DSV Report Series No. 13-003

Discovering Constructs and Dimensions for Information Privacy Metrics

Rasika Dayarathna

Doctoral Thesis in Computer and Systems Sciences at Stockholm University,

Sweden 2013.

Discovering Constructs and Dimensions for Information Privacy Metrics

Rasika Dayarathna

Stockholm
University

© Rasika Dayarathna, Stockholm 2013

ISSN 1101-8526
ISBN 978-91-7447-637-8

Printed in Sweden by US-AB, Stockholm 2013

Distributor: Department of Computer and Systems Sciences

To my late father...

Abstract

Privacy is a fundamental human right. During the last decades, in the information age, information privacy has become one of the most essential aspects of privacy. Information privacy is concerned with protecting personal information pertaining to individuals.

Organizations, which frequently process the personal information, and individuals, who are the subjects of the information, have different needs, rights and obligations. Organizations need to utilize personal information as a basis to develop tailored services and products to their customers in order to gain advantage over their competitors. Individuals need assurance from the organizations that their personal information is not changed, disclosed, deleted or misused in any other way. Without this guarantee from the organizations, individuals will be more unwilling to share their personal information.

Information privacy metrics is a set of parameters used for the quantitative assessment and benchmark of an organization's measures to protect personal information. These metrics can be used by organizations to demonstrate, and by individuals to evaluate, the type and level of protection given to personal information. Currently, there are no systematically developed, established or widely used information privacy metrics. Hence, the purpose of this study is to establish a solid foundation for building information privacy metrics by discovering some of the most critical constructs and dimensions of these metrics.

The research was conducted within the general research strategy of design science and by applying research methods such as data collection and analysis informed by grounded theory as well as surveys using interviews and questionnaires in Sweden and in Sri Lanka. The result is a conceptual model for information privacy metrics including its basic foundation; the constructs and dimensions of the metrics.

List of Papers

This thesis is based on the following papers.

I	Dayarathna, R., and Yngstrom, L. (2006) Attitude Towards Privacy Amongst Young International Academics. In 8th International Information Technology Conference (IITC), Colombo- Sri Lanka
II	Mahanamahewa, P., and Dayarathna, R. (2005) Workplace Communication Privacy in the Digital Age. In 7th International Information Technology Conference 2005, Colombo- Sri Lanka.
III	Dayarathna, R. (2008) Towards Bridging the Knowledge Gap between Lawyers and Technologists. *Int. J. Technology Transfer and Commercialisation* 7, (1): 34- 43.
IV	Dayarathna, R. (2008) The Principle of Security Safeguards: Accidental Activities. In Information Security South Africa (ISSA), Johannesburg-South Africa.
V	Dayarathna, R. (2009) The Principle of Security Safeguards: Unauthorized Activities. *Computer Law and Security Review* 25 (2): 165-172.
VI	Dayarathna, R. (2010) Towards Building Information Privacy Metrics to Measure Organizational Commitment to Protect Personal Information. In World Conference on Information Technology, Istanbul - Turkey (accepted but not presented)
VII	Dayarathna, R. (2011) Actors, Factors, and Concepts in the Information Privacy Domain. *International Journal of Commercial Law and Technology* 6 (4).
VIII	Zang, F., and Dayarathna, R. (2010) Is your E-mail Account Secure? *International Journal of Information Privacy and Security (JIPS)* 6 (1).
IX	Dayarathna, R. A self reflection on privacy. Social Science Research Network (SSEN) eLibrary (2011).

Reprints were made with permission from the publishers.

Contents

List of Tables

List of Figures

1. Introduction

1.1 Background of the Research

Alan Westin (1970), a prominent privacy advocate, defined privacy as "... the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others." Privacy has been articulated as a fundamental human right in many international treaties and national legislations. The International Covenant on Civil and Political Rights (ICCPR) adopted in 1966 and the Directive 95/46/EC adopted by the European Parliament and of the Council in 1995 (hereafter referred as "EU Directive") are good examples. Directive 95/46/EC mandates all member countries to adopt national data protection legislation that guarantees a minimum level of data protection across all member countries.

The importance of privacy has also been highlighted in opinion polls. On September 9, 2009, the *Wall Street Journal* published the results of a poll conducted in the USA in 2000 before the 9/11 attack. This survey revealed that the 'erosion of personal privacy' was considered the most worrisome threat at that time. Many other frightening issues such as international terrorism, global warming, and world war, trailed 'erosion of personal privacy' (cited in Swire & Steinfeld, 2002, p. 1). However, after the 9/11 attack, security issues have become of greater concern to individuals than personal privacy (Swire & Steinfeld, 2002). [1]

The Local—Germany's News in English (2009) reported that nearly 25,000 people gathered under the motto "Freedom rather than fear—Stop the surveillance madness" in Berlin in September 2009 to protest excessive surveillance and data collection by government authorities. Information privacy is one facet of privacy, which is explained in Chapter 2.

Information privacy has been defined as "the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves" (Clarke, 2009). Information privacy has been recognized as one of the key concerns in the field of information processing, especially in e-commerce. According to a survey conducted by the Opinion Research Corporation for RSA Security Inc., 25% of netizens who engage in online activities reduced their online business due to security and privacy concerns, and 43%

[1] The reason for citing a study conducted 12 years ago is to explain the importance of privacy in a peaceful environment. If society were to become peaceful again, then once again privacy would be a top issue.

expressed their reluctance to provide personal information to online merchants (RSA Security Inc., 2005). This is because netizens have been warned about the possibility of the mishandling of personal information in e-commerce. A survey conducted by Eurobarometer on behalf of the European Commission revealed that 90% of users had a fear of their personal data's being abused on the Internet and 42% had no confidence in online transactions (Eurobarometer, 2009). Bennett (2000, p. 36) argues that "[p]rivacy is recognized as the most important barrier to consumer participation." The mishandling of personal information causes a myriad of hardships, such as spam, identity theft, and excessive profiling. Identity theft, which is a clear violation of information privacy, has recently become a hot-button issue. In 2004, 39% percent of all complaints received by the United States Fair Trade Commission (FTC) were related to identity theft (Federal Trade Commission, 2005). A report published by the Australian Communications and Media Authority (ACMA) (2009) stated that identity theft is considered the most severe threat in disclosing personal information online. Another study has shown that insiders are responsible for more than 70% of all identity theft cases (Hedayati, 2012). Netizens' reactions to growing privacy threats hinder the progress of technology and the growth of business.

As is evident when considering the results of the surveys presented above, information privacy is undergoing a significant threat. Major contributing factors are the advent of more capable computer programs and hardware and a widespread use of information systems. Innovative computer hardware, which has drastically reduced data storage and communication costs (Martin et al., 2009), incites the transfer and storage of vast amounts of personal information. On the other hand, advanced searching and monitoring capabilities have made it more economical and convenient to identify one's personal information in a second. Admitting the recent developments in hardware and software, Lessig (1999) stated the efficient algorithms (code) have already limited our right to informational self-determination.

The Socio-Technical Security Model (Figure 1.1) developed by Kowalski (1994) explains the above-mentioned situations. Kowalski's model is based on General Systems Theory (GST), which states that a system always attempts to maintain its equilibrium by making certain changes. In other words, to reach a stable position, a change in one subsystem calls for changes in the other subsystems. Using this model, Kowalski has shown that a change in the machine subsystem affects the methods, culture, and structure subsystems as each one tries to re-establish a balance.

As a result of attempting to reach another equilibrium position, new changes take place in other subsystems (Kowalski, 1994). As presented in the previous paragraph, computer programs (the method subsystem) together with computer hardware (the machine subsystem) have challenged the social subsystems. One of the important reactions is the introduction of data protection and privacy laws (the structural subsystem). However, it is fair to state that people

are not fully confident in the positive changes that have taken place in reaction to privacy-invasive technological developments. The failure of subsystems to introduce new means to maintain the whole system at a stable/balanced position has led people to refrain from carrying out online business. In other words, the cultural subsystem has reacted in a negative way. More positive innovative steps in all four subsystems are needed to reach a privacy friendly equilibrium point.

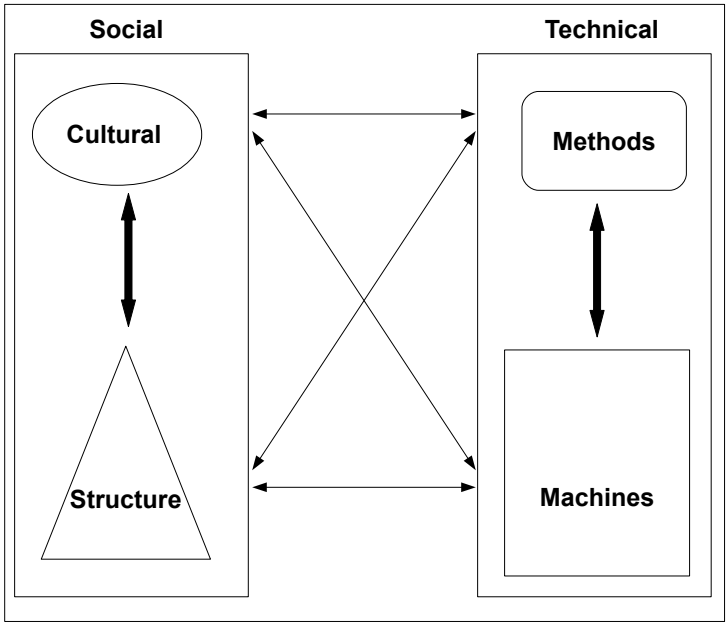


Figure 1.1: Socio-technical System – Kowalski, 1994, p. 10

There are some technological tools and methods in place to protect information privacy, but these privacy enhancing technologies are not widely used. A survey conducted by Harris Interactive (2001) for the Privacy Leadership Initiative (PLI) has reported that many people are unaware of the available means to protect their privacy and the commitment of organizations to protect privacy. Acquisti and Grossklags (2005) have also identified that privacy protection tools and techniques are not widely used. This researcher argues that in order to use tools and techniques to protect personal privacy, there must be a way to measure the effectiveness and usefulness of the tools used and measures taken. Payne (2006, p. 2) has stated that "[a] widely accepted management principle is that an activity cannot be managed if it cannot be measured" in *A Guide to Security Metrics* published by the SANS Institute InfoSec Reading Room,

Metrics, a subjective or objective interpretation of measurements (Payne, 2006), is a key management tool heavily used for decision-making purposes. In organizations, metrics help managers set goals and identify deviations, something which is essential for taking corrective action. Individuals compare food labels, a kind of metrics, to identify better food. Likewise, information privacy metrics could assist individuals in identifying privacy-friendly organizations and privacy protecting tools.

Even though researchers have been working hard on information security metrics for quite some time, they have not reached a universal agreement on how to approach this issue. Wang (2005, p. 182) stated, "[s]ecurity metrics are also hard because the discipline itself is still in the early stage of development." Building information privacy metrics is even harder since there is no commonly agreed definition for privacy. Furthermore, the development of information privacy metrics is in its infancy, compared to security metrics. Identifying the necessary constructs of information privacy metrics is one of primary steps in developing metrics.

This thesis focuses on contributing to the building of information privacy metrics by identifying important constructs and dimensions.

This chapter is organized as follows. The next section presents the research aim, followed by a justification for the research in Section 1.3. Sections 1.4 and 1.5 discuss the research questions and research design, respectively. The research contribution is presented in Section 1.6. The validation and limitation of the research are discussed in Sections 1.7 and 1.8. Finally, a summary of the published papers is given in Section 1.9.

1.2 Research Aim

As argued in the previous section, the full potential of the advancements and the widespread use of information and communication technology have not yet been achieved. There are many reasons for this. One of the important reasons mentioned above is the lack of protection given to personal information. Another closely associated reason is the fear of the invasion of information privacy.

Many efforts have been made to provide an appropriate level of protection for personal information. For example, one of the reasons for the introduction of EU Directive 95/46/EC was individuals' resistance to letting their personal information be handed over for processing in other European countries. This was due to the lack of protection given to personal information outside their own countries. The subjective word an 'appropriate level' (EU Directive) mentioned in the first sentence may be a bit controversial: EU Directive 95/46/EC says 'appropriate level' in Article 17 without giving a clear definition as to what the 'appropriate level' is. This researcher argues that 'appropriate level' is that level of protection given to personal information which

is sufficiently effective so that individuals are no longer worried about the misuse of their personal information. In other words, an 'appropriate level' of protection is achieved when individuals are satisfied with the amount of control they have over their personal information. The important point is building individuals' trust so they feel their personal information will not be misused. This can be further explained using a famous saying in the legal tradition. That is, "Justice should not only be done, but should manifestly and undoubtedly be seen to be done." Therefore, not only should protection be given, but also confidence of protection of personal information should be given. One way of identifying an 'appropriate level' is by conducting deductive surveys.

Hence, the normative aim of information privacy research is to introduce tools, techniques, procedures, and methods that facilitate providing an appropriate level of protection for personal information. One of the important means of improving the current level of protection given to personal information is measuring the level of protection given to personal information. In management, measuring is considered to be an important means for improvement. Lord Kelvin has stated that, "[y]ou can't improve what you can't measure" (cited in Jaquith, 2007).

This emphasizes the need for information privacy metrics. As further discussed in the research design section, Section 1.5, there are several steps to building information privacy metrics. One of the initial steps is to identify the constructs and dimensions of the metrics. Hence, the aim of this research in the context of the big picture is formulated as:

> ***To build a conceptual model for information privacy metrics by identifying their constructs and dimensions***

In summary, the identified constructs and dimensions from this research contribute to developing individual information privacy metrics. An aggregated information privacy metric is built by combining the identified individual information privacy metrics into a coherent whole. This aggregated information privacy metric facilitates managing information and other resources, making informed decisions, identifying deviations, and taking corrective action. All of these contribute to achieving an appropriate level of protection for personal information. [2] This is illustrated in Figure 1.2.

The term "constructs" refers to the basic building blocks of information privacy metrics. This definition is in line with the definition given by March and Smith (1995), which states that constructs form the vocabulary of a domain. Herrmann (2007) has used the word 'primitive' to refer to the building blocks of metrics. In this context, and throughout this thesis, the term *constructs* is used to refer to 'primitives' or 'the basic building blocks' of information privacy metrics. Constructs include actors, factors, and concepts. *Actor* refers to

[2] The term 'appropriate level' is taken from Article 17 of EU Directive 95/46/EC.

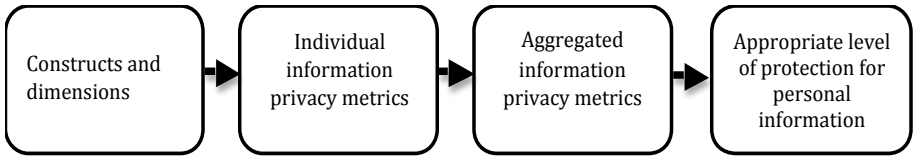


Figure 1.2: Research aim of this thesis in relation to the overall research aim in the information privacy domain

various roles played by people in the information privacy domain, and *factor* refer to tangible items, such as money, machinery, and equipment. Socially constructed concepts such as security, privacy, knowledge, and rights and duties, are known as *concepts*. *Dimension* refers to the context or environment in which the metrics are used, including the number of metrics needed.

As discussed above, the metrics should facilitate individuals' making efficient and effective decisions regarding their personal information and its protection.

1.3 Justification for the Research

Information privacy risk analysis is at an early stage. Measuring the processing risk of personal information is necessary for taking appropriate protective measures. For example, Article 17 of EU Directive 95/46/EC states that the protective measures should be appropriate to the risk of processing the personal information. Privacy risks in processing personal information and protective measures are two important key ingredients of information privacy metrics. According to the PISA project documentation, a lack of necessary financial resources and qualified staff are barriers for developing a proper method for analyzing information privacy risks (Blarkom et al., 2003). Many researchers in the area of information privacy have focused on solutions such as anonymity. Cvrcek and Matyas (2000, p. 1) have remarked on "... the common problem of many papers that narrow the considerations of privacy to anonymity only." On the other hand, the privacy risks involved with the processing of personal information are not well defined. A prominent privacy advisor has stated "There are some very precise technical notions for measuring anonymity, and at the other end of the spectrum measuring privacy in terms of operational risk in the context of Enterprise business practices is very nebulous" (Personal Communication, October 29, 2007).

The problems associated with the existing mechanisms that are used to communicate the commitment of an organization to protect personal information are discussed in the following two sections. Furthermore, these two sections justify this research in particular by arguing for the need for information privacy metrics from, first, the individuals' perspective, and then from an organizational perspective.

The Importance of Information Privacy Metrics to Individuals

Reading published privacy statements is the current practice for knowing how personal information is handled by an organization. McDonald and Cranor (2008) have shown that the reading of privacy statements is not helpful to individuals, since it requires substantial time and effort to read and understand. Furthermore, the authors reported that it costs $ 2,949 per annum per American to read privacy policies. Comparison of two policies doubles the cost. Privacy seals, also known as privacy certificates, issued by independent assurance organizations are another way to demonstrate an organizational commitment to protecting personal information. Even though a privacy seal is a convenient way of identifying privacy-friendly data controllers, it inherits certain limitations. For examples, the privacy seal does not provide enough information to make informed decisions such as identifying any progress in the recent past, comparing organizations who have privacy seals issued by different assurance organizations, and making more detailed comparisons of organizations. Another mechanism, which is currently being built in a research laboratory, is the privacy label, which is similar to the food label (Hills, 2009). It is reasonable to say that the concept of privacy label is a kind of privacy metric. In short, it is extremely difficult for individuals to make informed decisions by comparing the different levels of protection given to their personal information (Hansen et al., 2005). This is where information privacy metrics can bridge the gap.

Individuals ('data subjects' in legal terms) are primarily interested in information privacy metrics in that such metrics would facilitate their identifying privacy friendly organizations. In other words, organizations that provide better protection for personal information. Such metrics, which facilitate individuals' comparison of organizations in terms of the protection given to their personal information, empower individuals to demand more protection for their personal information. This empowerment also facilitates individuals' combining the level of protection given to their personal information with other relevant factors in choosing products and services. For example, a lender can demand a higher interest rate from a bank that provides comparatively less protection to their personal information. Demanding and choosing privacy friendly products and services encourages manufactures and service providers to invest more in privacy-enhancing technologies and privacy-friendly business processes.

The Importance to Organizations of Information Privacy Metrics

Organizations ('data controllers' in legal terms) are interested in information privacy metrics since such metrics assist them in demonstrating their commitment to protecting personal information. When Privacy International, an advocatory organization for privacy, ranked privacy friendly organizations (Privacy International, 2007), low ranking organizations reacted immediately. This immediate reaction showed the concern of organizations at being categorized as privacy unfriendly.

Demonstrating a high level of protection given to personal information gives a competitive advantage to organizations. A survey conducted by Ponemon Institute showed that 36% of the respondents indicated that demonstrating an organizational commitment to protecting privacy builds the image of the company (Ponemon Institute, 2003). Two key requirements prescribed by Bennett (2000) for having a competitive advantage are a means for consumers to identify privacy-friendly business organizations and having the appropriate cachet of privacy friendliness. He further stresses the need for a common yardstick to measure business practices. This yardstick empowers individuals in identifying privacy-friendly businesses. This is very important for comparison shopping, which has become the third most popular online shopping option (Kiang & Chi, 2009). In comparing products and services based on various criteria, an information privacy metric would help organizations demonstrate the level of protection given to personal information.

Organizations also need privacy metrics for their internal administrative functions. Performance measurement is one example. Peppers and Rogers (2007) pointed out that there are criteria for measuring the performance of all chief executives except privacy officers. Another important area is allocating organizational resources. For example, privacy officers need solid indicators, such as the return on investment (ROI), in order to convince financial departments of the importance of investing in privacy enhancing technologies and business practices. Furthermore, data controllers need benchmarks with for comparing their current performance with their past performance and with the performance of their peers. This is clearly highlighted in a report published by the Homeland Security Department's Inspector General (2009, p. 16), which states that "Without privacy-focused measurements and testing, TSA cannot compare the levels of PII[3] protections across different systems containing PII and improve overall privacy data protection and monitoring."

When organizations are sued for data breaches, one of the most common defenses is having a convincing organizational commitment to protecting personal information. Having a privacy metrics is a preferred defensive mechanism for privacy-friendly organizations.

Implementing an appropriate level of protection in processing personal information is an important managerial task. Articles 17 and 25 of EU Directive 95/46/EC insist on an appropriate level of protection for processing and transferring personal information to third countries. Information privacy metrics would assist managers in taking an appropriate level of protection in both cases.

[3]PII stands for 'personally identifiable information'

1.4 Research Questions

The research aim presented in Section 1.2 directed the formulation of the main research question. The main question was answered in seven research questions. These questions represent various aspects, facets, or considerations of the main research question. The relationships between the research questions are presented in Figure 1.4.

The main research question is formulated as:

> ***What are the constructs and dimensions of a conceptual information privacy metrics model ?***

This conceptual model has a number of individual information privacy metrics that are derived from the identified constructs. Furthermore, these individual information privacy metrics are used to build an overall information privacy metric that provides an aggregate value. *Dimensions* refer to the context or environment in which the metrics are used, including the number of metrics needed. It is important to identify various dimensions, since the metrics have to cover all the necessary aspects. This is called the comprehensiveness of the metrics. It is also important to keep the number of metrics at a minimum, since a large number of metrics needs more resources to collect and interpret the data. Therefore, the great challenge is to cover all relevant and necessary aspects while keeping the number of metrics at a minimum.

During the literature review, the EU Directive was identified as one of the most important information sources for the research. Article 17 of this directive sheds an initial light on the studied phenomenon. An illustration of this article is given in Figure 1.3. Here, the inner circle represents the personal information and the processing operations. The outer circle represents the measures used to protect the personal information from the threats depicted in the boxes. The gap between the two circles represents the strengths of the measures used to protect the personal information. Broadly speaking, these measures are organizational and technological measures. According to this article, the size of the gap is determined by the nature of the data, the risks of processing the personal information, the state of the art of protective measures, and the cost of implementing these measures. An increase in the sensitiveness of the personal data or the processing risk makes the gap wider, while a higher cost of implementation of the protective measures contracts the gap. State of the art measures have to be deployed to protect personal information. However, this must be balanced with their cost of implementation. In summary, the state of the art, the processing risk, and the nature of the data produce a wider gap between the two circles, while a higher cost of implementation contracts the gap. The former is depicted by arrows rising from the

state of the art, the nature of the data, and the processing risk, and the latter is depicted by arrows directed toward the cost of implementation in Figure 1.3. [4]

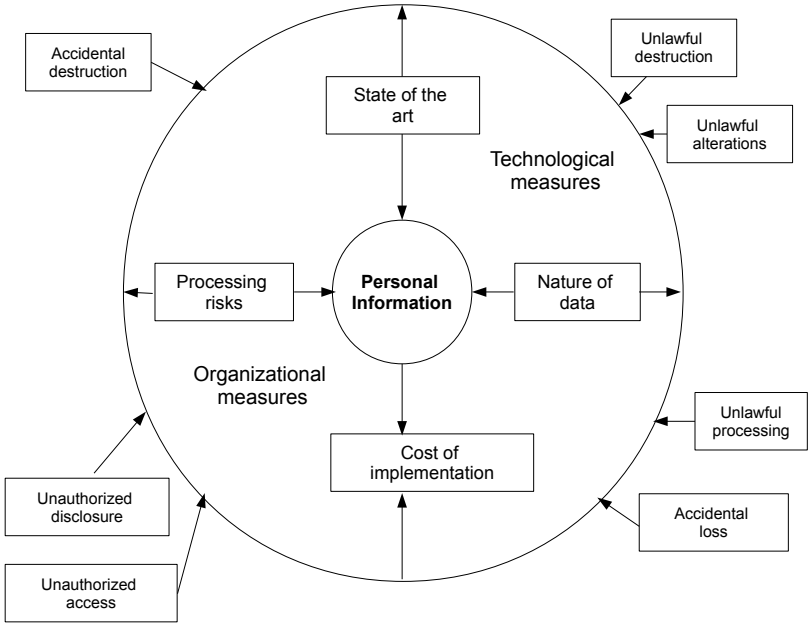


Figure 1.3: A graphical interpretation of Article 17 of EU Directive 95/46/EC

Research Question 1

The first step in the metric development process is the identification of the necessary constructs. As further discussed in the research design section, the first activity mentioned in the National Institute of Standards and Technology (NIST) security metrics guide for information technology systems by Swanson (2008) (hereafter referred as the "NIST guidelines") is the identification of the stakeholders' interests. However, at the time of starting this research, it was not clear who the stakeholders were. Not only the stakeholders, but also their actions and influencing factors were not clear. This could be due to the complexity of the subject domain and the lack of previous research. Therefore, the first research question was formulated as

[4] Another important category that is not included in Article 17 is accidental disclosure. This category also covers instances where the data subjects disclose their personal information without being concerned about the possible repercussions.

What are the actors, factors, and concepts in the information privacy domain?

The classical grounded theory (GT) approach (Glaser & Strauss, 1967) was used to answer this research question. A detailed discussion of the selection of grounded theory as a research approach is given in Chapter 3. Daily newsletters sent by the International Association of Privacy Professionals (IAPP) were the primary data source for this study.

Three important findings of the GT study were the nature of the data, the protective measures, and the privacy and security debate. Not only the GT study, but also the literature review emphasized the importance of these findings. Research questions 2, 3, and 4 further examine the nature of the data. Research question 5 studied the privacy and security debate, and questions 6 and 7 address the protective measures.

Research Question 2

After identifying the stakeholders, the focus was placed on the stakeholders' interests. The identification of the stakeholders' interests is the first activity mentioned in the NIST guideline. From the GT study, it was evident that the whole discussion is on the nature of personal data. Therefore, different aspects of the nature of the data were examined in research questions 2, 3, and 4. First, focus was placed on the sensitiveness of the personal data irrespective of the context. Therefore, the second research question was formulated as:

What personal information does an individual consider to be privacy sensitive?

This research question is addressed in Paper 1. This paper covered twenty-nine personal data items including education, health, financial status, attitudes, beliefs, etc. Paper 1 is based on a survey conducted among young international academics at the department of computer and systems sciences (DSV) in Sweden in early 2005. The questionnaire used is given in Appendix B.

The answer to this question suggests the need for two sets of metrics: one for sensitive personal data and the other one for non-sensitive personal data. Health care and financial information constitute the category of sensitive personal data. Having two sets of metrics keeps the overall number of metrics at a minimum, while covering the all the important personal data items. For example, there is no need for a separate set of metrics for the educational sector since educational data are categorized as non-sensitive personal data. This meets two important dimensions for the metrics: compliance and minimality, which are further explained in Section 1.5.

Research Question 3

Research question 2 investigated how participants perceived the level of protection required for their personal information in a context-independent manner. However, as explained in the privacy guideline given by the Organisation for Economic Co-operation and Development (1980) (OECD), it is not possible to discuss personal data without taking the context into account. Paragraph 3 of the OECD privacy guideline, titled "Different Degree on Sensitivity," gives an example, which states that "in one country universal personal identifiers may be considered both harmless and useful whereas in another country they may be regarded as highly sensitive and their use restricted or even forbidden." However, Article 8 of the EU Data Protection Directive gives a list of sensitive personal information that needs additional protection. Section 4.3.4 of the Personal Information Protection and Electronic Documents Act of Canada (PIPEDA, 2000) states that "... some information (for example, medical records and income records) is almost always considered to be sensitive; any information can be sensitive, depending on the context."

Not only in the information privacy domain, but also in the metric development process, context plays an important role. According to Jaquith (2007), 'context specificity' is an important characteristic of good metrics. Therefore, the focus was placed on the demographical and situational context, and the third research question was formulated as:

What are the relationships between the demographic data and the level of protection sought for personal information?

This question is also answered in Paper 1. The first part of the questionnaire asked for some demographic data relating to the respondents. These demographic data were matched with the level of protection sought for personal information. Additionally, this question also attempts to validate the claim made in the OECD's privacy guidelines, which states that the sensitivity of personal information is country specific.

The answer showed a more harmonized perception of information privacy issues among young academics in the field of IT. In other words, there was no statistical correlation between the level of protection sought for personal information and demographic data. This shows the possibility of building worldwide information privacy metrics, instead of building metrics for each demographic characteristic. This satisfies the minimality characteristic of good metrics.

However, the conducted explorative survey gave only an indication. Therefore, a well-formulated deductive research with an adequate representative sample would improve the validity of this claim.

Research Question 4

Research question 3 attempted to identify the correlation of the level of protection sought with demographic characteristics. Another important context is the situational context. Instead of asking for the level of protection sought in a given context, this question asked about a person's willingness to compromise privacy in a given context. Since the right of informational self-determination is a relative concept, there are certain situations where people have to compromise this right. In other words, there are certain situations where privacy has to be lessened. This led to the formulation of the fourth research question:

> ***Under what circumstances are data subjects willing to compromise their privacy?***

This question is also addressed in Paper 1. The third part of the questionnaire asked under what circumstance the participants would be willing to compromise their privacy.

The answer showed that the individuals' interest in personal information depends on the situational context, and it identified some circumstances under which individuals are willing to compromise their privacy. These circumstances are national security, public health and safety, and preventing and detecting criminal activity. As further discussed in Paper 1, these findings have been confirmed by similar studies. Therefore, it can be stated with confidence that the finding emphasizes the need for separate metrics for exceptional situations or for excluding exceptional events from ordinary information privacy metrics.

Research Question 5

Research question 5 is concerned with the debate on privacy *versus* security.

After discussing stakeholders' interests, the fifth research question turns to the goals and objectives of the stakeholders. This is discussed with an emphasis on the privacy and security interest of various parties. Identifying the goals and objectives of the stakeholders is the second step mentioned in the NIST (2008) metric development guidelines. The conflicting goals and objectives of stakeholders make the subject matter more complex. As concluded in the GT study (Paper 7), there are some issues that do not have immediate answers. One of these issues is the debate between privacy and security. This was clearly evident when conducting the GT study, as it showed the privacy and security debate in countries, organizations, and individuals. In answering research question 4, Paper 1 shows that some individuals are willing to compromise their privacy for the sake of national security and the detection of criminal activities, but others are not. Additionally, some cases pertaining to research question 7 indicate that some protective measures are considered pri-

vacy invasive in certain circumstances. The subjective nature of privacy makes it difficult to find the right balance between security and privacy. As Bennett (2000) noted, "It [privacy] is a value that is inherently and inescapably subjective." However, before answering this kind of complex issue, it is important to identify the influencing factors. Therefore, research question 5 was formulated as:

What is the nature of the conflicts between information security and privacy ?

This research question was approached in three different ways. The first approach was similar to interpretive research, where the researcher interprets other's expressions. In this case, this researcher's frame of reference on privacy is presented in Paper 9. That paper discusses several influencing factors through this researcher's lenses. That paper discusses privacy in the context of some social, religious, and legal circumstances; it discusses various personal data items, the need for the protection of these items, the means used to protect or to invade privacy, and the consequences of excessive privacy or of excessive lack of privacy. Finally, the paper presents the need for considering the privacy of stakeholders also when designing and implementing information systems.

The second approach is to study how different actors perceive privacy and security. A study was conducted on workplace privacy where mangers/employers want to protect organizational assets and to have an efficient workforce, while employees want to protect their privacy. Paper 2 answers this question by presenting the results of an empirical study conducted in public sector organizations in Sri Lanka in 2004–5. This study was conducted as part of a draft for policy measures aimed at managing email and Internet practices in the Sri Lankan public sector. The study environment was different from other workplace privacy studies, since employees use IT facilities at public workplaces for personal purposes. This researchers' personal experience in developed or technologically advanced countries is that using IT facilities in the workplace is mainly for official use and using these facilities at home is mainly for personal use[5]. In respect of using public IT resources for personal use, this study gives valuable insights into the body of the knowledge since, in most cases, many employees use the same computer for personal and official use. Some constructs identified in this paper are the presence of workplace privacy policy, permissible time period for browsing non-work related activities and for personal email communication.

The third approach was in studying how Data Protection and Privacy Commissioners have perceived the security and privacy issues in organizations.

[5]The Sri Lanka situation has changed greatly over the last few years.

According to the commissioners, appropriate protective measures should be in place to protect personal information and other organizational assets; simultaneously these measures should not invade individuals' privacy. Papers 4 and 5 address this issue.

Research Question 6

Reviewing system security program implementations is another step mentioned in the NIST guideline. In addition to security, it is important to include privacy protection measures. Two kinds of protection mechanisms identified in the GT study are technological and legislative measures. Legislative measures insist on using organizational and technological measures to protect personal information and other assets without invading privacy. This was formulated as the sixth research question.

> ***What are the best practices of leading email service providers in protecting personal information?***

Paper 8 identifies the technological protective measures taken by four leading web-based email service providers. These measures include both actions taken by the email service providers and measures they suggested their users take, for example, asking users to set a strong password. Protective measures taken by email service providers are important since these measures represent commonly used security and privacy protective measures on the Internet. Additionally, Paper 8 suggests some protective measures to overcome the limitations of existing measures.

Some of the identified protective measures discussed in Paper 8 are setting strong passwords, security questions and answers, properties of user names and passwords, password resetting mechanisms, information provided to the user, the presence of cookies and their lifetimes, options given to the user, data stored in the user's machine and at server's end, session termination, security in communication channels, the right to update and erase data stored at the server's end, and the amount of information disclosed to the recipient in sending an email message.

These constructs together with other identified constructs are used to derive metrics in the metric modeling stage. For example, measuring the strength of the protection mechanism against unauthorized access to an online account can be done at both the technical and non-technical level. At the technical level, it is a function of the number of characters in the password, combinations of special characters, the password-changing frequency, the possibility of reusing the password, etc. At the non-technical level, it is a function of the number of people who know the answer to the security question, the possibility of finding it, the availability of the answer in online forums, etc.

Research Question 7

Reviewing policies, procedures, and guidelines is the remaining step mentioned in the NIST guidelines. As Hustin (2009) mentioned (cited in Kucan, 2009), privacy and security are inseparable. Incorporating information security research into the protecting of the right of informational self-determination is a promising approach to protecting personal information. Danezis (2006) argues that instead of reinventing the wheel, it is more effective to take privacy as a security property and make use of the research done in the field of information security. Fischer-Hubner (2001) also advocates this idea in her book titled *IT-Security & Privacy*. However, some personal information protection measures are deemed inappropriate and some security measures taken to protect organizational assets are considered privacy invasive. Studying what protective measures have been considered as appropriate or recommended (in the case that protective measures are not sufficient or too privacy invasive) by Data Protection and Privacy Commissioners sheds light on this issue.

What personal information protective measures are deemed adequate against inadvertent and unauthorized incidents?

This research question was answered by presenting a set of approved and recommended personal information protection measures. These measures were identified by analyzing the verdicts given by the European Data Protection Commissioners in the ninth annual report compiled by the Article 29 working party and selected decisions of the Australian, New Zealand, Canadian, and Hong Kong Privacy Commissioners. Papers 4 and 5 answer which measures are judged adequate against inadvertent and unauthorized incidents.

Answering research question 7, Papers 4 and 5 present protective measures that an organization can take against accidental and unauthorized activities. Another important characteristic of the presented measures is that these measures are not privacy invasive in the given contexts. The constructs in these protective measures are used to derive the metrics in the metric modeling stage.

One of the problems faced in conducting the research presented in Papers 4 and 5 was identifying the protective measures sought in data protection and privacy legislations. On the other hand, as mentioned in Paper 3, some of the literature has stated that lawyers and judges can't understand technologies and their pros and cons. Paper 3 takes a step towards bridging this knowledge gap by prescribing a methodology for bridging the knowledge gap between lawyers and technologists. This paper laid the foundations for Paper 4 and 5.

Relations between the research questions

Figure 1.4 illustrates how the research questions relate to each other. The literature review, particularly the NIST guidelines and the discussion on research methodology, emphasize the importance of the GT study. The GT study together with the literature review, particularly Article 17 of the EU Directive, emphasize the need for the identification of protective measures, the nature of the data, and of having an "appropriate" level of protection. Additionally, the first two activities of the NIST guidelines prescribe the identification of stakeholders' interests and their goals and objectives. This led to the formulation of research questions 2, 3, and 4, which examined different aspects of the nature of the data. The conflicting goals and objectives of the stakeholders—the Privacy vs Security debate—are further examined in research question 5. The third step of the NIST guidelines is reviewing system security program implementations. This is addressed in research questions 6 and 7. Reviewing policies, procedures, and guidelines is the next step mentioned in the NIST guidelines. Research question 7 also addresses this requirement. The above-discussed research questions have contributed to the identification of possible constructs and dimensions.

All the research questions address the constructs and dimensions of information privacy metrics. Paper 6 presents the necessary procedural steps to be followed in building information privacy metrics. This relates to the research aim by prescribing a methodology for building information privacy metrics. This methodology suggests using the identified constructs and questions given in an information security and privacy questionnaire for building information privacy metrics. The prescribed methodology is based on the seven design science principles given by Hevner at al. (2004). Together with the metrics building methodology, a metrics evaluation criterion is also presented.

In "Further Research," Chapter 5, future research directions are presented, and how the conducted studies could have been improved.

1.5 Research Design

A concise discussion of the research methods used in this research, together with the applicability of design science, is given in Chapter 3. This section explains the way in which those research methods were applied in this research. By using Figure 1.5, which presents the original information system research framework proposed by Hevner et al., (2004), Figure 1.6 illustrates how this research was conducted.

