. Agarwal. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research*, 15(4):336–355, 2004.

[56] C. L. Miltgen and D. Peyrat-guillard. Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. *European Journal of Information Systems*, 23(2):103–125, 2014.

[57] T. Mirsch, C. Lehrer, and R. Jung. Digital Nudging: Altering User Behavior in Digital Environments. *13th International Conference on Wirtschaftsinformatik*, (February):634–648, 2017.

[58] P. A. Norberg, D. R. Horne, and D. A. Horne. The Privacy Paradox : Personal Information Disclosure Intentions versus Behaviors. *The Journal of Consumer Affairs*, 41(1):100–126, 2007.

[59] C. Phelan, C. Lampe, and P. Resnick. It's Creepy, But It Doesn't Bother Me. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 5240–5251, San Jose, 2016.

[60] K. B. Sheehan and M. G. Hoy. Dimensions of Privacy Concern Among Online Consumers. *Journal of Public Policy & Marketing*, 19(1):62–73, 2000.

[61] S. Sheth, G. Kaiser, and W. Maalej. Us and Them: A Study of Privacy Requirements Across North America, Asia, and Europe. *Proceedings of the 36th International Conference on Software Engineering*, pages 859–870, 2014.

[62] F. Slovic. The Affect Heuristic. In *Heuristics and Biases; The Psychology of Intuitive Judgement*, pages 397–420. Cambridge University Press, 2002.

[63] H. Smith, S. Milberg, and S. Burke. Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly*, 20(2):167–196, 1996.

[64] D. Solove. A taxonomy of privacy. *University of Pennsylvania Law Review*, (477):477–560, 2006.

[65] Sun Sun Lim, Hichang Cho, and M. Rivera-Sanchez. A multinational study on online privacy: global concerns and local responses. *New Media & Society*, 11(3):395–416, 2009.

[66] S. Sundar, H. Kang, M. Wu, E. Go, and B. Zhang. Unlocking the privacy paradox: do cognitive heuristics hold the key? In *CHI'13 Extended Abstracts*, pages 811–816, 2013.

[67] R. H. Thaler, D. Kahneman, and A. Tversky. Mental Accounting Matters. *Journal of Behavioral Decision Making*, 12:183–206, 1999.

[68] The Ministry of Education and Cultural Affairs. The act concerning the ethical review of research involving humans (2003:460), 2003.

[69] A. Tversky and D. Kahneman. The Framing of Decisions and the Psychology of Choice. *Science*, 211(4481):453–458, 1981.

[70] United States Department of Justice & Office of Privacy & Civil Liberties. Overview of the privacy act of 1974, 2018.

[71] R. Wakefield. The influence of user affect in online information disclosure. *Journal of Strategic Information Systems*, 22(2):157–174, 2013.

[72] S. D. Warren and L. Brandeis. The Right to Privacy. *Harvard Law Review*, 4(5):193–220, 1890.

[73] D. Wilson and J. Valacich. Unpacking the Privacy Paradox: Irrational Decision-Making within the Privacy Calculus. *33rd International Conference on Information Systems*, pages 1–11, 2012.

[74] H. Xu, J. Smith, and T. Dinev. Information Privacy Research : An Interdisciplinary Review. *MIS Quarterly*, 35(August):989–1015, 2011.

[75] YouGov. Most concerning issues about online usage according to internet users in the united states as of may 2017, 2017. Accessed: 2018-10-02.

[76] R. Zajonc. Feeling and Thinking. Preferences Need No Inferences. *American Psychologist*, 35(2):151–175, 1980.

Advancing Models of Privacy Decision Making

Growing dependency on Internet-connected devices and increasing privacy risks prompted policymakers to protect individuals' right to privacy. In Europe, the General Data Protection Regulation requires companies to provide users with adequate information about data collection and processing practices to increase privacy awareness and enable better decisions. Hence, multidisciplinary researchers aim at developing new privacy-enhancing solutions. However, to develop such solutions it is crucial to understand cognitive processes underpinning privacy decisions.

This thesis objective is to investigate privacy behaviours. We identify privacy concerns affecting perceptions of privacy and examine factors influencing information sharing. We show that simplified models of behaviour are insufficient predictors of privacy decisions, and that demographic characteristic, emotion and personality affect privacy attitudes and behaviours. Based on our findings we conclude that future models of privacy and designs of privacy user interfaces must incorporate such behavioural determinants.

ISBN 978-91-7063-891-6 (print)

ISBN 978-91-7063-986-9 (pdf)

ISSN 1403-8099

LICENTIATE THESIS | Karlstad University Studies | 2018:51