The Importance of Context-Dependent Privacy Requirements and Perceptions to the Design of Privacy-Aware Systems

Article · February 2010

CITATION
1

READS
45

4 authors, including:

Aggeliki Tsohou
Ionian University
35 PUBLICATIONS **228** CITATIONS
SEE PROFILE

Costas Lambrinoudakis
University of Piraeus
118 PUBLICATIONS **1,246** CITATIONS
SEE PROFILE

Spyros Kokolakis
University of the Aegean
61 PUBLICATIONS **845** CITATIONS
SEE PROFILE

UPGRADE is the European Journal for the Informatics Professional, published bimonthly at <http://www.upgrade-cepis.org/>

Publisher
UPGRADE is published on behalf of CEPIS (Council of European Professional Informatics Societies, <http://www.cepis.org/>) by Novática <http://www.ati.es/novatica/>, journal of the Spanish CEPIS society ATI (*Asociación de Técnicos de Informática*, <http://www.ati.es/>)

UPGRADE monographs are also published in Spanish (full version printed; summary, abstracts and some articles online) by Novática

UPGRADE was created in October 2000 by CEPIS and was first published by Novática and INFORMATIK/INFORMATIQUE, bimonthly journal of SVI/FSI (Swiss Federation of Professional Informatics Societies, <http://www.svifsi.ch/>)

UPGRADE is the anchor point for UPENET (UPGRADE European NETwork), the network of CEPIS member societies' publications, that currently includes the following ones:
- InfoRewiew, magazine from the Serbian CEPIS society JISA
- Informatica, journal from the Slovenian CEPIS society SDI
- Informatik-Spektrum, journal published by Springer Verlag on behalf of the CEPIS societies GI, Germany, and SI, Switzerland
- ITNOW, magazine published by Oxford University Press on behalf of the British CEPIS society BCS
- Mondo Digitale, digital journal from the Italian CEPIS society AICA
- Novática, journal from the Spanish CEPIS society ATI
- OCG Journal, journal from the Austrian CEPIS society OCG
- Pliroforiki, journal from the Cyprus CEPIS society CCS
- Tölvumál, journal from the Icelandic CEPIS society ISIP

Editorial correspondence: Llorenç Pagés-Casas <pages@ati.es>
Advertising correspondence: <novatica@ati.es>

UPGRADE Newslist available at
<http://www.upgrade-cepis.org/pages/editinfo.html#newslist>

ISSN 1684-5285

Monograph of next issue (April 2010)

"Information Technology inTourism Industry"

(The full schedule of **UP**GRADE is available at our website)

CEPIS UPGRADE
The European Journal for the Informatics Professional
http://www.upgrade-cepis.org

Vol. XI, issue No. 1, February 2010

* This monograph will be also published in Spanish (full version printed; summary, abstracts, and some articles online) by **Novática**, journal of the Spanish CEPIS society ATI (*Asociación de Técnicos de Informática*) at <http://www.ati.es/novatica/>.

The Importance of Context-Dependent Privacy Requirements and Perceptions to the Design of Privacy-Aware Systems

Aggeliki Tsohou, Costas Lambrinoudakis, Spyros Kokolakis, and Stefanos Gritzalis

The issue of information privacy protection is ensured nowadays by European and national legislation. However, it is not possible to protect information system user privacy adequately without establishing privacy requirements and employing an appropriate privacy assessment process that can identify the required privacy level and the possible countermeasures for achieving it. In this paper we draw upon security management tasks in order to highlight the gaps that need to be explored regarding privacy management, so as to be able to justifiably select the privacy enhancing technologies that fit a system's privacy requirements.

Keywords: Context-Dependent Privacy, Privacy Assurance, Privacy Enhancing Technologies, Privacy Requirements.

1 Introduction

As a result of the way that information and communication systems are utilized nowadays, personal data is becoming available or can be collected from various sites and in many different ways around the world. Undoubtedly the utilization of personal information leads to several advantages, such as personalized and more flexible customer services. At the same time, however, personal data may be misused in several ways, in violation of a user's privacy. An example could be drawn from the medical sector. Consider a web site providing medical information and advice; anyone can address, via the Internet, a specific request to the medical web site and obtain the information they want, provided that they have been registered. The organization maintaining the medical web site can easily generate "user profiles" by monitoring how often specific users are visiting the site and the type of medical information they are interested in. Such information can then be utilized for purposes that invade user privacy and are therefore in breach of Directive 95/46/EC of the European Union on the protection of individuals with regard to the processing of personal and sensitive data [[1]]. Evidently, electronic transactions have raised the major problem of user privacy protection.