The framework presented by Hevner et al. (2004) consists of three sections. The first section discusses *environmental* aspects (the left side of Figure 1.5), the second section addresses *IS Research* aspects (the middle area of Figure

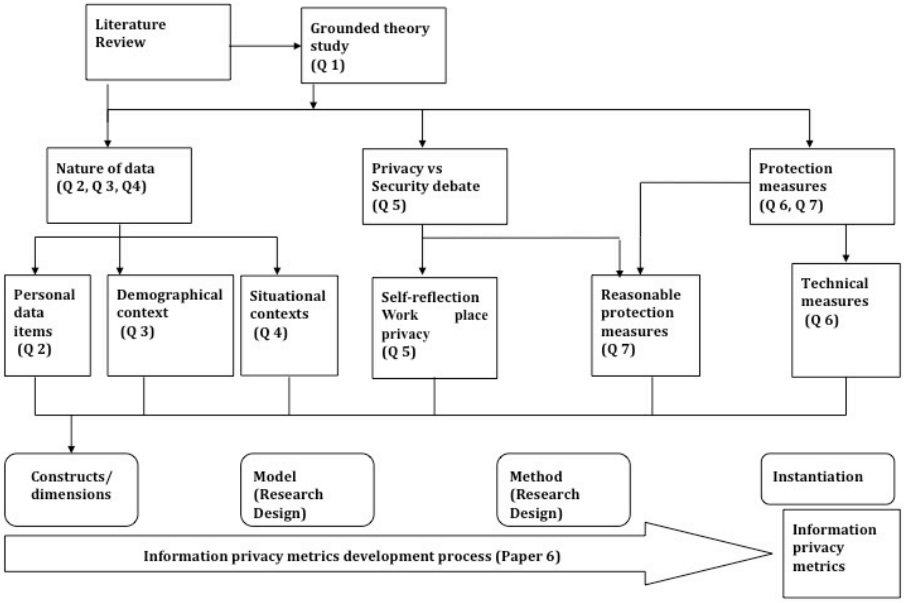


Figure 1.4: Relationship between research questions

1.5), and the last section discusses the *Knowledgebase* (right side of Figure 1.5).

Environment

Figure 1.5 shows that business needs are indicated by the *environment* and built artifacts are applied in the *environment* to meet those needs. In other words, the environment presents important business needs to the IS community, which are addressed by the IS community, and built artifacts are used to solve those important business needs. The three categories, people, organizations, and technologies, shown under the heading of environment in Figure 1.5 are taken from Silver, Markus, and Beath (1995). These categories establish the relevance of the research by expressing the importance of the identified business needs.

The left-hand side of Figure 1.6 represents how this research establishes its relevance. This is done in two stages: for individuals and for organizations. The survey presented in Paper 1 highlights individuals' concerns about information privacy. In addition, these concerns are further explained based on other researchers' work in the first part of the justification section (Section 1.3). Organizational concerns are discussed in Papers 2, 4, 5, and 8. Paper 2, which discusses the need for striking a balance between surveillance and privacy, emphasizes the need for measurement. The literature review presented in Chapter 2 presents attempts to measure the protection given to personal

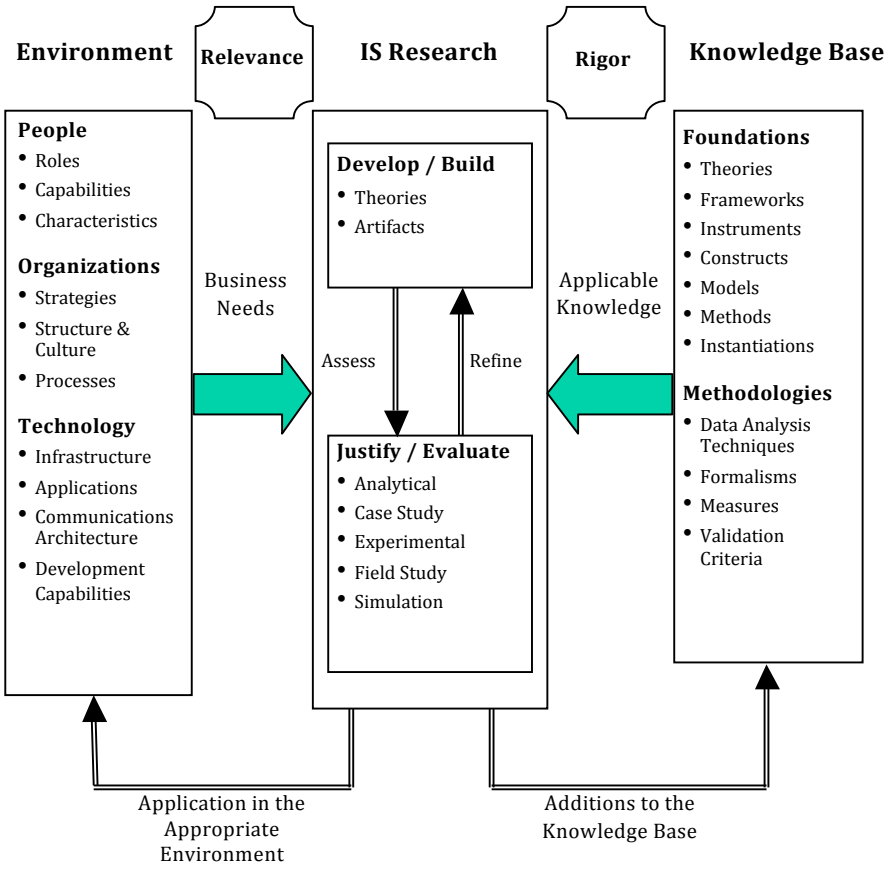


Figure 1.5: Information Systems Research Framework –Hevner et al., 2004

information. The last study, Paper 9, presented as an article, reflects this researcher's personal frame of reference on privacy. The justification section also emphasizes the need for privacy metrics for business organizations to demonstrate their commitment to protecting personal information and internal administrative purposes. As further explained in Chapter 2, the phenomenon of interest in this research is the protection given to personal information by organizations, more specifically, how organizations protect personal information during processing where technology is being heavily used. This short discussion explains how the relevant sections of this thesis present the business needs of the people and organizations to measure the level of protection given to their personal information. This establishes the relevance of this research.

Knowledge Base: Foundations

Knowledgebase is the most important aspect in design science since it distinguishes routine design from design science. Hevner et al. (2004) explains the difference as "[t]he key differentiator between routine design and design

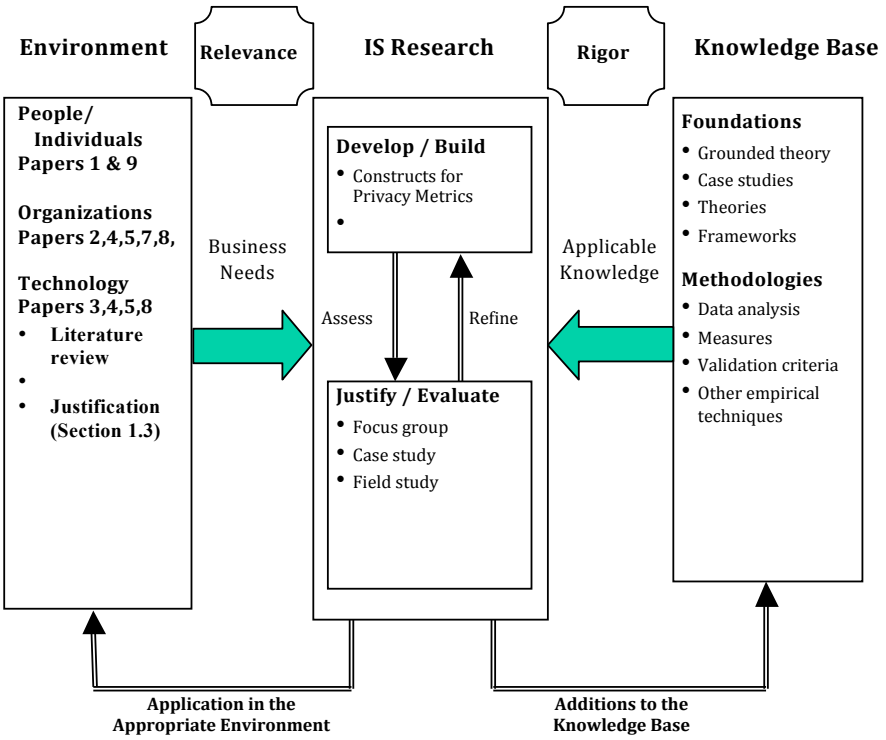


Figure 1.6: Application of the Information System Research Framework in this thesis.

research is the clear identification of a contribution to the archival *Knowledgebase* of foundations and methodologies" (p. 8). The *Knowledgebase* consists of foundations and methodologies. Foundations include theories, frameworks, instruments, constructs, models, methods, and instantiations that can be used to develop/build IS theories and artifacts. The methodologies in the Knowledgebase are data analysis techniques, formalisms, measures, and validation criteria. These guidelines are used to justify/evaluate the developed IS theories and artifacts. IS research and research in relevant disciplines contribute to the Knowledgebase. There are two complementary research phases: behavioral science and design science. The purpose of behavioral science is explained as "[b]ehavioral science addresses research through the development and justification of theories that explain or predict phenomena related to the identified business needs" (Hevner et al., 2004, p. 7).

After explaining the Knowledgebase, the discussion below continues about how the existing Knowledgebase is used in this thesis. The first part discusses some interpretations given to metrics, the second section discusses the qualities of a good metric, and finally, the metric development process is presented.

The NIST security metrics guidelines has defined metrics as "tools designed to facilitate decision making and improve performance and accountability

through collection, analysis, and reporting of relevant performance-related data" (p. 7). Similarly, Herrmann (2007) defined a metric as a value of one or more attributes of an object or event, derived from following a prescribed measurement process. Here, the objects and events may be either logical or physical. Metrics are collected from measurements, which is defined by Herrmann (2007, p. 27) as "the process of assigning numbers to object or event according to clearly defined rules." Furthermore, he calls the subcomponents of metrics *primitives*. According to Herrmann (2007, p. 25) primitives are "directly measurable or countable, or may be given a constant value or condition for a specific measure." Some examples of primitives are the number of attacks, normal incidents, and critical incidents. An example given by Herrmann (2007, p. 26) clearly illustrates the relationship between metrics and primitives: a metric defined for measuring the difficulty of cracking password may contain primitives such as the length of the password, and the password-changing frequency.

A *good metric* should have certain qualities. According to Jaquith (2007), a metric should be consistently measured, cheap to gather, expressed as a cardinal number or percentage, expressed using at least one unit of measure, and be contextually specific. Jaquith (2007) explained specificity by giving an example. According to that example, the average number of attacks given for an entire organization gives little value, but limiting the scope to a precise unit is more helpful (p. 25). Additionally, related disciplines, for instance, software development, shed lights on good characteristics of metrics. Importantly, one common characteristic of both software development metrics and information privacy metrics is that both focus on the process. Mustafa and Khan (2005) listed compliance, orthogonality, formality, minimality, usability, accuracy, validity, reliability, and implementability as qualities of good metrics. According to a white paper published by Laing and Coleman (2001), minimality refers to the minimum number of metrics that is good enough to meet the desired objective, and compliance refers to the ability to cover all important aspects.

After discussing the qualities of metrics, this section discusses the metric development process. The NIST guideline has outlined two metrics development stages: the metric development stage and the metric implementation stage. The metric development stage consists of two activities. The first activity is the identification and definition of the current IT security program and the second one is the development and selection of specific metrics to measure the implementation, efficiency, effectiveness, and impact of the security controls. The first activity refers to identifying the building blocks—constructs or primitives—of the metrics. The second activity is modeling personal information handling practices in terms of previously identified building blocks or primitives. Savola (2007) explained this process as simplifying a complex socio-technical situation down to numbers or partial orders. In addition to that,

there should be a method that clearly explains the necessary measuring steps (Herrmann, 2007).

The NIST (2008) guideline prescribes four steps for conducting the first activity. They are:

- Identification of the stakeholders' interest;
- Defining the goals and objectives;
- Reviewing the policies, procedures, and guidelines; and
- Reviewing system security program implementations.

Furthermore, the guidelines say that these steps need not be sequential.

As mentioned before, the foundations consist of prior research work that can be used for further IS research (Hevener et al., 2004). The above discussion on the metric building process together with the research methods discussed in Chapter 3 created the foundation for this research. How this foundation was applied in answering the research questions is briefly discussed in a following section, titled "IS Research: Develop/Build" and Section 1.4 as the answers to the research questions.

Knowledge Base: Methodologies

Methodologies, the last part of the Knowledgebase, provide guidelines to justify/evaluate the artifacts built. Possible methods given in the framework are data analysis techniques, formalisms, measures, and validation criteria. Furthermore, Lee (2004) and March and Smith (1995) suggested any appropriate validation techniques available in natural or social sciences. Furthermore, Hevner et al. (2004) explicitly mentioned the possibility of using empirical techniques. Section 1.7 discusses the appropriate methodologies and how they are applied in evaluating the constructs for privacy metrics.

IS Research

As shown in Figure 1.5, there are three parts to IS Research: develop/build, justify/evaluate, and their joint contributions to the environment and the Knowledgebase.

IS Research: Develop/Build

The result of the development process is either a theory or an artifact. An artifact can be a construct, model, method, or instantiation. As discussed in Chapter 3, a theory can be considered as a model. In the whole thesis, an information privacy metric is considered as a method that provides a set steps for data collection, analysis, and presentation, and as a model that represents the measures taken to protect personal information in the real world.

The qualities of the metrics and a metric development process are discussed under the foundation section of the Knowledgebase, and the research methods in general are discussed in Chapter 3. This section explains how this thesis followed the metric development process and applied the research methodologies.

The first activity—identification and definition of the current IT security program—mentioned in the NIST security metrics guide for information technology systems is slightly modified to suit the aim of this research. The focus of the NIST guideline is on information security, but the focus of this research is information privacy. Therefore, the first activity for this research was the identification and definition of the current IT security and privacy programs.

The first activity contains four steps. The first step mentioned in the NIST guidelines is the identification of the stakeholders' interests. However, before starting this research, it was not clear who the stakeholders were. This researcher argues that this could be due to the complexity of the subject domain and the lack of previous research. The rest of this section explains how the research methods were applied to carry out the four steps in the first activity.

By following rigorous research methods, the papers and the article filled in the Knowledgebase with the identified constructs, dimensions, and methodologies. Table 1.1 shows the empirically addressed research questions, research methods, and data collection methods.

Table 1.1: *Papers, research questions, research methods, and data collection techniques.*

Research question	Paper number	Research method	Data collection
1	7	Grounded theory	Online articles
2, 3 and 4	1	Survey (no. 1)	Questionnaire
5	2	Survey (no. 2)	Questionnaire and Interview
5	4 and 5	Case study	Reports
5	9	-	Personal thoughts and Interview
6	8	Experiment	Web-based email services
7	4 and 5	Case study	Reports

The aim of the case studies in Papers 4 and 5 was to identify the level of organizational and technological measures needed to protect personal data and to identify excessive security measures that invade privacy. Therefore, it can be said that the focus of these two case studies is the intersection of legal provisions and information protection measures.

Both the grounded theory study and above-mentioned legislative provisions stress the importance of the nature of the data. Survey 1 (Paper 1) was conducted to identify the stakeholders' interests in personal information. A conflicting between security and privacy was studied in a workplace privacy paper (Paper 2, Survey 2)—the way in which employers and employees perceive their rights in the workplace was the subject of Paper 2. Paper 8 presents a set of experiments conducted to identify the protective mechanisms given by four leading email service providers and the last study (Paper 9) presents a self-reflection on privacy. This paper sheds light on the privacy issues in aspects that were not covered elsewhere.

IS Research: Justify/ Evaluate

The evaluation/justifying stage focuses on refining the artifacts built and on explaining why the artifact built meets or does not meet business needs. The evaluation methods given in the framework are the case study, the field study, analytical methods, experiment, testing, and descriptive methods.

Without using the privacy metrics, it is not possible to explain how the metrics meet business needs. Therefore, the discussion is limited to the evaluation of the identified constructs and dimensions, which is discussed further in Section in 1.7, which discusses the validation of the findings.

IS Research: Contribution

The two arrows in Figure 1.5 start from the IS Research component and point towards the environment and Knowledgebase components. The left one shows the contributions to the environment. This is discussed in the first part of the

contribution section, Section 1.6. The right arrow indicates the contributions to the Knowledgebase. This is discussed in the second part of Section 1.6.

1.6 Contributions

The main contribution of this thesis is the identification of some constructs and dimensions for information privacy metrics. These are presented in Chapter 4 using a conceptual model. The constructs, which are presented as protective measures, and dimensions were presented in Section 1.4 as the answers to the research questions. This section discusses the contributions to the environment and Knowledgebase depicted in Figure 1.6 under IS Research. Additionally, "Papers" present their contributions in the respective discussion sections.

The arrow that runs from *IS research* to *environment* in Figure 1.6 illustrates the contribution of the artifacts built to the appropriate environment in order to solve the identified business needs. The business needs, which are mentioned in the justification section (Section 1.3), can be solved by successfully instantiating the intended information privacy metrics. Even though this thesis does not solve the identified business needs by introducing and instantiating information privacy metrics in practice, the thesis makes a substantial contribution towards solving the identified needs by identifying constructs as protective measures and the dimensions of information privacy metrics which are presented in Chapter 4. Paper 6 discusses the identified future research to develop and use the intended information privacy metrics.

An unintended outcome of the workplace privacy paper (Paper 2) was that that paper became a catalyst for the information privacy debate in Sri Lanka. After presenting the paper, key personnel in the audience recognized the importance of introducing a set of guidelines for the use of Internet facilities at public workplaces and the monitoring of the use of these facilities. Papers 4, 5, and 8 present a number of protective measures. Organizations can use these recommendations as a blueprint to identify weaknesses in their systems and remedy the shortcomings. System designers can also make use of the findings to design better security and privacy protection measures. The measures presented in Papers 4 and 5 have high value since they have been approved or recommended by data or privacy commissioners. In addition to organizations, the measures presented in Paper 8 educate users in taking measures to protect their online accounts. The grounded theory paper (Paper 7) describes an overall view of the information privacy domain. Paper 1 and the self-reflection paper (Paper 9) give an opportunity to reflect on one's own understanding of privacy in relation to various contexts. This might induce individuals to review their attitude towards privacy, and organizations to understand the criteria for the needed protection. A summary of the contribution of the papers is given in Table 1.2. A more detailed discussion on the contribution of the presented papers are presented in Chapter 4.

Table 1.2: *A summary of the contribution of the papers.*

Paper number	Contribution
1, 2 and 9	Individuals' concerns on personal information
2, 4, 5, 8 and 7	Constructs as protective measures
1	Dimensions for information privacy metrics
3	A conceptual method to bridge the knowledge gap between lawyers and technologists
6	A methodology for building information privacy metrics

The arrow that runs from *IS research* to the *Knowledgebase* shows the contribution of built artifacts to the *Knowledgebase*. The purpose of building the Knowledgebase is to use the knowledge in further IS research. This thesis filled in the Knowledgebase with several insights that can be used to develop or improve theories, constructs, models, and methods for protecting personal information.

Paper 3, which proposes a methodology for bridging the knowledge gap between lawyers and technologists, is a good starting point for bridging the mentioned knowledge gap. Papers 4 and 5 are good examples of how the contribution made to the Knowledgebase by Paper 3 can be used in subsequent research. The measures presented in Papers 4, 5, and 8 can be used to improve information security standards and best practice guidelines. The grounded theory paper (paper 7) also provides a complementary overall picture of the information privacy domain. This knowledge can be used to improve some existing theories or models. For example, the scope of the stakeholders' theory can be broadened to include personal information. The methodology presented in Paper 6 lays a foundation for building information privacy metrics and Paper 7 demonstrates the applicability of grounded theory to the information privacy domain.

Identified constructs

The primary purpose of having an information privacy metric is to demonstrate the level of protection given to personal information. The GT study shows there are two kinds of personal data. One is directly related to the identification of a data owner and the other one is about the behavioral aspects of the data owner. This category is further divided into behavioral, opinions, professional, and sensitive data. The identification category consists of direct identification, biometric, and weak identification data. Personal data owners are divided into highly privacy-concerned individuals, personal information disclosers, individuals under surveillance, and privacy victims. Personal data users are divided based on how they collect and use the personal information of personal data owners: with or without knowledge and consent. Protection

measures, which are used to protect personal information, are applied by personal data owners and personal data users. In addition to these two groups, there are other parties who contribute to the protection of personal data. One of the key measures is having the right attitude towards the protection of personal information. Additionally, the knowledge of legal rights and technological measures are also important. Personal data users should have the right attitude, a willingness to pay for protective measures, provide protection options to personal data owners, and enforcement. In terms of privacy protection technological measures, there are three broad categories: controls, transformations, and warnings.

Some high-level protective measures identified in Paper 2, 4, 5, and 8 are: personal information transmission media for sensitive and non-sensitive personal information, qualities of employees who handle personal information and administrative procedures in handling personal information, accounts creation and revocation procedures, the use of biometric-based access control systems, properties of good usernames, passwords, and security questions, best practices of reactivating lost-password accounts, managing cookies, terminating sessions, and measures to prevent accidental destruction, loss, and disclosures.

Chapter 4 presents the identified information privacy metrics based on the identified dimensions and constructs using a conceptual model. This conceptual model is also used to explain how these identified individual information privacy metrics can be put into a coherent information privacy metric that provides an overall indication.

1.7 Validation

Firstly, this section presents evaluation criteria for artifacts in general, followed by a discussion on evaluation criteria in the social and natural sciences together with how these criteria are met by the presented papers. This section concludes by discussing possible information privacy metric evaluation criteria.

1.7.1 Evaluation of a built artifact

The evaluation of a built artifact is important for demonstrating its utility, quality, and efficacy (Hevner et al., 2004). Utility refers to the usefulness of the designed artifact. In this particular research, utility is the usefulness to both organizations and individuals in fulfilling their needs, mentioned in the justification section (Section 1.3). Some quality attributes of metrics listed in the IS design literature are comprehensiveness, minimality, orthogonality, formality, usability, accuracy, validity, reliability, and implementability (Mustafa & Khan, 2005). As design science evaluation methods, Hevner et al. (2004) have

listed the observational case study or field study, analysis in the form of static, architecture, or dynamic, optimization, controlled experiments, simulations, functional and structural testing, and descriptive methods such as informed argument and scenarios. Moreover, Hevner et al. (2004) explicitly mentioned the possibility of using empirical techniques. Lee (2004) and March and Smith (1995) suggest any appropriate validation techniques available in the natural or social sciences.

Evaluation criteria

Yin (2003) has prescribed four validation tests for social scientists: construct validity, internal validity, external validity, and reliability. Lincoln and Guba (1985) have given four criteria for qualitative research validation: credibility, transferability, dependability, and conformability.

Construct validation:

As explained in Chapter 3, two methods suggested by Lee (2004) to generate constructs are Yin's (1994) case study research approach and Strauss and Cobin's (1998) grounded theory approach. Furthermore, Lee has suggested saturation for validating grounded theory based studies and construct validity for validating cases study based research. The construct validation criteria given by Yin (2003) are triangulation, chain of evidence, and the review of the draft case study. Triangulation can be done at several levels: data, investigator, theory, or methodological. Data triangulation can be done by getting the same fact from several means such as archival records, interviews, observations, surveys, and documents. Comparing conclusions reached from multiple sources of evidence is another construct validation criteria.

Saturation was applied in the GT work presented in Paper 7. The paper discusses how saturation and other validation criteria were applied in validating the study. A data triangulation is achieved in Papers 4 and 5 by gathering information from multiple parties such as Data Protection Commissioners in Europe and Privacy Commissioners in many other countries. Creating a case study database by giving references to online cases facilitates independent investigations. Reviewing the draft case study report by practitioners satisfied the construct validation criteria.

Credibility:

Since the purpose of qualitative research is to understand a social phenomenon (Pyett, 2003), the validity of the qualitative research is judged by how well the researcher presents the features of the investigated phenomena (Hammersley, 1987). According to Patton (1990), credibility depends on the analytical ability of a researcher and the quality of the empirical data. Therefore, the quality of social research can only be validated by the participants themselves (Trochim, 2006). Since this is not possible under normal circumstances, scholars have suggested some techniques to judge the credibility of qualitative re-

search. For example, peer debriefing has been proposed by Erlandson et al. (1993). Furthermore, prolonged engagement has been proposed by Lincoln and Guba (1985).

Paper 9, the self-reflection paper, invites the readers to corroborate the findings by comparing and contrasting their thoughts on privacy issues. The credibility of the studies presented in Papers 4 and 5 is established by creating a case study database with references to online cases. This facilitates others' independently investigating the findings. Peer debriefing was used in the study presented in Paper 1. A kind of peer debriefing was applied in the study presented in Paper 9. In preparing the first questionnaire, colleagues who did not work in the same research area were asked to analyze the research questions, research methods, settings, and design. Before finalizing the questionnaire, a drafted pilot questionnaire was given to some doctoral students working inside the department. The feedback helped modify the questions to make them simpler and more precise, eliminate ambiguity of language, and ensure the avoidance of leading questions. Member checking approach (Erlandson, 1993) suggests discussing the research method, the results, and the conclusions with the participants. This method was also applied, particularly in the study presented in Paper 2.

Reliability:

This is also known as dependability. This is the hardest part of social science research because social reality is always changing and there is no possible way to observe the same social setting twice. Quantitative researchers have constructed techniques such as true score testing to tackle this issue. Qualitative researchers tackle this issue by explaining research settings, any changes taking place, and the effects of those changes on the research settings. After explaining the research setting, it is up to readers to judge the repeatability of the research.

According to Yin (2003), reliability can also be established at the data collection stage by following a case study protocol and developing a case study database. The studies presented in Papers 4 and 5 have established their credibility by giving references to all the incidents examined. Similarly, other papers have given their respective research settings.

Internal Validity:

Internal validity discusses causal relationships. Therefore, it applies only to explanatory studies, not descriptive studies. This can be established at the data analysis stage by pattern-matching and explaining rival situations (Yin, 2003).

Conformability:

Conformability refers to the degree to which others corroborate the findings of the research (Lincoln & Guba, 1985). Auditing techniques are used to validate the dependability and conformability of qualitative research. This au-

diting process is quite similar to a financial audit. In the auditing process, an independent, competent person systematically reviews audit trails maintained by the researcher (Schwandt, 1997). Audit trails include but are not limited to raw data, personal notes, and field notes.

Peer reviews of the presented papers, presentations at conferences, and corroborating the findings with other similar studies, establishes the transferability and conformability of this research.

Papers 1 and 2 have also established their conformability by comparing and contrasting with similar studies.

Transferability and External Validity:

These refer to the use of the research findings in another setting. Building a strong theory from a single case study or using the replication logic in multiple case studies establishes its external validity (Yin, 2003).

Papers 1 and 2 meet this criterion by explaining the research setting. Once the research setting is explained, it is up to the second researcher to decide the transferability of the finding in another context. Another means of establishing the transferability is sending the findings to practitioners.

In general, it can be said that all the presented papers addressed the conformability and transferability criteria in qualitative research by presentions at conferences, reviews by peers, and corroborating the findings with other similar studies.

The validity of Paper 3, a conceptual paper, is established by successfully following the methodology presented in that paper for studies presented in Paper 4 and 5. The validity of this paper may be further established when other researchers start to follow the methodology.

The validity of Paper 8 is addressed in two different ways. Two authors independently explored the security and privacy issues of studied service providers. Then, both shared their experiences and conducted the experiments again. Then, the third author independently validated the claims made by the other two authors. In the exploring stage, we refrained from reading the privacy policies and security guidelines in order to not be guided by the information given by the service providers under examination.

1.7.2 Evaluation of metrics

Metrics have to be validated academically and practically. Academic validation focuses on the comprehensiveness of the metrics, while usability is the primary focus in practice.

A framework proposed for evaluating software engineering metrics (Kaner & Bond, 2004) can be customized to evaluate information privacy metrics. Tremblay et al. (2009) have conducted a focus group study to evaluate metrics designed for measuring information volatility in the health care system.

1.8 Limitations

One of the limitations of this research is that the research is heavily influenced by EU Directive 95/46/EC. Since this directive was introduced in 1995, the groundwork of this directive was carried out even before 1995. In that period, the Internet was not widely used. Therefore, sticking to EU Directive 95/46/EC, which is more than 15 years old, can be considered as one of the limitations. Secondly, not addressing the cost factor, which includes the cost of software, hardware, personnel, installation, running, maintenance, etc., is another limitation. The use of secondary data in the GT study is another limitation since the perceptions of the editorial board might have undermined the quality of the data. For example, the editorial board might have ignored some interesting articles, which would be interesting for this research, interviews' perceptions. Another limitation of the data in the GT study is the limited focus on countries outside the USA and Europe. The lack of adequate representative samples is one of the limitations of the surveys conducted. For example, it needs more representative and enough samples to validate the claim made in research question 3. As mentioned under research question 5, the Internet penetration and the cost of accessing the Internet has substantially reduced the use of IT resources at office space for private use. However, with the popularity of social media, there is a trend in accessing IT resources given for official work for private use. Another limitation of some studies is not continuously updating changes and improvements. For example, the latest changes made by online email services providers are not reflected in Paper 8 and the changes in perceptions are not reflected in Papers 4 and 5. Despite the fact that many surveys have shown that customers care about privacy (Taylor, 2003), the impact of a privacy label or metrics on changing the customers' attitudes has not been thoroughly studied. Only one study conducted by Tsai et al. (2007) has shown that a consumer is willing to pay extra for products and services supplied by more privacy friendly business entities. Therefore, it can be said that one of the identified limitations of this study and other research in information privacy policies is the lack of strong evidence illustrating the impact of presenting information handling practices in a more understandable and comparable manner. In other words, there is not enough research to demonstrate that individuals would use information privacy metric as a differentiator. One possible approach to identifying individuals' concerns about information privacy metrics and how they would use the metrics as a differentiator is conducting a grounded theory study with in-depth interviews of privacy-concerned individuals as the primary data source.

1.9 Summary of the Papers

This section provides a summary of the papers together with publication information of the published papers.

Paper 1: Attitudes Toward Privacy Amongst Young International Academics: Rasika Dayarathna and Louise Yngström

This paper was presented at the International Information Technology Conference (IITC) 2006 in Colombo, Sri Lanka. This paper presents the results of the study conducted at the Department of Computer and Systems Sciences (DSV) in Sweden in early 2005. The aim of this study is to identify privacy attitudes of young international academics in the field of information technology.

The participants were asked to provide demographic data, name the circumstances under which they would be willing to compromise their privacy, and identify the level, on a scale of 1 to 6, of the protection sought for twenty-nine given personal data items. Furthermore, there were some questions used to identify the respondents' experience using privacy enhancing technologies and their willingness to pay for those services.

This paper shows that the respondents strongly demand protection for their financial and medical records. Nevertheless, many sensitive personal data items defined in Article 8 of EU Directive 95/46/EC were not considered as being personal data items that need more protection. It also revealed that there is no significant relationship between demographic data and the level of protection required for personal information.

I took the main responsibility for conducting the study and writing the paper and the co-author guided me throughout the whole process.

Paper 2: Workplace Communication Privacy in the Digital Age: Prathiba Mahanamahewa and Rasika Dayarathna

This is one of the earliest papers on information privacy in Sri Lanka. Prathiba Mahanamahewa co-authored this paper and presented it at the International Information Technology Conference (IITC) 2005 in Colombo, Sri Lanka. The aim of this study was to gather the opinions of employees and employers regarding the monitoring of the Internet and email use by employees in public organizations.

Five public sector organizations covering telecommunications, education, public administration, and research were selected for the study. The reason for choosing these organizations was their experience with using ICT for a long time period. Out of three hundred and twenty-five questionnaires distributed, two hundred and fifty complete questionnaires were received.

This study is important in several aspects. First, it shows the perception of the parties in a situation of conflict. On the one hand, employers want to protect their assets and to have efficient services from employees. On the other hand, employees want to protect their privacy. This study gives a good insight into the conflicting goals, which are further discussed in the GT study. Another important aspect of the study was to lay a foundation for preparing a guideline for Sri Lankan public sector organizations. Indeed, this paper attracted the attention of policy makers and initiated the privacy debate in Sri Lanka. The paper proposes the importance of a written policy on email and Internet use, allocating separate time periods and resources for personal IT use, and publishing the policies of public agencies on the handling of personal information.

When the paper was written, Prathiba was a PhD student at the T.C. Berine School of Law at the University of Queensland, Australia. He had already collected the data and written the first two sections and most parts of Section 3. My contribution was data analysis and writing Sections 5, 6, and 7.

Paper 3: Towards Bridging the Knowledge Gap between Lawyers and Technologists: Rasika Dayarathna

This paper was published at the Second International Conference on Legal, Security, and Privacy Issues in IT (LSPI) in China and subsequent published in the *International Journal of Technology Transfer and Commercialisation* published by Inderscience.

This paper starts with examples of lawyers and technologists not knowing each other's languages. It then moves on to discuss the importance of having a globally accepted set of privacy principles. In the second section, a way to identify upper-level and functional-level information privacy requirements is presented. Finally, a template for the matrix that maps the identified organizational and technological measures and the functional-level requirements is drawn out. Another important focus of the paper is explaining how to deal with the exceptional circumstances mentioned in privacy legislation measures. Furthermore, this paper highlights the importance of incorporating court decisions, opinions, and verdicts given by the competent authorities, requirements mentioned in the existing security and privacy standards frameworks, and industry best practices.

The presented methodology would be useful for understanding legal privacy provisions, and the strengths and limitations of the technological measures used to protect personal information. This methodology was applied in the two studies presented in Papers 4 and 5.

Paper 4: The Principle of Security Safeguards: Accidental activities:

Rasika Dayarathna

This paper presents measures for protecting personal information against inadvertent incidents. The paper was presented at the Information Security South Africa (ISSA) 2008, Johannesburg, South Africa.

The principle of information security safeguards is a key information principle contained in every privacy legislation measure, framework, and guideline. This principle requires data controllers to use an appropriate level of safeguards before processing personal information. However, the privacy literature neither explains what this appropriate level is nor how to achieve it. Hence, a knowledge gap has been created between privacy advocates and data controllers. This paper takes a step towards bridging the aforementioned knowledge gap by presenting an analysis of how data protection and privacy commissioners have evaluated the level of adequacy of security protection given to personal information in selected cases of privacy invasion. This analysis also lays a foundation for building a set of guidelines for data controllers on designing, implementing, and operating both technological and organizational measures to protect personal information.

The empirical data for this study was obtained from decisions given by the European Data Protection Commissioners in the ninth annual report compiled by the Article 29 working party and selected decisions of the Australian, New Zealand, Canadian, and Hong Kong Privacy Commissioners.

Paper 5: The Principle of Security Safeguards: Unauthorized Activities:

Rasika Dayarathna

This paper was awarded the best student paper -runner award by the *Computer Law and Security Review—The International Journal of Technology Law and Practice*—at the third International Conference on Legal, Security, and Privacy Issues in IT (LSPI) in Prague, Czech Republic in 2008.

The methodology and empirical data sources discussed in Paper 4 were used in this study too. However, the focus of this study is protecting organizational assets and personal information from unauthorized activities, whereas Paper 4 addresses the prevention of inadvertent incidents. Both papers have identified instances where security measures invade personal privacy.

This paper presents several aspects of personal information, particularly when biometrics are allowed and disallowed in access control systems deployed at the entrance to physical premises, some privacy related functional requirements for information systems, how to train officers who handle personal information, some important aspects of training programs, and recommended personal information transmission media in sensitive cases.

Paper 6: Towards Building Information Privacy Metrics to Measure Organizational Commitment to Protect Personal Information: Rasika Dayarathna

This paper was accepted for presentation at the World Conference on Information Technology Bahcesehir University, 07–10 October 2010, Istanbul, Turkey (2010), but not presented [6].

The prescribed methodology is based on design science principles and a kind of grounded theory approach. In this study, the metric is considered as a scientific measurement instrument that is primarily used for the decision-making process. It is expected that the proposed metrics facilitate organizations in demonstrating their commitment to protect personal information. The methodology and metrics evaluation criteria are based on the seven design science guidelines presented by Hevner et al. (2004) for developing information system artifacts.

The constructs identified from the previously mentioned studies and from privacy and security surveys conducted by others are used as the primary building blocks for the intended metrics.

[6]This paper was accepted. The first part of the acceptance letter states "I am pleased to inform you that your full paper titled “Towards Building Information Privacy Metrics to Measure Organizational Commitment to Protect Personal Information” to the World Conference on Information Technology – 2010 has been accepted for oral presentation. Papers are oral presentations lasting 15 – 20 minutes, plus some time for questions. Your paper will be published in Procedia-Computer Science Journal (ISSN: 1877-0509) and at the same time indexed on the ScienceDirect, Scopus and Thomson Reuters Conference Proceedings Citation Index (Web of Science)."

Paper 7: Taxonomy for Information Privacy Metrics: Rasika Dayarathna

This paper was published in the *Journal of International Commercial Law and Technology*, vol. 6(4) (2011).

A comprehensive privacy framework is essential for the progress of the information privacy field. Some practical implications of a comprehensive framework would be the laying of a foundation for building information privacy metrics and having fruitful discussions. An important step in building a comprehensive framework is creating a taxonomy. This research study attempts to build a taxonomy for the information privacy domain based on empirical data. The classical grounded theory approach introduced by Glaser was applied, and incidents reported by the International Association of Privacy Professionals (IAPP) were used for building the taxonomy. These incidents include privacy related current research works, data breaches, personal views, interviews, and technological innovations. TAMZAnalyzer, an open source qualitative data analysis tool, was used in coding, keeping memos, sorting, and creating categories. The taxonomy is presented in seven themes and several categories, including legal, technical, and ethical aspects. The findings of this study could facilitate practitioners' understanding and discussing the subjects, and academics' carrying out research on building a comprehensive framework and metrics for the information privacy domain.

Paper 8: Is your E-mail Account Secure? : Feng Zang and Rasika Dayarathna

This paper was published in the *International Journal of Information Privacy and Security* vol. 6(1) (2010).

