A methodology for bridging the gap between Lawyers and Technologist

Rasika Dayarathna[1] and Louise Yngström[2]

1 si-ika@dsv.su.se
2 louise@fc.dsv.su.se
Department of System Science
Stockholm University/ Royal Institute of Technology
Kista, Stockholm. Sweden

Abstract. Though Information and Communication Technology (ICT) has made life more comfortable, it has also widened threats to our privacy by making processing and storing of personal information more convenient and economical. Therefore, a huge demand has been created for the proper handling of personal information. Broadly speaking, information privacy protection measures can be divided into legal measures and technological measures. However, it has been shown that there is a gap between technological and legal measures used to protect information privacy. This gap demands a common platform for both technologist and legal privacy advocates to have a healthy dialog. This paper presents a methodology for building a platform which bridges the gap between technologists and legal privacy advocates. This platform facilitates both the parties to have a fruitful dialog. This study is an intermediate stage of building a framework for comparing information privacy protection measures.

1 Introduction

It is a well accepted phenomenon that information is power as it enables us to make informed decisions. With the advancement of Information and Communication Technologies (ICT), the power of information is far above the ground enabling us to make well informed decision within a very short period of time. However, the advancement of ICT has also widened threats to personal information privacy by making processing and storing personal information more convenient and economical. People believe that their life would be ruined, if their personal information goes into wrong hands. That is one of the reasons behind their reluctance to disclose personal information. Once the people are confident the way in which their personal information is handled, they may not hesitate to share their personal information. The willingness to provide personal information is a very crucial success factor for the growth of business, especially the online businesses. This leads us to an impotent point, i.e. how to build customers' trust in the ICT

environment. “Trust” which has been defined as the belief or confidence in the honesty, goodness, skills or safety of a person, organization or a thing [1] plays a prominent role in the world. Once a trustworthy ICT environment including information collectors and processors would be built, the full potential the ICT could be enjoyed. However, trust is a relative term and it is not possible to have an absolute trustworthy environment. One of the most significant ways of earning public trust on the ICT is protecting stakeholders’ privacy. The measures used to protect privacy can broadly be divided into technical measures and legal measures.

Privacy has obtained a prominent place in today’s legal context. The Privacy right has been recognized as a fundamental human right in Article 12 of the Universal Declaration of Human Rights [2], Article 17 of the International Covenant on Civil and Political Rights [3], and in many other international and regional human rights treaties. Privacy has many aspects; location privacy, information privacy, physical privacy etc [4]. Information privacy deals with the protection of personal information. A number of legislations on the protection of personal information have been introduced in many countries intending to protect personal data and providing necessary safeguards in transferring personal data. The significant milestones are the EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [5] and the EU Directive 2002/58/EC on concerning the processing of personal data and the protection of privacy in the electronic communications sector [6]. The EU Directive 95/46/EC is a general data protection directive which covers every sector while the EU Directive 2002/58/EC specifically focuses on the telecommunication sector. The member countries of the European Union have implemented their national legislations based on these directives. The United State of America has adopted a sector specific and self regulatory approach. Without introducing a general data protection legislation, it has enacted data protection legislations for specific sectors such as financial, health care and asked other sectors such as online businesses to be self disciplined [4].

These legislative measures also insist on the appropriate level of personal information protection. Article 17 of the EU Directive 95/46/EC states that controllers must implement appropriate measures to protect personal data before processing them and Article 25 of the said directive requires data exporters to ensure that adequate level of data protection is in place in the third country before exporting personal data. The Canadian data protection act also states that comparable level of personal data protection must be guaranteed [7]. Even though these legal provisions have given some indicators to be taken into account in deciding the appropriate level of protection, they are silent on how to determine the appropriate level. Thus, technologists, who deal with technological measures used to protect personal information, face a number of problems in determining the adequate level of protection required. This is a great challenge for them. On the other hand, the privacy legal advocates are not in a position to determine the merits of the measures used to protect information privacy without having an adequate knowledge on the technological measures.

