Privacy by Design in Software Engineering: a Systematic Mapping Study

Miguel Ehécatl Morales-Trujillo[a], Erick Orlando Matla-Cruz[b], Gabriel Alberto García-Mireles[c] and Mario Piattini[d]

[a] Computer Science and Software Engineering Department, University of Canterbury, Christchurch, New Zealand

miguel.morales@canterbury.ac.nz

[b] Posgrado de la Facultad de Medicina, Universidad Nacional Autónoma de México, Av. Universidad 3000, Ciudad Universitaria, 04510, Mexico City, Mexico

ematla@fmposgrado.unam.mx

[c] Departamento de Matemáticas, Universidad de Sonora, Hermosillo, México

mireles@mat.uson.mx

[d] Alarcos Research Group, University of Castilla – La Mancha, Paseo de la Universidad 4, 13071, Ciudad Real, Spain

mario.piattini@uclm.es

Abstract. Privacy by Design (PbD) is becoming a relevant issue that challenge the way software is developed. The objective of this paper is to determine the extent to which PbD has been applied in software development endeavors. A Systematic Mapping Study was carried out to identify primary papers that describe the way PbD is considered in software engineering, which principles or goals pursues, and what PbD practices or techniques are used in software development efforts. As a whole, we identified a deficiency of sound PbD-related research in the area of software development. The selected primary papers address PbD from a general experience-based perspective. However, good PbD-related practices are neither fully developed nor validated. Furthermore, we observed a strong tendency toward following principles rather than explicit practices.

Keywords: privacy by design, software engineering, software development, systematic mapping study, GDPR

1 Introduction

According to Warren and Brandeis [1], privacy is a state of social withdrawal or the right to be 'left alone'. Altman [2], Nissenbaum [3], Palen and Dourish [4] state that privacy is not just a state of withdrawal, but a contextual, situated, practically achieved

M. Genero, M. Kalinowski (Eds.): CIbSE 2018, Bogotá - Colombia, 2018

matter of boundary management. This means that the context in which information is disclosed and the mechanisms to handle it are essential to determine the extent privacy is addressed in a particular situation [A1]. In this document, square bracket references that contain the letter 'A' refer to the primary papers in this SMS, full reference list can be consulted in the additional material (https://goo.gl/iKTLLr).

In the context of people, personal data is sensitive data that must be safeguarded on two fronts: by technological means and by legal means [5]. Almost any up-to-date system whose goal is to automate and speed up processes stores sensitive data. Being concerned about data privacy should, therefore, be part of any software development, regardless of the industry for which it is intended. In software development efforts, the protection of data is usually resolved through the use of encryption and security applications frameworks. These solutions are, however, applied in the last stages of software development and, moreover, developers must be aware of the usage and exposure of data that the system manipulates or extracts.

Several data protection laws supported by governmental bodies have been created. One example of these is the recent General Data Protection Regulation (GDPR) (Regulation EU 2016/679), which is supported by the European Parliament, the Council of the European Union (EU) and the European Commission and was brought into being with the intention of strengthening and unifying data protection for all individuals within the EU. This regulation incorporates data protection rules that cover design, safety and security measures, and conduct policies; it also defines a special role in charge of evaluating and analyzing data privacy measures.

The concept of Privacy by Design (PbD) has become important in this environment, and has been highly advocated by policy makers; it was conceived in order to mitigate privacy threats from the very beginning, by creating a process that designs information systems in a privacy-respectful manner [A2]. The PbD approach is relatively new and has been unanimously acclaimed as a global privacy standard by the body of International Data Protection Commissioners[1]. In fact, the lack of robust privacy methodologies has led to an increasing acceptance of PbD [A3], which seeks to influence technology design, business practices, and physical infrastructure by embedding privacy protection at its core [A4].