Electronic mail (email) is a widely used communication mechanism and is often used for communicating sensitive and confidential information. Therefore, the security of email communication has become an important issue. The media has often reported incidents of compromised email accounts. Therefore, studies of the strengths, limitations, and possible improvements of email are essential to protect the email communication system. This study examined the security and privacy protection mechanisms of four leading email service providers: Gmail, Yahoo mail, Hotmail, and AOL mail. A number of observations and experiments were conducted to understand the existing security and privacy protection mechanisms. For example, information stored at the user's machine and the service provider's end, the user's right to update and erase personal information stored at the service provider's end, and the strength of passwords and security questions were examined. In this study, several best practices and shortcomings were identified. These findings would facilitate not only the examined email service providers but also other online service providers' implementing better mechanisms to protect the security of their email services and their users' privacy. Additionally, this paper proposes some protection mechanisms that can be implemented by service providers, system developers, or both. This study also explores several research avenues for academia. For example, user friendly metrics for comparing the level of security and privacy protection given by service providers, and choosing memorable, but strong passwords and security questions.

Rasika conducted the initial experiments and invited Feng to validate the findings. Feng conducted the experiments again and joined with Rasika to finish writing the paper. The paper was written in an iterative manner.

Paper 9: A Self Reflection on Privacy: Rasika Dayarathna

This paper is published at the Social Science Research Network (SSRN) eLibrary. This paper can be accessed from http://ssrn.com/paper=1879904

Privacy is very subjective and has been interpreted in a number of ways. Additionally, there are several paradoxes in the field. For example, a number of researchers have shown a substantial gap between privacy attitudes and the related behavior. These kinds of paradoxes hinder progress in the field. One way of addressing these issues is studying privacy attitudes and the underlying rationales behind these attitudes on the part of individuals. This study presents this researcher's frame of reference for privacy, with a special emphasis on information privacy. This paper explains privacy in religious, social, and legal contexts, reasons for privacy invasive behaviors, ways and means of privacy protection, and reasons for demanding privacy. The aim of this paper is to take a step in building a common understanding, which is essential for developing a global data protection regime. At the end, elaborating some real-world examples, this paper discusses the importance of information privacy for information system researchers. Furthermore, this paper invites the readers to compare and contrast their own views on privacy.

Outline of the thesis

This chapter, Chapter 1, laid the foundations for this thesis. It presented the main research problem and research problems, the justification for the research, the research design, the research evaluation, limitations, contributions, avenues of future research, and a summary of the papers presented. Chapter 2 contains a literature review that discusses the existing literature, and Chapter 3 presents research methodologies that lead to the foundation for the research decision given in Section 1.5. Chapter 4 presents the research contribution and Chapter 5 discusses some concluding remarks. Finally, the nine papers are included.

2. Literature Review

2.1 Chapter Introduction

This chapter gives a brief but comprehensive overview of information privacy with a special emphasis on privacy principles, privacy assurance methods, and the measures taken by organizations to inform the user about the level of protection given to their personal information. This chapter concludes, in Section 2.8, by emphasizing the need for identifying constructs for building information privacy metrics through future research work. The following part of this section and Sections 2.2, 2.3, 2.4, and 2.6 have previously been presented in a thesis for the degree of Licentiate of Philosophy (Dayarathna, 2007) [1].

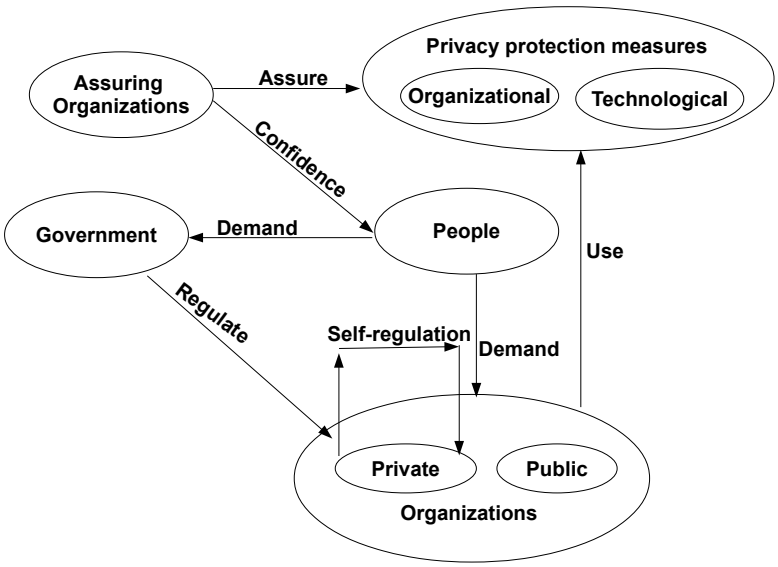


Figure 2.1: Actors, factors, and their relationships in information privacy

Figure 2.1 shows the actors, factors, and their relationships in the area of information privacy. This diagram depicts the demand for the protection of personal information from governments and organizations. Here, the organi-

[1] minor corrections were made

zation can be either governmental or private. Laws made by legislators for the protection of personal information regulate the conduct of these organizations. In addition to fulfilling their legal obligations, private organizations react to customers' demands by adopting a self-regulatory approach. Organizational and technological measures are used by both kinds of organizations to protect personal information. To gain a competitive advantage, private organizations showcase the quality of the protection they give to personal information. However, people are not ready to blindly accept the claims made by private organizations. Assurance organizations come to help organizations and users alike. They play the role of an independent, trusted third party. They evaluate the protection measures deployed and grant a certificate of conformity if the organization meets the evaluated criteria. Once a certificate is obtained, an organization is in a good position to showcase its concern for customers' personal information. This helps the organization build customers' trust.

Throughout this chapter, the above-mentioned actors and their roles are discussed. The second section lays out a discussion on privacy, information privacy, and how the demand for information privacy has been evolving over time. Section 2.3 discusses privacy principles and Section 2.4 gives an overview of the assurance criteria applied in information security and privacy. Privacy policies and alternatives are discussed in Section 2.5, and Section 2.6 emphasizes the need for a methodology for measuring information privacy protection measures and the advantages of having a methodology. Section 2.7 discusses information privacy in the future. This chapter concludes by suggesting future research into building a criterion to measure information privacy protection measures.

This literature survey was mainly driven by Article 17 of EU Directive 95/46/EC. That article mainly focuses on the concept of an adequate level of protection for personal information. This article also gives some indicators for determining the appropriate level of protection. It states:

> "Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected."

This statement is depicted in Figure 1.3 and explained in Section 1.4 in Chapter 1.

2.2 Information Privacy: A Hot Topic

This section discusses the importance of privacy protection in the information era, some definitions that have been given to privacy, the historical background of privacy, and the approaches used to legislate for the protection of information privacy.

When one hears the terms 'information privacy' or 'data protection,' the first question that one might ask is 'why are these concepts so important?' Some people say they have nothing to hide; this is not true. According to Solove (2007), everyone has something to hide. The answer to the question posed above is simple: Privacy has become one of the most important human rights (Rotenberg, 2000). Volio (1981), a leading privacy advocate, stated that "in one sense, all human rights are aspects of the right to privacy." The Australian Privacy Charter states: "Privacy is a key value which underpins human dignity and other key values" (Australian Privacy Charter Council, 2009). The advancement and heavy use of technology has made it more convenient and economical to infringe on privacy rights by collecting, processing, and disseminating personal information. In order to counter these threats, a number of initiatives in different fields have been taken. These measures are called data protection or information privacy protection. These measures include, but are not limited to: studies of personal information handling practices, the introduction of technological countermeasures, and the adoption of data protection legislation measures.

Some blame technology for widening privacy threats. However, when we take a closer look, it can be seen that technology facilitates privacy protection. For example, in the conventional postal mail system it is not possible to get a magazine without revealing one's residential address. Thanks to email, it is now possible to obtain an electronic version of the same magazine without revealing this information. Though the possibility of identifying the subscriber's address still remains, finding this information would take a great amount of effort. Another example is the Caller Line Identification (CLI) facility that enables call receivers to decide whether to answer or drop a telephone call. This feature was not available in the traditional analog telephone system.

2.2.1 Defining Privacy

There are many definitions of privacy. However, there is no universally accepted definition for privacy. One reason for the lack of a generally accepted definition for privacy is that privacy is perceived from different angles. As the Privacy and Human Rights Report published by Electronic Privacy Information Center (EPIC) (2003) points out, the perception of privacy depends on various factors, such as context and environment.

The definition of privacy given by Alan Westin is widely cited in privacy papers and articles. He has defined privacy as follows:

> "The claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others (Westin, 1970)."

According to a report published by the Calcutt Committee in the United Kingdom, privacy is

> "The right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information (Calcutt, 1990)"

Some Aspects of Privacy

There are many aspects of privacy. Obtaining an exclusive list of different aspects of privacy is not possible. The Privacy and Human Rights Report—2003 lists four aspects of privacy including information privacy, bodily privacy, privacy of communication, and territorial privacy (EPIC, 2003). The Australian Privacy Charter has one more item which is termed "...the freedom from surveillance" (Australian Privacy Charter Council, 2009). The Privacy and Human Rights Report—2003 has incorporated the freedom from surveillance as a part of territorial privacy. It is difficult to draw a line between these two privacy concepts. For example, in most cases, information privacy has become a part of the privacy of communication, since personal information is communicated through communication channels. This reveals the lack of common standards on the issue. The following list is extracted from various literature sources. There are many overlaps between these concepts.

- **Information privacy**. Information privacy is related to the protection of personal information. According to the Australian Privacy Charter, personal information is any kind of information about an identified person (Australian Privacy Charter Council, 2009). However, European Directive 95/46/EC extends this to an identifiable person (95/46/EC, 1995).
- **Bodily privacy**. Bodily privacy entails protection from experiencing invasive bodily inspections. This includes protection against the testing of bodily elements including blood, DNA, and genetic material (EPIC, 2003).
- **Privacy of communication**. Privacy of communication covers privacy related to all types of communication such as postal mail, email, and telephone conversations (EPIC, 2003).
- **Territorial privacy**. Territorial privacy prevents intrusions into domestic places, work places, and public spaces (EPIC, 2003).
- **Surveillance privacy**. Surveillance privacy includes the prevention of various searches including video surveillance and ID checks. Some of

the literature categorizes this as a kind of territorial privacy (Westin, 2004).

- **Spatial privacy or location privacy**. Spatial or location privacy covers masking the current geographical location and the surrounding environment (Onsrud, Johnson, & Lopez, 1994).

2.2.2 Historical Background

The underlying grounds of current privacy invasion cases are quite similar to those of past cases. The key difference is the wide use of ICT in present cases. In other words, the grounds are the same but the face is different due to the involvement of ICT in present cases. The lessons learned from past privacy cases can be applied to shape modern ICT systems and make new laws. The following legal cases are extracted from the electronic document titled "Rights of the People—Individual Freedom and the Bill of Rights" (Rights of the People—Individual Freedom and the Bill of Rights, 2003).

The demands for information privacy protection and their evolution are very interesting and worth studying. In 1763, Sir William Pitt and the Earl of Chatham commented on the right of an Englishman in his home. They stated:

> "The poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail its roof may shake the wind may blow through it the storm may enter the rain may enter but the King of England cannot enter; all his forces dare not cross the threshold of that ruined tenement."

In the 18th century, many families lived in very small houses that had a single room. In this situation, privacy was closely tied up with reputation and defamation. It was prohibited to make one's behavior or picture public without the individual's consent. This was done to prevent reputation damage.

Pamphelt, in commenting on the government's attempt to collect taxes based on the consumption of beers in Massachusetts in 1754, stated:

> "It is essential to the English Constitution, that a Man should be safe in his own House; his House is commonly called his Castle, which the Law will not permit even a sheriff to enter into, but by his own Consent, unless in a criminal case."

The historical cases highlighted above represent some important milestones and also reveal the importance of privacy. According to the aforementioned cases and other reported cases, privacy is directly related to reputation, dignity, democracy, discrimination, oppression, genocide, freedom of association, freedom of expression, etc. (Mahanamahewa & Dayarathna, 2005).

The rapid growth and advancement of information and communication technologies has enabled many parties to enter into others' houses without tres-

passing. It is now possible to retrieve more data from one's residence through technology than would be possible to collect by physically trespassing. In the ICT era, placing orders via the Internet and mobile phones leaves many records in many hands. For example, parties such as service providers, network service providers, suppliers, delivery agencies, and bankers may get some personal information. With the immense power and low cost of storing and processing data, an individual's profile can be built within a matter of seconds. Privacy infringers can learn a lot about their victims from this profile without stepping into their residences. Governments may use this profile not only for tax collection but also to get obtain other sensitive information such as political opinions, trade union affiliations, etc. Some other parties might get to know very sensitive information such as health information, sexual preferences, and religious and philosophical beliefs. Under these circumstances, physically living alone does not mean that one enjoys a true sense of the right to be left alone, especially when the individual does not have information privacy protection. According to Mohammed, the key aspects of information privacy are not being subject to unwanted intrusions, having control over personal data, and being aware of the movement of such data (Mohammed, 1999). There is a massive threat to information and spatial privacy in the information era.

The difference between data protection and information privacy is marginal. Since data protection covers only a limited aspect of information privacy, it can be said that data protection is a subset of information privacy. According to Article 3 of EU Directive 95/46/EC, the directive applies to data processing done wholly or partly by automated means or through the processing of data forms, a filing system, or part of a filing system (95/46/EC, 1995). However, the Privacy and Human Rights Report—2003 states that information privacy is also known as data protection (EPIC, 2003).

Before introducing data protection legislation measures, many countries had their own privacy legislation laws in place. The intention of those privacy legislation measures was to protect the privacy of individuals from unwanted intrusion. Studying the rationality behind those privacy legislation measures gives valuable insights on information privacy.

One interesting milestone is the introduction of the Fourth Amendment to the Constitution of the United States. This was intended to protect "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures…" (Amsterdam, 1974). Even though the term 'privacy' is not mentioned in this clause, it can be seen that the intention of the writers was to protect individuals' privacy. In the 1928 case *Olmstead v. United States* (Olmstead v. United States), Justice Louis Brandeis, giving a dissenting judgment, stated that every unjustifiable invasion of an individuals' privacy violated the fourth amendment irrespective of the methods applied. The case *Katz v. United States* (Katz v. United States) provided the basis for having a "reasonable expectation of privacy." The Katz test states that when

an individual expects a reasonable level of privacy, any governmental action invading that expectation violates the individual's right to privacy.

The dissenting judgment given in *Olmstead v. United States* and the judgment resulting from *Katz v. United States* suggest that unjustifiable government invasions in any form or nature violate one's right to privacy. This broad suggestion can be carried over and applied to any technological means used in the information era. Even though the previously mentioned judgments focused only on the actions of governments, the judgments can be extended to cover any means of invasion of one's privacy on the basis that privacy is a fundamental human right. However, the legislation measures introduced thereafter as well as some recent judgments have limited the scope of the rights recognized in the judgments illustrated above. For example, the Wiretap Act applies only to voice and face to face communication. The judgment given in the case *United States v. Miller* (Bellia, 2006) pointed out that having a reasonable expectation to privacy is not possible when information is given voluntarily. In the case *Smith v. Marylan* (Bellia, 2006), it was suggested that the acquisition of transactional data does not violate one's right to privacy because, in this case, the plaintiff was well aware that transactional data was available to his telephone service providers.

In 1968, the Wiretap Act was introduced by the United States Congress. The basis for this act was the judgment given in *Katz v. United States* (Bellia, 2006). This act prevented unwarranted seizure and searches of public communication lines. It also laid down strict rules for obtaining a warrant. The Electronic Communications Privacy Act (ECPA) of 1986 extended some of the provisions contained in the Wiretap Act to cover electronic communication.

2.2.3 Privacy in the Legal Context

Privacy has been recognized as a fundamental human right in Article 12 of the Universal Declaration of Human Rights *(The United Nations and Human Rights 1945–1995, 1995)*, Article 17 of the International Covenant on Civil and Political Rights *(International Covenant on Civil and Political Rights, 1966)*, and in many other international and regional human rights treaties. There are three different legal means used to protect information privacy. They are the general data protection approach, which covers almost every sector, sector specific laws, which focus on specific sectors, and the self regulation approach based on best practices. European countries have applied the first approach while the USA prefers the sector specific and self regulatory approaches (EPIC, 2003).

General Data Protection Laws

The first data protection act was passed by the parliament of the West German state of Hesse. The first national data protection act, Sweden's Data Act, was

passed in 1973. The German Parliament passed the German Federal Data Protection Act in 1997. After that, many counties such as France, Austria, Denmark, and Norway introduced similar legislation measures (Fischer-Hübner, 2001).

Significant milestones include EU Directive 95/46/EC on the protection of individuals with regard to the processing and free movement of personal data and EU Directive 2002/58/EC on data protection in telecommunications. EU Directive 95/46/EC is a general data protection directive which applies to every sector while EU Directive 2002/58/EC focuses on the telecommunications sector. Member countries of the European Union are compelled to implement national laws based on these directives. They can also incorporate more strict regulations; however, they can not lessen the requirements imposed in the directives.

Sector Specific Laws

The USA has taken the sector specific and self regulatory approaches. It has enacted data protection legislation for targeted sectors including the financial, medical, and video rental sectors. The rest of the sectors are asked to be self disciplined. In other words, those sectors are expected to adopt the self regulatory approach. Some of the sector specific acts in the USA are The Cable Communications Privacy Act of 1984, the Video Privacy Protection Act of 1988, the Fair Credit Reporting Act (FCRA)of 1970, the Driver's Privacy Protection Act of 1994, the Health Insurance Portability and Accountability Act (HIPAA) of 1996, and the Electronic Communications Privacy Act (ECPA) of 1986.

Self Regulation

This approach has certain advantages and limitations. The key advantages are the possibility of immediately reacting to market demands and the limited burden on the merchant. On the other hand, there is very little room for legal enforcement. For example, in the case *Dyer V. Northwest Airlines Corp* (Dyer V. Northwest) the court held that a privacy policy can not be legally enforced. In addition, there is no mechanism to compensate the harmed individuals (Noam, Swire, Varian et al., 1997).

2.3 Privacy Principles

The following section gives an overview of the history of the Fair Information Practice (FIP) and an analysis of the OECD privacy principles. The discussion then moves on to compare different sets of privacy principles introduced by leading privacy groups. The next section lists some suggested privacy principles. The final section discusses the importance of developing a new set of privacy principles.

In the early 1970s, a committee was appointed by the United States Congress to study matters relating to the social security number (SSN) system in the USA. The committee presented its report titled "Records, Computers and Rights of Citizens" in 1973. The Code of Fair Information Practices was introduced in this report. This set of codes was influenced by the Fair Credit Reporting Act (FCRA) of 1970. The Code of Fair Information Practices became the base for the Federal Privacy Act of 1974. Another committee, the Privacy Protection Study Commission, presented a report titled "Personal Privacy in an Information Society" in 1977 (Ware, 2007). The Organization for Economic Co-operation and Development (OECD) presented a set of privacy guidelines in 1980 (Clarke, 2009), which was the first attempt to protect information privacy at the global level.

1. Principle of Collection Limitation

P1. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

This principle has three parts; they are:

1. Limits to the collection of personal data
2. Obtaining personal data by lawful and fair means
3. Obtaining personal data with the knowledge and consent of the data subject

Limits to the Collection of Personal Data.

This principle does not specifically mention any limits. In his article "Asia–Pacific Developments on Information Privacy Law and its Interpretation," Greenleaf argues that this is one of the weak points of this principle (Greenleaf, 2006). The explanatory notes to the OECD privacy guidelines suggest some criteria to limit the collection of personal data. According to that report, the committee studied various ways to specify the limitations. One of the approaches was categorizing personal data according to its sensitivity. In the end, they concluded that it was not possible to identify a universally acceptable criterion (OECD, 1980). Although this argument has some merit, the European Data Protection Directive has categorized some personal data as sensitive; consequently, the European Union has demanded additional protection for sensitive data (95/46/EC, 1995). Another suggested means is limiting the collection of personal data to the intended purpose. In other words, it has been suggested that data controllers be prevented from obtaining more personal data than is necessary for the intended purpose. This concept is also known as purpose binding. Figure 2.3 illustrates this position.

The triangles in the big circle represent data items such as date of birth, name, address, and telephone number. An organization collects information

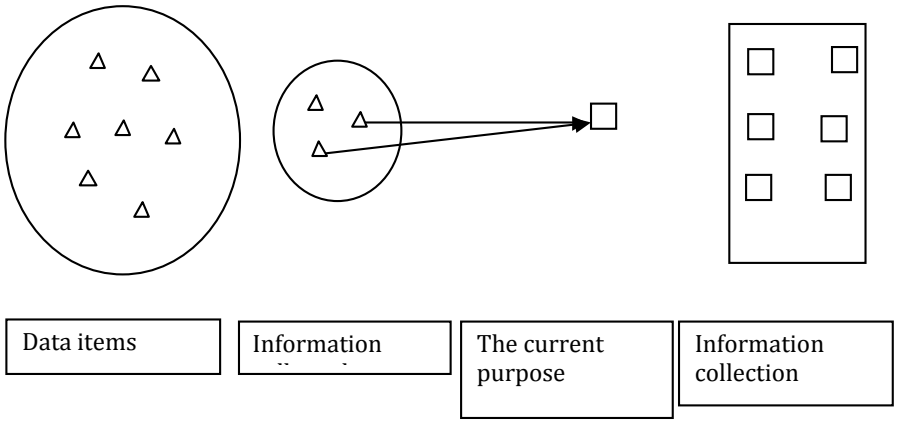


Figure 2.2: The principle of collection limitation

for various purposes. These purposes are represented by the small boxes in the large rectangle on the right-hand side of the diagram. The isolated box represents the current purpose. In this case, the organization collects three data items but uses only two of them for the intended purpose. For example, an organization may collect a full name and address to send a mailer. However, it can be shown that obtaining the intended recipient's full name is not necessary for the purpose. In some contexts, a full name may reveal other information such as caste, religion, place of birth, etc.

Obtaining Personal Data by Lawful and Fair Means

This OECD guideline does not adequately explain this condition.

Obtaining Personal Data With the Knowledge and Consent of the Data Subject

There are two parts in this clause. One is knowledge; the other is the consent of the data subject.

Knowledge – There may be cases where personal data is collected with the knowledge but without the consent of data subjects. The knowledge of data subjects regarding data collection prevents collecting personal information through hidden or covert channels.

Consent – Personal data is collected with the knowledge and consent of the data subjects. Consent is a much broader term than knowledge because it conveys the willingness of the data subjects to provide personal information. However, the guideline is silent on when and for what purposes consent is needed. There are some cases where it is not possible to get the consent of data subjects. For example, consent may not be possible in cases where the data subjects are minors or are mentally disabled. Another example is where data collection is being administered by law enforcement authorities who are conducting investigations.

2. Principle of Data Quality

P2. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

According to this principle, obtaining perfect data is not required; however, the data collected must be fit for the purpose(s) for which it will be used. This is to ensure that the intended purpose is effectively fulfilled. This prevents using irrelevant, inaccurate, incomplete, or outdated data for the intended purpose.

3. Principle of Purpose Specification

P3. The purposes for which personal data are collected should be specified not later than at the time of collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

According to this principle, informing the data subjects of the purpose for which the data is to be collected and used is required. The data subjects must be informed before the data is collected. This enables the data subjects to make an informed decision about whether or not to disclose personal data. The collected data can only be used for the initial purposes and for other purposes which are not incompatible with the original purpose. If the collected data is to be used for unrelated purposes, the data subjects must be informed. However, according to the principle mentioned above, obtaining a new consent is not required. Another controversial point is how to determine whether a given purpose is incompatible with the original intended purpose. Some of the literature mentions terms such as directly related purposes, related purposes, loosely related purposes, compatible purposes, non-compatible purposes, reasonable expectations, etc. This shows the need for a better mechanism to identify what constitutes a compatible purpose. The explanatory note to this principle further suggests that the data be erased or made anonymous once the purpose is fulfilled.

4. Principle of Use Limitation

P4. Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified in accordance with [Principle 3] except: (a) with the consent of the data subject; or (b) by the authority of law.

The collected personal data should be used only for the purposes for which the data was collected. If the collected data is necessary for other purposes, a fresh consent has to be obtained from the data subjects. One exception to this is when the data is to be used for legally authorized purposes.

5. Principle of Security Safeguards

P5. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.

This principle is about using security measures to protect personal data against loss, destruction, and modification. It is also intended to prevent the use of information for unintended purposes. The measures used to fulfill this principle can broadly be divided into physical measures, organizational measures, and technical measures.

6. Principle of Openness

P6. There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data and the main purposes of their use as well as the identity and usual residence of the data controller.

This principle gives data subjects the right to get to know the following at no cost or at a reasonable cost:

1. The identity of the controller and its residential address
2. The nature of the personal data held by the controller
3. The main purpose of retaining the data
4. The way in which the collected personal information is handled

One of the limitations of this principle is that it does not give the right to know the secondary purposes.

7. Principle of Individual Participation

P7. An individual should have the right

1. to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
2. to have the data relating to him communicated to him
3. The main purpose for retaining the data

   I within a reasonable time;
   II at a charge, if any, that is not excessive;
   III in a reasonable manner; and
   IV in a form that is readily intelligible to him;

5. to be given reasons if a request made under sub-paragraphs (a) and (b) is denied, and to be able to challenge such denial; and
6. to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Some of the key features of this principle are:

The right to access the collected personal data. Data subjects have the right to obtain a copy of personal data that was retained by the data controller.

The right to make necessary corrections. Data subjects or another party acting on behalf of the subjects have the right to correct and/or complete the information retained.

The right to challenge the data controller. Data subjects have the right to make a complaint to the data protection authority if a legitimate request by a data subject to access the retained data has been turned down by the data controller.

8. Principle of Accountability

P8. A data controller should be accountable for complying with measures which give effect to the principles stated above.

This means all parties engaged in handling personal data are responsible for the collected personal information. This includes data controllers and other parties working for data controllers.

There is no well accepted set of privacy principles. The OECD itself points out that its privacy principles have overlaps (OECD, 1980). The overlaps make it difficult to understand the principles and to build a privacy risk classification scheme. These weaknesses have led other organizations to introduce their own proprietary sets of privacy principles. However, it can be seen that there are some common elements written in different terminologies. Table 2.1 makes a comparison of four different sets of privacy principles introduced by four leading parties in the domain of information privacy. The eight principles introduced by the OECD are given in the first column. The second and third columns present the privacy principles introduced by the AICPA/CICA and the ISTPA, respectively. A brief description of these organizations is given in pp. 82–84. The last column presents the privacy principles introduced by the Privacy Incorporated Software Agent (PISA) project (Blarkom et al., 2003). As shown in the table, except for the PISA principles, three other organizations have presented eight (8) privacy principles. Furthermore, these principles have similar meanings [2], though they have different titles. The PISA project, which is a very European project, introduced two additional principles. These are transferring personal information outside the Europe Union and processing personal information by a processor.

Greenleaf (2006) presents the privacy principles mentioned in some national data protection legislation measures for the Asia–Pacific Economic Cooperation (APEC). However, some of these suggested principles are mentioned in the OECD guidelines in an implicit manner. The principles are:

Collection from the individual. Personal information should be collected from the data subject. Collecting personal information of the data subject from other sources is admissible when it is not possible to collect information directly from the data subject.

[2] see Section 2.3 for more detail

Table 2.1: *A comparison of the data protection principles defined by various organizations.*

OECD Guidelines	**AICPA/CICA**	**ISTPA**	**PISA**
Purpose specification	Notice	Interaction	Lawful basis for data processing
Collection limitation	Choice and consent Collection	Negotiation	As required
Data quality	Quality	Validation	Data quality
Use Limitation	Disclosure use and Retention	Usage	
Security safeguards	Security	Control	Protection against loss and unlawful processing of personal data
Openness	Management	Audit	Transparent processing
Individual participation	Access	Agent, Access	Rights of the parties involved
Accountability	Monitoring and Enforcement	Enforcement, Certification	Reporting the processing
			Data transfer to countries outside the EU
			Processing personal data by a processor

Data retention. Once the collected data have fulfilled the purposes for which the data was collected, the collected data must be erased.

Third party notice of correction. The recipient of incorrect information has a right to be informed when the correction is made.

Anonymity. Subjects have the right to have anonymous transactions whenever it is possible and practical.

Identifiers. Sharing identifiers is limited or restricted.

Automated decision. Individuals have the right to ask for a revision of an adverse decision taken by an automated processor. The review must be done by a human.

Sensitive information. This kind of information requires special protection.

Public register principle. There must be limits on the collection of personal information by public registers.

There is a need for a more human friendly set of privacy principles. A more fundamental objection to the OECD privacy guidelines is the lack of attention given to the human rights aspect. By the 1980s, many developed countries had their own data protection laws. Unfortunately, these laws created some barriers for the free movement of personal information. The main intention of introducing the OECD privacy guidelines was to lift the barriers and construct an environment conducive for business (Clarke, 1997). The guidelines were not meant to protect our privacy rights. The above grounds stress the importance of having a new set of privacy principles which are more related to the protection of individuals' privacy rights. They can be an enhancement to the existing privacy principles or a completely new set of principles. There is a movement for privacy friendly information protection principles. Justice Michael Kirby, who was the chair of the expert group of the OECD privacy guidelines development team, is at the forefront of this movement.

2.4 Privacy Assurance

Legal privacy provisions, acts, case laws, and privacy principles were discussed in the previous section. One of the challenging questions in the area of information privacy is how to assure that the protections given to personal information are reasonably adequate. The following section discusses various approaches used to assure the protection given to personal information. Furthermore, it discusses the merits, demerits, applicability, and effectiveness of personal information protection measures.

2.4.1 Assurance

An organization has many policies. A privacy policy is one of them. It is a statement which directs the handling of personal information. In other words, it spells out what is allowed and disallowed for the personal information held or to be collected. The AICPA/CICA Privacy Framework defines a privacy policy as a written statement that conveys the management's intents, objectives, requirements, responsibilities, and/or standards (AICPA/CICA, 2004). The privacy policy is based on privacy and other relevant legislation measures, directives, privacy standards, industry best practices, social demands, etc. A combination of privacy tools, methods, standards, and procedures is used to implement and enforce a privacy policy. The next problem is how to measure the effectiveness of a privacy policy and its enforcement measures.

We have privacy principles. The important question, however, is how to know whether an organization is adhering to these principles. How can we assess and compare products and services offered by different organizations in

terms of the protection given to personal information? Can we trust the claims given by an organization?

Organizations simply say their products and services are in accordance with the accepted privacy principles. How can we validate their claims? Do we have enough competence and ability to assess their claims? There is a solution to these questions based on the following simple trust model. That is: if X can trust Y and Y can trust Z, then X can trust Z. Here, Y is a trusted third party that independently evaluates and certifies products and services. The given certificate is a formal and official document. It states that the evaluated product or system has the properties and functionality claimed in its documentation and that the evaluation process was conducted in a systematic manner (ITSEC). The evaluation can be based on different aspects, such as security, privacy, legal compliance, etc. In this study, the focus is put on information privacy aspects. The certificate facilitates our making informed decisions.

Even though trust can not be precisely quantified, assurance gives some sort of indication of the trustworthiness of the evaluated system. Figure 2.4 depicts the meaning of assurance in a graphical manner. Here, the deliverables are meant to fulfill the stakeholders' needs. These deliverables can fulfill the stakeholders' needs if they have the required properties. Before using the deliverables, the stakeholders want to make sure that the deliverables contain the necessary and adequate level of properties needed to meet their requirements. Assurance organizations that act as independent third parties come into the scene at this point. After evaluating the systems, they certify that the deliverables have the ability to fulfill the users' requirements. The assurance certificate gives confidence to the stakeholders since a competent, trusted third party has certified the quality of the deliverables.

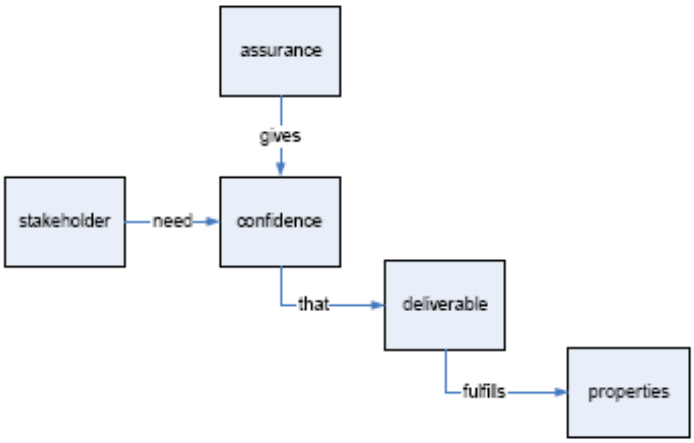


Figure 2.3: Assurance and confidence – Hansen, Kohlweiss, Probst, Rannenberg, & Fritsch et al., (2005)

An assurance process focuses on the entire life cycle; a system specification focuses on design and implementation. The process requires a thorough review of the system from different angles. For example, giving an assurance certificate for a computer requires a sequence of steps including a detailed specification of the desired (or undesirable) behavior and an analysis of the design of the hardware, software, and other components. These are needed to demonstrate the quality of the life cycle of the deliverable.

From the Privacy Point of View

As discussed above, and shown in Figure 2.4, an assurance process requires a thorough review of the system under investigation. The next questions are in the domain of information privacy: they ask what are the necessary elements of a review process, whose job it is to do what, etc. Looking at the life cycle of the personal information and the life cycle of an IT system, two different sets of requirements can be identified. The other vital aspect is the environment of the operation because different environments (i.e., sectors, geographical areas, and jurisdictions) require various assurances and assurance levels (Hansen et al., 2005). The following list, which has been extracted from data protection legislation measures and directives, gives some identified elements for a review process. However, this list is not complete. These elements are: data contents, the amount of data, the purpose of the processing, processing methods, processing operations, circumstances surrounding the processing operations, technological methods used, social demands and pressures, employees' personal perspectives, the nature and size of the processing organization, and the consequences of mishandling the data.

2.4.2 Benefits of Assurance

In the previous sections, the need for information privacy assurance was discussed. This section discusses the advantages of information privacy assurance.

Ordinary users do not possess enough technical capabilities and legal knowledge to assess information systems in terms of information security and privacy. Therefore, they need the services of other competent parties to assess the quality of an ICT system. However, only a few consumers can afford the cost. The role of assurance parties is needed at this point. Here, the cost of assurance is paid for by vendors and manufacturers in most cases. The benefits of this go to the customers. A system can be assured based on a number of assurance criteria and assurance levels. Customers have a choice in selecting the assurance criteria and the levels. For example, a legal compliance certificate states that the system is in compliance with the given legislation.

There are some cases where possessing this certificate is mandatory for engaging in a business. For example, GMSH, the central procurement authority

of the German Federal State, has integrated the privacy seal into its tender evaluation processes (Hansen et al. ,2005).

Service providers and developers use assurance certificates to build their customers' trust. The trusted third party assurance process plays a vital role. The assurance certificate is the key trust building method in countries where there is no legislative protection for information privacy or where the existing legislative protection does not cover specific sectors. In addition, there are cases where the existing legislative coverage is insufficient or outdated due to changes in societal contacts or technological developments. In these cases, the trusted third party assurance process fills the gap.

Organizations can use their assurance certificate to gain a competitive advantage. A thorough assurance process identifies system vulnerabilities at very early stages. This process leaves room to fix bugs before putting the products in the market. Another advantage is that the level of assurance can be used as a yardstick to measure improvements over time.

2.4.3 The Existing Security Evaluation Criteria

Since there are few privacy specific assurance criteria, the way information security could help is worth looking at. There are good reasons for looking at the information security field. In a technical report published by the Privacy and Identity Management for Europe (PRIME) group, Hansen et al. (2005) state that the knowledge of information security is at a more mature stage than is that of information privacy. The same report has quoted a statement made by the Privacy Enhancing Technology Testing and Evaluation (PETTEP) project, which states: "The same building blocks can be used for building a privacy house as for building a security house" (Hansen et al., 2005). The International Security, Trust and Privacy Alliance (ISTPA) project thanks the existing information security frameworks and standardized security technologies and services because they have made the duties of information privacy practitioners much easier (ISTPA, 2001).

It is also argued that information privacy can be viewed as a part of information security and that all information security protection measures can be applied toward information privacy protection. For example, information privacy can be well covered by implementing a proper access control mechanism for personal information (Hansen et al., 2005). Some legislation measures have taken information security as a part of information privacy. Articles 17 and 25 of EU Directive 95/46/EC and other privacy assurance frameworks have included information security as a part of data protection.

2.4.4 Privacy Assurance Methods

Information privacy assurance criteria can be divided into three categories: privacy process oriented assurance, organizational assurance, and privacy product

assurance. Privacy process assurance focuses on how the information processing operations are carried out. This process is quite similar to process oriented information security audits such as COBIT, ISO/IEC 17799, and BS 7799. Sometimes privacy process assurance is called a privacy audit. Organizational assurance focuses on the management of information privacy, which includes how an organization adapts to new or changed processes, new privacy laws, and technological developments. Privacy product assurance evaluates the effective implementation of privacy protection measures in IT products, which covers software, hardware, or any other static state (Hansen et al., 2005).

Privacy Product Assurance

The following section discusses some product specific security evaluation criteria. The ITSEC, the TCSEC, and the Common Criteria (CC) are classical security evaluation criteria used to evaluate the information security aspects of IT products. The CC has a special class for information privacy and some other classes in the CC can also be used to evaluate privacy protection measures. At the end of this section, some suggestions given by scholars for improvements of the CC are given. Special attention is given to information privacy.