The above points show the importance of having a common platform, which supports both legal privacy advocators and technologists to have a common dialog. However, many academics have stated that there is lack of common understanding between technologist, legal advocates and sociologists on information technology, privacy regulations and social and economical demands created by society. They further stressed the importance of mutual understanding between parties in these fields, especially legal privacy advocators and technologists. They further stressed

the importance of mutual understanding between parties in these fields, especially lawyers and technologists. James and Ira in their paper titled “Lawyers and Technologists Joined at the Hip?” have cited some interesting incidents took place due to the lack of understanding between them. One of them is that they had heard systems administrators and engineers stating, “CALEA (Communications Assistance for Law Enforcement Act) requires X” or “the Patriot Act requires Y,” when no such mandate actually exists. The lack of common understanding, which leads to under or over interpretation of legal provisions by technologists, is one of the major problems in this field [8].

The approach presented in this paper aims at building a common platform which facilitates both technologists and lawyers to have a healthy dialog by bridging the gap between them. In simple terms, the proposed approach presents a platform which maps the legal privacy provisions in data protection legislations into technical level functionalities and also gives appropriate technological and organizational measures to fulfill the identified privacy requirements. One of the main intentions is to make it more convenient for technologists to apply the most appropriate and feasible technical measures to fulfill the legal privacy requirements.

The development of a common platform is a complex process since a mapping between legal provisions and functional level requirements needs thorough understanding of legal texts, technical knowledge and industry specific issues.

1.1 Beneficiaries of the platform

Knowing the exact requirement imposed by law would make technologists’ work much easier. This knowledge enables them to design systems in accordance with the legal requirements which eventually promotes security, privacy and user controls [8]. Not only technologists but also privacy legal advocators can get certain benefits by using the proposed platform. They can get a solid foundation of the ICT measures used to protect information privacy and their merits and limitations. This understanding helps them to identify potential threats created by the technology and introduce necessary legal safeguards to protect privacy and security. It is also very useful to make sound legal arguments in courts and to judge the appropriateness of applicable technological and organizational measures used to protect information privacy.

Apart from technologists and lawyers, other beneficiaries are privacy auditors, law enforcing agencies etc.. Privacy auditors can easily grasp relevant legal requirements and verify appropriateness of the technological and organizational measures used to meet the legal requirements. This platform also lays a foundation for end users to demand more advanced and secure technological measures. Showcasing the high quality of its personal information protection measures, an organization can gain a competitive advantage over its competitors. This platform helps law enforcing agencies to obtain a clear understanding of legal requirements imposed by legislations and how those requirements can be fulfilled by technical means. This knowledge is useful for them to make sure, in a very early stage, that systems provide enough facilities to prevent and detect illegal activities.

2 The foundation of the proposed platform

The following section describes the methodology used in this paper. First, a literature review of data protection directives, laws, regulations and guidelines and

other related work and project documentations will be done with a view to understand how the data protection principles are interpreted and applied in the literature. Three motives can be seen behind the evolution of data protection laws. Those are to remedy past injustices, to promote electronic commerce and to be on par with the European Union data protection directives [4]. The criteria for selecting other regulations and frameworks are availability of documents, novelty and involvement of experts in drafting those documents. It is also worth noting how the market forces have demanded information privacy protection. For example, it is worth to study how the market forces demand operating in countries such as the USA demand information privacy.

The proposed approach is used as a proof of concept to build a comprehensive platform covering both technological and legal aspects. It was realized that it is not possible to cover every sector due to constraints. Therefore, the complexity of the problem is reduced to a particular sector. The other criterion for reducing the complexity is focusing on a few data protection principles. However, most of the findings of this study can easily be incorporated into other sectors. In the proposed approach, both the sector specific data protection laws and the general data protection laws are reviewed since they have their own merits and strengths in defining legal privacy requirements. Since the EU Directive 95/46/EC and legislations based on it do not specifically focus on a particular sector, it is not easy and straight forward to identify the applicable legal-privacy provision. However, it is quite easy and straight forward to grasp legal-privacy requirements from the sector specific legislations such as the EU Directive 2002/58/EC.