The existent research addresses the PbD approach; however, good PbD-related practices and tasks are not, as yet, fully developed. According to [6], the next stage of PbD evolution is to translate its "7 Foundational Principles" into more prescriptive requirements, specifications, standards, best practices, and operational-performance criteria. Indeed, IT practitioners cannot find appropriate methodological support to implement PbD in software development [A5] and there is a lack of tools to support the design and construction of privacy-friendly systems [A6].

We believe that introducing PbD into software developments is both viable and useful because it is a potential means of including best practices that address data protection in information systems. Moreover, PbD is ideally focused on or targeted at technology developers/providers/designers and manufacturers [7]. The objective of this paper is, therefore, to carry out a systematic mapping study (SMS) in order to determine

[1] https://icdppc.org/

the State of the Art of PbD and its best practices as regards use in software development endeavors.

This paper is organized as follows: Section 2 describes the background of PbD, while Section 3 describes the design of the SMS and its results. The discussion is presented in Section 4. Finally, our conclusions are covered in Section 5.

2 PbD Background

2.1 Towards Understanding Privacy by Design

"Privacy by design" is a concept developed in the 1990s whose purpose is to embed privacy into the design of technology [A7]. The PbD concept relies on a set of seven principles that provide a framework for addressing privacy and data protection throughout all stages of IT and information systems development, including IT design, operation, and management [A7] [8]. The PbD principles are: privacy as default, end-to-end security, respect for user privacy, openness and transparency, proactive not reactive, privacy embedded into design, and full functionality [8] [9]. These principles were derived from the Fair Information Practices [A7] which serve to translate privacy and data protections objectives to law, policy and technologies [8].

Relevant concepts in PbD that need to be described are privacy and data protection. Privacy is related to the control that individuals have over the collection, use, and disclosure of personally identifiable information [9]. Informational privacy is defined as "the ability to maintain control over the use and dissemination of one's personal information" [9]. On the other hand, data protection refers to "an individual's information rights, along with the legal structures that enable them and impose obligations on organizations that process personal data" [8]. Comparing with data protection scope, PbD approach is broader and look for "the highest possible global standard of privacy" [8].

Working with privacy goals in developing information systems and software requires that security safeguards were included during system design and construction. Indeed, assuring privacy requires assuring security [8] [10]. On the one hand, security protection goals - confidentiality, integrity and availability - are driving factors for assessing the risks and potential consequences if their desired level is not achieved [11]. On the other hand, privacy protection goals should consider security protection goals as well as unlinkability, transparency and intervenability [11] [12]. However, several papers address privacy requirements as a special case of security requirements, but this approach overlooks fundamental privacy goals [13]. Thus, this work is centered on mapping current published research on privacy protection goals when software and information systems are developed.

2.2 Literature reviews on PbD

Literature reviews on the "privacy by design" approach are seldom published. However, if we widen the search for papers addressing the "privacy" concept for software engineering endeavors, we find that several literature reviews focused on specific domains have been published. In the case of "privacy by design" search, there is one paper that addresses the topic of ontologies for privacy requirements [13]. The authors report a set of papers addressing privacy by design concepts and relations. Based on the selection of key concepts, a meta-model for addressing privacy requirements is provided, with specific privacy terms such as notice, anonymity, and transparency.

In the case of a wider search, there are several papers that address privacy in different domains, such as healthcare systems and Internet of Things (IoT) technologies, among others. In these reviews, the main topic is understanding the extent to which privacy goals, principles, mechanisms, or stakeholders' privacy concerns are addressed in the systems under consideration. In the domain of healthcare systems, the literature reviews have been focused on cross-organizational data sharing [14], cloud-assisted systems [15], and factors that trigger privacy concerns [16]. However, none of these literature reviews analyses what software development practices were used to develop those systems.

In the context of IoT, Loukil et al. [10] found that data protection and privacy needs deal more with current deficiencies. Privacy should be considered in each data phase to protect sensitive data of an individual, group, or organization [10]. Thus, current privacy-related literature reviews address several systems privacy properties, mainly in usage stage, without focusing on the practices needed to build system software based on the "privacy by design" approach.