Trusted Computer System Evaluation Criteria (Orange Book)

This standard was developed by the Department of Defense of the United States (DoD). The primary objective of this standard is to support the evaluation and classification of information security controls. This standard can also be used to select appropriate security mechanisms for a computer system. Since the primary interest of the DoD is confidentiality, this standard heavily focuses on confidentiality when sensitive or classified information is concerned. It defines two security policies. One is the mandatory security policy, which enforces access control rules. These rules define individual users, their authorization status, and information classification categories. The other policy is the discretionary security policy. The three assurance stages defined are operational assurance, which focuses on technical items such as the system architecture and system integrity, life cycle assurance, which focuses on security testing, verification, and trusted distribution, and enforcement assurance. There are four assurance levels; however, the last three assurance levels are further divided into sub-assurance levels. Once a system is evaluated, an assurance level is given to the evaluated system. This assurance level shows the effectiveness of the system in terms of confidentiality (Rannenberg, 2000).

Information Technology Security Evaluation Criteria

After experiencing their own assurance criteria, France, the United Kingdom, Germany, and the Netherlands realized the importance of a more comprehensive standard. They joined hands and introduced a new standard called the Information Technology Security Evaluation Criteria (ITSEC). This combined effort gave these countries a number of advantages, such as sharing their pre-

vious experiences and having a common criterion across the countries. This is the first criterion that supports defining flexible security enforcement functionalities and assurance levels. This flexibility facilitates assessing a product or service against a given evaluation criterion. The users can define security requirements in a security target document that is used as the criterion to evaluate IT products. Before evaluating a product, the document has to be evaluated. The functionalities in the ITSEC are divided into four classes and there are six different evaluation levels, ranging from level E0 to E6. A higher evaluation level means that the target of the evaluation has substantially reached the desired security level. According to Rannenberg (2000), the ITSEC shifted the concept of security criteria to evaluation criteria. This enabled interested parties to define their own criteria. Apart from these advantages, the ITSEC initiated a harmonization process of the evaluation criteria (Rannenberg, 2000).

The experience gained by using the TCSEC and the ITSEC stressed the importance of a multilateral security which goes beyond the limits of the conventional information security domain. In addition to the conventional security threats, the TCSEC and ITSEC take the activities of operators and manufacturers as threats to information privacy (Hansen et al., 2005; Muelle & Rannenberg, 1999).

The Common Criteria

The Common Criteria (CC) has become the de-facto standard in IT security evaluation. This standard facilitates assessing the security compliance of IT products against specified objectives. ISO 15408, the ISO version of the CC, was introduced in 1999. This standard serves as a framework for end users, manufacturers, and evaluators taking part in the evaluation process. Users can define their desired security properties of the TOE (the subject of the evaluation) in a protection profile (PP) which is an implementation independent catalogue. Developers can develop systems based on the PP and claim that their products have met the security properties defined in the PPs. Evaluators can evaluate the products to determine the level of conformity of the developers' claims (Herrmann, 2003).

Protection Profile (PP) The protection profile is a statement of the desired security functionalities and assurance requirements of a particular product or service. This is an implementation independent statement written by groups of users or other interested parties.

Security Target (ST) The security target is an implementation dependent set of security properties of the TOE. This defines desired security objectives, desired functionalities, assurance methods, etc. In the evaluation process, the effectiveness of the SFR is evaluated based on this statement.

TOE Security Policy (TSP) The TSP policy states all allowable and non-allowable states of the TOE.

TOE Security Function (TSF) The TSF contains individual security functions provided by the TOE to enforce the TSP.

Assurance covers both the measures used to produce a TOE in a secure manner and the thoroughness of the evaluation process of the TOE. This covers the effectiveness of the implemented measures in meeting the desired security objectives, the strengths of those measures, and the effective implementation of those measures (Rannenberg, 2000).

Evaluation Assurance Levels (EAL) Evaluation assurance levels are based on the fulfillment of the assurance requirements of the TOE. The range of levels varies from EAL1 to EAL 7. EAL1 corresponds to a basic testing package while EAL 7 corresponds to a package of more stringent testing requirements.

Security Functional Requirements (SFRs) SFRs are the second part of the CC. This part contains standard security functional components which are used to define the TSFs of the TOE. There are seven security functionality classes. Those classes are FAU (Security Audit), FCO (Communication), FSC (Cryptographic Support), FDP (User Data Protection), FIA (Identification and Authentication), FMT (Security Management), FPR (Privacy), FPT (Protection of the TSF), FRU (Resource Utilization), FTA (TOE Access), and FTP (Trusted Path/ Channels).

Privacy Family of the CC

The FPR class provides the functionalities required to protect information privacy. It has four privacy families: anonymity, pseudonymity, unlinkability, and unobservability. However, the CC is not sufficient to meet all information privacy requirements.

Anonymity (FPR-ANO) This class ensures that a user can use services or resources without revealing his/her identity to other users, subjects, or objects. However, this class does not protect the identity of the subject from the system. The user's identity is protected by FPR-ANO.2 (i.e., in this case, the TSF should not ask for the user's identity). Anonymity is important in assessing electronic voting, anonymous donations, payments, and inquiring for confidential information from public databases.

FPR-ANO.1 The identity of the user is protected from others.

FPR-ANO.2 This prohibits asking for the user's identity by the TSF.

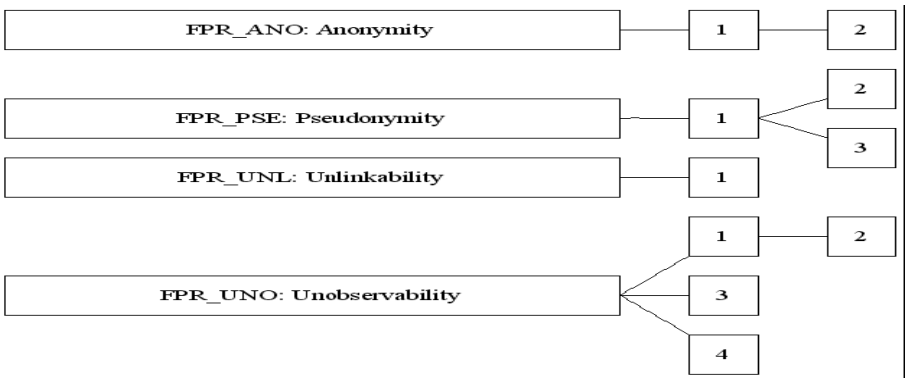


Figure 2.4: Privacy class families and their sub-components – Blarkom, Borking, Giezen, Coolen, & Verhaar (2003)

Ppseudonymity (FPR-PSE) This class ensures that a user can use resources without his/her identity being revealed; however, the user is accountable for his/her activities. This is realized by using aliases.

FPR-PSE.1 Pseudonymity This does not specify any requirements, but is the root of two sub-requirements.

FPR-PSE.2 Reversible pseudonymity The TSF is capable of identifying the real identity of the user based on the given alias under special conditions. Digital cash systems need this property. A user's identity is protected when the user is honest but his/her identity is revealed when he/she breaks the rules.

Unlinkability (FPR-UNL) This ensures that a user may make multiple uses of resources or services without others being able to link these uses together. This class intends to protect against user profiling. For example, it prohibits building a user profile which can be used to identify the user.

Unobservability (FPR-UNO) This ensures that a user may use a resource or service giving no room for others, especially third parties, to observe that the resource or service is being used. Here, the identity of services or resources is being protected.

FPR-UNO.1 The use of a function or resource can not be observed by an unauthorized party.

FPR-UNO.2 This is hierarchical to FPR-UNO.1. The use of a function or resource can not be observed by a specific group of subjects or users and the privacy of users is distributed among many parts of the TOE in such a way that it makes it difficult for an attacker to target the system.

FPR-UNO.3 This is unobservability without soliciting information. TSF does not solicit any information that may leak the privacy of a subject.

FPR-UNO.4 Authorized User Observability. There is at least one authorized user with the ability to observe resource utilization. However, a review of resource utilization is allowed without this.

Limitation of the Common Criteria and Some Suggested Improvements

There have been many criticisms leveled against the concept of the PP. One such criticism is its lack of flexibility. In producing a protection profile for Mix networks, it was realized that different parties have different objectives and goals. Therefore, having a single protection profile was not possible. This requires many protection profiles for parties with various requirements. For example, a network operator wants to log as much as information as possible to protect his system. On the other hand, users want the system to have a minimal amount of their personal information. These kinds of conflicting interests drive the desire for a multiplicity of protection profiles. For example, the studied Mix network required three PPs. One PP was required for the users; one PP was required for the operators of the mix nodes; and the last was a compromise for both parties. Another criticism leveled against the PP is that it does not prevent specifying some design conflicts. One example is that the PP does not prevent specifying two conflicting functionalities (Mercuri, 2002). Other criticisms are its lack of support for multilateral security, its over emphasis on data collection functionality, under emphasis on data economical functionality, and its lack of reorganization given to the functions that are not in the CC but are specifically mentioned in an ST (Rannenberg, 2000).

The CC does not provide adequate attention to the aspect of information privacy. Iachello and Rannenberg (2001) have proposed three privacy families and components for the CC. One is an information retention control (FDP-IRC) family for the user data protection (UDP) class. This addresses the secure management of data that are no longer needed for the basic operations of the TOE but are needed for other additional functionalities. Not keeping an excessive amount of data provides a number of advantages, such as saving storage space, reducing the system's risk of divulging personal information, and building the customers' trust. However, there are cases where it is not possible to erase the data permanently. In these cases, some precautionary measures must be taken. Some possible precautionary measures are preventing unauthorized access to the information objects stored in the TOE and obtaining the protected information from users when needed. The second one is an additional family for the privacy class. This family intends to distribute trust among many parts of the TOE. This has some similarities to the FPR-UNO.2 component. The rationale behind this family is that it allocates assets to different components in such a way that the misbehavior of one or more parts would not cause serious harm to the system: this minimizes the risk. Implementation approaches are the distribution of information into many parts of the TOE and distribution processing activities to many sub-components. The intention of these approaches is to protect privacy related information from unauthorized parties. The third

one is an extension to the FPR-UNL. This extension extends the current unlinkability (FPR-UNL.1) operation to the unlinkability of users.

The CC is a complex process that provides little help for ordinary customers who wish to identify products that give high levels of information security capabilities. The CC can be improved to make it easy for ordinary users to make informed decisions. One suggested mechanism is giving more information to customers. The customers should be informed of the criteria used to evaluate each part of the TOE because a TOE can be evaluated against many PPs. In other words, one part is evaluated against one PP and another part of the TOE is evaluated against another PP. Another suggested improvement is providing a more user friendly mechanism to compare TOEs. One possible approach is categorizing products according to the level of protection given and awarding separate seals for each category. At that point, customers can easily identify products with higher protection capabilities (Rannenberg, 2000).

Working Groups on the Privacy Aspect of IT Products

The PET Testing and Evaluation Project (PETTEP) works on evaluation methods for privacy enhancing technologies (PETs). One of these areas is looking at the possibility of using the CC for evaluating PETs. Among the work done by the project, one of the major contributions is the mapping of the Fair Information Practice (FIP) to SFR-FIPs. They have introduced new families to the CC's privacy class. Those are accountability (FPR-ACT), identifying purposes (FPR-PUR), inform-prior to consent (FPE-INF), consent (FPR-CON), collection (FPR-COL), storage (FPR-STR), limiting linkability (FPR-LCO), limiting use, disclosure and retention (FPR-LUS), data quality (FPR-ACC), safeguards (FPR-SAF), openness (FPR-OPN), individual access (FPR-IAC), and challenging compliance (FPR-CHL). It is also expected that where the existing SFRs are insufficient, new SFRs will be proposed (Hansen et al., 2005).

The Independent Centre for Privacy Protection (ICPP)

The Independent Centre for Privacy Protection (2007) was instituted by the *Land* Government Acts of Schleswig-Holstein. This centre serves as an independent supervisory authority. One of the primary purposes of the centre is awarding privacy seals for compliant products. In addition, it also provides a catalogue of legal privacy requirements. Once a product has obtained a legally and technically compliant certificate from an independent expert, the ICPP grants the privacy seal for a period of two years. This certifies that the product has met both the general data protection laws and the sector specific laws. The latter is important if the product is to be used in a particular sector. The seal helps both private customers and government institutes. Private customers can gain a competitive advantage by showcasing the seal while public authorities can demonstrate the compliance of their products. For example, GMSH, the central procurement authority of the German Federal State, has integrated the privacy seal into its tender evaluation processes (Hansen et al., 2005).

2.4.5 Privacy Process Assurance

Privacy process assurance is also known as a privacy audit. Privacy audits are quite similar to financial audits. A privacy audit is conducted to ensure that an organization handles personal data in compliance with its applicable data protection laws. It also focuses on the effectiveness of the implemented privacy control systems and the effectiveness of the controls throughout the personal information life cycle. In a privacy audit, the information handling practice of an organization is inspected and reviewed systematically. This process also calculates the privacy audit risk, which is the possibility of incurring privacy breaches in an organization. There are three kinds of risks involved in a privacy audit. Those are inherent risks, control risks, and confirmatory risks. Privacy inherent risks focus on the inherent risks of the environment. Privacy control risks entail the non-applicability of the implemented privacy controls. Confirmatory risks deal with deficiencies in the privacy auditing process (Australian Privacy Commissioner, 1995).

The Dutch Data Protection Authority introduced a privacy audit framework and a privacy awareness tool. The audit framework facilitates identifying the relevant and applicable organizational and technological measures. In identifying these measures, the framework takes general data protection laws and other sector specific laws into account. In addition, the framework provides guidelines for writing an effective privacy audit plan. The privacy awareness tool is called Quickscan; it is intended to identify the level of awareness of personal data protection. It can also be used as a self-assessment test to assess the effectiveness of the controls deployed to protect personal information. The test result can be used to identify appropriate improvements (Dutch Data Protection Authority, 2001).

There are few privacy specific assurance frameworks. The leading privacy frameworks are the ISTPA privacy framework (2001) and the AICPA/CICA privacy framework (2004). Blarkom et al. (2003) explain some work done by the Dutch Data Protection Authority in the information privacy area. These assurance frameworks are not specific to a particular jurisprudence. Therefore, these frameworks can not substitute for privacy audits because privacy principles and expectations are jurisdiction specific and these two frameworks are international. These frameworks can be used to identify the limitations of the existing information systems, to suggest appropriate measures, and to measure the level of compliance. The following section discusses the ISTPA framework, the AICPA/CICA privacy framework, and the PISA project.

ISTPA

The International Security Trust and Privacy Alliance (ISTPA) released version 1.1 of its privacy framework in 2002. According to the introduction to the framework, it defines security and privacy solutions for IT systems in consistent, compliant, and interoperable manners. The framework is based on fair

information practices (FIP). The designers have stated that the FIPs are meant to define how to put the privacy principles into practice, but they had not yet been implemented in a consistent manner in terms of terminology and legal, technical, and operational forms. These limitations caused several difficulties for creating a dialog on privacy issues. Furthermore, they have stressed the importance of a well-defined privacy framework which gives a well formulated vocabulary along with operational privacy controls. They have highlighted the difficulties faced in developing the framework. One of the difficulties was the lack of a global, collaborative, and multi-disciplinary approach. In addition, there was a need for a common platform for multi-disciplinary work. This common platform had to support the experts in various fields such as trust management, information security, privacy and technological measures, business processes, and legislative measures.

According to the introduction to the framework, the objective is to express privacy practices in a practical and consistent manner so that they could easily be implemented in the technical environment. These information privacy expressions can be used by technologists to understand high-level privacy guidelines and legal privacy provisions and to apply the knowledge in designing technological solutions.

In this work, the FIPs were mapped to seven services and three capabilities. A service is a collection of related mechanisms used to fulfill one particular task. A capability fulfills a particular task by invoking two or more services. These services and capabilities provide the functionalities necessary for protecting personal information throughout the personal information life cycle in a consistent manner. Table 2.1 presents the principles presented by the ISTPA together with privacy principles introduced by other organizations.

This framework provides a number of advantages. The defined common vocabulary and toolkit lay a foundation for privacy debates and discussions. It can be possible to integrate the framework with the existing security mechanisms to provide better privacy protection mechanisms. Organizations can make use of this framework as a template for designing information privacy management practices. System designers and implementers can use the services and capabilities to implement privacy principles and practices. In developing the framework, some important functions that had not been available in the existing privacy principles and practices were identified. One such limitation is the privacy policy management function that manages the privacy preferences of data subjects. By going beyond the intended original purpose, the framework has presented a mechanism for measuring the effectiveness of the deployed privacy controls.

This framework is at an intermediary stage. The framework can be further enhanced in a number of ways. The defined services and capabilities are at an engineering requirement level. Therefore, this framework needs to be transformed into a formal architectural level of design. It would then be easy to implement privacy controls in a consistent manner. Another suggestion given

in the report is studying the possibilities of automating the services and capabilities.

There is no evidence of framework validity. Even though the framework says it can be customized to suit a particular jurisdiction, there are no sufficient instructions for how to customize the framework. If the privacy framework is customized to a particular jurisdiction, the applicability and effectiveness of the framework can easily be verified. Another way of validating the framework is defining more use cases and testing them in a given context. This kind of thorough testing process would guarantee the applicability and robustness of the framework.

AICPA/CICA Privacy Framework

The American Institute of Certified Public Accountants, Inc. and the Canadian Institute of Chartered Accountants introduced this privacy framework in November, 2003 and revised it in March, 2004. The intention of these accounting bodies was to provide better privacy advisory services to their customers. The knowledge of chartered accountants about business processes, business risk management, information flows, and controls inspired them to develop this framework. According to the introduction to the framework, their expertise in the business domain places them in a better position to provide privacy strategic plans, identify privacy gaps, conduct privacy risk assessments, design and implement privacy policies, and verify privacy controls. These accounting bodies established two subcommittees, the Assurance Services Executive Committee of the AICPA and the Assurance Services Development Board of the CICA, to develop this framework.

The development team focused on many international data protection legislation measures, laws, regulations, and guidelines for developing the framework. However, special attention was given to the USA's privacy legislation measures. A comparison of ten different legislation measures and guidelines is given in the Appendix of the AICPA/CICA Privacy Framework. These legislations and guidelines are the Canadaian Personal Information Protection and Electronic Documents Act (PIPEDA), the Australian Privacy Act of 1988, the U.S. Safe Harbor agreement, EU Directive 95/46/EC, the OECD Guidelines, The United States Health Insurance Portability and Accountability Act of 1996 (HIPAA), The U.S. Financial Services Modernization Act, The Gramm–Leach–Bliley Act (GLBA), and the U.S. Children's Online Privacy Protection Act of 1998 (COPPA) (AICPA/CICA, 2004).

This framework contains ten privacy components. They are further divided into subcomponents. These subcomponents contain measurable criteria for evaluating privacy policies, communications, procedures, and controls. These can also be used to measure the effectiveness of the implemented privacy protection controls. The designers have used the term 'components' instead of 'principles' to maintain internal consistency. All of these components and subcomponents are presented in the first column of a three-column table. The sec-

ond column presents illustrations and explanations for a better understanding of the framework. The third column gives additional information such as the best practices and specific legal provisions pertaining to a specific country or sector (AICPA/CICA, 2004). Table 2.1 presents the principles presented in the AICPA/CICA Privacy Framework together with privacy principles introduced by other organizations.

One of the limitations of the AICPA/CICA Privacy Framework which has been identified is the incompleteness of its third column. For example, some spaces in the third column are blank. This shows that adequate attention has not been given to specific sectors and jurisdictions. There are some instances where the given information is not sufficient. For example, section 2.2.3 states:

> "Some regulations, such as GLBA, may contain specific information that a disclosure must contain. Illustrative notices are often available for certain industries and types of collection, use, retention, and disclosure."

These two sentences are vague because they do not specifically mention the relevant legal provisions. In these cases a user has to go through all regulations pertaining to a particular industry to identify the relevant provisions.

Even though there is no section on limitations and further improvements, the AICPA/CICA Privacy Framework framework can be further improved in several ways. Some of the possible improvements are as follows: The third column of the AICPA/CICA Privacy Framework must be filled with the specific provisions of the relevant data protection legal measures. This would make it convenient for practitioners to identify the relevant legal provisions. Identifying the specific provisions of the relevant legal provisions would help further studies of the identified provisions. This simple but important improvement would save cost and the time of practitioners.

This framework has not adequately addressed some specific issues in European legislative measures. For example, the nature of the data, which is an important factor in determining the appropriate level of protection required, has only lightly been taken into account. For example, Section 3.2.3 refers to Article 8 of EU Directive 95/46/EC.

Another suggested improvement is giving a criterion for calculating the costs associated with the given measures. For example, section 6.1.1 states: “A privacy policy should explain how individuals may gain access to their personal information and any costs associated with obtaining such access.” It would be convenient for practitioners if a list of possible access methods was given together with the relevant costs associated with them. This would allow practitioners to suggest better access mechanisms after taking costs and other relevant factors into account.

It could be further enhanced by giving all possible technical mechanisms or referring to the appropriate technical manuals for further references.

PISA

The Privacy Incorporated Software Agent (PISA) project is aimed at developing a privacy-friendly, intelligent, software agent framework. A software agent carries out tasks on behalf of its owners. An intelligent software agent needs few instructions from its owner. There is a threat to the agent owner's personal information because an agent travels across many networks carrying personal information belonging to its owner. The motivation behind the project was to protect the personal information held by software agents. Software agents are more international and data protection legislation measures are specific to particular jurisdictions. The challenge was how to place software agents in the local context. In other words, the project was intended to empower software agents with data protection principles. The lack of a universally accepted means for incorporating information privacy protection mechanisms into software products further deepened the challenge. First, the project addressed this problem. Otherwise, it would be very difficult to incorporate privacy protection mechanisms into software systems at a later stage. Therefore, the initial attention was on incorporating privacy protection measures at the very early design stage and throughout the development process (Blarkom et al., 2003).

Before addressing the privacy aspect of intelligent software agents, this book addresses privacy specific issues such as privacy preferences, privacy risk analysis, privacy principles and rules, data protection directives, privacy audits, public key infrastructures (PKI), privacy ontology, privacy design issues, etc. The comprehensive coverage of privacy aspects of information systems is very useful for developers, managers, and users.

The project identified the necessary human computer interaction (HCI) requirements for designing information systems. Among the nine privacy principles extracted from EU Directive 95/46/EC, four of them have been identified as critical HCI requirements for the ISA. These four principles are transparency processing, as-required processing, lawful basis for data processing, and the rights of the parties involved.

Numerical Value Based Scale by Robert Gellman

According to Cavoukian and Crompton (2000), Robert Gellman has developed a numerical scale for measuring information privacy protection measures based on the OECD privacy guidelines. The OECD privacy principles are given in the first column of Table 2.1. As shown in Table 2.2, one point has been given for each privacy principle. Some privacy principles were divided into two or four sub-components and points were allocated accordingly. When the investigated system meets the requirement imposed by a principle or sub-principle, the corresponding point is awarded. Thereafter, the awarded points are summed up. The aggregate value represents the level of compliance of the deliverable against the criteria, which is the OECD guideline. When a system satisfactorily fulfills all privacy principles, it obtains the maximum value of

eight points. Table 2.2 shows the breakdown of the OECD guidelines and the values assigned to each sub-principle.

This scale was modified and used as a template for evaluating web-based privacy seal programs by the office of the Information and Privacy Commissioner of Ontario and the office of the Federal Privacy Commissioner of Australia. In this study, three web-based privacy seal programs were evaluated and scored based on the merit of the information provided by the three seal providers on the web (Cavoukian & Crompton, 2000).

This template inherited several limitations. First, evaluating the information provided by privacy seal programs is not easy due to the complexity of these web-based privacy seal programs, the ambiguity of their language, etc. For example, Yahoo, which was awarded the TRUSTe web privacy seal, contains several ambiguities and unclear statements about its privacy policy. Its privacy policy contains terms which are not clear to its users. For example, terms like 'such as,' and 'may' are present. Another limitation is that the breakdown of the OECD guidelines was not adequate. It needs a further granularity to get an accurate picture. On the other hand, several scholars have pointed out the limitation of the OECD guidelines which was stated in Section 2.3. This work can be further improved by going beyond the OECD guidelines and breaking the privacy principles down into many meaningful subcomponents.

Web-based Trusted Seal Programs

As shown in Figure 2.1, business organizations adopt self-regulation methods to make their businesses more trustworthy. Trustworthiness is a very important success factor for online businesses. One of the trust building methods is publishing an online privacy policy. However, this method inherits certain limitations. One limitation is that a privacy policy can not be legally enforced (Northwest, 2004). Another limitation is that online visitors do not know whether the online policy publishers honor the claims made in their privacy policies.

Trusted third parties come in at this point to help both online visitors and merchants. They evaluate the online policies against their proprietary evaluation criteria. Once an organization meets the requirements imposed by the criteria, a privacy seal is awarded to the organization. Showcasing the seal indicates the commitment of the organization to protect the personal information of its visitors. Since the privacy policy has already been evaluated by an independent trusted third party, online shoppers do not have to worry about how their personal information is handled. Otherwise, it is extremely difficult for them to understand a privacy policy and get to know the information handling practice of an organization. This mechanism helps online merchants build visitors' trust in their web sites. The following three sections give an overview of three leading online web seal providers.

Table 2.2: *Numerical Scale by Robert Gellman – Cavoukian and Crompton (2000)*

Collection Limitation Principle:	
(a) Limits to collection by lawful and fair means	.5
(b) Knowledge or consent of data subject	.5
Data Quality Principle:	
(a) Relevant to purposes of use	.5
(b) Accurate, complete and kept up-to-date	.5
Purpose Specification Principle:	
(a) Specify purposes to data subject not later than time of collection	.5
(b) Uses limited to purposes or specified consistent purposes	.5
Use Limitation Principle:	
(a) Use and disclose in accordance with specified purposes	.5
(b) Except with data subject's consent or by authority of law	.5
Security Safeguards Principle:	
(a) Reasonable security safeguards	1
Openness Principle:	
(a) General policy of openness	.5
(b) Ready means for data subject to know about personal information, and purposes, including identity and location of data controller.	.5
Individual Participation Principle:	
(a) Data subject able to know data controller has personal information	.25
(b) Data communicated in reasonable time and manner, and in intelligible form	.25
(c) Reasons for denial of access	.25
(d) Ability to challenge and correct	.25
Accountability Principle:	
(a) Data Controller accountable for compliance with principles	1

BBB Online Privacy Seal

The Council of Better Business Bureaus (BBB) (2012) awards a privacy seal to organizations that meet the requirements imposed by the council. The aim of the project is to promote trust and confidence in the Internet. The long-standing practice of the council in the field of business consultancy has given the council a comparative advantage. The evaluation criterion consists of 29 questions. Some of the key requirements in the criteria are appointing responsible persons for the formulation of the privacy policy and monitoring the adherence to the privacy policy. The first step in obtaining the seal is submitting an application form and the privacy profile. The price for obtaining the seal varies from US$ 200 to US$ 7000. Apart from the general privacy seal, there are two other privacy seals. One is for children and the other is for the Japanese. The Children's Online Privacy Seal is based on the Children's Online Privacy Protection Act. Furthermore, a privacy dispute resolution board has been established to hear personal information misuse complaints.

Web Trust Online Privacy Seal

Two institutes of chartered accountants have developed this program. These two institutes have been engaged in developing a core set of principles and related criteria for information systems. This seal program is an extension of the AICPA/CICA (2004) privacy framework discussed in the privacy process assurance section. The recognition gained by functioning as chartered accountants has greatly contributed to getting global acceptance for the criterion. The criterion can broadly be divided into four sub-criteria. Those are defining policies to build online visitors' trust, means of communicating privacy policies to them, procedures to ensure the adherence to the policies, and means of monitoring the information handling practices. In order to obtain the seal, an organization must get the services of a certified chartered accountant. The accountant must review the personal information handling process to make sure that the process is in accordance with the claimed privacy policy. It must also meet the AICPA/CICA trust services privacy criteria. The price for the company is the accountant's fee plus an annual service charge.

TRUSTe Online Privacy Seal

This program was founded by the Electronic Frontier Foundation and the CommerceNet Consortium. The sponsors of the program include many large corporations such as AOL, Intel, Excite, and Microsoft. TRUSTe (2012) provides a number of privacy seals including the Children's Privacy Seal, the Email Privacy Seal, the EU Safe Harbor Seal, the Japan Privacy Seal, and the Web Privacy Seal. It gives a self-assessment questionnaire for business organizations to have a self-assessment of their current information handling practices. A requesting organization has to submit the assessment questionnaire together with its current privacy statement. TRUSTe then conducts a site review to make sure

that the site adheres to the TRUSTe's privacy criterion. In addition to awarding privacy seals, it provides dispute resolution services.

2.5 Privacy policies and alternatives

Publishing information privacy policy is a prominent way of giving out information about the information handling practices of an organization. However, the privacy policy has several limitations. Its understandability is one of its major limitations. This is due to the terms and language used in writing the privacy policy (Kelley, 2009; Jensen & Potts, 2004). Supporting this argument, Jensen & Potts (2004) have shown that at least a college level education is required to read and understand a privacy policy. Other limitations are finding the right information and comparing two privacy policies (Kelley et al., 2009). Additionally, surveys have shown that customers do not pay much attention to the privacy policy (Culnan & Milne, 2001) and privacy policies are not used in decision-making (Acquisti & Grossklags, 2005).

As an alternative to the privacy policy, the World Wide Web Consortium (W3C) introduced the Platform for Privacy Preferences (P3P), which is a standard way of presenting a privacy policy in a machine-readable manner. However, very few have benefited from P3P based privacy agents (Cranor et al., 2008).

The P3P Expandable Grid, which presents a privacy policy in various categories, was introduced as an alternative to plaintext privacy policy. In a comparison study, it was shown that users undervalued the P3P Expanded Grid (Kelley, 2009).

Then, research began on how to present a privacy policy in a manner similar to the nutrition fact label on dietary products. This approach was taken since several organizations in other similar fields had started presenting labels in a metric form. For example, energy ratings (MEPS, 2009), water efficiency ratings (WELS, 2009), and an example of a nutrition label is the Food Standard Agency of the United Kingdom (Food Standard Agency, 2009). Studies have shown that a presentation in metric form improves the ability of consumers to compare the products. Furthermore, the same studies have shown that consumers are highly interested in this format (Hills, 2009).

Another focus group study illustrated that this approach is better than plaintext privacy policies for comparing two services (Kelley, Bresee, Cranor, & Reeder, 2009). However, this researcher argues that presenting a privacy policy similar to the nutrition label severely limits the information provided to make informed decisions. Additionally, the focus of privacy label research is on presenting a privacy policy in a more understandable and comparable manner. In contrast, privacy metrics should present all the information that is necessary for making informed decisions.

2.6 Measuring Information Privacy Protection

The previous sections gave a general overview of privacy assurance measures. However, except for Robert Gellman's work and the presentation of privacy policies as food labels, none of above measures facilitate the comparison of ICT systems in terms of information privacy protection. As discussed in the suggestions to improve the CC, there is a need for a method to compare ICT systems. Some benefits of measuring information privacy protection measures are given in the following sections.

Nevertheless, some argue that measuring abstract concepts is not possible. In the case of information privacy, another challenge is the lack of a proper definition for privacy (Solove, 2007). The following sections discuss the demand for measuring information privacy protection measures along with attempts to quantify information privacy assets and threats.

2.6.1 The Need for Measuring and Challenges

It is very difficult to build a methodology to quantify information privacy assets or the measures used to protect information privacy assets. However, doing this is required for risk management, something which includes the identification of risks, an assessment of the severity of the identified risks to any assets, and developing strategies to manage the identified risks. According to Jaquith, risk managers should be able to answer the following: what is the value of the information assets in a system, what is the velocity of circulation, what are the most valuable assets, and what assets are at risk (Jaquith, 2007). He argues that without answering these questions, it is not possible to measure the effectiveness of security programs.

The PISA project has presented an information privacy risk assessment model. This model was derived from general risk analysis approaches. It requires quantitative measures at three stages. These stages are: valuing information assets, the quantifying of the severity of the threats to the information assets, and the probability of the occurrence of a threatening event (Blarkom et al., 2003). The challenging questions are how to measure these items, what the unit of measurement is, etc. These questions have not been addressed in the project documentation. Converting all values into a compatible unit is also required. Otherwise, calculations are difficult to carry out. In addition to this, the calculations are better expressed in monetary terms. It would then be easy to use financial modeling techniques. The other alternative is introducing a ranking mechanism such as very high, high, medium, low, and very low. A decision tree approach could then be used to model the outcomes.

One of the challenges is measuring the value of information assets. Information assets can be broadly divided into two categories: personal information held by organizations; and its information handling systems themselves, which

include both hardware and software. Even though there are a number of suggested mechanisms for valuing personal information, there is no commonly accepted method (Noam et al., 1997). The general understanding is that more personal information causes a higher risk. Apart from the quantity, both the quality and the nature of the personal information contribute to the value of the information assets.

The other challenges are identifying the threats and quantifying the severity of the threats. One approach is scrutinizing personal information life cycles. There are two different personal information life cycles: the personal information life cycle consists of its collection, use, retention, and discard; the other life cycle consists of the design, implementation, testing, and operating stages of the information systems (Hansen et al., 2005). Another approach is analyzing privacy threat categories. Generally speaking, information privacy threats can be broadly divided into the following five categories: the violation of privacy regulations, threats created by general solutions, threats emanating from a use situation, threats created by the chosen technology, and threats created by the system's purpose (Blarkom et al., 2003). Once all potential information privacy threats are identified, estimating the severity of these threats and knowing the probabilities of their occurrence is required. However, knowing the probabilities is a difficult task because some identified threatening events have not yet occurred. This leaves a lack of knowledge about the possible threatening events due to the unavailability of a systematic way of knowing the occurrence of future events (Cybenko, 2006).

2.6.2 Advantages

Measuring and classifying information systems in terms of the protection given to personal information is advantageous for many parties, including the consumers of IT products or services, the service providers, the IT product manufacturers, and legal privacy advocates.

Customers in privacy-unregulated markets get more benefits than customers of privacy-regulated markets. In terms of information privacy, the European market is regulated, since data protection commissioners keep an eye on the level of protection given in handling personal information. On the other hand, in unregulated markets, it is up to consumers to take measures to protect their personal information. Here, consumers make informed decisions before buying a commodity (products or service). In order to make informed decisions about IT related commodities, customers should have a good understanding of the provided services and the strengths of the provided services. In addition, customers need to have a simple way of knowing the measures taken to protect their personal information and the strengths of those measures.

Several leading privacy advocates have shown the need for knowing the level of protection given to their personal information. For example, Jay Libove,

the CISSP, CIPP Privacy & Information Security Advisor for Delta AirLines, Atlanta, stated:

> "I will not look at a company with a good-enough privacy policy and be willing to pay that company $X for its product or service, but be willing to pay $X+ for the same product or service from a company with a better privacy policy; I will however not buy a product (at any price) from a company which has a not-good-enough privacy policy. I exercise this choice routinely in highly competitive marketplaces such as online electronics/computer goods purchases (Peppers & Rogers, 2007)."

In answering whether sound privacy policies would entice him to pay more for goods purchased online, Alex Rose, president of Alex Rose LLC, stated: "It would not entice me to pay more for online purchases because I would expect this. In fact, I like many others would avoid companies like this (say for instance Amazon)" (Peppers & Rogers, 2007).

The decision-making process plays a role even in the regulated market since the regulated market defines only the minimum requirements. Customers need more protection than what is defined by the law, and some providers are willing to meet that demand. For example, data protection acts define only the minimum requirements and providers are allowed to provide more.

How does an individual find out that organization A is providing more privacy protection than that of organization B, or vice versa? Today, it is not easy for a non-expert user to compare the security and privacy functionalities of ICT systems (Hansen et al., 2005). This demands a simple mechanism for comparing the privacy functions or privacy levels of products and services.

Apart from the privacy certificates discussed earlier in this chapter, there has been little work done in this area. According to Cvrcek and Matyas (2000), many research papers have narrowed the topic of privacy to that of anonymity. According to Caspar Bowden, Senior Security & Privacy Officer, Microsoft EMEA Region, the privacy risks of processing personal information are not well defined (Personal Communication, October 29, 2007).

Jaquith highlights some of the advantages of quantifying information security controls and the desirable properties of the measurement. Expressing the measurement in terms of money or time would enable security managers to use the result as a benchmark. This sort of benchmarking would enable them to compare their current performance to their past performance. It would also enables them to compare their performance with that of other organizations in the same domain. Business managers can make use of the value to calculate their contingency liability as required by various acts. In addition, the value indicates the worthiness of spending a dollar on information security. As discussed above, PISA projects also proposed a risk assessment model which was intended to address the same questions.

2.7 Privacy in the future

Some scholars have argued that privacy is already dead or it will die soon. Therefore, individuals are advised to give up their expectations about privacy. Privacy is dying because it has failed to meet the challenges posed by technological advances and the widespread use of information technology. As discussed in the preceding sections in this chapter, there are several technological, legal, and organizational measures for protecting personal information. However, these measures inherit flaws in principle. As a result of these flaws, individuals' privacy is weakened. Some examples of flaws in privacy protection measures are giving too much focus to individuals instead of the organizations that collect and use personal information, limitations in fair information practices (FIPs), and taking a piecemeal and reactive approach instead of a comprehensive and proactive approach in addressing privacy issues. As discussed below, the major weakness is the way privacy is being looked at: protecting privacy has been considered as being opposed to achieving many other competing goals. Some examples of these competing goals are providing public safety, protecting organizational assets, monitoring the behavior and performance of employees, and building consumers' profiles. The paradigm in which privacy is compromised for competing goals is called "the zero-sum paradigm." This is a win–lose situation since enhancing privacy causes a lessening of the fulfillment of the other goals, and vice versa. In this paradigm, privacy always loses its battle. Therefore, some have argued that privacy is dead or will die soon.

On the other hand, scholars from other schools of thought have argued that privacy is a fundamental human need. Therefore, people will not give up their privacy expectations under any circumstances. In other words, privacy is well internalized. Therefore, it is hard for individuals to give up their privacy expectations. According to them, the challenge in the information era is to take all necessary measures to protect individuals' privacy. Information scientists in the information privacy domain have been researching how information technology invades individuals' privacy and what possible measures can be taken to protect individuals' privacy. However, all these initiatives have failed to provide an adequate level of protection to personal information.