2.1 A rich set of privacy principles

The very first objective of this study is to come up with a rich set of complete privacy principles since privacy principles are the basic building blocks of privacy legislations, directives and best practices. According to the ISTPA privacy framework, privacy principles describe how personal information should be handled in a more abstract manner [9]. Since there is no generally accepted set of privacy principles, some organizations and legislators have defined their own sets of privacy principles. The ISTPA privacy framework has listed eight privacy principles namely *accountability, collection limitation, disclosure, participation, relevance, security, use limitation and verification* [9]. The AICPA/CICA privacy framework defines ten privacy components (components is used instead of principles) namely *management, notice, choice and consent, collection, use and retention, access, disclosure, security, monitoring and enforcement and quality* [10]. The Australian Privacy Act 1988 lists ten privacy principles namely *collection, use and disclosure, data quality, data security, openness, access and correction, identifiers, anonymity, transboarder data flows and sensitive information* [11]. The PISA project has derived nine privacy principles from the EU Directive 95/46/EC namely *reporting the processing, transparent processing, 'As required' processing, lawful basis for data processing, data quality, rights of parties involved, processing personal data by a processor, protection against loss and unlawful processing of personal data, data traffic with countries outside the EU* [12]. Another further important aspect is how judges have interpreted these privacy principles. The IPPP study has stressed the importance of understanding how the privacy principles have been interpreted by judges [13] since it may help us to clearly demarcate boundaries of privacy principles.

2.2 High level privacy requirements

The next step is bridging lawyers and technologists. In this stage, the high level privacy requirements sought by the derived privacy principles are identified. According to the ISTPA privacy framework, the Fair Information Practices (FIP)s are meant to fulfill the privacy principles [9]. However, the same report lists a number of shortcomings of the FIPs and stresses that the FIPs are not rich enough to fill the gap between the privacy principles and functional level operations [9]. The final outcome of this stage is a mapping between privacy principles and higher level requirements. Literatures such as EU directives on data protection, national legislations on data protection, sector specific laws, technical manuals and interviews with domain experts would contribute the necessary knowledge for this step. Figure 1 shows, as an example, how the principle of data security imposes higher level requirements of confidentiality of communication according to article 5.1 of the EU directive 2002/58/EC.

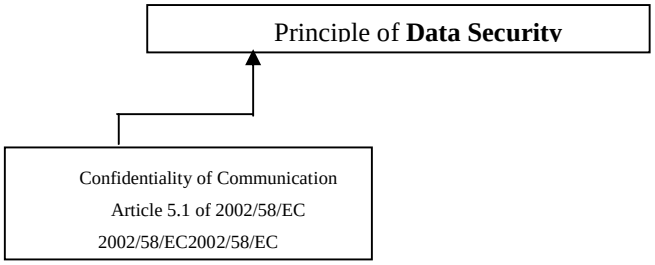

Figure1

The third step is, identifying the necessary functional level requirements to fulfill the identified upper level requirements. Functional level requirements fill the middle layer between the high level privacy requirements and technological and organizational measures. In other words, a functional level requirement is a sub component of a high level requirement. A high level requirement is fulfilled by one or more functional level requirements. The purpose of identifying the functional level requirements is making it easy and straight to identify the appropriate organizational and technological measures. Some of the desired properties of a functional level requirement are clear, unambiguous, specific, and verifiable. For example, article 5.1 of the EU directive 2002/58/EC lists some functional level requirements for having confidentiality in the telecommunication sector as shown in figure 2.

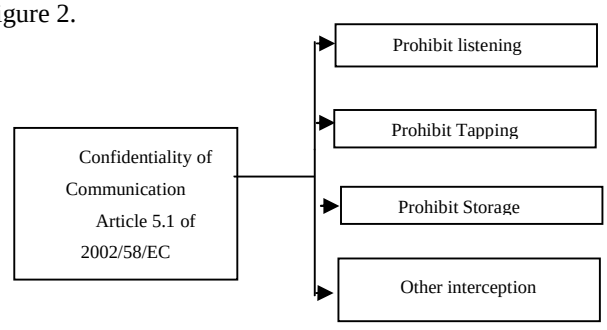

Figure 2

But, in most cases, there is no straight forward way of identifying these functional level requirements. Court decisions, directions given by data protection commissioners and sector specific laws would give some insights. Further, court decisions and directions given by data protection authorities may give some extra