In order to avoid confusion, it is important to stress the difference between *privacy* and *security:* a piece of information is secure when its content is protected, whereas it is private when the identity of its owner is protected. It is true to say that, irrespective of the application domain (i.e. e-government, e-commerce, e-health etc), the most common reservation users have with regard to using the Internet is the lack of privacy, rather than cost, difficulties in using the service, or undesirable marketing messages.

Privacy must be understood as a *non-Boolean (on-off) property*, in the sense that a person may give away part of the control over his/her personal information in exchange for some benefit. Furthermore, it may be perceived as an *autonomy* in the sense that people are free to partially or fully authorize a third party to obtain, process, distribute, share, and use their personal information for a specific aim.

Authors

Aggeliki Tsohou is currently a Ph.D. student at the University of the Aegean, Greece, Department of Information and Communication Systems Engineering. She holds a BSc. in Informatics and a MSc in Information Systems, both acquired from Athens University of Economics and Business. Her research interests include information systems security management, risk management, standardization and security awareness. <agt@aegean.gr>.

Costas Lambrinoudakis holds a BSc in Electrical and Electronic Engineering from the University of Salford, UK, an MSc in Control Systems and a PhD in Computer Science from the University of London, UK. He is currently an Assistant Professor at the Department of Digital Systems, University of Piraeus, Greece. From 1998 until 2009 he held a teaching position with the University of the Aegean, Dept. t of Information and Communication Systems Engineering, Greece. The focus of his published scientific work is on Information and Communication Systems Security and Privacy Enhancing Technologies. <clam@unipi.gr>.

Spyros Kokolakis is an Assistant Professor at the Dept. of Information and Communication Systems Engineering at the University of the Aegean, Greece. He received a BSc in Informatics from the Athens University of Economics and Business in 1991 and a PhD in Information Systems from the same university in 2000. His current research interests include information systems security management, risk analysis, and security policies design and implementation. He is a member of IEEE and ACM. <sak@aegean.gr>.

Stefanos Gritzalis holds a BSc in Physics, an MSc in Electronic Automation and a PhD in Informatics all from the University of Athens, Greece. He is currently the Deputy Head of the Dept. of Information and Communication Systems Engineering, University of the Aegean, Greece, and the Director of the Laboratory of Information and Communication Systems Security (Info-Sec-Lab). The focus of his research is on Information and Communications Security and Privacy. <sgritz@aegean.gr>.

However, there is strong evidence that people are willing to exchange personal information for some economic benefit or personalized services [2][3][4]. In [2], specifically, an attempt is made to estimate the monetary value of privacy concerns to individuals. This is interestingly found to be much less than the cost of proposed privacy legislation estimated in [5]. This willingness to trade off privacy concerns in exchange for economic benefit supports proposals like that of [6] for regulating privacy through National Information Markets, where personal information would be bought and sold at market prices.

As rapid computerization brought a fear of a surveillance society, some nations sought to protect individuals from the misuse of personal data through the implementation of appropriate Data Protection Laws. In the European Union, 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" [1], sets the prerequisites for data owners and processors for collecting, processing and exchanging personal information. The US government promotes the notion of "self regulation", a set of data protection rules applying to a plurality of market sectors, the content of which has been primarily determined by members of the specific trade sector. Furthermore, telecommunication services, as stipulated in Directives 2002/58/EC and 2006/24/EC [7][8], are protected by provisions for the secrecy of telecommunications. Public authorities may be allowed to access secret information, thereby compromising secrecy, only for specific reasons and under specific conditions and procedures provided by the domestic country's legal framework.