Cavoukian (2011) argues that the failure is due to addressing privacy issues under a flawed paradigm. Therefore, she suggests a paradigm shift, called the *Privacy by Design* paradigm, which has seven foundational principles:

1. Proactive not Reactive: Preventive 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 Lifestyle Protection
6. Visibility and Transparency—Keep it Open

7. Respect for User Privacy—Keep it User-Centric

Except for *Full Functionality—Positive-sum, not Zero-sum*, all other PbD principles have been widely discussed in the literature. What is new in this new paradigm is the principle *Full Functionality—Positive-sum, not Zero-sum*. This principle states that privacy should not be compromised for other competing goals. In other words, this principle stresses the possibility of achieving other competing goals without weakening privacy. For example, designing the information system to protect public safety without compromising individuals' privacy.

Privacy by Design (PbD) will take a leading role in protecting privacy in the future. However, the major challenge for PbD advocates is providing guidelines for designing fully functional systems. In other words, designing systems so that the way in which they achieve their objectives does not compromise information privacy. This challenge is further discussed in Chapter 5.

Furthermore, Cavoukian (2011) states that organizations can gain a competitive advantage by following the privacy by design approach. This competitive advantage is achieved by improving customer satisfaction, enhancing the reputation of the organizations, reducing legal liability, improving efficiency, and obtaining a better return on investment (ROI).

As discussed in Section in 2.6, information privacy metrics are needed to showcase the above-mentioned advantages. For example, privacy metrics can be used to explain how various levels of privacy protection contribute to a better ROI.

2.8 Future Research

Individuals need to know how organizations handle their personal information and organizations need to inform individuals how organizations handle individuals' personal information. After studying various approaches used to explain personal information handling practices, it was realized that using information privacy metrics would be an appropriate method for describing the personal information handling practices of organizations. Therefore, the aim of this research is to facilitate the building of information privacy metrics that present the information handling practices of an organization in a metric form. In order to achieve this goal, the following research projects have been identified.

1. Understanding the overall view of the information privacy domain:
   Having an overall view of the subject domain is an essential step at the beginning of any research project. Therefore, it was decided to identify and understand the major actors in the information privacy domain. Additionally, understanding how the identified actors inter-

play with the factors and concepts in the information privacy domain is also important for getting an overview of the subject domain.

2. Understanding the interests of the stakeholders:
   Once the actors are identified, understanding their interests is needed. In other words, for what kinds of personal information is more protection sought by the actors. Furthermore, their interests have to be examined in the demographic and situational context. Another important context is how the actors react when their privacy goals compete with other goals. It is expected that some constructs and dimensions will emerge in these examinations.
3. Identifying protection measures:
   The constructs needed for building information privacy metrics can be identified by examining personal information protection measures. These protective measures can be identified by reviewing information privacy and security programs and information privacy and security policies, guidelines, and procedures. Therefore, the next step is reviewing various kinds of information privacy and security programs.
4. Metrics building approach:
   Once the necessary constructs and dimensions have been identified, the metrics building approach has to be pursued. By following this approach and using the identified constructs and dimensions, information privacy metrics can be successfully constructed and applied.

3. Research Methodology

3.1 Introduction

This section discusses the research approaches and methods used throughout the entire research process. The motivation of writing this section is to provide insight into how this researcher looks at theories of science and research methodologies in the perspective of this research work. Several scholars have emphasized the importance of reflecting on the philosophical stance of the researcher. For example, Walsham (1995) states, "researchers need to reflect on their own philosophical stance, which should be stated explicitly when writing up their work" (p. 76).

The word 'science' is derived from the Latin word *Scire*, which means "to know." The purpose of conducting scientific research is building knowledge, which has been defined as true, justified, belief. However, a mere body of knowledge is not science. As Poincare (1903) so aptly noted, "[s]cience is facts, just as houses are made of stone... [b]ut a pile of stones is not a house, and a collection of facts is not necessarily science" (cited in Whetten, 1989, p. 493). The aim of this research is to get to know the constructs and dimensions for building information privacy metrics. This goal is achieved by following acceptable research methods. By following a systematic approach to build new knowledge, this research falls into the category of scientific research.

Empirical science that deals with facts from experience is one branch of research. Two very important branches in empirical science are natural science and social science. According to Shoemaker et al. (2004), natural science is about naturally occurring phenomena and their relationships and social science deals with socially constructed phenomena and their relationships. Computer science is a part of natural science (Fitzgerald & Howcroft, 1998). However, a number of social issues have emerged as computer use has become widespread. These emerging social issues, such as understanding human interpretations and meanings, have attracted the interest of social scientists (Walsham, 1995). Today, information system (IS) research has moved toward social sciences. This argument is supported by Iivari et al. (1998), who argue that IS research is more similar to social science research, which typically focuses on individuals, organizations, and society. Lee (1999) states that the importance of IS research is placing the focus "on the rich phenomena that emerge whenever the technological and the social come into contact with, react to, and transform each other."

Organizations process personal information for various purposes. The process of processing personal information begins with soliciting personal information and ends with discarding personal information. Today, information systems take a prominent part in processing personal information. Information systems store personal information for a long period of time, which was not possible in the past. Additionally, they facilitate the dissemination of personal information to many parties and also make it possible to build profiles by gathering information from various sourcs. Individuals are greatly concerned with all these capabilities. This research is about how individuals perceive the protection given to their personal information by organizations in using information systems for processing individuals' personal information. In this background, it can be said that this research focuses on "... phenomena that emerge whenever the technological and the social come into contact with, react to, and transform each other" (Lee, 1999). Therefore, this research falls into the subject field of information systems (IS) research.

Since this research falls into IS research, it is worth discussing the pragmatic assumptions of IS, the particularly information system development approaches presented by Iivarli et al. (1998). Their discussion is based on four aspects of IS, namely ontology, epistemology, methodology, and ethics.

3.2 Epistemology and Ontology

Epistemology concerns the theoretical aspects of knowledge, knowledge acquiring methods, the nature of knowledge, the limitations and validity of knowledge, and other similarly related topics (Heylighen, 2000). Epistemology guides one on how to acquire knowledge in a scientific manner using the appropriate research methods and approaches. For example, it provides a guideline as to when and where to use quantitative and qualitative research methods.

According to Chua (1986), the three main categories in epistemology are positivist, interpretive, and critical. Walsham (1995) has mentioned another category—normativism. Positivists believe that reality is independent of the observer; therefore, it can objectively be extracted, measured, explicated, and codified. Interpretive scholars state that people have constructed everything; therefore, nothing is independent of the observer. In other words, reality is subjective and nothing can be measured independent of the researcher. A very clear definition of this was given by Geertz (1973) when he stated, "[w]hat we call our data are really our own constructions of other people's constructions of what they and their compatriots are up to" (p. 9). The third category, the critical research approach, is based on the notion that social reality is constructed by humans. Furthermore, critical researchers believe this reality cannot be changed due to various constraints. Normativism is another category. By referring to Archer (1988), Walsham (1995) defines normativism as something

Table 3.1: *Alternative stances on knowledge and reality, Walsham, 1995, p. 76*

Epistemology	Ontology
Positivism: Facts and values are distinct and scientific knowledge consists only of facts.	External realism: reality exists independently of our construction of it.
Non-positivism: Facts and values are intertwined; both are involved in scientific knowledge.	Internal realism: Reality-for-us is an intersubjective construction of the shared human cognitive apparatus.
Normativism: Scientific knowledge is ideological and inevitably conducive to particular sets of social ends.	Subjective idealism: Each person constructs his or her own reality.

that "...takes the view that scientific knowledge is ideological and inevitably conducive to particular sets of social ends" (p. 75).

Ontology is concerned with the structure and properties of "what is assumed to exist," i.e., the basic building blocks that make up the phenomena or objects to be investigated (Iivari 1998). A summary of ontology and epistemology is presented in Table 3.1.

According to Walsham (1995), Archer (1988) argues that interpretive researchers take a non-positivist or normativist approach from an epistemological stance and adopt 'internal realism' or 'subjective idealism' for their ontological stance. Klein and Myers (1999) have recommended interpretive epistemology for information systems research studies when the knowledge of reality is acquired through shared meanings, documents, tools, and other artifacts. According to Myers and Avison (1997), interpretive researchers acquire knowledge by understanding the meanings given to social phenomena by people.

As shown in Figure 3.1, the underlying assumptions for the qualitative research method are positivist, interpretive, or critical. In other words, qualitative research can be based on a positivist, interpretive, or critical epistemology. On the other side of the spectrum, quantitative research methods are based on positivist epistemology (Chua, 1986). However, there is no clear borderline between the three outlined epistemological paradigms. Furthermore, a researcher should follow an appropriate research approach for a given environment. For example, Lee (1991) has suggested both positivist and interpretive approaches for organizational research.

Some research methods based on an interpretive epistemological assumption are ethnography, hermeneutics, phenomenology, and case studies (Klein & Myers, 1999).

This researcher took a positivist stance in quantitative studies where the primary data collection method was the questionnaire. Furthermore, a positivist stance was taken in the grounded theory based study. In these studies, this re-

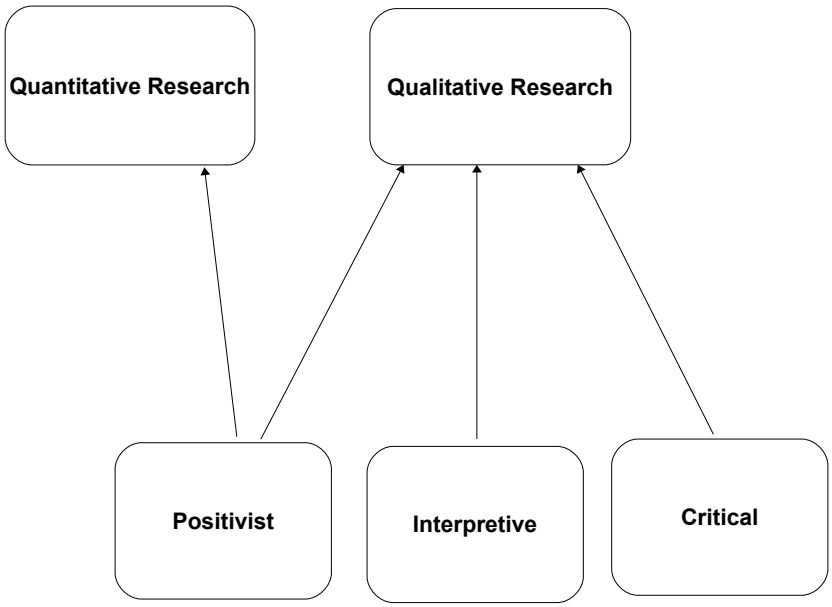


Figure 3.1: Abstract level of theories, Chua, 1986

searcher assumed that reality is independent of the researcher and only facts, which were separated from values, were considered. On the other hand, in qualitative studies where interviews and case studies were used, this researcher took an interpretive stance.

According to Chua (1986), IS scientists' contributions to the world can be categorized into means–end oriented, interpretive, and critical. Means–end oriented refers to achieving given goals and interpretivists help people understand their actions. According to Chua, the contributions of critical research are "identification and removal of domination and ideological practice" (p. 622).

The aim of this research is to present some constructs for building information privacy metrics. Once the intended metrics are built, individuals can use them to take better actions. Therefore, it can be said that this research contributes to the world in both a means–end and an interpretive manner.

3.3 Research Methodology

The research domain can be explained in several dimensions including research strategy, logic, type, method, data collection, and analysis.

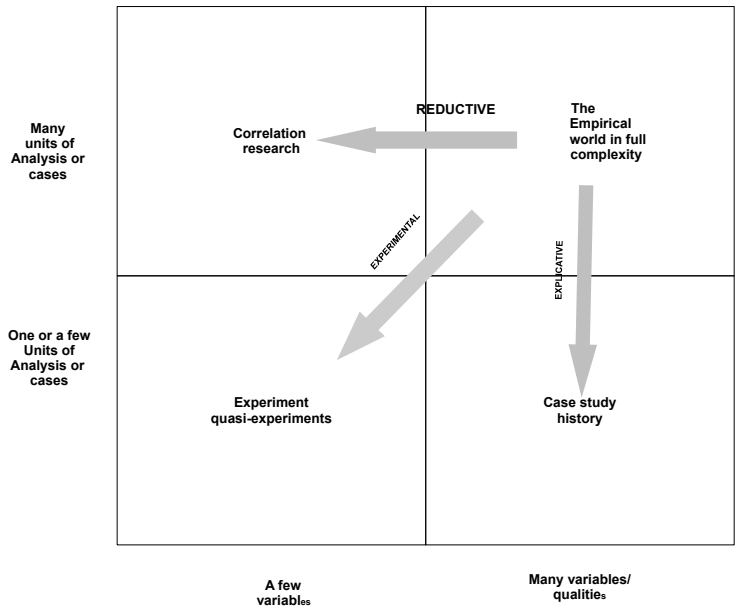


Figure 3.2: Research strategies, Johansson, 2004, p. 17

3.3.1 Research Strategy

Research strategies break down the complexity of reality into researchable units. As shown in Figure 3.2, Johansson (2004) explains three research strategies. The first strategy, experiments and quasi-experiments, reduces the number of variables and units of analysis. The second research strategy reduces the number of units of analysis. Examples of this strategy are case studies and historical studies. The third one reduces only the number of variables. Correlation research is an example of the last one.

Experiments select subjects in such a way that the bias is minimized. In quasi-experiments, any bias is controlled by introducing a control group. In non-experiments, the influencing factors are mentioned.

An experimental approach was applied in Paper 8, where the security and privacy protection given by email services were presented. In this experiment, the independent variables were changed to identify the reactions of the dependent variables. Correlation research, which focuses on a few variables but many units of analysis or cases, were used in all the survey-based research. These studies were presented in Papers 1 and 2. The case study approach was applied in Papers 4 and 5. It can be said that the study presented in Paper 9 neither limits the unit of analysis nor the number of variables. In the GT study presented in Paper 7, the empirical world in its full complexity was studied.

3.3.2 Logical Level

The logical aspect is another dimension found in the domain of research methodology. This includes induction, deduction, and abduction. Inductive researchers focus on building theories based on empirical data whereas deductive researchers focus on testing an existing theory in a given empirical context (Trochim, 2006). Abduction is building a theory from empirical data and testing the theory in an empirical setting (Peirce & Buchler, 1995).

3.3.3 Type Level

The next level, the type level, has several classification schemes. One classification scheme based on the purpose of the research is confirmatory or exploratory research. Confirmatory researchers attempt to confirm or disconfirm existing theories (SuperSurvey, 2008). In other words, they confirm or disconfirm the relationships between the variables. Exploratory researchers attempt to identify the relationships between variables in a general form, which provides many avenues for further research. In addition, explorative researchers identify appropriate research methods and data collection methods (SuperSurvey, 2008; Trochim, 2006). Another classification is quantitative and qualitative research. Quantitative researchers focus on studying quantitative properties of subjects under investigation. Statistical techniques are then used to answer questions such as 'how often' or 'how many.' Qualitative researchers focus on understanding behaviors and the reasons for them. This method focuses on why, how, and when something occurs. Although these are different research approaches, the findings of qualitative research studies can be verified by quantitative techniques (Marczyk et al., 2005). Research studies can also be classified as descriptive and normative. In the descriptive research approach, a model is built that explains the true picture of the studied subject without disturbing it. On the other hand, normative researchers take a step further and design new methods to improve the studied subject (Routio, 2007).

In terms of research, the aim of this research is to lay the foundations for identifying higher level theories. Therefore, the entire research process has taken an inductive approach. Furthermore, it has taken an explorative research approach since the attempt was to identify the relationships of the variables in a more general form. Additionally, this research has identified some limitations of the research methods in the domain of information privacy. For example, questionnaire based information gathering is not appropriate since there is enough evidence that there is a big gap between what people say and what they do. In general, this thesis has taken more of a qualitative research approach together with a few quantitative analyses.

Table 3.2: *Research methods and circumstances under which they are applicable methods. Figure 1.1, Case study research design and methods, 3rd edition, Robert K. Yin*

Methods	Form of Research Question	Requires Control of Behavioral Events?	Focuses on Contemporary Events?
Experiment	How, why?	Yes	Yes
Survey	Who, what, where, how many, how much?	No	Yes
Archival analysis	Who, what, where	No	Yes/No
History	How, why?	No	No
Case study	How, why?	No	Yes

3.3.4 Research Methods

The research method is another level. Research methods give well-defined procedures to be followed while conducting research. Selecting the most suitable research methods is the key to successful research (Yin, 2003). According to Yin, the factors to be considered in selecting an appropriate research method are the type of research question, the researcher's control over the research setting, and the contemporary or non-contemporary nature of the events. Table 3.2 presents how these three factors relate to five research methods. He further states that a study may need more than one research method and it is the responsibility of the researcher to identify the research methods appropriate for the study (Yin, 2003).

According to Yin, there are two kinds of 'what' questions. The first category does not answer frequencies. Explorative research studies, which do not answer 'how many' or 'how much,' can take the shape of the five research methods illustrated above. These questions are meant to build relevant hypotheses and propositions for later validation. Other explorative research studies that answer questions such as 'who,' 'where,' 'how much,' and 'how many,' can be used by taking surveys or analyzing archival records. Explanatory research, which answers 'how' and 'why' questions, can be carried out by using case studies, historical facts, or experiments. However, it is not necessary to restrict the study to a single research method: multiple research methods can be used in a single study (Yin, 2003).

Palvia et al. (2003) provides a list of specific research methods found in the leading IS journals. These self-explanatory methodologies are speculation/commentary, frameworks and conceptual models, library research, literature analysis, case study, survey, field study, field experiment, laboratory experiment, interviews, secondary data, and qualitative research that covers ethnography, action research, case research, interpretive studies, and the examination

of documents and texts. Furthermore, these authors state that these research methods have different levels of rigor, quality, and relevance. The factors which influence a researcher to choose one or another, or more than one, research methodology are the area of the topic, the research question, the researcher's background, and the intended audience. Table 1.1 in Chapter 1 gives the research methods used in the studies presented in this thesis.

3.3.5 Data Collection

Data collection is another level. In general, it can be said that quantitative research methods are surveys, laboratory experiments, formal methods, and mathematical modeling. Qualitative research methods are action research, case study research, ethnography, and grounded theory (Myers & Avison, 1997). However, some research studies can be carried out by using both qualitative and quantitative methods. For example, the survey method is categorized as a data collection technique (Avison & Pries-Heje, 2005) and a research strategy (Denscombe, 2007). Subsection 3.4.2 explains the data collection techniques applied in this research.

3.3.6 Data Analysis

Data analysis is another level. This level includes statistical, mathematical, logical, content analysis, and grounded theory. The grounded theory based approach was used in Paper 7. Some statistical techniques were applied in the survey based studies presented in Papers 1 and 2. Content analysis was applied in case studies where documents were used as the data source.

3.4 Theories

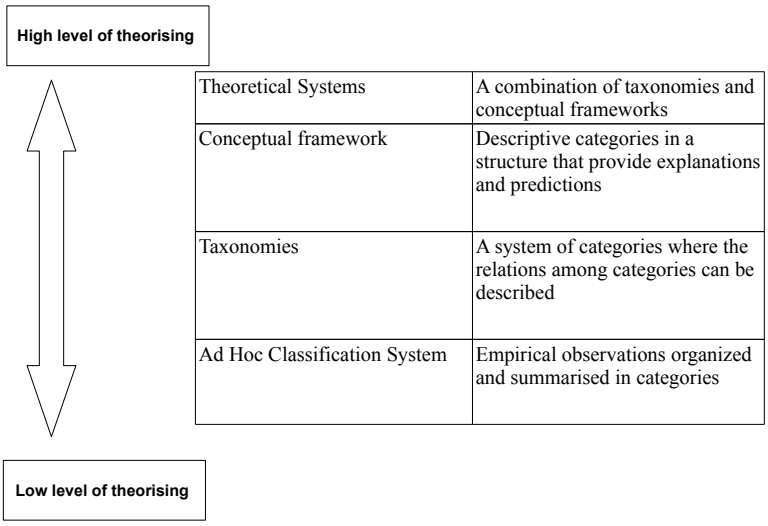
The above-mentioned research process develops and falsifies theories. Theories have been defined by Gregor (2006) as "... abstract entities that aim to describe, explain and enhance understanding of the world and, in some cases, to provide predictions of what will happen in the future and to give a basis for intervention and action." Essential ingredients of a theory are description and explanation (Whetten, 1989). According to Dubin (1978), the essential elements of a theory are the constituent elements (what), the relationship between the factors (how), the reasons for the relationship (why), and the boundaries of the theory (proposition). The constituent factors should include the all-important factors (variables, constructs, and concepts), but unimportant factors or factors of little importance should be excluded. In other words, a theory must have both comprehensiveness and parsimony. Secondly, a theory must explain how the constituent elements relate to each other. A good example for a relationship between constituent elements is causality. Thirdly, a theory must explain

why the relationship exists. The last element, proposition, should provide a foundation to test the theory by deriving testable concepts. A proposition also explains where, who, and when a theory works and doesn't. Additionally, a theory may provide a foundation for deriving a hypothesis that can be tested by quantitative methods.

Gregor (2006) has explained seven structural components of a theory: means of representation, constructs, statement of relationship, scope, theory component (components contingent on the theory's purpose), causal explanation, testable propositions or hypotheses, and perspective statements.

Theories can also be classified according to generalization and the breadth of the focus. According to Gregor (2006), meta theories are a high level of abstraction that possibly apply across disciplines. Grand theories are theories that are not relatively fixed in time and space. Substantive theories focus on specific areas while formal theories are applied within a broad area. Mid-range theories are moderately abstract theories in which testable hypotheses can be easily derived.

As shown in Figure 3.3, Johansson (2004) presented another classification scheme. According to this classification scheme, there are four type of theories. They are ad-hoc classification systems, taxonomies, conceptual frameworks, and theoretical systems. Theoretical systems are at a higher level of theorizing and ad-hoc classification systems are at a lower level of theorizing.



Theoretical Systems	A combination of taxonomies and conceptual frameworks
Conceptual framework	Descriptive categories in a structure that provide explanations and predictions
Taxonomies	A system of categories where the relations among categories can be described
Ad Hoc Classification System	Empirical observations organized and summarised in categories

Figure 3.3: Abstract level of theories, Johansson, 2004, p. 7

The researcher needs theories as (i) an initial guide to design the research and data collection, (ii) a part of the iterative process of data collection, (iii) a final product of the research (Walsham, 1995).

Gregor (2006) has listed five types of theories that are common in the IS discipline. These are theory for analysis, explanation, prediction, explanation and prediction (EP), and design and action. The theory for analyzing explains the dimensions or characteristics of an investigated phenomenon. It simply answers "what is." The second type of theory, explanation theory, explains "why" and "how" some phenomena happen. This kind of theory is important for understanding the subject. Theory for predicting is a kind of black box theory that explains "what will be" but not "why." The theory for explaining and predicting (EP theory) presents both causes and prediction together with theoretical constructs and their relationships. This category of theory simply answers "what is," "how," "why," "when," and "what will be." The last category is theory for design and action, which says "how to do" something. A further discussion on this category is given in the design science section (Section 3.4.1). Another type of theory which is not specifically mentioned by Gregor (2006) is normative theory, which explains "what should be."

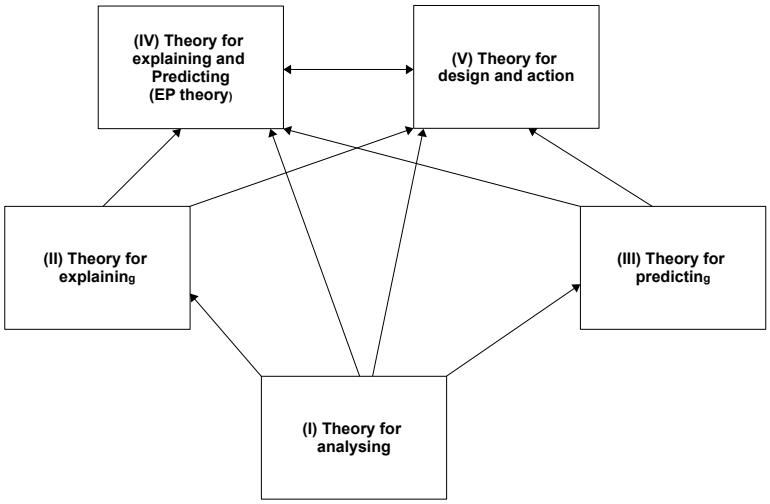


Figure 3.4: Theories used in information science, Gregor, 2006, p. 27

Figure 3.4 shows the relationships among the above-mentioned five types of theories. The diagram shows that the theory for analyzing is the basis for the other theories. The theory for explaining and predicting (EP theory) can take

in components from the theory for explaining and theory for predicting. The interrelationship between design and action theory and EP theory is discussed in the section devoted to design science.

As shown in Figure 3.3, taxonomy is one kind of theory. The grounded theory paper presents a taxonomy of the information privacy domain. As shown in Figure 3.4, Gregor (2006) has presented five types of theory. These types are (i) theory for analyzing, (ii) theory for explaining, (iii) theory for predicting, (iv) theory for explaining and predicting, and (v) theory for design and action. Furthermore, these theories are related and also some theories depend on other theories. This research is a part of developing a theory for predicting. The part that is addressed in this thesis is identifying the necessary constructs and dimensions for building information privacy metrics. Once the metrics are developed, they can be used for predicting the level of protection provided by data controllers. This also helps individuals to take actions. Therefore, this research has contributed to the IS research field by presenting a new taxonomy and identifying the constructs and dimensions for building new theories.

After discussing the research methodologies and theories in information system science, this discussion goes on to the information science discipline.

3.4.1 Information Systems Research

Lee (2000) has mentioned three challenges faced by IS researchers. The first challenge is that IS practitioners do not adequately welcome impressive rigorous research. On the other hand, professionally sound articles lack academic rigor. The second challenge is finding an identity for the IS field. The last challenge is whether to take the technological or the behavioral path. Furthermore, Lee proposes design science, true system sciences, and paradigms as solutions to meet these challenges.

As shown in the diagram below (Figure 3.5), the interaction between the behavioral subsystem and the technology subsystem creates a new system that is completely different from its parent subsystems. In Lee's words, the "IS field deals with the unique phenomena that emerge when the technological and the behavioral interact—just like different chemical elements that react when they form a compound." (Lee, 2000. Slide 12). Lee suggests adopting true system science to study this new subsystem and to follow design science that focuses on designing new, effective artifacts that solve real world problems.

Knowledge, mentioned at the beginning of this section, has two parts. One part is called "techne." This deals with practical knowledge (know how). The second part is "episteme." This is the theoretical aspect of knowledge (know why/that). Design science is the practical aspect of knowledge that explains "how to."

> "I thought I began to see in the problem of artificiality an explanation of the difficulty that has been experienced in filling engineering and other professions

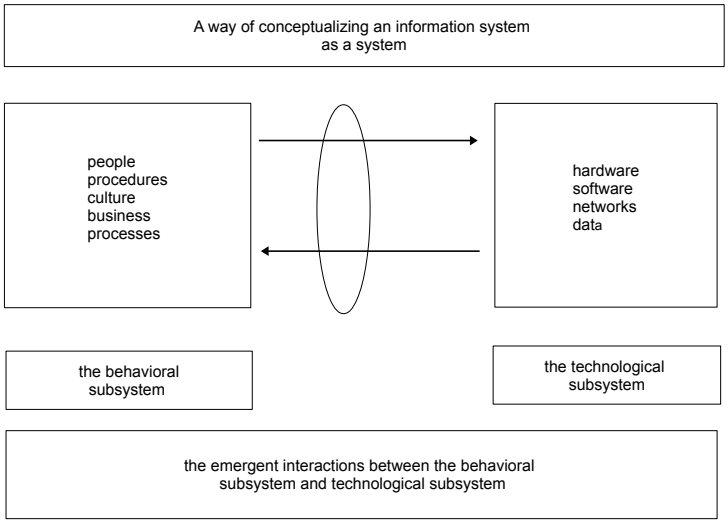


Figure 3.5: Information systems research framework, Lee, 2000, Slide 12

> with empirical and theoretical substance distinct from the substance of their supporting sciences. Engineering, medicine, business, architecture and painting are concerned not with the necessary but with the contingent—not with how things are but with how they might be—in short, with design. (Simon, 1996. p. xii)."

In his keynote speech, Lee stated that the book titled *The Sciences of the Artificial* by Herbert Simon in 1960 explains design science. The primary difference between design science and natural science is the aim. According to March and Smith (1995), who proposed a framework for design scientists, "[n]atural science aims at understanding and explaining phenomena; design sciences at developing ways to achieve human goals" (p. 254). Furthermore, the authors state that natural scientists have to explain, using theories, how and why IT systems work in an operating environment. Lee (2004) has mentioned another difference between design science and natural science. He states:

> "Design science, like action research, presumes intervention in the real world, while natural science and social science consider intervention as something to be avoided because it contaminates the subject matter and can give the appearance of biasing the analysis so as to lead to favorable findings. (p. 49)"

Truth is the primary focus of natural science and utility is the aim of design science. These are two sides of the same coin (Aboulafia, 1991). Two aspects of IT are descriptive and prescriptive. According to March and Smith (1995), Hempel (1966) defines descriptive research as "[a] knowledge-producing activity corresponding to natural science" and Simon (1981) defines prescriptive research as "... aims at improving IT performance. It is a knowledge-using activity corresponding to design science" (p. 252).

Hevner et al. (2004) have proposed a broad framework for IS researchers. This framework is shown in Figure 1.5 and described in Section 1.5 in Chapter 1.

Phenomena related to business needs are developed and justified using behavioral science theories (Hevner el al., 2004). March and Smith (1995) use the term natural science instead of behavioral science, which is a part of the former. The knowledge base consists of a contribution from both design science and natural science research. March and Smith (1995) state that "... natural scientists create knowledge which design scientists can exploit in their attempts to develop technology" (p. 254).

The framework presented by March and Smith explains four design science products and four design science processes. Lee (2004) extended this framework by incorporating the action research strategy proposed by Martensson and Lee (2004). This is shown in Figure 3.6. It is worth discussing the extended framework together with the explanation given by March and Smith (1995). The four products explained in March and Smith's paper are constructs, models, methods, and instantiations. According their definitions, constructs stand for the vocabulary of a domain. A model is a set of propositions or statements expressing relationships among constructs (operationally represented with boxes and arrows). A method is a set of steps used to perform a task. An instantiation is the realization of an artifact in its environment. The first two research activities mentioned by March and Smith are building and evaluating. Building refers to successfully demonstrating the possibility of building the artifact and evaluating refers to fulfilling the intended purpose with a desired level of performance. The last two stages, theorizing and justifying, are responsibilities of natural scientists. Theorizing refers to building theories that explain how and why the developed artifacts work in a given environment. Justifying refers to proving theories using collected scientific evidence. As shown in Figure 3.6, by labeling cells in the extended framework (DSAR), Lee (2004) explains how an action and practitioner follow the framework. In Figure 3.6, the box denoted by (i) represents the constructs. Cell (ii) is about evaluating the built constructs. Cells (iii) and (iv) are devoted to the models, while cells (v) and (vi) discuss the methods. Cells (vii) and (viii) are carried out only by practitioners. The planning carried out by the practitioner together with the action researcher is denoted in cells (ix) and (x). As discussed in the previous paragraph, theorizing and justifying are given to natural scientists and Lee (2004) assigned these tasks to design science.

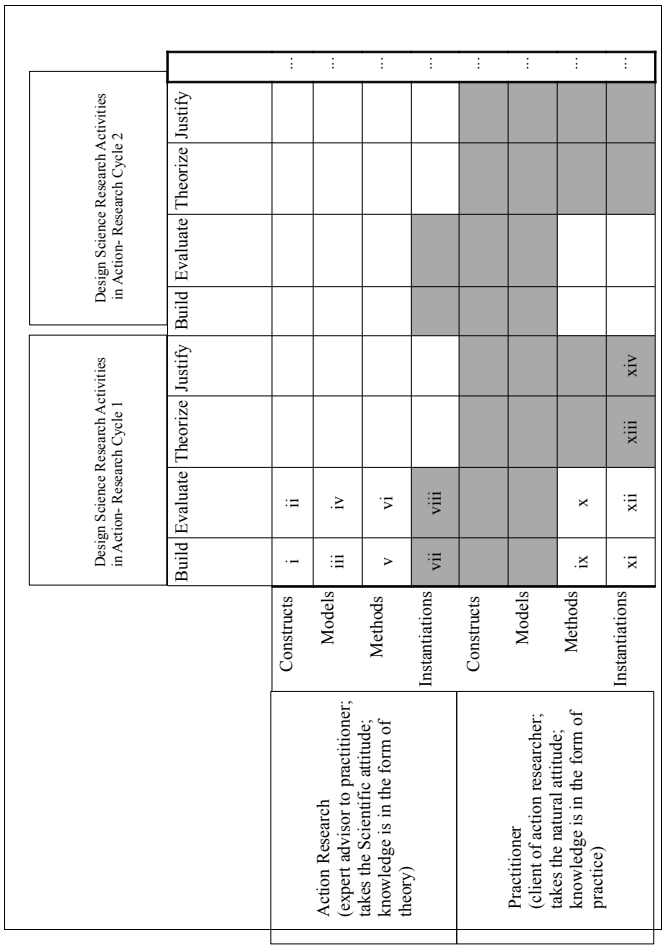


Figure 3.6: Design Science and Action Research (DSAR) Framework, Lee, 2004, p. 53

The box denoted by (i) in Figure 3.6 represents the constructs. Lee (2004) defined constructs as "[a] product of the coding is what grounded theory calls 'categories,' which design science would recognize as 'constructs' " (p. 55). Furthermore, Lee (2004) stated that constructs could be developed either following case study research as proposed by Yin (1994) or Strauss and Cobin's grounded theory approach (1990, 1998).

3.5 Methodologies applied

Instead of Strauss and Cobin's grounded theory approach (1990, 1998), the classical grounded theory approach presented by Glasser and Staruss (1967) and Glasser (1978, 1998) was used to identify the constructs: actors, factors and concepts. The reason for using the classical grounded theory approach instead of Cobin's grounded theory approach was that the classical grounded theory approach makes it possible to focus only on the key points. According to Lee (2004), the other method of identifying constructs is Yin's (1994) case study method. This method was applied in conducting the two case studies presented in Papers 4 and 5.

Papers 1 and 2 are based on survey research. As shown before in Table 3.2, survey research is recommended for answering questions such as 'who,' 'what,' 'where,' 'how many,' and 'how much.' In addition, survey research focuses on contemporary events where the researcher does not have control over the events (Yin, 2003). Surveys focus on the breadth of entities rather than their depth. The advantages of using surveys include the possibility of focusing on a large amount of empirical data, the availability of a rich set of statistical techniques for data analysis, the ease of processing the data, and cost effectiveness. Some disadvantages include the limited number of entities (humans and artifacts), the possibility of getting inaccurate data, and having a less response rate. The surveys presented in Papers 1 and 2 attempted to identify correlations between the privacy attitudes of individuals with various demographic and other characteristics.

3.6 Data Collection Techniques

Data collection techniques directly affect the quality of data. For example, an observation technique gives a more accurate picture of the data subjects than does a questionnaire. This is because the data collector is in a position to directly observe the respondents' behavior. However, a number of factors affect the selection of the appropriate data collection techniques. Some of these are the purpose of the research, the research approaches and methods, the time allocated, and the cost. According to Biemer et al. (1991), the underlying factors for choosing one or more data collection technique are the quality of the expected data, the cost of the data collection, the expected error rate, and the time required to collect the needed data. Some leading data collection techniques are surveys, interviews, transcript analysis, participant observation, field work, and archival research including published and unpublished documents (Avison & Pries-Heje, 2005).

According to Yin (2003), archival records and documents such as written materials, published, and unpublished administrative documents are empirical data for case study research. There are certain cases where obtaining primary data is not possible. For example, the ideal data source for the studies presented

in Papers 4, 5, 7 would be the original case records. In cases where it is not possible to obtain the data from primary sources, the researcher has to obtain the data from secondary sources. Otherwise, conducting the study is not possible. No matter the origin of the sources, it is the researcher's duty to make sure the quality of the data is suitable for the purpose. There are some advantages and disadvantages to using secondary data sources. One advantage of using secondary data is that it saves time and reduces the cost, since the data has already been processed to a certain extent. A major disadvantage of using secondary data is that it increases the chance of making inaccurate conclusions. For the studies presented in Papers 4 and 5, the empirical data were collected from the Ninth Annual Report of the Article 29 Working Party and online-published decisions given by the Canadian, Australian, Hong Kong, and New Zealand Privacy Commissioners. Since it was not possible to obtain the original case records, summarized versions of the cases published by the commissioners were used as secondary data sources, assuming that all the published cases on the commissioners' web sites reflect a true and fair picture.

The questionnaire is another data collection technique employed. A questionnaire consists of a set of questions. These questions are meant to gather factual information such as age, sex, opinions, and attitudes. A questionnaire can be well structured, semi-structured, or unstructured. Structured questions give a set of possible answers and require the respondent to choose one or more selections from the given set of answers. This approach makes data processing easy. However, a well-planned study for drafting questions is required. One drawback is that respondents do not get the chance to express their true feelings and positions. This method was applied in the study presented in Paper 1. An unstructured questionnaire allows the respondents to freely express their views, feelings, and positions. Semi-structured questionnaires are a balance between these two extremes. The advantages of this data collection technique are the possibility of collecting data from many respondents within a short time period, obtaining first-hand information, and their cost effectiveness. A semi-structured questionnaire was used in Study 2. In order to obtain clarity, interviews were also conducted in Study 2.