requirements which are not included in legislations. Today, the adequacy of standardized best practices which is used to fill the gap between the high level abstract legislation and the low level technical functionalities is highly questionable [14].However, the expected outcome of this stage would give some insights to the standardized best practices and also make it easy for technicians to identify appropriate technical solutions to fulfill the identified functional level requirements. The relevant and applicable technical measures are partly covered in some privacy frameworks such as the ISTPA privacy framework, the AICPA/CICA privacy frameworks, security frameworks, industry standards and best practices. Many technical measures may be needed to fulfill a single legal requirement and one technical measure may fulfill many legal requirements. But, the most appropriate solution has to be identified by considering other factors such as strengths and weaknesses of the proposed solution, cost of implementation, recurring cost, the existing infrastructure and the possibility of further expansions.

Another limiting factor to be considered in choosing the appropriate technical measures is the exceptional circumstances mentioned in legislations. There is no room to use technology measures which do not support the handling of exceptional circumstances. This factor has also been taken into our study by identifying exceptional circumstances under which privacy have to be lessened. For example, in case of a crime, law enforcement authority has powers to intercept communication channels. Article 5.1 of the EU Directive 2002/58/EC mentions two circumstances under which a communication channel can be tapped. Figure 3 shows these exceptional circumstances along with the functional level requirements.

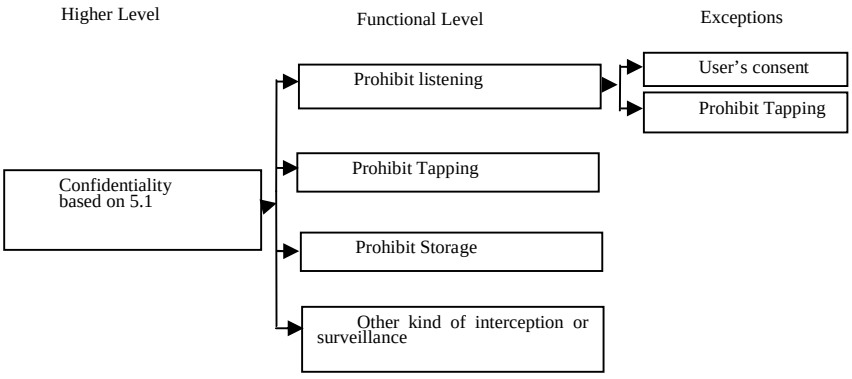

Figure 3

At the end of this phase, a summary of the studied legislations, directives, standards and best practices is presented as shown in Figure 4. The horizontal axis lists functional level privacy requirements while the horizontal axis is giving the corresponding provision/article/ paragraph of privacy legislations and policies which imposes the functional level requirement. For example, figure 4 shows the requirement of prohibit listening on the horizontal axis and the corresponding legal provision, which is Article 5.1 of the EU directive 2002/58/EC [6], is given on the vertical axis. Most of the cases, functional level requirements are not given in privacy legislations and policies. In these cases, the derived functional level requirements are used along with the corresponding high level requirement. The boxes labeled with Policy 1,2,3 etc. on the vertical axis of figure 4 is to be filled with other privacy policies and legislations in a focused domain. In this case, legislations and policies relate to the communication sector. Figure 4 illustrate that the policy 3

insists on prohibit listening and requirement 4 while policy 2 insists only on prohibit tapping.