Regarding the design of a *privacy-aware system*, it is clear that it should be driven by the identification of relevant privacy requirements. These privacy requirements may be imposed by the legal framework, in which case they are neither negotiable nor disputable, or they may be introduced by the service providers and/or the users themselves. In the latter case the requirements may be classified in different levels of severity according to the type of the electronic service, the nature of the data involved, the environment in which the service is offered etc.; i.e. the context of the service. Furthermore, privacy requirements should, in some way, express the *subjectiveness* with which different people may deal with a potential privacy violation incident. For instance, when a bank uses the credit history of a client without his or her consent in order to issue a pre-signed credit card then it is subjective whether or not the client will feel upset about it and bring an action for breach of the Personal Data Act. In fact, banks may issue hundreds of pre-signed credit cards but only one customer may decide to bring an action and claim compensation. And once this has happened, what is the likely amount of the compensation? Again this is a very personal thing, (whether the court awards compensation or not) and should in some way be related to how much the particular client values his or her privacy. As a result, in order to estimate the required *privacy level* it is necessary to have some way of investigating how individuals subjectively value their privacy.

To sum up, what is needed is a structured method for identifying context-dependent privacy requirements. These identified privacy requirements can then be used to support privacy assessment and, subsequently, privacy management. In order to describe the unresolved issues in this process, we draw upon security management tasks; identification of security attributes, determination of security requirements, risk analysis and management.

The rest of this paper is structured as follows: Section 2

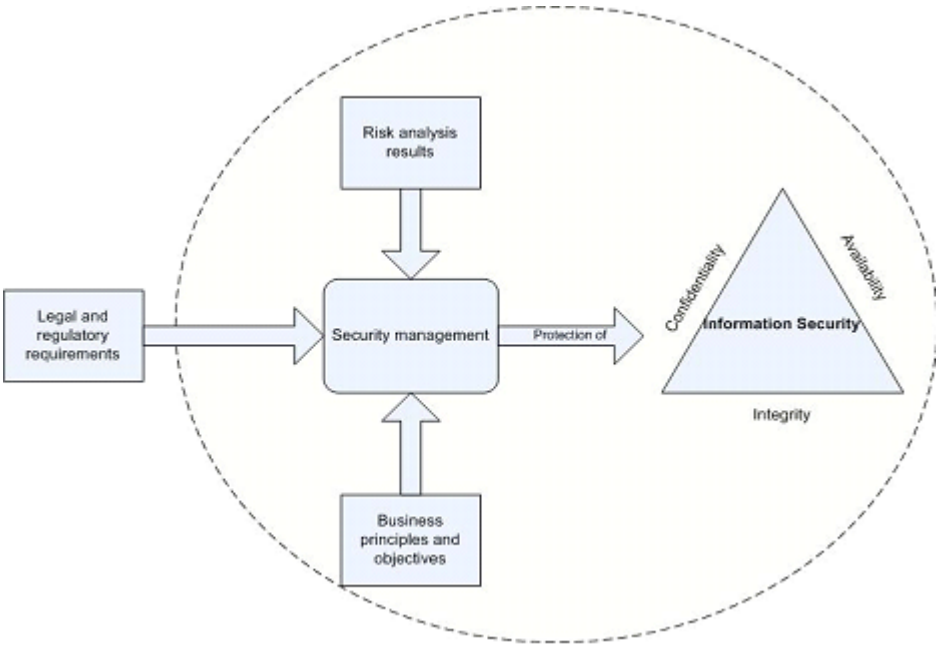

Figure 1: Security Requirements Sources (Based on ISO/IEC 27002:2005).

provides an overview of the common risk assessment process and how it is used for determining and prioritizing security requirements. Section 3 highlights the non-existence of a respective privacy assessment and privacy requirements elicitation process, providing guidelines for the identification of privacy requirements and for their classification into different privacy levels. Section 4 gives an overview of Privacy Enhancing Technologies, while in Section 5 the reader can find a summary and some concluding remarks.

2 Risk Assessment Process and Security Requirements

According to a typical risk assessment process described in ISO/IEC 27005:2008 [9], risks should be identified, quantitatively or qualitatively described, and prioritized against risk evaluation criteria and objectives relevant to the organization. A *risk* is a combination of the consequences that would follow from the occurrence of an unwanted event and the likelihood of the occurrence of the event.

There are many well established methods that support the risk assessment process by providing well defined and structured guidelines on how to preserve the key security attributes of *confidentiality*, *integrity* and *availability*. Specifically, such risk assessment methods support the valuation of the information assets, the identification of the applicable threats and vulnerabilities that exist (or could exist), the identification of existing controls and their effect on the identified risks, the determination of potential consequences and, finally, the prioritization of the derived risks and their ranking against the risk evaluation criteria set in the context establishment.