3.7 Conclusion

This chapter discussed the research approaches and methods used throughout this research process. The chapter started with describing what science is, and then the discussion went on to explaining how and why this research falls into the information systems (IS) research domain. Then, the epistemological and ontological stance taken in conducting this research was presented. Section 3.3 discussed research methodology on several levels, together with explaining how this research can be viewed through these levels. Section 3.4 gave an overview of the theories used in this research. Information systems research

was discussed in Section 3.4.1. That section was based on the information systems research framework introduced by Hevner el al. (2004) and the design science and action research (DSAR) framework introduced by Lee (2004). Explaining Lee's (2004) framework, the discussion then explained why the each one of the various research methods was employed, and how the research papers presented fit into Lee's framework. This discusion was concluded by discussing the methods used in collecting data.

4. Research Contribution

This chapter presents the identified information privacy metrics. A conceptual model is used in presenting these metrics. This conceptual model is also used to explain how these identified individual information privacy metrics can be put into a coherent information privacy metric that provides an overall indication. Furthermore, two examples are presented as a proof concept of this conceptual model.

4.1 Dimensions and Constructs

These identified constructs and dimensions, which are presented in Figures 4.2–4.23, are used in developing information privacy metrics. The conceptual model followed in presenting these metrics is shown in Figure 4.1. Five vertical columns can be seen in Figure 4.1. The first column represents the construct or dimension concerned and the second column represents how the identified construct or dimension contributes to develop an individual information privacy metric. The third column presents the individual metric. One or a combination of these individual metrics forms an intermediate level information privacy metric. For example, Section 4.2.1 shows how five individual information privacy metrics form an intermediate level information privacy metric that presents the quality of the training program given to personal information handling officers. These intermediate level information privacy metrics form the overall information privacy metric. The overall one indicates the full commitment of the organization to protecting personal information.

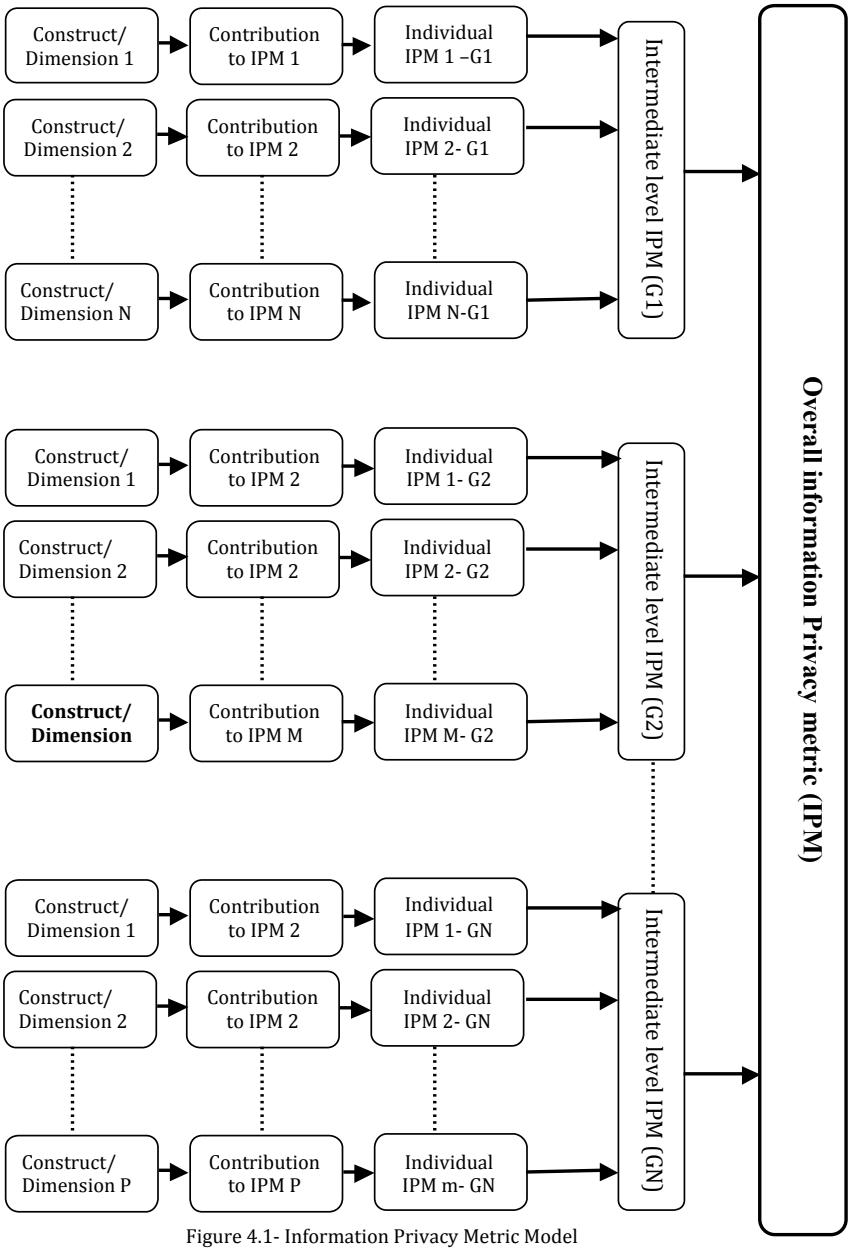


Figure 4.1- Information Privacy Metric Model

Figure 4.1: The Conceptual Model for Information Privacy Metrics

Figure 4.2 shows how the identified dimensions shape the intended overall information privacy metric. This figure consists of four columns. The last column represents the intended overall information privacy metric. This overall metric is a coherent whole that includes the individual privacy metrics represented in the third column. The various dimensions given in the first column

shape these individual metrics. How these dimensions contribute to identifying the individual information privacy metrics is explained in the second column.

Dimensions of the Intended Information Privacy Metrics

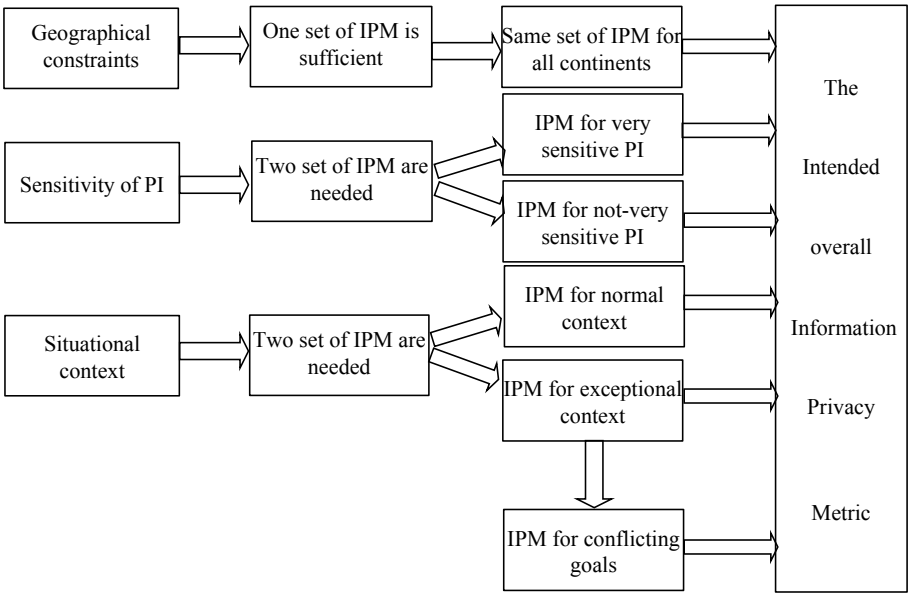


Figure 4.2: Identified dimensions for information privacy metrics

According to the findings of Paper 1, there is no significant relationship between the investigated demographical data and the level of protection sought for personal information. Therefore, it can be said that the findings indicate that there is little need for a separate set of metrics for each continent. In other words, the set of intended metrics appears to be useful in any continent. This is represented by the top row of Figure 4.2.

Furthermore, Paper 1 stresses the need for two sets of metrics: one for very sensitive personal information and the other one for non-sensitive personal information. The second row of Figure 4.2 addresses the dimension of sensitivity of PI. In other words, it addresses the number of metrics required for different sensitivity levels of personal information. As the second column of the second row of Figure 4.2, it stresses the need for two sets of IPM. One set is needed for very sensitive personal information and the other one is for less sensitive personal information. These two sets of metrics are shown in the third column.

Another identified dimension is the situation context. As discussed in Paper 1, a different set of IPM is needed for exceptional situations. The identified exceptional situations are national security, public health and safety, and preventing and detecting criminal acts. These findings have been confirmed by similar studies. These findings emphasize the need for separate metrics for ex-

ceptional situations. This is represented in the last, the third, row of Figure 4.2. One set is for ordinary contexts and another one for exceptional contexts.

In these exceptional situations, other goals conflict with information privacy goals. As discussed in Section 2.7, in these situations, privacy should be considered a total-sum game instead of a zero-sum one. Thus, there is a need to measure how an organization plays the total-sum game. This is reflected in Figure 4.2 by showing a separate metrics labeled as "IPM for conflicting goals". These situations arise in exceptional situations. This is reflected in the arrow from "IPM for exceptional context". As discussed in Section 2.8, further research is needed to identify constructs for this set of metrics.

Constructs of the Intended Information Privacy Metrics

This section presents the identified individual information privacy metrics. In order to make it more convenient for readers to understand, these metrics are grouped based on the information privacy taxonomy presented in Paper 7. The purpose of the taxonomy is to provide an overview of the actors, factors, and concepts in the information privacy domain. On the other hand, a protective measure touches more than one actor, factor, or concept. Therefore, deciding on the proper place for an individual metric was not straightforward. In these cases, the metric is placed in the most appropriate place. However, this leaves room for questioning the way the metrics are grouped and presented. For example, the "user name" used in an identity verification system can be placed in the subcategory of identification data in the personal data theme since it is a kind of personal data, or else be put in the subcategory in the technology theme since "user name" is used in the authentication system. In this case, the "user name" is placed in the subcategory of identification data in the personal data theme due to its uniqueness. Another example is that a protective measure can be placed in either in the financial subcategory or the enforcement subcategory in the protective measure theme. The reason is the close relationship between these two categories. One category represents the financial commitment of an organization to deploying protective measures, while the other category represents the commitment of the organization to enforcing the use of the same protective measures.

Table 4.1 presents the individual information privacy metrics and the paper number where the corresponding constructs are presented as a protective measure, and the theme and subcategories of the construct in the context of the information privacy taxonomy presented in Paper 7. The very left hand column refers to the diagram that presents a group of individual information privacy metrics. The next column gives the order of a horizontal layer of the diagram. The horizontal layer presents the construct, its contribution to building an individual information privacy metric, and the individual information privacy metric, respectively. The third and fourth columns of Table 4.1 represent the paper and the place where the protective measure is discussed, respectively. In order to make it convenient to identify the exact position in which to read

more about the protective measure, the number of the section (S), table (T), or page (P) is given in the fourth column. The last two columns present the corresponding theme and the subcategory(ies) where the construct is placed in the presented information privacy taxonomy, respectively.

Even though every effort has been made to make the text in the boxes self-explanatory, there are cases where the text is insufficient. This is due to limitations of space. [1]

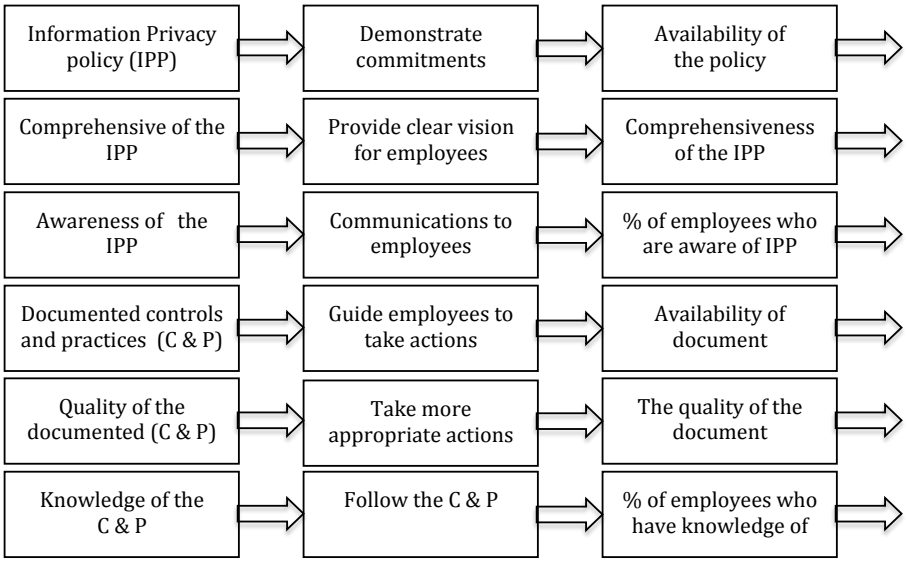


Figure 4.3: Metrics to measure the quality and awareness of key information privacy articles

Information privacy policy (IPP) is the document that spells out how an organization handles personal information. Having an IPP demonstrates how seriously an organization takes properly handling personal information. The first metric in this category is the availability of an information privacy policy. However, the policy itself is not enough. The policy should cover every aspects of fair personal information handling practices of all types of personal information. The comprehensiveness of the IPP is another measurement. Then only employees can take proper action in handling personal information. The second metric in this category measures the comprehensiveness of the IPP. A comprehensive IPP also demonstrates an organizational commitment to protecting personal information. Measuring its quality is a subjective judgment. In order to measure the comprehensiveness of the IPP, the policy is broken down into several measurable individual units, which are discussed in the subsequent sections. Another important aspect is the communication of the IPP to

[1] From Figure 4.3 onwards, neither the overall information privacy metrics nor the intermediary level metrics are shown. This is to allow more space for explaining the constructs, their contribution to developing the individual metrics, and the individual metrics. The arrow going from the metric shows the relationship to the intermediary level metrics.

employees. In other words, employees must be aware of the IPP. Thus, another metric is developed to measure the percentage of employees who are aware of the IPP.

Controls are designed and practices are introduced based on the IPP. Having these practices and controls in a written document indicates a greater commitment to protecting personal information. This leads to introducing another metric that measures the availability of the documented controls and practices. In addition to comprehensiveness, the documented controls and practices must be easy to read and understand. This introduces another metric that measures the quality of the documented controls and practices. In order to follow them, employees must have a good knowledge of the documented controls and practices. The last metric in this group measures the percentage of employees who have a good knowledge of them. Figure 4.3 shows these metrics.

User Identification

Almost every online information system has an identification system. The identification system has a "username", which is usually chosen by the user. Even though the user chooses the username, the system should not allow user names that can be used for social engineering attacks. For example, some user names give the false impression that these usernames belong to the service provider. This deceptive impression leads users to expose their personal information. Therefore, the system should not accept these kinds of misleading user names. Additionally, these usernames should not be offensive or disruptive. Taking all these factors into account, a metric is derived to measure the quality of the username. This metric is shown in Figure 4.4.

Figure 4.4: Metrics to measure the quality of identification information

Identity Verification System

An identity verification system is used to verify the identity of a person, more precisely, a requester. An adequate identity verification system is very important in an online environment where individuals do not appear physically. The first metric in this category measures the strength of the identity verification system. The term adequate is used since the measures should be strong enough to protect personal information from various unauthorized activities but at the same time the processing algorithm and collected personal data should not be privacy invasive. One of the recommended methods in matching templates is comparing one template with another template to verify the authenticity of the claimed identity instead of comparing one template with all template stored. The second metric measures the privacy invasiveness of the matching algorithm. It is also accepted that excessive personal information such as very sensitive biometric data should not be used in identification

systems. Therefore, the third metric in this group is to measure the excessive use of personal information. Having a captcha and blocking an account after a predefined number of failed login attempts are two other protective measures. Two metrics are presented here based on these two protective measures. Another deterrence control measure is forcing the user to wait some time (some days) before allowing the user to use the alternative or backup authentication mechanism. The availability of deterrence control is the basis for the next basis. Even though the practicality of this measure has been questioned in the information era, it is presented here since it was found that this deterrence control is the practice of some leading email service providers. These six metrics are presented in Figure 4.5.

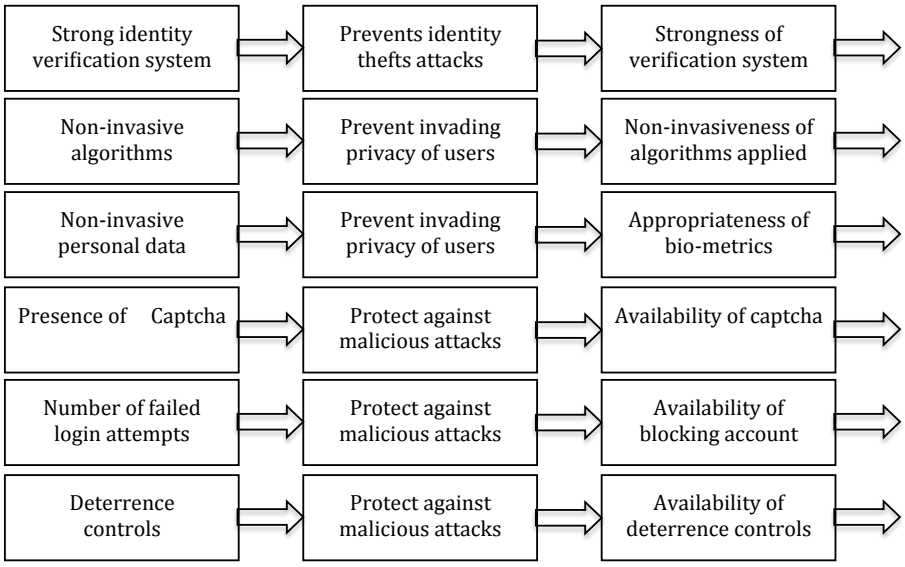


Figure 4.5: Metrics to measure the appropriateness of an identity verification system

Passwords

A password is widely used in the primary user authenticating method. Figure 4.6 presents several metrics to measure various properties of the password and related functionalities. A strong password should not contain personal information and other known information. This is the basis for the first metric in this category. The second metric is to measure the length of the password and the third one is to measure the combination of different types of characters in a password. Having a good length and various types of characters in a password makes it difficult to break the password. These are the basis for the next two metrics. Facilitating users' identifying the strength of their password encourage them to choose a strong password based on their security requirements. Unfortunately, the strength meters of different online service providers do not attribute the same level of strength to the same password. The quality of the password strength meter is the basis for the next metric. Allowing weak pass-

words and previous passwords makes systems more vulnerable. Therefore, the next two metrics are designed to identify the availability of a mechanism to reject weak passwords and previous passwords. Limiting the validity period of the password compels the user to make the system more secure by changing the password. The availability of an expiry period for the password is the criterion for the next metric. Furthermore, having a simple but robust password changing mechanism provokes less hesitation for the user to make the account more secure by frequently changing their password. This is the basis for the last metric in this category.

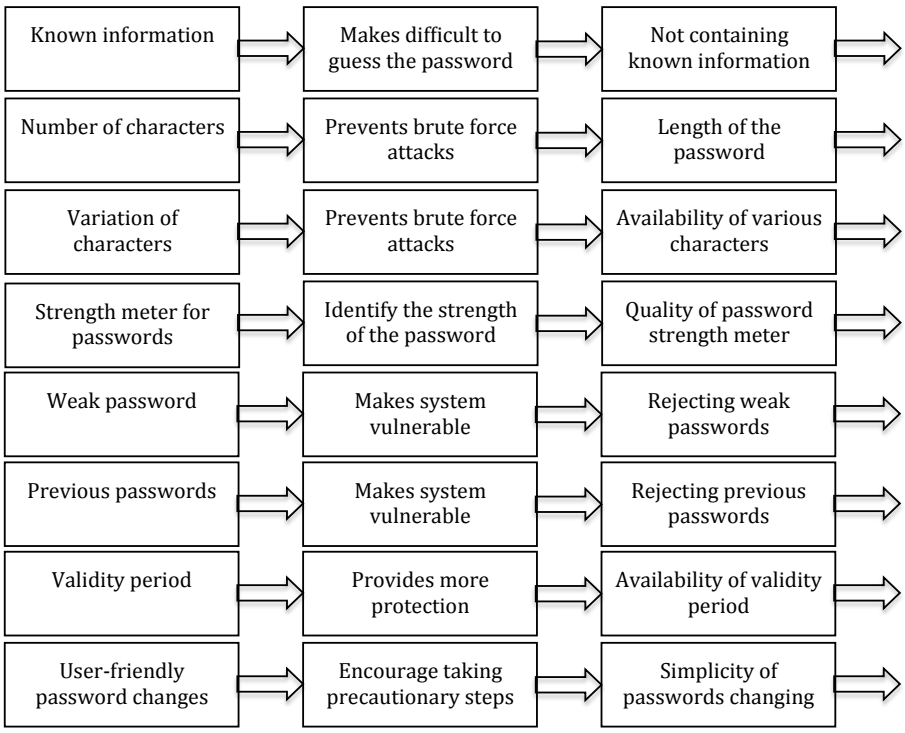


Figure 4.6: Metrics to measure the strength of password and related features

Backup Authentication

A backup authentication method is essential in cases where the primary authentication measure has failed. A backup authentication system should be as strong as the primary authentication mechanism. Otherwise, malicious attackers can gain access to an online account by compromising the backup authentication mechanism. The metric, shown in Figure 4.7, is designed to measure the strength of the backup authentication mechanism.

Security Questions

Security questions are widely used in backup authentication mechanisms. The qualities of a security question are presented in the set of metrics given in Figure 4.8. The first criterion is the appropriateness of the security ques-

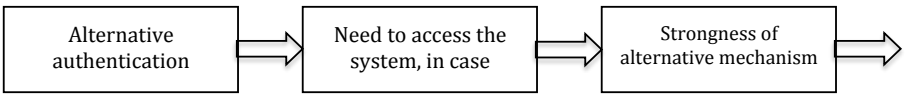


Figure 4.7: Metrics to measure the strength of backup authentication mechanism

tion, which is about the applicability of the question to the target audience and also the exclusiveness of the personal information. This is very important since collecting sensitive personal information as an answer to the security question creates an additional responsibility for the organization. Therefore, the first metric is to measure the appropriateness of the security question. Another important aspect is the ability to uniquely identify the user. This is possible with a large answer space. Therefore, the next metric is to measure the size of the answer space. The third one is to measure the difficulty of finding the answer to the security question. This is known as the integrity of the security question. This metric measures the resistance to impersonation. The fourth one in this category is accuracy. It is about the applicability of the security question over a longer period. This is due to the fact that some users tend to forget answers to the security question over a period of time. This is measured in terms of the likelihood of remembering the answer to the security question. The last item in this metric category measures the quality of a security question. Having a quality meter for security questions empower users to set proper security questions.

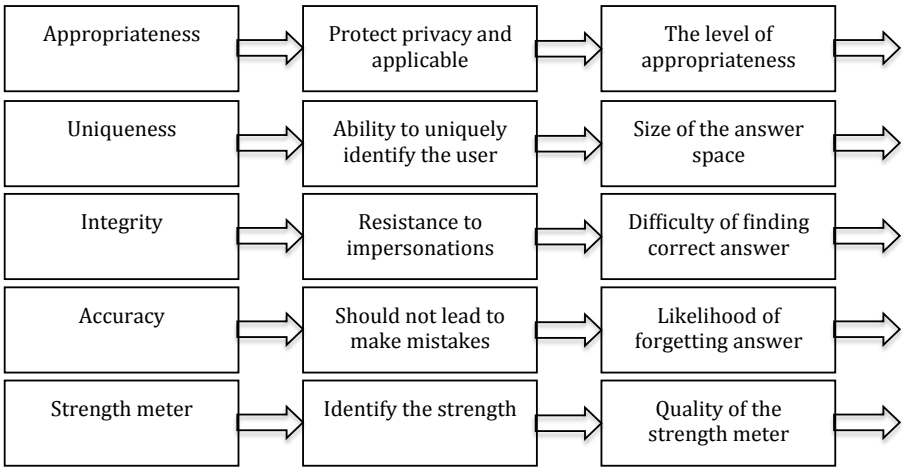


Figure 4.8: Metrics to measure the strength of security questions

Personal Information Handling Officers

A personal information handling officer could have prevented a large number of the reported privacy violations. In order to prevent these violations, personal information handling officers must have certain qualities. The qualities that encourage and facilitate these officers in handling personal information in a protective manner are having the proper training for handling personal information and academic and professional qualifications. The first metric in this category measures the percentage of officers who have received the necessary training for handling personal information. Likewise, the second metric measures the percentage of employees who have the necessary academic and professional qualifications for handling personal information. One example is that only qualified medical professionals should access certain medical information of the patients. It is assumed that at least in some countries that the permanent officers take seriously the performance of their duties and responsibilities. [2] The third metric measures the percentage of officers who have a permanent position in the organization. It is also expected that officers who have signed a code of conduct handle personal information in a protective manner. Therefore, the next metric measures the percentage of officers who have signed a code of conduct on information privacy. Furthermore, signing a code of conduct prevents disclaimers such as non-awareness.

In analyzing reported privacy violation cases, the major cause for privacy violations are carelessness, inattentiveness, and human error. Since it is not possible to predict the future, the most appropriate assumption with which to derive the metrics is that the previous privacy violations will be repeated in the future. Therefore, the metrics are based on the reported cases. These metrics are the number of reported human errors, incidents of carelessness,

[2] As mentioned before, these kinds of subjective metrics can be eliminated at the metric modeling stage depending on the industry and culture.

and unattended information systems. It is also assumed that these weaknesses of personal information handling officers lead to privacy violations. Figure 4.9 present these metrics.

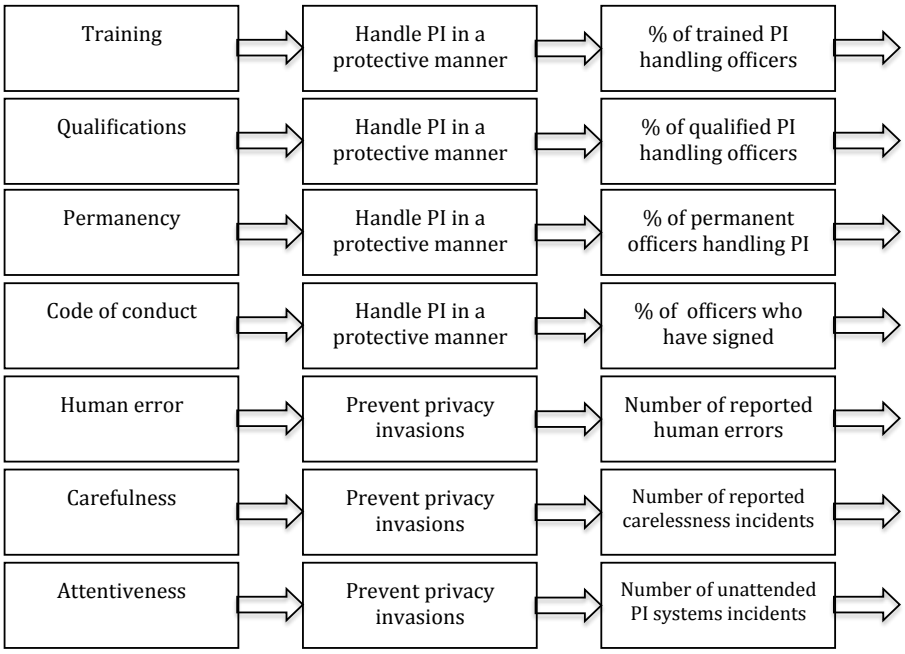


Figure 4.9: Metrics to measure the qualities of personal information handling officers

Personal Information Handling Practices

Several recommended protective measures that should be followed when in possession of personal information have been identified and presented in the form of metrics in Figure 4.10. One measure is to limit the access to personal information to only those officers who need the information to perform their duties. Limiting access to personal information should be carried out by the top-level management and it should be properly formulated who has access to what personal information. The effectiveness of the need-to-know policy is one metric presented in Figure 4.10. Likewise, the segregation of duties also prevents an officer from accessing different types of personal information. This is very important when personal information has been collected for various purposes from various sources. Once a malicious inside attacker gains access to two datasets, strong profiles of individuals can be derived. The second metric in this category measures the effectiveness of the segregation of duties in handling personal information. Other managerial approaches are minimizing the number of personal information handling officers who have access to personal information. This measure reduces the exposure of the personal information to many officers. The third metric measures the effectiveness of this measure. Then, the limited number of officers have to take responsibility for and take due

care in processing personal information. Then it is easy to identify the responsible and accountable officers. Another measure is limiting access to personal information to personal information handling officers only; others should not have access to personal information. The effectiveness of the access control policy is measured in the fourth metric. Monitoring whether the officers handle personal information in a protective manner is another protective measure. The fifth metric is based on this premise. When it is found that the manner of handling personal information has caused a privacy breach, disciplinary action should be taken against the responsible officers. This punishment gives a good lesson to other officers too. Therefore, the punishment should aim at reducing occurrences of privacy breaches in the future. Therefore, the effectiveness of the disciplinary action is taken as a metric.

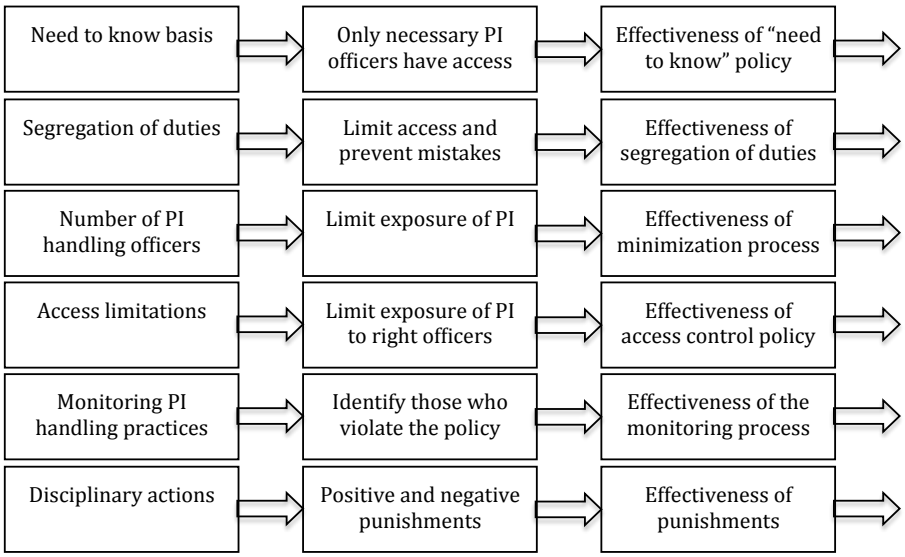


Figure 4.10: Metrics to measure personal information handling practices

Training Programs One of the measures discussed is the training of the personal information handling officers. The quality of the training program has a direct impact on the quality of the trained personal information handling officers. Measuring the quality of any training program is not straightforward. One possible method of measuring the quality of a training program is breaking down the training program into measurable components. Three such identified components are the depth and breadth of the training program, the frequency of conducting such programs, having training sessions after a major incident, and the frequency of program reviews. Training programs should be conducted frequently since frequently conducting training program refreshes the knowledge of the officers. Training after a major privacy breach inside or outside of the organization can be used to explain the mistake or circumstances that led to the privacy breach and to possible protective measures for preventing this kind of

breach in the future and also to educate the personnel as to the consequences of the breach. Since technology is changing and people use information in diverse ways, the periodic review of the training program is important. This review process can introduce new threats, vulnerabilities, and protective measures to protect personal information. The last one in this category measures the level of understanding of officers of how to properly handle personal information. The five metrics derived from these measures are presented in Figure 4.11.

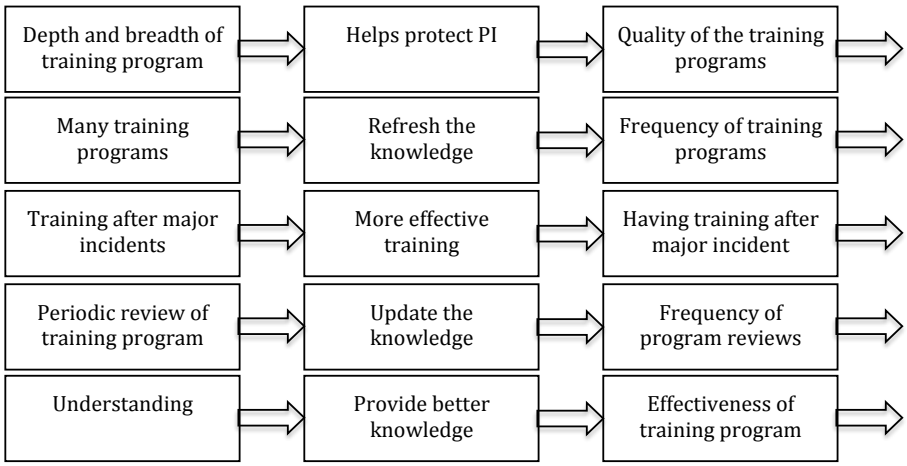


Figure 4.11: Metrics to measure the qualities of the training program

User education

Organizations have a duty to inform users about the information handling practices of the organization. The amount of information provided and the way of presenting it is an indication of the organization's commitment to protecting personal information. Based on this premise, the derived information privacy metrics are presented in Figure 4.12. In order to offer very personalized services and make the information handling process simple, certain personal information including cookies are stored in the user's computer. The user should be informed about the information which is going to be stored in his/her machine. This knowledge enables the user to make an informed decision. Some of these informed decisions are whether to allow or deny their storage, and if the cookies are stored, when to delete them. The first two metrics in this category measure the effectiveness of informing the users about personal information including behavioral information and cookies before storing them on the user's computer. Knowing how to terminate a session is a very important step in protecting personal information. If a user does not properly terminate a session, vital personal information might be exposed. Therefore, informing the user on how to properly terminate a session is important. The next metric is to measure the effectiveness of the way in which the user is informed about terminating the current session. It is possible to login to an

online account from many computers. Sometime, users forget to terminate the session before leaving the computer. In these cases, informing the user about previous login sessions and the corresponding machines and IP addresses is an effective measure to prevent unauthorized accesses. Therefore, effective notification of previous logins is important and the next metrics are based on this premise. Another means of protecting a user account is informing the user about previous failed login attempts and online real-time information about login attempts. The effectiveness of providing this information is the basis for the next metric. Likewise, informing the user about changes in passwords and security questions is also an important measure for protecting the account from unauthorized access. The effectiveness of providing this information is the basis for the next metric. Changing passwords at regular interval is a suggested protective measure. Users expect the system to inform them when to change the password. The effectiveness of informing the user is measured in the next metric. Once a user logs in to a system, the user can maintain the session forever or for only a limited time period. The protective approach is limiting the valid session time. Then, the user is requested to log into the system again. The user should have the right to decide on the default login period. In order to make that decision and also to know the default login period, the user should be informed. The next metric measures the effectiveness of informing the user about the default login period. In order to take effective protective measures, the user must be well informed about protective measures. The last metric is about the effectiveness of all measures taken to educate users.

Rights of the users

Organizations need the support of individuals to protect individuals' personal information. One of the ways of getting individuals' support is providing convenient means to control individuals' personal information. Online services demand individuals to store information such as cookies in their computers and also encourage users to store credentials in their machine. There are situations where users want to delete personal information and credentials stored in their computers. This is also the right of an individual. Providing simple means for deleting the stored information facilitates the users' having more control over their personal information. As shown in Figure 4.13, two metrics are developed based on the simplicity of deleting credentials and other personal information stored in the user's computer. Furthermore, users need to update or correct their personal information stored at the service provider's. In order to exercise this right, the user needs to have a simple mechanism to update the stored personal information. The next metric is to measure the simplicity of the updating mechanism. The users should have the right to decide the security level of the communication channels. In certain cases, the user wants to have a secured channel. Therefore, the process of shifting to a secured channel should be simple. The next metric measures the simplicity of the shifting process. There are cases where the user needs to close the account and delete the stored personal information. Organizations should provide a simple process for closing down

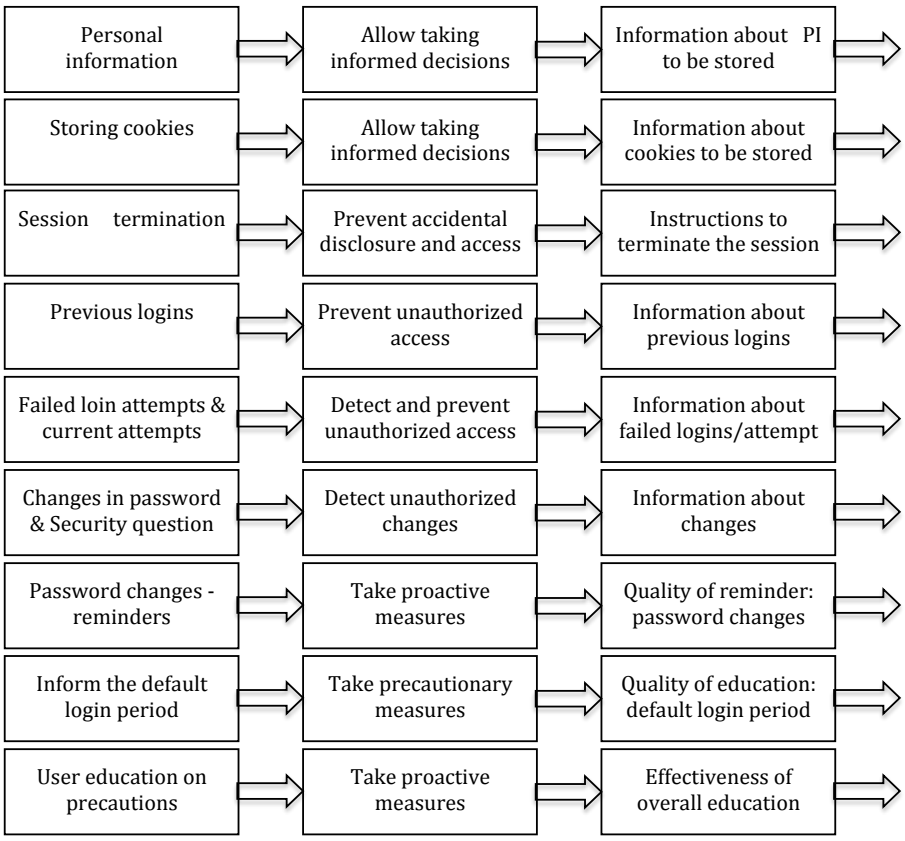


Figure 4.12: Metrics to measure effectiveness of user education

the account and erasing the stored information. In a case where the stored information must be kept to meet legal requirements, steps should be taken to delete the stored personal information once the legal time bar is reached. There are cases where users need additional security for a higher risk level. In these cases, organizations should provide a mechanism to provide additional security for a fee or free of charge. The next metric, the last in this series, measures the readiness of the organization to provide additional security.