Policy1		x	X	
Policy2		x		
Policy3	x			x
Article 5.1	x	x	X	
	Prohibit listening	Prohibit tapping	Prohibit storage	Requirements4

Figure 4

The next step is mapping the identified functional level requirements to the appropriate privacy enhancing technologies (PET) and organizational measures. The vertical axis of figure 5 lists the possible technological and organizational measures and the horizontal axis lists the functional level requirements identified in the previous stage. If a functional level requirement can be fulfilled by a measure in the vertical axis, the intersecting box is marked with "X". If the measure is not capable enough to fulfill the requirement then the intersecting box is marked with "Not sufficient". A blank box indicates that there is no relationship between the two. Before applying a measure, the technologist must make sure that the exceptional situations listed in figure 3 are supported by the particular measure. There may be cases, where the existing technological and organizational measures are not sufficient to fulfill the functional level requirements. These kinds of cases are highlighted for the attention of the privacy researchers.

Org: measure 1	**x**	**x**		
Org: measure 2	**Not sufficient**			**x**
Tech: measure 1	**x**			
	Prohibit listening	Prohibit tapping	Prohibit storage	Requirements4

Figure 5

3 Future works and Conclusion

First, the platform has to be customized with the focus on a particular domain. Once the platform is customized, the effectiveness of the platform can be tested by conducting case studies and workshops. The expert knowledge of both the technologists in the focused domain and legal privacy advocates are very essential for the evaluation process. If the experts are satisfied with the outcome, the focus can be given to another domain.

The proposed platform cannot be used for measuring legal compliance of information systems since this platform does not adhere to a particular jurisdiction. However, it can easily be transformed into a tool for measuring legal privacy compliance by limiting the focus to a particular jurisdiction and incorporating other factors mentioned in privacy legislations. For example, according to article 17 of the

EU Directive 95/46/EC [5] the cost factor plays a significant role in determining the adequacy of the data protection.

It is expected that the platform could be used further enhanced to make a yardstick to measure privacy protection measures deployed at organizational entity levels. The purpose of measuring is to compare information systems within a single domain with respect to the information privacy protection. For example making comparisons of the information privacy protection measures applied in network operating centers managed by different organizations.

The intention of presenting the proposed platform is to facilitate technologists to identify appropriate technologist measures to meet legal privacy requirements. Mangers can make use of this platform to calculate cost associated with the possible privacy controls. Legal advocates can easily identify suitable technological measures. The right decision taken by the relevant parties would give enough protection for our personal information. Hopefully, this platform contributes, at least to some extent, to obtain the benefits provide by the advancement and heavy usage of technology without leaving any room or minimizing the possibilities to invade our privacy.

Reference:

[1] E. W. (Editor), *Cambridge Advanced Learner's Dictionary*, 2 ed: Cambridge University Press, 2005.

[2] "The United Nations and Human Rights 1945-1995," Department of Public Information, United Nations, New York 1995.

[3] "International Covenant on Civil and Political Rights," United Nations General Assembly Resolution 2200A [XX1] 16 December 1966.

[4] "Privacy and Human Rights-2003," Privacy and Human Rights Commission, Washington, DC 2003.

[5] European Parliament and of the Council. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, in *Official Journal L No. 281*, 1995.

[6] European Parliament and of the Council. Directive 2002/58/ECconcerning the processing of personal data and the protection of privacy in the electronic communications sector, in *Official Journal L No. 201*, 2002.

[7] Personal Information Protection and Electronic Documents Act -Canada, in *C.5*, 2000.

[8] J. X. Dempsey and I. Rubinstein, "Guest Editors' Introduction: Lawyers and Technologists--Joined at the Hip?," *IEEE Security and Privacy*, vol. 4, pp. 15-19, 2006.

[9] "ISTPA Privacy Framework," The International Security, Trust and Privacy Alliance 2002.

[10] "AICPA/CICA Privacy Framework 2004," American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants. 2004.

[11] Australian Privacy Act, in *Act No. 119 of 1988 as amended*, 1998.

[12] G. W. V. Blarkom, J. J. Borking, et al., *Handbook of Privacy and Privacy-Enhancing Technologies*: College bescherming persoonsgegevens, 2003.

[13] "Interpreting Privacy Principles (iPP) Project," UNSW Faculty of Law - Cyberspace Law and Policy Centre 2006.

[14] G. Iachello, "Protecting Personal Data: Can IT Security Management Standards Help?," *19 th Annual Computer Security Applications Conference* pp. 266, 2003.