As shown in Figure 1, security requirements derive from three main sources (ISO/IEC 27002: 2005) [10]: firstly, the legal and regulatory framework; secondly, the principles, objectives and business requirements for information processing that an organization has developed to support its operations; and thirdly the risk assessment results. The first category of requirements comprises the *outer context security requirements* while the latter two make up the *inner context security requirements*.

After the identification and prioritization of security requirements, the security measures can be selected. Their main purpose is to ensure that the security requirements will be satisfied and thus the security attributes associated with the data assets will be preserved.

3 Assessing and Managing Privacy

Unlike the risk assessment process there is no established method for performing a similar assessment for privacy issues. However, on the basis of the risk assessment process we can expect the key to the protection of the main privacy attributes (as briefly presented in the following subsection) to lie in the identification and satisfaction of privacy requirements.

Furthermore, as shown in Figure 2, privacy requirements are also divided into *inner and outer context privacy requirements.* As in the case of security requirements, outer context privacy requirements result from the associated legal and regulatory framework. What we are really missing are the inner context privacy requirements and their

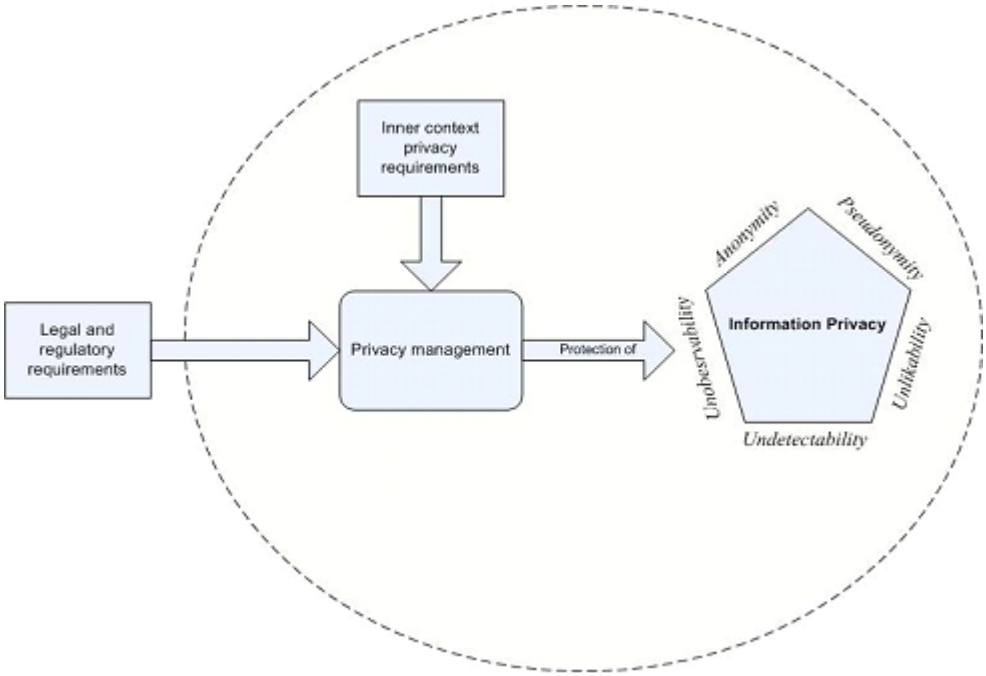

Figure 2: Privacy Requirements Sources.

prioritization through some quantitative or qualitative description. Section 3.2 below provides some initial guidelines for the identification of privacy requirements as well as their classification in different privacy levels.

3.1 Privacy Attributes

According to [11] the main privacy attributes are the following:

- ***Anonymity:*** Anonymity is the state of being not identifiable within a set of subjects (users), known as the anonymity set. To enable anonymity of a subject (user), there always has to be an appropriate set of subjects with potentially the same attributes.
- ***Pseudonymity:*** Being pseudonymous is the state of using a pseudonym as identification. Therefore, users can be identified through their pseudonym but they remain anonymous as far as their real identity is concerned. Clearly, it is assumed that each pseudonym refers to exactly one holder, invariant over time, and is not transferred to other users.
- ***Unlinkability:*** Ensures that a user may make multiple uses of resources or services without others being able to link these uses together. It requires users to be unable to determine whether the same user caused certain specific operations in the system.
- ***Undetectability:*** Undetectability of a user, from an attacker's perspective, means that the attacker cannot sufficiently distinguish whether it exists or not. Undetectability can be regarded as a possible and desirable property of steganographic systems.
- ***Unobservability:*** Ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used. It requires users to be unable to determine whether an operation is being performed.