Enforcing users

As discussed above, the support of individuals is very important in protecting their personal information. However, in many cases, individuals do not listen to the instructions given to protect their personal information. In these cases, users should be forced to take precautionary measures. The effectiveness of forcing users to take a precautionary measure is used to derive a metric and is shown in Figure 4.14. One example in this category is forcing the user to change the password, when the same password is used longer than a certain time period. Another example is not allowing a user to operate a teller machine when another person is standing beside.

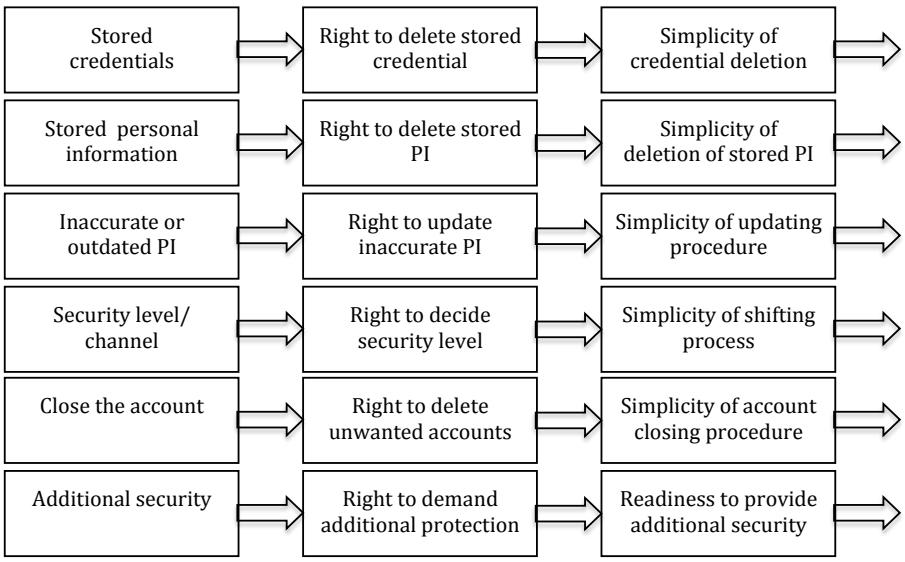


Figure 4.13: Metrics to measure the convenience of exercising users' rights

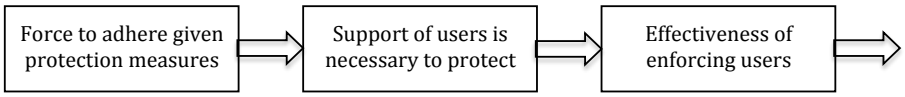


Figure 4.14: Metrics to measure the effectiveness of enforcing users to take actions

Security of Physical Media

Organizations should keep personal information to provide required services. Therefore, special emphasis should be placed on the availability of personal information. Data cannot be kept for long on some media, such as thermal papers and other vulnerable physical storage devices. Therefore, information on these media should be transferred to permanent physical media. A metric is derived to measure the percentage of personal information on permanent media. Then, these permanent media have to be protected so that the personal information is available when required. Therefore, a metric is derived to measure the effectiveness of the overall protection given to the physical media. This metric can be greatly improved by taking insights from the information security domain. A special kind of device used to store personal information is the portable device. The overall protection given to the portable devices is another metric in this category. These metrics are shown in Figure 4.15. The protection given to portable devices is broken down into several components and metrics are derived to measure the effectiveness of each component. These metrics are given in Figure 4.16 and discussed below.

Security of Portable Devices

These days, officers are used to keeping personal information together with other information on small handheld devices. These devices are vulnerable to

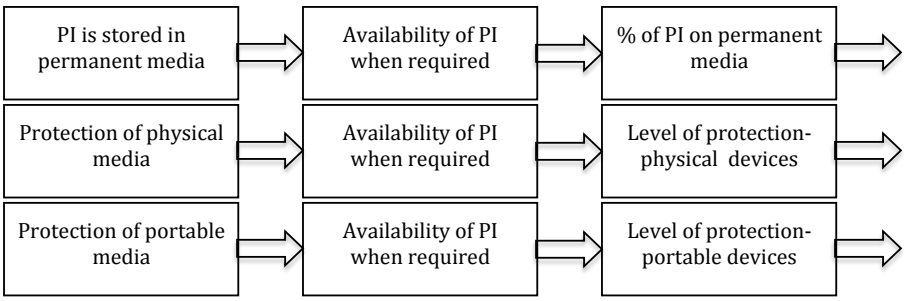


Figure 4.15: Metrics to measure the protection given to physical media that contain personal information

many threats. Therefore, the effectiveness of the protection given to portable devices is important. This is very important in cases where the portable devices are taken outside the office premisses. In addition to the metric to measure the effectiveness of the overall protection given to portable devices, several other metrics that contribute to calculating the overall protection have been identified. These submetrics are identified from the protective measures that must be taken before taking portable devices out of office. One measure is minimizing the contained personal information. This measure reduces the likelihood of unwanted disclosures. Another method is encrypting the stored personal information and keeping the copy of personal data within the office premisses. The strength of encryption including the encryption algorithm and key size has been used in measuring the strength of the protection. Officers who take portable devices out of the office premisses must be aware of the threats and vulnerabilities of taking them out. Based on this awareness, another metric has been derived. Before taking them out, it is essential to make sure that all recommended technical measures have been taken. For example, the personal information should have been encrypted with the approved level of keys and algorithm. The effectiveness of the technical measures is the basis for the metric that is to measure the effectiveness of the technical approval process. Similarly, the final approval should be taken from management. Based on this, another metric has been derived to measure the effectiveness of the managerial approval process. In this process, management has to decide whether it is really necessary to take the personal data out of the office premisses and also whether the responsible officer is aware of the threats and vulnerabilities. These metrics are shown in Figure 4.16.

Transferring Personal Information

Personal information is transferred from one place to another place. There are many transmission media on which personal information can be transferred. However, not all media are allowed to transfer personal information due to their inherent vulnerabilities. Therefore, one derived metric is about the appropriateness of the transmission media used in sending personal information. As mentioned in the section on portable devices, personal data minimization

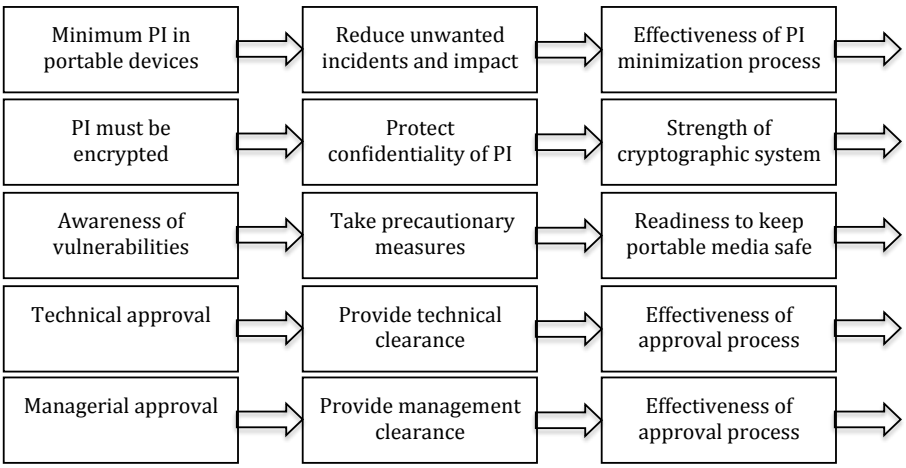


Figure 4.16: Metrics to measure the protection of portable devices that contain personal information

and encrypting personal data before transferring information are vital precautionary measures. Therefore, the effectiveness of the personal information minimization process is taken as another information privacy metric. Likewise, the strength of the cryptographic protection is also taken as another information privacy metric. Before sending sensitive personal information, it is important to double check whether the appropriate protective measures have been taken. This prevents some unintended data disclosures. Therefore, another metric is derived based on the effectiveness of the double verification procedure. Verifying the recipient's address and making sure the delivery of the information is to the intended recipient gives a high level of guarantee that the message has not gone wrong. Based on these premises, metrics for the effectiveness of address verification, the delivery process, and the availability of a delivery report have been presented in Figure 4.17.

Inbuilt Security Features

Systems should be designed so that the system itself takes care of protecting personal information when the user ignores the recommended protective measures. The effectiveness of the protection given to personal information when the user is careless is the first metric in this series. The system should be secure by default. As mentioned before, when the user thinks that the security level is too high, the user can lower the security level. Even though the user has a right to determine the security level, the point insisted on here is that the system should come with complete security. This provides maximum protection even without user involvement. The security metric derived on this basis checks the percentage of by-default security features that provide maximum security. All credentials should be transmitted over a secure channel. This prevents unauthorized access to a greater extent. The availability and effectiveness of this secure channel is the basis for the next metric. Cookies, which are stored to

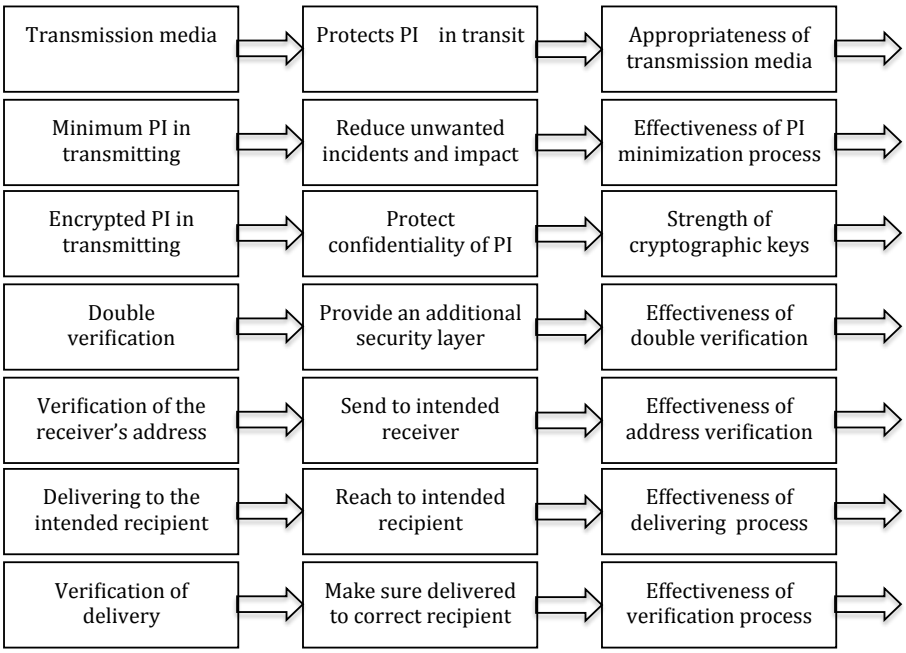


Figure 4.17: Metrics to measure the effectiveness of the transfer process

maintain sessions, should not be kept for more than the necessary time period. The next metric is about measuring the reasonableness of the lifetime of cookies. When the user does not logoff, the system should automatically logoff. This prevents unauthorized access. The effectiveness of the auto logoff mechanism is the basis for the next metric. These metrics are shown in Figure 4.18.

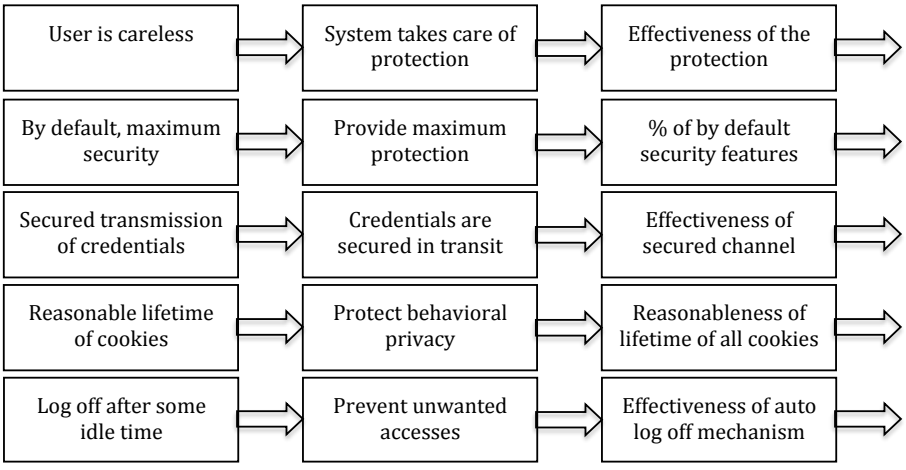


Figure 4.18: Metrics to measures built-in security features

Security in Collecting Personal Information

Protective measures have to be taken even at the point of the collection of personal information since there have been a number of reported privacy breaches at that stage. Therefore, the appropriate protective measures have to be taken in order to protect personal information from accidental disclosure. The first metric in this category is to measure the overall effective protection at the stage of the collection of the personal information. Obtaining the consent of the user is also an important step in collecting personal information. Obtaining that consent facilitates the user's taking more informed decisions. This also prevents the user from denying the involvement later. The next metric is to measure the effectiveness of obtaining the consent of the user. One method of obtaining the consent of the user is to provide an opt-in option when collecting the personal information. This is very important in collecting sensitive personal information. Therefore, the next metric is to measure the percentage of available opt-in options with respect to sensitive personal information. An opt-in option may not be the preferred option when collecting non-sensitive personal information. However, it indicates the explicit consent of the user. Therefore, the next metric is derived to measure the percentage of opt-in options in case of non-sensitive personal information. These metrics are shown in Figure 4.19.

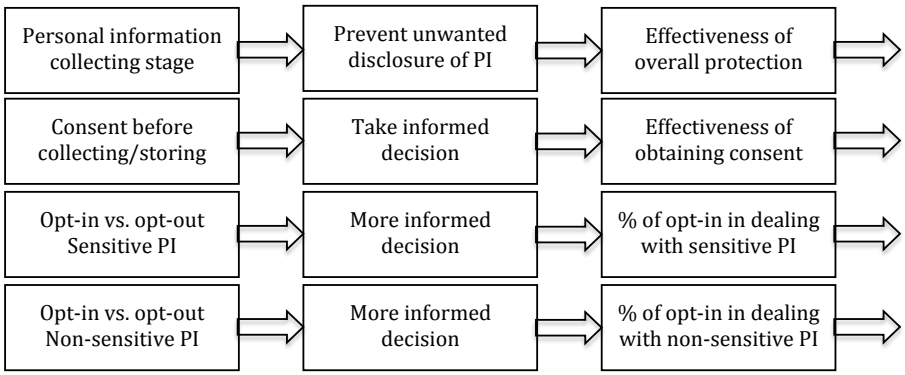


Figure 4.19: Metrics to measure the level of protection given in collecting PI

Security in Processing Personal Information

The personal information collected should be protected at the processing stage too. In processing, there can be cases where manual verification is needed. One instance is where the system is not capable of differentiating between two individuals. The identification of cases where manual verification is needed and providing manual verification in these cases are the basis for the first metric in this group. This metric measures the effectiveness of the manual verification process. The organization should be ready to provide additional security when the personal data itself demands more protection. Based on this, the next metric is built, which asks for the quality of this additional protection.

Personal information handling officers should be warned when they access cases that need extra protection. Placing a warning system inside the process of accessing extremely critical personal information makes officers be more careful and also take extra protective measures. Therefore, the next metric is built to measure the effectiveness of the warning system. Keeping log records of every data access is important for detecting malicious activities and also accidental events. Therefore, the next metric is built to measure the quality of the log records. Two important characteristics of log records are completeness and accuracy. These metrics are shown in Figure 4.20.

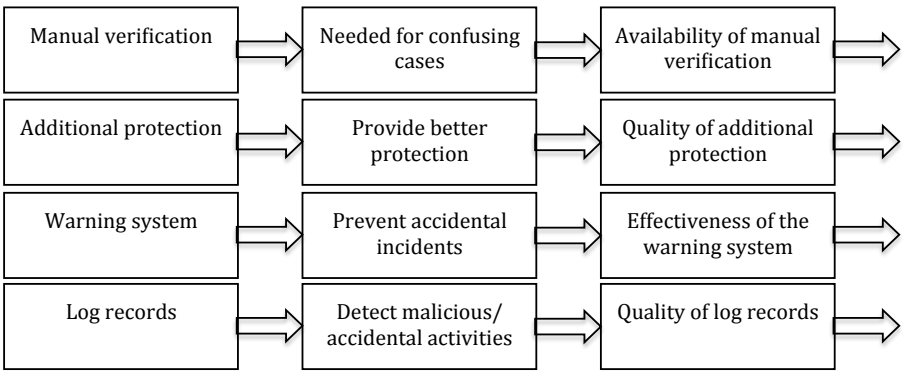


Figure 4.20: Metrics to measure the level of protection given to processing personal information

Physical Devices given to Outsiders

There are situations where physical devices have to be given to outsiders for various purposes. One such instance is handing over physical devices for maintenance or repairs. Third parties should respect the privacy of the individuals whose personal information is stored in the machine. The commitment of third parties is obtained by getting a non-disclosure agreement. Therefore, a metric is derived to measure the quality of the non-disclosure agreement. This metric is shown in Figure 4.21.

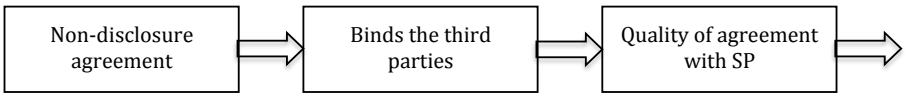


Figure 4.21: Metrics to measure the quality of a non-disclosure agreement

Personal Information Discarding Process

At a certain stage, the collected personal information has to be discarded. Proper precautions have to be taken on discarding since several privacy breaches have been reported in cases where the personal data was not properly discarded. Therefore, as shown in Figure 4.22, a metric is derived to measure the quality of the overall discard process.

Workplace privacy

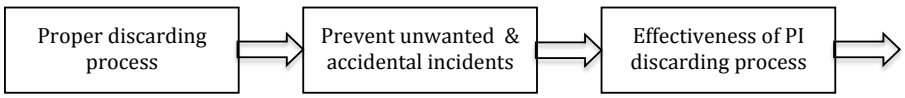


Figure 4.22: Metrics to measure PI discard process

The previous discussion has been about outside individuals who have a relationship with the organization. The other category is employees who work for the organization. Employees also expect that their employers and managers respect their privacy in the workplace. Even though the level of workplace privacy is hard to measure, some insights can be gained from both parties. Employers can express whether they recognize the privacy rights of employees. Employees can express their perception of the freedom of privacy at their workplace. It can be expected that a high level of recognition of the right to privacy correlates with a high level of commitment to protecting personal information. Therefore, the first metric in this category is to measure the level of recognition of the right to privacy of the employees. One way to respect the privacy of employees is to have a clear workplace privacy policy that provides principles to be followed. The next metric is to measure the quality of the workplace privacy policy. Employees must be aware of this policy in order to demand and exercise their privacy rights. Therefore, the next metric is to measure the awareness of the workplace's privacy policy. The most important aspect of workplace privacy is the monitoring of employees' activities. Monitoring practices, including means and methods, should be clearly specified in the workplace policy. The quality of surveillance practice, which is a subjective measurement, is the focus of the next metric, which measures the quality of the surveillance policy. The last metric is to measure the freedom given to employees to engage in their personal work that is not monitored by the managers. This is also a subjective judgment, but time intervals and references to non-monitored activities can be measured objectively. These metrics are shown in Figure 4.23.

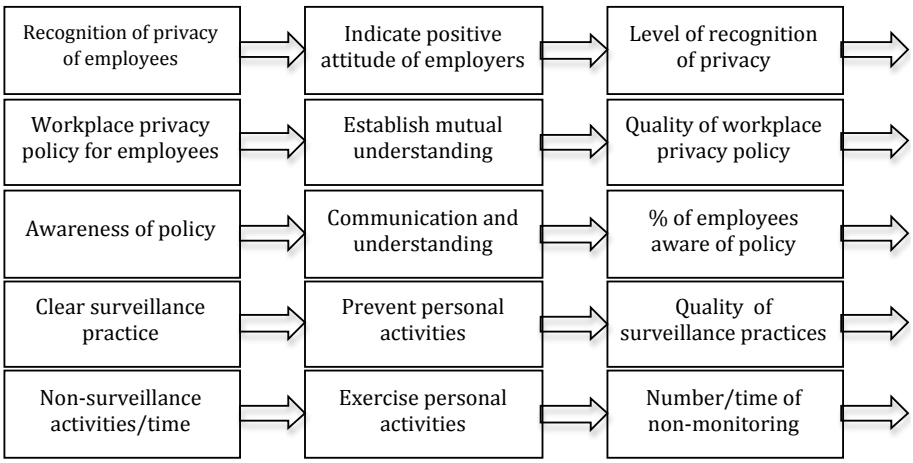


Figure 4.23: Metrics to measure work place privacy practices

Limitations of the presented metrics

The presented metrics inherit certain limitations at this stage. One argument against these metrics might be that the presented metrics are similar to information security metrics. The similarity is because the main focus of this research is the secure safeguarding of personal information. Hence, limited attention was given to other fair information practices. Therefore, most of these metrics could be seen in the information security domain. On the other hand, the quality of a security metric is already established since a similar set of metrics has been developed from the information privacy domain. All these facts show the need for closely cooperating with the development of information security metrics and also show the possibility of adapting information security metrics to the information privacy domain.

Additionally, the quality of the identified information privacy metrics can be improved by comparing them with information privacy and security standards, guidelines, privacy surveys, and other relevant studies. For example, many of the actors, factors, and concepts identified in this research can be used to derive a number of additional metrics. These improvements are to be made at the metric modeling stage. Such research is left for later investigators.

The appropriateness and completeness of the presented metrics can be questioned. These metrics are not in their final form. Some of the presented metrics can be further divided into several submetrics, and some of them can be merged. For example, the quality of a username can be measured in terms of offensiveness, disruptiveness, and the likelihood of misleading (deceptiveness). Even though it is possible to present three information privacy metrics, only one is presented, which incorporates all three factors.

Some of the metrics presented are at a very abstract level while others are at a very detailed level. For example, metrics that contain terms such as quality, strength, etc., require a subjective judgment. On the other hand, metrics that

ask for the availability of a specific feature can be answered in a more objective manner. A possible improvement in the metric modeling stage would be breaking down the abstract metrics into more specific metrics that can be answered more objectively. This can be done at the metric modeling stage where the metrics presented are improved with additional information sources and aimed at a particular sector.

it is also possible to ask for the quality of a function or feature. For example, the availability of captcha is used to measure the strength of a protective measure. It would also be possible to ask for the quality of the captcha and the user friendliness of that captcha. However, these questions have not been presented in this discussion since simply having many metrics at this stage does not improve the overall quality. Except for the metrics presented in Figure 4.3, both the availability and the quality of a particular feature or function has not been presented.

One of the challenges faced in this exercise has been the lack of common standards for benchmarking. For example, how many failed login attempts should be allowed before presenting a captcha. Since there are no widely accepted answers to some questions, there is room for subjective judgments.

Comparing the information privacy taxonomy presented in Paper 7 with the presented metrics, it can be seen that there are many untouched areas where further research is needed to identify other metrics.

4.2 Directions for building information privacy metrics

The previous section provided a summary of the research contributions of this thesis.

As a proof of concept, it is important to explain how to develop the intended privacy metrics (IPM) from the identified constructs. The development process is guided by the second part of the NIST (2008) guide, which explains three phases in the metric development process. These phases are modified to suit better the aims of this thesis. The modified phases are:

- Measure development approach: Identify target privacy protective measures and generate a scale that reflects the commitment to fulfilling the target protective measure.
- Measure prioritization and selection: Identifying a few key high priority measures.
- Establishing performance targets: This explains the goals to be achieved in a given period of time.

4.2.1 An exemplified metric development process

The first phase is identifying a particular target and then identifying an appropriate criterion to measure the success in hitting that target.

Selecting a target is the first activity of the modified phase. The selected target for this example is some given level of quality of the training program given to the personal information handling officers for the purpose of protecting personal information against unauthorized activities. Paper 5 presents six protective measures. Constructs are derived from these protective measures. These constructs are:

- A1 – The depth and breadth of the training program
- A2 – The frequency of conducting training programs
- A3 – Conducting training session after a major incident
- A4 – Conducting a periodic review of the training program
- A5 – Conducting reviews of the effectiveness of the training program

The second activity is identifying an appropriate criterion for measuring the achievement of the goal aimed at. In this particular example, the required criterion is to measure the effectiveness of the training program given to the personal information handling officers. One basic criterion can be presented as:

Basic criterion

The overall strength of the training program = x1 A1 + x2 A2 + x3 A3 + x4 A4 + x5 A5 ,
where x1, x2, x3, x4, and x5 are weighing factors.

This basic criterion has many weaknesses. For example, a training program without adequate depth and breadth may get a higher rating due the presence of other factors. This kind of weakness can be overcome by setting threshold levels for certain individual constructs.

Slightly advanced version

Overall strength of the training program = (x1 A1 + x3 A3 + x4 A4 + x5 A5) * f2,
where x1, x3, x4, and x5 are weighing factors and f2 represents the depth and breadth of the training program. The possible values that can be taken by f2 are given in Table 4.2 as an example.

In this slightly advanced version, the depth and breadth of the training program plays a significant role. In other word, the depth and breadth of the training program significantly impact the overall rating of the training program. For example, when the depth and breadth of the training program is not adequate at all, the f2 factor becomes zero. Hence, the overall value becomes zero. As shown above, this metric can be further improved by placing more emphasis on each factor.

Table 4.1: *Information privacy metrics and protective measures in the context of the privacy taxonomy*

Privacy Metrics		**Research Paper**		**Information privacy Taxonomy**	
Figure	**Item #**	**Paper #**	**Section (S) Table (T) Page (P)**	**Theme**	**Sub category**
4.3	1-3	2	S 7.3	Right of data owners	Through users/ Knowing
4.3	1-3	2	S 7.3	Protection measure	Data users/ Attitude
4.3	4-6	4	S 2.2	Protection measure	Data users/ Enforcement
4.3	4-6	5	T 3 & S 2.1.3	Protection measure	Data users/ Enforcement
4.4	1	8	P 30	Personal Data	Identification data/
4.5	1	5	S 2.1.3	Technology	PET/ Controls
4.5	2-3	5	T 1	Technology	PIT/ General
4.5	4	8	T 2.2	Technology	PET/ Controls
4.5	5-6	8	T 2.4	Technology	PET/ Controls
4.6	1-2	8	T 3.1 & T 2.2	Technology	PET/ Controls
4.6	3	8	T 2.1	Technology	PET/ Controls
4.6	4	8	T 3.1 & T 1.1	Technology	PET/ Controls
4.6	5	8	T 2.1	Technology	PET/ Controls
4.6	6	8	T 2.10	Technology	PET/ Controls
4.6	7-8	8	T 3.1	Technology	PET/ Controls
4.7	1	8	T 3.1	Technology	PET/ Controls
4.8	1-5	8	P 43-44 T 3.2	Technology	PET/ Controls
4.9	1	5	T 4	Protection Measures	Data users/ Financial and Enforcement
4.9	2-4	5	T 3	Protection Measures	Data users/ Financial and Enforcement
4.9	5-7	4	S 2.1 & S 2.2	Protection Measures	Data users/ Financial and Enforcement
4.10	1-3	5	T 3	Protection Measures	Data users/ Financial and Enforcement
4.10	4	5	S 2.1.2	Protection Measures	Data users/ Financial and Enforcement
4.10	5	5	S 2.5	Protection Measures	Data users/ Financial and Enforcement
4.10	6	5	T 3	Protection Measures	Data users/ Financial and Enforcement
4.11	1-5	5	T 4	Protection Measures	Data users/ Financial and Enforcement
4.12	1	8	P 36	Rights of data owners	Through user/ Knowing
4.12	2	8	T 3.1	Rights of data owners	Through user/ Knowing
4.12	3	8	P 39	Rights of data owners	Through user/ Knowing

Privacy Metrics		Research Paper		Information privacy Taxonomy	
Figure	**Item #**	**Paper #**	**Section (S) Table (T) Page (P)**	**Theme**	**Sub category**
4.12	4	8	T 3.2	Rights of data owners	Through user/ Knowing
4.12	5	8	T 3.1	Rights of data owners	Through user/ Knowing
4.12	6	8	T 2 (appendix)	Rights of data owners	Through user/ Knowing
4.12	7	8	T 5/1.4	Rights of data owners	Through user/ Knowing
4.12	8	8	T 3.1/	Rights of data owners	Through user/ Knowing
4.12	9	8	P 48	Rights of data owners	Through user/ Knowing
4.13	1	8	P 37	Rights of data owners	Through user/ Requesting
4.13	2	8	T 3.1	Rights of data owners	Through user/ Requesting
4.13	3	8	T 2.10	Rights of data owners	Through user/ Requesting
4.13	4	8	2.11	Rights of data owners	Through user/ Requesting
4.13	5	8	T 3.1	Rights of data owners	Through user/ Requesting
4.13	6	5	S 2.5	Rights of data owners	Through user/ Requesting
4.14	1	8	T 3.1	Protection measures	Data users/ Options
4.14	2	4	2.2	Protection measures	Data users/ Options
4.15	1	4	S 2.1	Protection measures	Data users/ Enforcement
4.15	2	4	S 2.1	Protection measures	Data users/ Enforcement
4.15	3	4	S 2.1	Protection measures	Data users/ Financial
4.16	1-5	4	S 2.1	Protection measures	Data users/ Financial
4.17	1	5	T 5	Protection measures	Data users/ Enforcement
4.17	2	4	S 2.1	Protection measures	Data users/ Enforcement
4.17	3	5	T 5	Protection measures	Data users/ Enforcement
4.17	3	5	T 5	Technology	PET/ Transformation
4.17	4-7	4	S 2.2	Protection measures	Data users/ Enforcement
4.18	1	8	P 39	Protection measures	Data users/ Enforcement
4.18	2-3	8	T 2.11	Protection measures	Data users/ Enforcement
4.18	4	8	T 3.1	Protection measures	Data users/ Enforcement
4.19	1	4	S 2.2	Protection measures	Data users/ Enforcement
4.19	2	5	S 2.1.2	Rights of data owners	Through user/ Requesting
4.19	3-4	8	T 3.1 & P 36	Rights of data owners	Through user/ Requesting
4.20	1	4	S 2.2	Protection measures	Data users/ Enforcement
4.20	2	5	T 3	Protection measures	Data users/ Enforcement

Privacy Metrics		Research Paper		Information privacy Taxonomy	
Figure	**Item #**	**Paper #**	**Section (S) Table (T) Page (P)**	**Theme**	**Sub category**
4.20	3-4	5	T 2	Protection measures	Data users/ Enforcement
4.21	1	4	S 2.2	Protection measures	Data users/ Enforcement
4.22	1	4	S 2.2	Protection measures	Data users/ Enforcement
4.23	1-5	2	S 7	Protection measures	Data users/ Financial

Table 4.2: *Values given for the depth and breadth of a training program.*

possible value for f2	**Description**
1	Training program is internationally accepted for the particular domain
0.75	Training program is accepted for the particular domain
0.50	Training program is a common program—not for the domain concerned
0.25	Training program is a basic program
0.00	Training program is not sufficient at all

5. Concluding Remarks and Future Research

5.1 Concluding Remarks

This chapter presents the concluding remarks, the high level research contribution, and some reflections on the approach and research contribution. This chapter concludes by presenting avenues for future research.

The main goal of the researchers working in the information privacy domain is to provide an appropriate level of protection for individuals' personal information. The organizations that process personal information have legal and moral obligations to protect such personal information. Furthermore, these organizations can gain a competitive advantage by protecting personal information. In order to provide protection to personal information, these organizations need a kind of yardstick to identify the level of protection given to personal information. Identifying the level of protection received by the personal information is needed in order to measure any progress over time, make comparisons with other organizations, benchmark against national and international standards, and demonstrate to any interested parties the level of protection received by the personal information. Information privacy metrics serve all these needs.

Organizations expect an aggregate value from the information privacy metrics. However, it is not straightforward to provide such an aggregate value since the processing of personal information in an organization contains many sub-processing stages. Therefore, a set of information privacy metrics has to be derived to measure the protection given at each sub-processing stage. In the conceptual model given in Figure 4.1, these metrics are labelled "intermediate level information privacy metrics." In turn, a single sub-processing stage contains many information processing activities. Therefore, information privacy metrics are needed to measure the protection given at the stage of each processing activity. In the conceptual model given in Figure 4.1, these metrics are labelled "individual information privacy metrics." An individual privacy metric is derived from constructs. The constructs identified in this research were presented as protective measures in the published papers. These papers are presented in Appendix A.

The conceptual model was further explained in Chapter 4. Furthermore, Chapter 4 presented all the identified individual metrics derived from the dimensions and constructs. The metric modeling stages based on Paper 6 were

also explained in Chapter 4, together with an example to demonstrate the concept.

5.1.1 Research Contribution

An overview of the contributions of this thesis to the theoretical knowledge base and application area follows.

- Presenting a conceptual model of information privacy metrics is the main contribution of this thesis. This conceptual model contains the identified dimensions and constructs from the presented research papers. Furthermore, the framework explains how to derive an aggregate metric from the individual information privacy metrics that were built on the identified constructs.
- One of the main contributions of this research to the knowledge base is the taxonomy for the information privacy domain. This taxonomy provides an overview of the information privacy domain and depicts the areas where information privacy metrics are needed. This taxonomy provides a basis for developing a comprehensive information privacy framework, something which is very important for the further progress of the information privacy field.
- Application of the grounded theory approach in developing the taxonomy established the potential of the grounded theory approach to develop taxonomies.
- The methodology proposed in Paper 3 for bridging the knowledge gap between lawyers and technologists can be used for both to achieve a mutual understanding. Successfully applying this methodology in subsequent research, the validity of this methodology was established.
- Paper 6 presented a methodology based on design science principles to build information privacy metrics. The methodology demonstrates the applicability of design science principles to the information privacy domain.
- The published papers presented a large number of recommendations for protecting personal information. Organizations can use these recommendations as a blueprint to identify weaknesses in their systems and remedy any shortcomings. System designers can also make use of the recommendations to design better security and privacy protection mechanisms.

5.1.2 Reflections

Reflections on the research contribution

The overall aim of researchers in the information privacy domain is to protect the personal information of data subjects. More precisely, researchers are working on providing an adequate level of protection for personal information.

To achieve this goal, researchers have taken many paths. As shown in Figure 1.2 in Chapter 1, the approach taken in this research was to identify some dimensions and constructs for building information privacy metrics.

Paper 6 explains the stages for developing information privacy metrics. The first stage is identifying the necessary constructs and dimensions. The next stage is the metric modeling stage. In this stage, information privacy metrics are developed by using the constructs identified in the papers presented in this thesis together with privacy and security standards, guidelines, privacy surveys, and other relevant studies. In this stage, various of the dimensions identified can be taken into account, for example, the differentiation between one set of metrics for very sensitive personal information and another set for non-sensitive personal information.

This thesis attempted to identify the necessary constructs and dimensions for the entire information privacy domain, instead of limiting the focus to a specific sector. For example, Paper 1 presented the privacy attitude of young international students, Paper 2 presented the privacy issues at public working places, Papers 4 and 5 presented the decisions of the Information Privacy Commissioners and Data Protection Commissioners of several countries on a number of privacy infringements in almost every sector, Paper 7 also presented privacy-related incidents reported by the International Association of Privacy Professionals (IAPP), and Paper 8 presented the implementations of the privacy and security features of four email service providers. By exploring various sectors, this explorative thesis has contributed to the establishment of an overall picture of the information privacy domain. The focus can be put on a particular sector during the metric building stage.

Reflections on the direction taken

At the beginning of this research study, it was decided not to limit this research to a particular sector. One of the factors that contributed to making this decision is that the European data protection approach is more general, unlike the American approach. The American approach is sector specific and self-regulatory. Another factor is the intention of this researcher to give a general view of information privacy metrics. Once a general information privacy metric is introduced, it can be tailored to specific sectors.

5.1.3 An alternative metric development approach

The approach presented in this thesis is considered to be an organizational centric approach because most of the focus was given to organizations instead of end users. However, the study presented in Paper 1 looked at the attitudes of users and discussed some dimensional aspects of the intended information privacy metrics. For example, Paper 1 stated that there is no need for separate metrics for each continent, but separate metrics are needed for sensitive and non-sensitive personal information.

Another approach is the user centric approach where the focus is place on the needs of end users/customers. In this approach, the focus is put on a very specific customer/user segment, such as users highly concerned with privacy in social networking sites. In this approach, the target group is asked about the factors that make them feel more comfortable when sharing and handling their personal information with service providers. These factors may be the instances where the user feels more comfortable or uncomfortable, the reasons for feeling so, and what make them feel so. In other words, when, why, and what makes online users feel comfortable or uncomfortable. Based on these findings, metrics can be developed. One of the limitations of this approach is the lack of user awareness of threats and vulnerabilities.