3 SMS methodology and results

3.1 Planning the SMS

The purpose of this SMS is to determine the State of the Art of PbD, find out its principles and analyze the best practices that the authors of the papers have addressed. This paper seeks to respond to the following question, which guides this SMS:

What is the State of the Art of PbD when applied to software engineering?

In this section, we present the methodology of the study, which is developed as follows. We start by defining relevant research questions, after which we expand on the data extraction resources employed, and finally, we discuss the evaluation and classification criteria applied to the primary papers. The SMS was carried out following the suggestions presented in [17] and [18].

3.1.1. Research methods and questions. The research questions seek, on the one hand, to define the term PbD, its objective and its principles, and, on the other, to identify its best practices. The research questions and the motivation behind each one are presented in Table 1.

Table 1**.** Research questions and their motivation

Research Question		Motivation
RQ1	What is PbD?	Defining the concept of PbD.
RQ2	What are the principles/goals of PbD?	Identifying the principles or goals that PbD pursues.
RQ3	Which are the PbD practices or techniques?	Identifying software development practices or techniques that address PbD.

3.1.2. Data sources and search strategy. The search string was built using two major search terms: "privacy by design" and "software engineering". These terms were selected because they are the most general possible and are the main topic of the SMS, since the objective is to know and expand PbD in software engineering. As synonyms to "software engineering", "software development", "information systems" and "requirements engineering" were used.

It is important to highlight that synonyms for "privacy by design" were not used in order to avoid the issue highlighted by [13], in which privacy is seen as a special case of security. This misguides to believe that security covers privacy aspects by default. However, a system may be considered secured and may still not address privacy aspects.

The search scope is focused on peer-reviewed research papers published in journals, academic conferences and workshops. We decided to use Scopus, IEEE Xplore Digital Library and ACM Digital Library as the main search engines in order to preserve the quality of the studies. The fields used were title, abstract and keywords (Scopus); and title and abstract (IEEE Xplore and ACM Digital Libraries).

The search was carried out only for papers written in English. The search date was December, 10th 2017.

The SMS included papers if they addressed PbD in software engineering and reported it as a theoretical or empirical study; and if it was a paper, a book chapter or a poster.

The SMS excluded papers if they reported research that did not deal with PbD in software engineering endeavors; if the document was neither a paper, a book chapter nor a poster, and if the paper was duplicated or unavailable.

The selection criteria for papers were developed by the first two authors; peer-debriefing sessions were developed in order to solve disagreements. The last step, validating how the criteria were applied, was done by the third author.

The data collection was carried out using a table that registered papers' metadata (title, authors, year of publication, type), exclusion details, which research questions were targeted and the actual response to the questions such as definitions, principles, goals, practices or techniques discovered in the papers. This work was done by the first two authors and validated by the third and fourth. The inconsistencies were solved through peer-debriefing.

3.1.3. Classification. The search results were refined by carrying out a classification based on 3 categories. These categories were defined according to the research questions:

1. **PbD definition:** Papers in this category contain an explicit definition of PbD. This category is related to RQ1.
2. **PbD principles or goals:** Papers in this category were classified according to the principles or goals that PbD pursues. This category is related to RQ2.
3. **PbD practices or techniques:** Papers in this category were classified according to the practices or techniques they discuss. This category is related to RQ3.

3.2 Results of the SMS

The search was developed according to the steps and criteria described in the previous section. 92 papers were retrieved from databases. After removing duplicates (16) and applying selection criteria, 35 primary papers were identified. The comparison of the number of documents by year is shown in Figure 1. It will be observed that the interest in this topic has increased since 2011, and of the 35 primary studies found, 31 were published in the period 2011 to 2017 (until December). The full list of primary studies is presented in additional material (https://goo.gl/iKTLLr).