3.2 Specification of Privacy Levels and Privacy Assessment

There are currently no methods specifically designed for performing privacy assessment. Furthermore, existing risk analysis methods do not exhibit the required knowledge and/or techniques for handling privacy issues thoroughly. Needless to say there is no structured way available for prioritizing privacy requirements.

Therefore, in order to correctly identify privacy requirements in qualitative and/or quantitative terms and rank them, it is vital to clearly understand why these requirements are raised or, alternatively, what privacy attributes we are aiming to preserve. Considering two privacy-sensitive application domains, namely e-Government and e-Health, we have compiled a list of issues that should be systematically considered during the privacy assessment process. These are:

- Usually the services offered in both aforementioned application domains collect, process or communicate *personal and/or sensitive data* (such as healthcare records, financial data, data related to someone's professional career etc), as well as the identifiers of the persons involved (such as VAT number, social insurance number, etc.) that facilitate linkability between data and persons. The aim in all the above cases is to protect or hide the identity of the users involved while, from the privacy point of view, the protection of the data itself is irrelevant.
- The complexity of the operations imposes the need for very *complex workflows* and/or dataflows as well as *interoperability* between different national and international information systems (for instance, we may have distributed healthcare records, or in order to issue a birth certificate we may need to collect information from various governmental information systems). This complexity makes the task of personal/sensitive data protection really hard.
- Another important issue is the identification of users. There is a great variety of ways, ranging from the use of identifiers such as passport numbers, social security numbers, VAT numbers etc., to the employment of biometric characteristics or RFID tags. It is therefore clear that some *identification methods* (such as the use of biometrics) raise privacy issues by their very nature.
- During the registration or use of an electronic service, users may voluntarily provide an electronic service with their personal data (for example, during the registration phase). However, personal data may also be collected without users' consent, through the appropriate processing of *cookies* left by users on a number of Internet sites or directly by an internet service provider (accessing information such as the web pages users visit, the exact time and duration of their browsing, etc.). In this way it is feasible to simulate the "electronic behaviour" of users (i.e. preferences), something that should clearly be protected.
- Another risk is that the identity of the user can be revealed through a *trace-back attack*, whereby someone traces the path back to the initiator along the forward or the reverse path. Furthermore, by linking specific communication channels/sequences/sessions with certain client-server, pairs can be achieved by tracing the contents and/or the size of a message travelling over a communication link or by attempting to detect and analyse periodically transmitted packets, aiming to discover their source through specific time correlations.

The identification and expression of privacy requirements is tightly coupled with the aforementioned issues [12][13][14]. However, in order to facilitate the differentiation of each privacy requirement's weight, i.e. introduce the concept of different *Privacy Levels*, it is vital to agree on ways of estimating the impact that may result from a privacy violation incident. This impact estimation phase is perhaps the only phase that cannot be directly ported from the typical risk analysis methods; the reason being that there are new aspects that need to be considered. Specifically, while estimating the impact that may result from a privacy violation incident, in addition to the legal, financial, operational and other type of consequences that we normally consider, we should also take into account issues such as:

- Subjectiveness of privacy: i.e. it is necessary to capture the subjective nature of the question "How important

is a privacy violation incident to someone?" [15].

- How much does each person value his or her privacy? For instance, somebody may be prepared to give away his or her personal/sensitive data in order obtain some economic benefit.
- It is possible that under some circumstances the user may choose not to protect her privacy (privacy protection on/off option); an example is that of location privacy. If someone is in an isolated area, they may choose not to protect their privacy in order to allow other people to know where they are. Therefore, the identification of inner context privacy requirements relies on the determination of a concept of privacy levels (accordingly to risk levels). The conceptualization of privacy levels requires not only the identification of privacy threats and vulnerabilities, but also the determination of the potential impact of a privacy violation. However, being able to determine and assess privacy levels is the path towards the selection of privacy protection measures.