5.2 Future Research

This research has discussed only two aspects of quality metrics. These aspects are compliance and minimality. Further studies of these two aspects are also needed. In addition to these, other quality aspects of quality metrics such as formality, usability, etc., have to be studied. For example, this thesis suggested a more harmonized perception of privacy among young academia representing several continents. Thus, there is no need for separate metrics for each continent. However, this statement can not be generalized without deductive studies with adequate and representative samples. Another dimension of the minimality aspect is the appropriateness of using the same set of metrics for addressing the privacy concerns of both adults and young people.

More constructs can be identified by studying how technical systems have been designed and implemented. Two important technical systems are privacy enhancing technologies and technologies that have the potential of invading information privacy. Examples of the latter are workplace monitoring tools and digital rights management tools. The reason for placing special emphasis on these two types of technologies is their direct relationship with information privacy. Examining privacy enhancing technologies, the principles behind the privacy enhancing mechanism can be identified. For example, examining the mechanism of onion routing, the concept of segregation of duties can be identified as one of the design principles. Once a principle is identified, a metric can be built on that principle. For example, in this case, a metric can be derived to measure the extent to which segregation of duties has been implemented in a workplace monitoring tool. Likewise, it is also possible to identify the factors that have the potential of invading privacy, and build metrics based on these factors.

Another method of identifying constructs is examining the questions and the responses given in privacy surveys. This user centric approach can also provide insights with which to identify constructs. One probable issue in a privacy questionnaire is the willingness to allow strangers to make comments on

a Facebook page. This question itself indicates that users have close groups, and probably users allow only the members in a close group to make comments. Based on this fact, a metric can be derived to measure the possibility of building close groups in a social networking service.

After identifying the constructs and dimensions, the next step is modeling information privacy metrics. This process was explained in Paper 6. Initially, this can be started with one organization and subsequently expanded to similar organizations. It also needs to go through several iterative refining processes. Identifying the necessary steps for data collection and interpretation is also important at this stage.

Once an information privacy metric has been built and procedural steps identified, they can be instantiated in one organization. As discussed in the justify/theorize paragraph in Section 1.5 (the research design section), studies that take approaches similar to the evaluative processes in the natural sciences have to be conducted in order to understand why information privacy metrics work or fail.

Related future research

Apart from building the information privacy metrics, several indirectly related avenues for further research have been identified.

Many surveys have shown that there is a demand for privacy, but people do not read privacy policies (Cranor, 2005) nor do they use privacy enhancing tools. There is a huge gap between 'what people say' and 'what people do.' This problem is not only in information privacy, but also in many other fields. For instance, this is prevalent in the health care sector. Therefore, it would be interesting to further explore the reasons for the gap between 'what people say' and 'what people do.' Identifying simple theories for explaining phenomena in the information privacy domain would be a significant contribution to the further progress of the field. This is also closely related to the studies in the natural sciences, as mentioned above.

Comparing and contrasting the protection measures identified in this thesis with existing security assurance guidelines and best practices may help identify some improvements for the existing security standards and guidelines.

It is now clear that, in the coming years, information privacy research will be mainly around Privacy by Design (PbD) [1] principles. Researchers may attempt to introduce new principles, redefine existing principles, and apply and design information systems based on these principles. These researches may take different approaches. Some of them may be technical, for example, making anonymous communication in peer-to-peer communication addresses the fifth principle that insists on end-to-end security. Some of them may be organizational, for example, investing in a privacy program falls into the first principle—proactive, not reactive. Researchers in the legal domain have at-

[1] More information about PbD was given in Section 2.7

tempted to make the information privacy handling practices more transparent and visible. In this context, PbD principles provide an umbrella for information privacy researchers. However, there is a long way to go.

A lot of work remains to be done to make organizations incorporate the principles of PbD. There are a few ways to promote these principles. Organizations that are keen on obtaining a competitive advantage by showcasing their personal information handling practices could adopt PbD principles as the basis for their personal information handling practices. Information privacy advocates need to guide these organizations on how to use these principles for their organizational practices. Industry associations and professional bodies could incorporate PbD principles into their code of best practices. This would encourage and facilitate members to follow PbD principles. Obtaining legal recognition for PbD principles is another approach. This would make organizations that do not take seriously the protection of personal information redesign their personal information handling practices in accordance with these principles. Additionally, much time and effort must be made to educate information system designers, researchers, developers, regulators, and users.

Furthermore, there are more challenges to be faced by PbD advocates. Current information systems are not based on PbD principles, they are based on the zero-sum approach. Re-designing existing systems so as to be based on PbD principles is not possible. Therefore, privacy advocates need to explain how to incorporate the principles of PbD into the existing information systems.

Another challenge is incorporating these principles into different types of information systems. There are several examples based on PbD principles. For example, Cavoukian (2011) describes a privacy architecture where the advertisement server generates and delivers well-aimed advertisements without obtaining the subscribers' information. In this case, the privacy architecture is designed in such a way that the Internet Service Provider (ISP) hides certain information from the ad-serving organization. Some other examples are smart grid, privacy-protective biometric facial recognition system, and mobile applications. However, further guidelines are needed to incorporate these principles into other information systems. It may seem that it is not possible to re-design every system so as to be in accordance with PbD principles. However, a positive and encouraging approach, and facilitating out-of-box thinking, might transform these impossibilities into innovations.

Having a deeper understanding of the reasons behind the demand for protecting personal information, and knowing the ways in which the demand is made, are both needed to design and build information systems in accordance with PbD principles, particularly with the principle of full functionality—total-sum, not zero-sum. Conducting well grounded qualitative research is a way to get this understanding and knowledge. Paper 9, presented in this thesis, has taken a step by presenting this author's frame of reference on why and how individuals demand protection for various personal data items. More research

on how technology shapes human behavior is needed to design and develop information systems in accordance with PbD principles.

The sixth principle of privacy by design (PbD) is visibility and transparency. This principle states that personal information must be handled in accordance with the promises given when it was collected, and that the personal information handling practices must be visible and transparent to all interested parties. This visibility and transparency can be best achieved by presenting personal information handling practices in a metric form.

The fourth principle states that systems must support full functionalities, that is, positive-sum – not zero-sum. In order to address this principle, information privacy metric developers have to come up with a new approach where information privacy metrics reflect the interests of the various parties. In other words, metrics should reflect to what extent the information system meets the expected functionalities. For example, an employee monitoring system should provide employers the necessary information to make informed decisions without invading the employees' privacy. Therefore, a metric under the new paradigm should represent the goals of every stakeholder. As was evident in the example, designing metrics with the fourth principle in mind is a great challenge for privacy metric developers.

Summary in Swedish

En privat och personlig sfär är en grundläggande mänsklig rättighet. Under de senaste decennierna har dataskydd blivit en av de viktigaste aspekterna av en sådan sfär i och med informationssamhällets utbredning. Dataskydd omfattar skydd av uppgifter som kan hänföras till en individ.

Organisationer, vilka ofta behandlar personuppgifter, och individer, vilka är de som uppgifterna handlar om, har olika behov, rättigheter och skyldigheter. Organisationer behöver använda personuppgifter som en grund för att utveckla skräddarsydda tjänster och produkter till sina kunder, för att därigenom uppnå konkurrensfördelar gentemot sina konkurrenter. Individer behöver försäkran att deras personuppgifter inte förändras, avslöjas, raderas eller missbrukas på något annat sätt. Utan denna utfästelse från organisationer är individer mer obenägna att dela med sig av sina personuppgifter.

Information privacy metrics är mått och mätmetoder i form av en uppsättning parametrar vilka kan användas för kvantitativ utvärdering och jämförelse av en organisations dataskyddsåtgärder. Detta kan användas av en organisation för att förevisa, och av individer för att utvärdera, typen och nivån av det skydd som ges till personuppgifter. I dagsläget finns inga systematiskt utvecklade, etablerade eller allmänt använda mått och mätmetoder för dataskydd. Syftet med denna studie är därmed att etablera ett vetenskapligt förankrat fundament för att utveckla information privacy metrics genom utforskning av några av dess mest kritiska beståndsdelar och aspekter.

Denna studie genomfördes i enlighet med de övergripande principerna för design science. Vid datainsamling och dataanalys tillämpades forskningsmetoder i linje med grounded theory, inklusive enkäter och intervjuer vilka genomfördes i Sverige och på Sri Lanka. Resultatet är en konceptuell modell för information privacy metrics inklusive dess grundläggande beståndsdelar; constructs och dimensions.

Acknowledment

First, I would like to thank my main supervisor, Professor Louise Yngström, for her valuable advice and support. I must also give a special thank you to Dr. Fredrik Björck, my friend and co-supervisor, for encouraging me throughout the research period and also for sharing my pleasant and hard times over the past few years.

My gratitude also goes to the late Professor V.K. Samaranayake for his invaluable lessons and encouragement and the late M.P.J.U Samanthilaka for his support.

Appreciation must also be given to my good friends Wah-Sui Almberg, Johan Hellström, Tharaka Illayperuma, Thashmee Karunaratne and other PhD students. My gratitude goes to Fatima Santala, Birgitta Olsson and all DSV staff members.

I would like to extend my thanks to the sida/SAREC project and the Swedish taxpayers who provided financial assistance for my PhD studies.

Thanks must also be given to those who have read my licentiate thesis and given me valuable comments and suggestions.

I would like to thank my family members and friends as well.

Finally, I thank my daughter, Savidya Sathsarani and my son, Damseth Chandradithya for bringing me so much joy and for teaching me so many valuable lessons.

List of Abbreviations

ACMA	Australian Communications and Media Authority
AICPA	American Institute of Certified Public Accountants
BBB	Council of Better Business Bureaus
CC	Common Criteria
CICA	Canadian Institute of Chartered Accountants
CLI	Caller Line Identification
COBIT	Control Objectives for Information and related Technology
COPPA	Children's Online Privacy Protection Act
DoD	Department of Defense of the United States
DSAR	Design Science and Action Research
DSV	Department of Computer and Systems Sciences
ECPA	Electronic Communications Privacy Act
EPIC	Electronic Privacy Information Center
FCRA	Fair Credit Reporting Act
FIP	Fair Information Practice
FTC	Fair Trade Commission
GLBA	Gramm-Leach-Bliley Act
GST	General Systems Theory
GT	Grounded Theory
HCI	Human Computer Interaction
HIPAA	Health Insurance Portability and Accountability Act
IAPP	International Association of Privacy Professionals
ICCPR	International Covenant on Civil and Political Rights
ICPP	Independent Centre for Privacy Protection
IITC	International Information Technology Conference
IS	Information System
ISP	Internet Service Provider
ISSA	Information Security South Africa
ISTPA	International Security, Trust and Privacy Alliance
ITSEC	Information Technology Security Evaluation Criteria

JIPS	Journal of Information Privacy and Security
LSPI	International Conference on Legal, Security, and Privacy Issues in IT
NIST	National Institute of Standards and Technology
OECD	Organisation forEconomic Co-operation and Development
P3P	Platform for Privacy Preferences
PbD	Privacy by Design
PETTEP	PET Testing and Evaluation Project
PI	Personal Information
PII	Personally Identifiable Information
PIPEDA	Personal Information Protection and Electronic Documents Act
PISA	Privacy Incorporated Software Agent
PKI	Public Key Infrastructures
PLI	Privacy Leadership Initiative
PRIME	Privacy and Identity Management for Europe
ROI	Return on Investment
SSRN	Social Science Research Network
SSN	Social Security Number
TCSEC	Trusted Computer System Evaluation Criteria
TSA	Transportation Security Administration
W3C	World Wide Web Consortium

Bibliography

Aboulafia, M. (1991). *Philosophy, social theory, and the thought of george herbert mead*. New York: State University of New York Press.

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*, *3*(1), 26-33.

AICPA/CICA. (2004). *AICPA and CICA privacy framework* (Tech. Rep.). New York and Ontario: American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants (CICA).

Amsterdam, A. (1974). Perspectives on the fourth amendment. *Minnesota Law Review*, *58*, 349.

Australian Privacy Commissioner. (1995). *Privacy Audit* (Manual - Part 1 (Information Privacy Principles)). Sydney: The Australian Privacy Commissioner. Available from www.privacy.gov.au/publications/ippam1a.pdf

Australian Communications and Media Authority. (2009, August). *Attitudes towards use of personal information online qualitative research report* (Tech. Rep.). Melbourne: Author.

Australian Privacy Charter Council. (2009, January 11). *Australian Privacy Charter*. Retrieved January 19, 2012, from http://www.privacy.org.au/About/PrivacyCharter.html

Avison, D., & Pries-Heje, J. (2005). *Research in information systems: A handbook for research supervisors and their students*. Amsterdam: Butterworth-Heinemann.

Basden, A. (2007). *Philosophical frameworks for understanding information systems*. Hershey, PA: IGI Global.

Bellia, P. L. (2006). The fourth amendment and emerging communications technologies. *IEEE Security and Privacy*, *4*(3), 20-28.

Bennett, C. J. (2000). An international standard for privacy protection: objections to the objections. In *Proceedings of the tenth conference on computers, freedom and privacy: challenging the assumptions* (p. 33-38). Ontario, Canada: ACM.

Better Business Bureaus. (2012). *Better Business Bureaus.* online http://www.bbb.org/us/Business-Accreditation/.

Biemer, P. P., Groves, R. M., Lyberg, L. E., Mathiowetz, N. A., & Sudman, S. (1991). *Measurement errors in surveys*. New York: Wiley.

Bjorck, F. J. (2005). *Discovering information security management*. Stockholm: Stockholm University. (PhD Thesis)

Blarkom, G. V., Borking, J., Giezen, J., Coolen, R., & Verhaar, P. (2003). *Handbook of privacy and privacy-enhancing technologies:the case of intelligent software agents*. The Hague: College bescherming persoonsgegevens.

Burrell, G., & Morgan, G. (1979). *Sociological paradigms and organisational analysis*. London: Heinemann.

Calcutt, D. (1990). *Report of the committee on privacy and related matters:presented to parliament by the secretary of state for the home office by command of her majesty.* London: HMSO.

Cavoukian, A. (2011). Patience, persistence, and faith: Evolving the gold standard in privacy and data protection. In A. Cavoukian, J. Camenisch, S. Fischer-Hbner, Y. Murayama, A. Portmann, & C. Rieder (Eds.), (Vol. 354, pp. 1–16). Boston: Springer. Available from http://dx.doi.org/10.1007/978-3-642-21424-0_1

Cavoukian, A., & Crompton, M. (2000). Web seals: A review of online privacy programs. In *22nd international conference on privacy and personal data protection.* Venice: Federal Privacy Commissioner.

Chua, W. F. (1986). Radical developments in accounting thought. *The Accounting Review*, *61*(4), 601-632.

Clarke, R. (1997, August 28). *A Template for Evaluating Information Privacy Law and Proposals for Information Privacy Law* (No. 2007-07-28). Retrieved January 25,2012, from http://www.rogerclarke.com/DV/PaperOECD.html

Clarke, R. (2009, February 15). *Introduction to dataveillance and information privacy, and definitions of terms* (No. 2007-07-28). Retrieved January 25,2012, from http://www.rogerclarke.com/DV/Intro.html#InfoPriv

Cranor, L. (2005). Giving notice: Why privacy policies and security breach notifications aren't enough [Editorial Material]. *IEEE Communications Magazine*, *43*(8), 18-19.

Cranor, L. F., Egelman, S., Sheng, S., McDonald, A. M., & Chowdhury, A. (2008). P3P deployment on websites. *Electronic Commerce Research and Applications*, *7*(3).

Culnan, M. J., & Milne, G. R. (2001). The culnan-milne survey on consumers & online privacy notices: Summary of responses. In *Interagency public workshop: Get noticed: Effective financial privacy notices* (pp. 47–54). Washington, D.C.: Federal Trade Commission.

Cvrcek, D., & Matyas, V. (2000, January 1). *Pre-print: On the role of contextual information for privacy attacks and classification.* Information and Privacy Commissioner of Ontario. Retrieved January 19, 2012, from http://www.ipc.on.ca/images/Resources/up-PPPP064.pdf

Cybenko, G. (2006). Why Johnny Can't Evaluate Security Risk. *Security & Privacy Magazine, IEEE*, *4*(1), 5.

Danezis, G. (2006, February 17). *Viewing privacy as a security property.* Research Channel. Retrieved January 25, 2012, from http://research.microsoft.com/apps/video/default.aspx?id=104403

Dayarathna, R. (2007, December). *Towards Comparing Personal Information Protection Measures.* Stockholm University. (Licentiate Thesis)

Dayarathna, R. (2008a). The Principle of Security Safeguards: Accidental Activities. In H. Venter, M. Eloff, J. Eloff, & L.Labuschagne (Eds.), *Proceedings of the innovative minds conference.* Johannesburg: ISSA 2008.

Dayarathna, R. (2008b). Towards bridging the knowledge gap between lawyers and technologists. *Int. J. Technology Transfer and Commercialisation*, *7*(1), 34-43.

Dayarathna, R. (2009). The principle of security safeguards: Unauthorized activities. *Computer Law and Security Review*, *25*(2), 165-172.

Dayarathna, R. (2011a). Actors, Factors, and Concepts in the Information Privacy Domain. *International Journal of Commercial Law and Technology*, *6 (4)*.

Dayarathna, R. (2011b, July 6). A self reflection on privacy. *Social Science Research Network (SSEN) eLibrary*. (Available at SSRN: http://ssrn.com/abstract=1879918 or doi:10.2139/ssrn.1879918)

Dayarathna, R., & Yngstrom, L. (2006). Attitude Towards Privacy Amongst Young International Academics. In *8th international information technology conference.* Colombo, Sri Lanka: IITC.

Denscombe, M. (2007). *The good research guide: for small-scale social research projects*. Berkshire:UK: Open University Press.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61-80.

Dubin, R. (1978). *Theory development.* New York: Free Press.

Dutch Data Protection Authority. (2001). *Privacy Audit Framework under the new Dutch Data Protection Act (WBP)* (Tech. Rep.). Haag: The Dutch Data Protection Authority. Available from http://www.cbpweb.nl/en/download_audit/PrivacyAuditFramework.pdf

Dyer V. Northwest. (A1-04-33). *Dyer V. Northwest Airlines Corp.* (Vols. 334 F. Supp.2d 1196, 1200 (D.N.D. 2004)). online http://www.internetlibrary.com/pdf/Dyer-Northwest-Airlines.pdf.

EPIC- Electronic Privacy Information Center and Privacy International. (2003). *Privacy and Human Rights An International Survey of Privacy Laws and Developments.* onlinehttp://epic.org/bookstore/phr2003/. Electronic Privacy Information Center and Privacy International.

Erlandson, D. A. (1993). *Doing naturalistic inquiry: a guide to methods*. CA, USA: Sage Publications Inc.

EU Directive 95/46/EC. (1995). *Directive 95/46/ec of the european parliament and of 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.* Brussels:Belgium.

Eurobarometer. (2009). *Confidence in Information Society*. Retrieved January 25, 2012, from http://ec.europa.eu/public_opinion/flash/fl_250_en.pdf

Federal Trade Commission. (2005). *National and State Trends in Fraud and Identity Theft* (Tech. Rep.). Washington, DC: FTC.

Fischer-Hubner, S. (2001). *IT-security and privacy: design and use of privacy-enhancing security mechanisms*. Verlag: Springer.

Fitzgerald, B., & Howcroft, D. (1998). Towards dissolution of the is research debate: from polarization to polarity. *Journal of Information Technology*, *13*, 313–326.

Food Standard Agency. (2009, November). *Front-of-pack. Traffic light signpost labelling* (Tech. Rep. No. 2). London: Author.

Geertz, C. (1973). *The interpretation of cultures: selected essays*. New York: Basic Books. Available from http://www.loc.gov/catdir/enhancements/fy0833/73081196-d.html

Glaser, B. (1978). *Theoretical sensitivity: Advances in the methodology of grounded theor*. Mill Valley, CA: Sociology Press.

Glaser, B. (1998). *Doing grounded theory - issues and discussions*. Mill Valley, CA: Sociology Press.

Glaser, B., & Strauss, A. (1967). *Discovery of grounded theory. strategies for qualitative research*. Mill Valley, CA: Sociology Press.

Greenleaf, G. (2006, March 30). *Asia-Pacific developments in information privacy law and its interpretation.* Presentation. University of New South Wales At the Privacy Issues Forum, Wellington. Retrieved January 25,2012, from http://www.privacy.org.nz/asia-pacific-developments-in-information-privacy-law-and-its-interpretation-graham-greenleaf/

Gregor, S. (2006). The nature of theory in information systems. *MIS Quarterly*, *30*(3), 611-642.

Hammersley, M. (1987). Some Notes on the Terms' Validity'and'Realiability'. *British Educational Research Journal*, *13*(1), 73-81.

Hansen, M., Kohlweiss, M., Probst, T., Rannenberg, K., Fritsch, L., & Radmacher, M. (2005). *Overview of existing assurance methods in the area of privacy and it security* (Tech. Rep.). http://www.prime-project.eu.org: Privacy and Identity Management for Europe.

Harris Interactive. (2001). *A survey of consumer privacy attitudes and behaviors* (http://www.docstoc.com/docs/42981736/A-Survey-of-Consumer-Privacy-Attitudes-and-Behaviors). Rockester, NY: Author.

Hedayati, A. (2012). An analysis of identity theft: Motives, related frauds, techniques and prevention. *Journal of Law and Conflict Resolution*, *4*(1), 1-12.

Herrmann, D. (2003). *Using the common criteria for it security evaluation*. New York: Auerbach publications.

Herrmann, D. S. (2007). *Complete guide to security and privacy metrics: Measuring regulatory compliance, operational resilience, and roi*. New York: Auerbach Publications.

Hevner, A., March, S., Park, J., & Ram, S. (2004, March). Design science in information systems research. *MIS Quarterly*, *28*(1), 75-105.

Heylighen, F. (2000). Epistemology, introduction. In F. Heylighen, C. Joslyn, & V. Turchin (Eds.), *Principia cybernetica web (principia cybernetica, brussels)*. online: http://cleamc11.vub.ac.be/EPISTEMI.html. Available from URL: http://cleamc11.vub.ac.be/EPISTEMI.html

Hills, S. (2009, April 6). *Further evidence backs traffic light food label scheme.* Retrieved January 25, 2012, from http://www.foodnavigator.com/Legislation/Further-evidence-backs-traffic-light-food-label-scheme

Homeland Security Department's Inspector General. (2009, August 28). *Transportation Security Administration Privacy Stewardship* (Tech. Rep.). Washington, DC: Office of Inspector General U.S. Department of Homeland Security.

Iachello, G., & Rannenberg, K. (2001). Protection profiles for remailer mixes. In *International workshop on designing privacy enhancing technologies: design issues in anonymity and unobservability* (p. 181-230). New York: Springer-Verlag.

Iivari, J., Hirschheim, R., & Klein, H. (1998). A paradigmatic analysis contrasting information systems development approaches and methodologies. *Information Systems Research*, *9*, 164-193.

Independent Centre for Privacy Protection Schleswig-Holstein Germany. (2007). *Independent Centre for Privacy Protection Schleswig-Holstein Germany.* online -https://www.european-privacy-seal.eu/press-room/press-releases/privacy-seal-2013-on-its-way-from-kiel-to-europe.

International Covenant on Civil and Political Rights. (1966, December 16). *International Covenant on Civil and Political Rights :Adopted by General Assembly resolution 2200A (XXI).*

ISTPA. (2001). *ISTPA Privacy Framework* (Tech. Rep.). Online: International Security, Trust, and Privacy Alliance. Retrieved January 25, 2012, from http://emoglen.law.columbia.edu/LIS/archive/privacy-legis/ISTPA-FrameworkWhitePaper013101.pdf

Jaquith, A. (2007). *Security metrics: Replacing fear, uncertanity and doubt*. NJ, USA: Pearson Education, Inc.

Jensen, C., & Potts, C. (2003). *Privacy Policies Examined: Fair Warning or Fair Game?* (Tech. Rep. No. 03-04). Atlanta, GA: Georgia Institute of Technology.

Jensen, C., & Potts, C. (2004). Privacy policies as decision-making tools: an evaluation of online privacy notices. In *Proceedings of the sigchi conference on human factors in computing systems* (pp. 471–478). New York, USA: ACM Press.

Johansson, R. (2004). *Theory of science and. research methodology.* Royal Institute of Technology. Stockholm. (Lecture note)

Kaner, C., & Bond, W. (2004). Software engineering metrics: What do they measure and how do we know? In *Proceedings of 10th international software metrics symposium* (Vol. 8). Chicago: METRICS.

Katz v. United States. (1967). *Katz v. United States* (Vol. 389). Retrieved January 25, 2012, from http://www.oyez.org/cases/1960-1969/1967/1967_35 (389 U.S. 347 (1967), Warren Court)

Kelley, P. G. (2009). Designing a privacy label: assisting consumer understanding of online privacy practices. In *CHIEA '09: Proceedings of the 27th international conference extended abstracts on human factors in computing systems* (pp. 3347–3352). NY, USA: ACM.

Kelley, P. G., Bresee, J., Cranor, L. F., & Reeder, R. W. (2009). A "nutrition label" for privacy. In *Proceedings of the 5th symposium on usable privacy and security* (pp. 1–12). NY, USA: ACM.

Kiang, M., & Chi, R. (2009, November). *Call for papers: Special issue on comparison-shopping and related recommender intelligent agents.* Retrieved January 25,2012, from http://eventseer.net/e/11040/50510/

Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly*, *23*(1), 67-93.

Kowalski, S. (1994). *IT Insecurity: A Multi-disciplinary Inquiry*. Stockholm: The Royal Institue of Technology. (PhD Thesis)

Kucan, B. (2009, September 18). *Privacy and data protection in the european union.* Retrieved January 25,2012, from http://www.net-security.org/secworld.php?id=8129 (reporting from ENISA NIS '09 Summer School)

Laing, V., & Coleman, C. (2001, October). *Principal components of orthogonal object-oriented metrics* (Tech. Rep.). Washington, D.C.: Software Assurance Technology Center.

Lee, A. (1991). Integrating positivist and interpretive approaches to organizational research. *Organization science*, *2*(4), 342–365.

Lee, A. (2004). Action is an artifact. *MIS Quarterly*, *28*(3).

Lee, A. S. (1999). The MIS Field, the Publication Process, and the Future Course of MIS Quarterly. *MIS Quarterly Quarterly*, *23*(1). (Inaugural Editor's Comments)

Lee, A. S. (2000). *Systems thinking, design science, and paradigms.* http://www.people.vcu.edu/ aslee/ICIM-keynote-2000/ICIM-keynote-2000.htm. Retrieved 22, February 2010, from http://www.people.vcu.edu/~aslee/ICIM-keynote-2000/ICIM-keynote-2000.htm (Keynote Address at The 11th National Conference on Information Management, Kaohsiung)

Lee, A. S., & Hubona, G. S. (2009). A scientific basis for rigor in information systems research. *Mis Quarterly*, *33*(2), 237-262.

Lessig, L. (1999). *Code and other laws of cyberspace*. New York: Basic Books.

Lincoln, Y., & Guba, E. (1985). *Naturalistic inquiry*. CA, USA: Sage Publications.

Mahanamahewa, P., & Dayarathna, R. (2005). Workplace communication privacy in the digital age. In *7th international information technology conference IITC*. Colombo, Sri Lanka: International Information Technology Conference 2005.

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*, *15*(4), 251-266.

Marczyk, G. R., DeMatteo, D., & Festinger, D. (2005). *Essential of research design and methodology*. Indianapolis: Wiley Publishing.

Martensson, P., & Lee, A. (2004). Dialogical action research at omega corporation. *MIS Quarterly*, *28*(3), 507-536.

Martin, E., Brown, C., Hoffer, J., Perkins, W., & DeHayes, D. (2009). *Managing information technology: What managers need to know*. NJ, USA: Prentice Hall.

McCarthy, J. (1999, November 8). *TRUSTe decides its own fate today.* Retrieved February 2, 2012, from http://yro.slashdot.org/article.pl?sid=99/11/05/1021214

McDonald, A., & Cranor, L. (2008). The cost of reading privacy policies. *ACM Transactions on Computer-Human Interaction*, *4*(3), 1–22.

MEPS -Department of Climate Change and Energy Efficiency. (2009). *Minimum Energy Performance Standards.* Retrieved February 2, 2012, from http://www.energyrating.gov.au/products-themes/cooling/air-conditioners/sample-labels/

Mercuri, R. (2002). Uncommon criteria. *Communication of the ACM*, *45*(1), 172.

Mohammed, E. A. (1999). An examination of surveillance technology and their implications for privacy and related issues - the philosophical legal perspective. *Journal of Information, Law & Technology*, *1999*(2).

Muelle, G., & Rannenberg, K. (Eds.). (1999). *It security and multilateral security*. Boston, MA: Addison-Wesley-Longman.

Mustafa, K., & Khan, R. (2005). Quality Metric Development Framework (qMDF). *Journal of Computer Science*, *1*(3), 437–444.

Myers, M., & Avison, D. (1997). Qualitative research in information systems. *Management Information Systems Quarterly*, *21*, 241–242.

Noam, E. M., Swire, P. P., Varian, H. R., Laudon, K. C., Culnan, M. J., Westin, A. F., et al. (1997). *Theory of Markets and Privacy.* The National Telecommunications and Information Administration (NTIA). Retrieved February 2, 2012, from http://www.ntia.doc.gov/page/chapter-1-theory-markets-and-privacy

Northwest. (2004). *In re Northwest Airlines Privacy Litigation, U.S. Dist. Lexis 18010 (D. North Dakota september 8, 2004).* Retrieved February 2, 2012, from http://www.internetlibrary.com/cases/lib_case355.cfm

OECD -Organisation for Economic Co-operation and Development. (1980). *OECD Guidlines on the protection of Privacy and Transborder Flows of Personal Data* (Tech. Rep.). France: Organisation for Economic Co-operation and Development.

Olmstead v. United States. (1928). *Docket no.493 Taft Court (1925-1930) 277 U.S. 438 (1928).* Retrieved February 2, 2012, from http://www.oyez.org/cases/1901-1939/1927/1927_493

Onsrud, H. J., Johnson, J. P., & Lopez, X. (1994). Protecting personal privacy in using geographic information systems. *Photogrammetric Engineering and Remote Sensing*, *60*(9), 1083.

Palvia, P., Mao, E., Salam, A., & Soliman, K. (2003). Management information systems research: what's there in a methodology. *Communications of the Association for Information Systems*, *11*(1), 289.

Patton, M. Q. (1990). *Qualitative evaluation and research methods*. CA, USA: Sage Publications, Inc.

Payne, S. C. (2006, June). *A Guide to Security Metrics* (Tech. Rep.). Maryland:USA: SANS Institute. Available from http://www.sans.org/reading_room/whitepapers/auditing/guide-security-metrics_55

Peirce, C., & Buchler, J. (1955). *Philosophical writings of peirce*. New York, USA: Dover Pubns.

Peppers, D., & Rogers, M. (2007, October 1). *How to measure a CPO's value.* Retrieved February 2, 2012, from https://www.privacyassociation.org/publications/2007_10_how_to_measure_a_cpos_value/

Philbin, M. (2009). *Identity commitment in the context of psychosis: A grounded theory study.* Dublin City University. (PhD Thesis)

PIPEDA - Personal Information Protection and Electronic Documents Act. (2000). *Senate and House of Commons of Canada (S.C 2000, c.5).* Available from DepartmentofJusticeWebsitehttp://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-1.html#h-1

Ponemon Institute. (2003). *Benchmark Study of Corporate Privacy Practices* (Tech. Rep.). MI:USA: Author. (presented at United States Federal Trade Commission Workshop on Privacy - June 5, 2003.)

Privacy International. (2007, June 8). *A race to the bottom - privacy ranking of internet service companies.* Retrieved February 2, 2012, from https://www.privacyinternational.org/foreignids/553961

Pyett, P. M. (2003). Validation of qualitative research in the "real world". *Qualitative Health Research*, *13*(8).

Rannenberg, K. (2000). It security certification and criteria. progress, problems and perspectives. In *Proceedings of the ifip tc11 fifteenth annual working conference on information security for global information infrastructures* (pp. 1–10). Deventer, The Netherlands, The Netherlands: Kluwer, B.V. Available from http://dl.acm.org/citation.cfm?id=647183.719502

Rannenberg, K., & Mller, G. (1999). It security and multilateral security. In K. Rannenberg, A. Pfitzmann, & G. Mller (Eds.), *Multilateral security in communications* (pp. 21–29). Longman: Addison-Wesley.

Rights of the people - individual freedom and the bill of rights. (2003). Washington DC: the U.S. Department of State's Bureau of International Information Programs.

Rotenberg, M. (2000). *Protecting Human Dignity in the Digital Age.* Retrieved February 2, 2012, from http://webworld.unesco.org/infoethics2000/documents/study_rotenberg.rtf

Routio, P. (2007, March 22). *Arteology or the science of artifacts.* Retrieved February 2, 2012, from http://www2.uiah.fi/projects/metodi/e00.htm

RSA. (2005, February 14). *RSA Security Consumer Study Reveals Major Concerns Over Online Security and Identity Protection.* Retrieved February 2, 2012, from http://www.rsa.com/press_release.aspx?id=5522

Savola, R. (2007). Towards a security metrics taxonomy for the information and communication technology industry. In *ICSEA '07: Proceedings of the international conference on software engineering advances* (p. 60). DC, USA: IEEE Computer Society.

Schwandt, T. A. (1997). *Qualitative inquiry: A dictionary of terms*. CA, USA: Sage Publications Inc.

Shoemaker, P. J., Tankard, J. W., & Lasorsa, D. L. (2004). *How to build social science theories*. CA, USA: Sage.

Silver, M., Markus, M., & Beath, C. (1995). The information technology interaction model: a foundation for the MBA core course. *MIS Quarterly*, 361–390.

Simon, H. (1996). *The sciences of the artificial* (3rd ed.). Cambridge: MIT Press.

Solove, D. J. (2007). 'I've got nothing to hide and other misunderstandings of privacy. *San Diego Law Review*, *44*(1).

Strauss, A., & Corbin, J. (1998). *Basics of qualitative research techniques and procedures for developing grounded theory*. London: Sage Publications.

Strauss, A. L., & Corbin, J. (1990). *Basics of qualitative research:grounded theory procedures and techniques*. London: Sage Publications.

SuperSurvey Knowledge Base. (2008, October 07). *Research Methods Knowledge Base.* SuperSurvey. Retrieved February 2, 2012, from http://knowledge-base.supersurvey.com/

Swanson, M., Chew, E., Stine, K., Bartol, N., Brown, A., & Robinson, W. (2008, July). *Security metrics guide for information technology systems* (NIST Special Publication 800-55 Revision 1). MD, USA: National Institute of Standards and Technology. Available from http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

Swire, P., & Steinfeld, L. (2002). Security and privacy after september 11: the health care example. In *CFP '02: Proceedings of the 12th annual conference on computers, freedom and privacy* (pp. 1–13). Califonia: ACM.

Taylor, H. (2003, March 19). *Most people are "privacy pragmatists" who, while concerned about privacy, will sometimes trade it off for other benefits.* The Harris Poll. Retrieved 22, February 2010, from http://www.harrisinteractive.com/vault/Harris-Interactive-Poll-Research-Most-People-Are-Privacy-Pragmatists-Who-While-Conc-2003-03.pdf

The Local-Germany's News in English. (2009, September 19). *Freedom rather than fear – stop the surveillance madness.* Retrieved 2 February, 2012, from http://www.thelocal.de/society/20090913-21897.html

Tremblay, M. C., Berndt, D. J., & Hevner, A. R. (2009). Measuring information volatility in a health care information supply chain. In *DESRIST '09: Proceedings*

of the 4th international conference on design science research in information systems and technology (pp. 1–10). NY, USA: ACM.

Trochim, W. M. (2006, October 20). *The research methods knowledge base.* Retrieved February 2, 2012, from http://www.socialresearchmethods.net/kb/

TRUSTe. (2012). *Truste.* online http://www.truste.com.

Tsai, J., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research*, *22*(2), 254-268.

United Nations. (1995). *The United Nations and Human Rights 1945-1995*. New York: United Nations Department of Public Information .

Volio, F. (1981). *The international bill of rights: The covenant on civil and political rights, chapter legal personality, privacy and the family*. Columbia: Columbia University Press.

Walsham, G. (1995). Interpretive case-studies in is research - nature and method. *European Journal of Information Systems*, *4*(2), 74-81.

Wang, A. J. A. (2005). Information Security Models and Metrics. In Mrio Guimares (Ed.), *Proceedings of the 43rd annual southeast regional conference-volume 2* (p. 178-184). NY, USA: ACM.

Ware, W. H. (2007). *Contemporary Privacy Issues: History of privacy laws in the USA.* Retrieved 2 February, 2012, from http://www.southernct.edu/organizations/rccs/oldsite/resources/r%esearch/comp_and_priv/ware/hist_dev.html

WELS. (2009). *Water Efficiency Labelling and Standards (WELS) Scheme.* online http://www.waterrating.gov.au/.

Westin, A. (1970). *Privacy and freedom.* NY, USA: The Bodley Head Ltd.

Westin, A. F. (2004). *A Guide to Understanding Privacy.* Retrieved February 2, 2012, from https://sites.google.com/site/privacyrelatedarticles/

Whetten, D. (1989). What constitutes a theoretical contribution? *Academy of Management Review*, *14*(4), 490-495.

Yin, R. K. (1994). *Case study research: Design and methods.* CA, USA: Sage Publications.

Yin, R. K. (2003). *Case study research: Design and methods.* CA, USA: Sage Publications.

Zang, F., & Dayarathna, R. (2010). Is your E-mail Account Secure? *International Journal of Information Privacy and Security (JIPS)*, *6 (1)*.