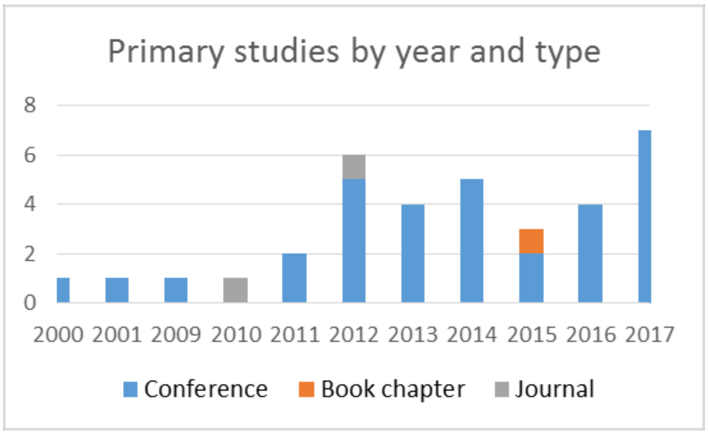

Fig. 1. Distribution of the primary studies by year

The first primary study was published in 2000; it describes obstacles as regards designing technology that could be used to protect civil liberties and, in particular, the difficulties involved in creating and deploying liberty-protecting software [A8]. In 2001, [A9] establishes that no definition is possible for the concept of privacy, and, instead, offers its description from three different angles: its history, its legal status, and its utility.

33 papers have been published since that time, they describe particular cases of compliance with privacy requirements in health care systems [A10] [A11], Internet of Things [A12] [A13], mobile phones [A14] and e-commerce [A15]. Or they provide

guidelines that can be used to include PbD in information systems [A16] and [A17] in the form of patterns. 13 of 35 are experience reports while 22 are theoretical proposals. Following sections describe the main findings considering the research questions.

3.2.1 RQ1. What is PbD?

The primary results led us to define PbD from two perspectives: establishing its scope and objectives, or determining its characteristics and principles.

According to [A2], PbD is "an example of an approach highly advocated by policy makers, intended to mitigate privacy threats from the very beginning, by creating a process that designs information systems in a privacy-respectful way".

Similarly, [A18] establishes that "PbD is an approach to protecting privacy by embedding it into the design specifications of information technologies, accountable business practices, and networked infrastructures, right from the outset".

Three authors cited [6] in connection with the concept of PbD:

- "PbD is an approach that argues building privacy into technologies as a default" [A3].
- "the concept of PbD, aiming at enhancing privacy to IT systems, from the very start of their inception or design, has emerged as an imperative to privacy protection" [A19].
- "PbD is an engineering and strategic management approach that commits to selectively and sustainably minimize information systems' privacy risks through technical and governance controls" [A20].

We found similar definitions that strongly recommend considering privacy during the software design process:

- "PbD approach integrates privacy requirements into the design process right from the beginning" [A21].
- "PbD designates a software design approach that incorporates privacy requirements from the beginning and throughout the software development process, instead of considering them as an afterthought", respectively [A5]

These statements are reinforced by [A22], which points out that "security and privacy by design can be achieved only by design".

However, there is a wider opinion regarding the inclusion of privacy practices in the whole development process. As [A23] states, "PbD incorporates privacy protections into an organization's practices, and maintains comprehensive data management procedures throughout the lifecycle of their products and services". A similar definition is used in [A24]: "PbD is the embedding of privacy awareness throughout all stages of a technology's design and implementation lifecycle". Wohlgemuth [A25] provides a similar definition: "PbD postulates to consider IT security requirements in all phases of software development to reduce vulnerabilities".

Colesky and Ghanavati [A26] provide a related definition and return to Ayalon [A2] and Rowan's [A23] ideas: "PbD is an approach to software development which protects privacy from the early/concept stages of the software development life cycle". Another paper [A6] states that "PbD philosophy "bakes-in" privacy throughout the system development lifecycle".