4 Privacy-Enhancing Technologies

Given that common security mechanisms, such as encryption, cannot ensure privacy protection (encryption, for instance, can only protect the confidentiality of a message), new Privacy-Enhancing Technologies (PETs) are necessary and have been developed.

There are systems based on single HTTP proxies, such as Anonymizer [16] and LPWA [17][18], that can be easily employed to ensure anonymous browsing, while systems like Onion Routing [19], Crowds [20], and Hordes [21] are scoring better in protecting information and in preventing attacks. Onion Routing can form the basis upon which other protocols could be employed in order to improve the level of global user protection.

On the other hand, services like TRUSTe [22] and P3P [23] negotiate, assure and periodically re-confirm the completeness and correctness of web sites' privacy policies. Freedom is a system that fulfils most of the user requirements, exhibiting a satisfactory level of protection against security threats; however its high cost may downsize all these advantages. Finally, GAP can be used in secure peer-to-peer networks, such as GNUnet, to deploy secure and anonymous transactions between peers. This is extremely useful for Internet users since many of them use peer-to-peer applications that focus on file sharing (GNUtella, KaZaa, iMesh etc.) and frequently violate the privacy and anonymity of their peers.

As we mentioned earlier, privacy is defined as the right to informational self-determination; i.e. the right of individuals to determine for themselves when, how, to what extent, and for what purposes information about them is communicated to others. In order to reinforce their right to informational self-determination, users need technical tools that allow them to manage their (partial) identities and to control what personal data about them is revealed to others under what conditions. Identity Management (IDM) can be defined to subsume all functionality that supports the use of multiple identities, by the identity owners (user-side IDM) and by those parties with whom the owners interact (services-side IDM). According to Pfitzmann and Hansen, identity management means managing various partial identities (i.e. a set of attributes, usually denoted by pseudonyms) of a person; i.e. the administration of identity attributes including the development and choice of the partial identity and pseudonym to be re-used in a specific context or role [11]. Privacy-enhancing identity management technology enforcing legal privacy principles of data minimization, purpose binding and transparency have been developed within the EU FP6 project PRIME [24] (Privacy and Identity Management for Europe) and the EU FP7 project PrimeLife [25] (Privacy and Identity Management for Life).

When considering the forms of protection that are needed, it is important to recognize that user actions will often be based upon their perceptions of risk, which may not always be very accurately aligned with the reality of the situation. For example, they may under- or over-estimate the extent of the threats facing them, or be under- or over-assured by the presence of technical safeguards. For example, some people simply need to be told that a service is secure in order to use it with confidence. Meanwhile, others will only be reassured by seeing an abundance of explicit safeguards in use. Thus, if trust is to be established, security and privacy measures need to be provided in accordance with what users expect to see and are comfortable using in a given context.

Invasion of privacy is not only a technical problem but also has social, legal and psychological dimensions; therefore, a holistic approach to a privacy-friendly use and design of security and privacy enhancing mechanisms is necessary.

5 Summary and Conclusions

Protection of information privacy is a major challenge today, especially because of the imbalance between the personalized customer services that can be offered by the processing of personal and private data and the right of individuals to determine for themselves when, how, to what extent and for what purposes information about them is communicated to others. To this we can also add the problems caused by the complexity and interoperability of current information systems, the widespread use of technical methods for user identification and action tracing (such as RFIDs and cookies). Finally, the subjective value of privacy also inhibits the design of information systems and services that respect and protect users' privacy. However, information systems nowadays should not be only security aware, but also privacy-aware; therefore privacy requirements (e.g. anonymity, unlinkability, undetectability, unobservability etc.) should also be taken into account during information system analysis and design.

In order to highlight the dimensions of the solution required, we have examined the processes typically executed in information systems security management. The core of current risk management methods includes the calculation

of risk levels, in regard to security threats, vulnerabilities and potential impacts. In sequence, risk levels are compared to risk evaluation criteria and finally adequate countermeasures that reduce these risks are implemented. Privacy management cannot be methodologically supported without a representation of privacy requirements and a method of expressing and assessing privacy levels. This remains a problematic issue, especially since the impact of a privacy violation incident strongly depends on the subjective nature of the answer to the question "how much should a privacy violation matter to someone?". Thus as future work we intend to build a framework that describes the processes required to collect privacy requirements, and also design a formalized privacy assessment methodology to calculate privacy levels. Such research would enhance the formulation of countermeasures that protect the privacy attributes described above.