Moreover, [A4] declares that "PbD seeks to influence technology design, business practices, and physical infrastructure by embedding privacy protection at its core". "The general philosophy of PbD is that privacy should not be treated as an afterthought but rather as a first-class requirement during the design of a system" [A27].

We have used all the aforementioned definitions as a basis to propose a unified definition:

PbD is an approach whose objective is to discover, represent, implement and manage the rules and tasks that preserve the data privacy of any stakeholder of a software system. PbD should be considered from the project inception phase and throughout the entire software lifecycle.

3.2.2 RQ2. What are the principles/goals of PbD?

The second criteria according to which the papers were classified and data were extracted were the principles or goals of PbD. The essential objectives as regards determining whether PbD is involved in software development are stated as the following 7 principles [6]:

1. Proactive not reactive; preventative not remedial.
2. Privacy as the default setting.
3. Privacy embedded into design.
4. Full functionality positive-sum, not zero-sum.
5. End-to-end security, full life-cycle protection.
6. Visibility and transparency- keep it open.
7. Respect for user privacy, keep it user-centric.

These principles are also mentioned by [A12], [A15], [A19] and [A28].

Furthermore, [A29] proposes the following privacy goals: anonymity, pseudonymity, unlinkability, undetectability and unobservability. The author of the paper in question formulates the principles in the form of a pattern and proposes a set of techniques by which to implement each of them in an information system.

PbD lacks of systematic methodologies that address privacy issues and support the translation of its principles into engineering activities [A30]. However, it is important to mention that authors refer to some practices that can be carried out in order to achieve privacy. For example, "PbD means to embed privacy proactively in the design process of a technical system by data minimization techniques" [A28]. However, methodological support for developing software systems belong to the category of guidelines.

The most frequently goals mentioned by the authors are the following:

Minimize (in 8 primary studies) recollection and access to data is defined by [A6] [A26] as "limiting usage as much as possible by excluding, selecting, stripping, or destroying any storage, collection, retention or operation on personal data, within the constraints”.

Anonymization and pseudonymization (6 and 5 times respectively) are defined by [A29] as “a characteristic of information that does not permit a personally identifiable information principal to be identified directly or indirectly”.

Separation (5) is “personal data should be processed in a distributed fashion, in separate compartments whenever possible” by the same author [A19].

Control (5) is defined by [A6] [A26] as “providing as abundant means as possible for consenting to, choosing, updating, and retracting from storage, collection, retention, sharing or operation on personal data, in a timely manner, within the constraints of the agreed upon purposes”.

Consent (5) which is defined as only processing the personal data for which explicit, freely-given, and informed consent is received [A6].

Other 51 goals appear four or less times in the primary studies. The full list is presented in additional materials (https://goo.gl/iKTLLr).

3.2.3 RQ3. Which are the PbD practices or techniques?

In 2010, [A22] stated categorically that security and privacy are two distinct disciplines with two common factors: both need to receive more explicit and direct attention from research and education and can be achieved only by design. In [A21], a PbD process that aims to support privacy requirements engineering is presented, in addition to which a formal method to evaluate the realization of the specified privacy constraints is proposed.

Kost et al. define a four-phase process with which to include and validate privacy in the development of systems:

1. Identify high-level privacy requirements.
2. Map the high-level privacy requirements onto a formal description.
3. Outline the formal requirements and model the system.
4. Match the formal requirements with the formal model system.

In [A30] three privacy requirement engineering methods are analyzed. The framework for Privacy-Friendly Systems Design (PFSD) is a methodology that aims to incorporate privacy into a software development process through three steps [19]:

- Elicit privacy-related goals;
- Analyze the impact of privacy goals on the process; and
- Identify the techniques that best support/implement the aforementioned process.

According to [A30], PFSD is not accompanied by guidelines on how to identify privacy expectations in a structured manner.

The second is LINDDUN, a privacy threat analysis framework for supporting the elicitation and fulfilment of privacy requirements [20]. And the third is the PriS method, which aims to integrate privacy requirements into the early stages of the design process by modelling privacy requirements as organizational goals [19].