References

[1] 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.

[2] I. Hann, K.L. Hui, T.S. Lee and I.P.L. Png. "Online information privacy: Measuring the cost-benefit tradeoffs". Proceedings of the 23rd International Conference on Information Systems, Barcelona, Spain, 1-10, 2002.

[3] A. F. Westin. "Privacy and American Business Study", 1997.

[4] S. Faja. "Privacy in E-Commerce: Understanding user trade-offs". Issues in Information Systems, VI(2), pp 83-89, (2005).

[5] R. Hahn. "An Assessment of the Costs of Proposed Online Privacy Legislation", working paper. AEI Brookings Joint Center for Regulatory Studies, 2001.

[6] K.C. Laudon. "Markets and Privacy", Communications of the ACM, 39(9), 92-104, Sep. 1996.

[7] 2002/58/EC Directive European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[8] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[9] ISO/IEC 27005:2008. Information technology - Security techniques - Information security risk management.

[10] ISO/IEC 27002:2005. Information technology - Security techniques - Code of practice for information security management.

[11] A. Pfitzmann, M. Hansen. Anonymity. "Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology", version v0.31, <http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.doc#_Toc64643839>.

[12] Christos Kalloniatis, Evangelia Kavakli, Stefanos Gritzalis. "Addressing privacy requirements in system design: The PriS method". Requirements Eng. Vol. 13, No 3, pp 241-255, Springer, 2008. [16] Anonymizer, available at <http://www.anonymizer.com>, 2003.

[13] A. Antün. Goal-based requirements analysis. ICRE'96. Colorado Springs, Colorado, USA, IEEE, pp 136-144, (1996).

[14] H. Mouratidis, P. Giorgini and G. Manson. "Integrating security and systems engineering: Towards the modelling of secure information systems". LNCS 2681. Springer-Verlag. Berlin Heidelberg 63-78, 2003.

[15] A. Yannakopoulos, C. Lambrinoudakis, S. Gritzalis, S. Xanthopoulos, S. Katsikas. "Modeling Privacy Insurance Contracts and Their Utilization in Risk Management for ICT Firms". Proceedings of the 13th European Symposium on Research in Computer Security – ESORICS 2008, S. Jajodia, J. Lopez (Eds.), pp 207-222, Springer LNCS 5283, Malaga, Spain, 2008.

[16] Anonymizer, available at <http://www.anonymizer.com>, 2003.

[17] E. Gabber, P.B. Gibbons, D. Kristol, Y. Matias, A. Mayer. "Consistent, Yet Anonymous Web Access with LPWA", Communications of the ACM, Vol.42, No.2, pp 42-47, 1999.

[18] Lucent Personalized Web Assistant LPWA, available at <http://www.bell-labs.com/projects/lpwa>, 2003.

[19] M. Reed, P. Syverson, D. Goldschlag. "Anonymous Connections and Onion Routing". IEEE Journal on Selected Areas in Communications, Vol.16, No.4, pp 482-494, 1998.

[20] M. Reiter, A. Rubin. "Crowds: Anonymity for Web transactions". ACM Transactions on Information and System Security, Vol. 1, No.1, pp 66-92, 1998.

[21] C. Shields, B.N. Levine. "A Protocol for Anonymous Communication Over the Internet". Proceedings of the 7th ACM Conference on Computer and Communications Security, P. Samarati, S. Jajodia (Eds.), ACM Press, New York, pp 33-42, 2000.

[22] TRUSTe, available at <htp://www.truste.org>, 2003.

[23] World-Wide-Web Consortium W3C, Platform for Privacy Preferences Project - P3P, available at <http://www.w3.org/P3P>, 2003.

[24] R. Leenes, M. Lips, R. Poels, M. Hoogwout. "User aspects of Privacy and Identity Management in Online Environments: towards a theoretical model of social factors". In: PRIME Framework V1 (chapter 9), Editors: S. Fischer-Hübner, Ch. Andersson, T. Holleboom. PRIME project Deliverable D14.1.a, 2005.

[25] S. Fischer-Hübner, Ch. Köffel, E. Wästlund, P. Wolkerstorfer. PrimeLife HCI Research Report, Version V1, PrimeLife EU FP7 Project Deliverable D4.1.1, 26, 2009.