Diamantopoulou et al. [A29] claim that moving from a design (in which the privacy requirements of an information system have been elicited) to an implementation that fulfils those requirements is a challenging task in the context of PbD. It can be observed that the integration of PbD into the software development process must include almost all of its phases [A23] [A25].

Furthermore, and with regard to the project management activities, Ali [A31] mentions that negotiation and agreements with the clients should be made by: “Obtaining explicit consent”, “Maintaining privacy audit trails”, “Creating and maintaining privacy policies”, and “Privacy negotiation”.

Martín [A5] suggests gathering stakeholders from different communities and defining a collection of roles that are involved in the provision of privacy requirements. In addition, [A5] emphasizes the need to identify, analyze and structure privacy requirements from the requirements specification phase.

With regard to the software development activities, in [A4], an extension to UML Use Case diagram is proposed, which implies that privacy restrictions should still be dealt with at the requirements specification stage.

As expected, in the majority of the papers PbD is included in the design and construction phase by, as stated in [A28] and [A32], embedding “privacy proactively in the design process”; “heightening sensitivity to privacy issues during design” [A1]; applying privacy patterns has been identified as a feasible way in which to support the design of such systems [A29] [A33]. An architectural model based on access control policies is proposed in [A34], and this approach is also implemented at the design phase.

In the case of software verification and validation phase, Oetzel and Spiekermann [A35] present a six-step privacy assessment methodology that could be useful as regards validating how systems manage privacy requirements. In [A12] a set of guidelines that incorporate PbD principles in order to guide software engineers in the systematic assessment of the privacy capabilities of IoT applications and platforms is presented.

However, the authors of [A21] establish that “a comprehensive approach for privacy requirement engineering, implementation, and verification is largely missing”, which emphasizes the lack of privacy support in the development process as a whole.

4 Discussion

Our study revealed that the objective of PbD is, according to [A18], to ensure privacy and gain personal control over one's information and, for organizations, to gain a sustainable competitive advantage. We also determined that organizations are forced to deal with data privacy in order to comply with national and international legislation and perceive it as an obligation rather than an advantage for their business and clients.

As can be observed in the results shown in the previous section, on the one hand, the issue of data privacy involves developers, stakeholders and users. On the other, in the majority of cases, it involves discussing questions concerning social privacy rights rather than applying and following best practices and standards.

PbD has not yet been established as either a widespread approach or as a widespread engineering practice [A2]. In addition, most of the proposed methodologies target the treatment of privacy during construction or during early design activities, while none treats privacy as a separate design criterion [19]. Moreover, PbD in itself lacks concrete tools to help software developers design and implement privacy friendly systems. It also lacks clear guidelines regarding how to map specific legal data protection requirements onto system requirements [A6].

Moreover, *minimize the collection and access to data* is the most frequent goal. This goal can be paraphrased as *do not collect or store data that is not needed or will not be used*.

If we analyze the practices that were found during the SMS, it will be noted that they are not yet best practices but rather suggestions and pieces of advice in order to facilitate or comply with data privacy requirements, which denotes that the status of including PbD in the software development process is still preliminary.

We consider that PbD is in its initial stage; its foundations and principles are in the process of being established and a former set of practices, whose intention to follow the principles, has been proposed recently. The next step for PbD is to create more practices and prove their usefulness and applicability in software developments.

In this scenario, we firmly believe that it is important to integrate best PbD practices into software development processes. The objective of this integration is to strengthen systems that are and will be developed by organizations. In addition, it will unify the best practices that guide the software development with PbD, which will, in turn, protect the privacy of sensitive data in the current ever-growing systems.

A first step towards this goal is to integrate PbD practices into particular process models, for example, the ISO/IEC 29110 Software Implementation process. Another example is to create a set of interrelated PbD practices adding a new profile.

4.1 Validity threats

A SMS protocol was built to address the selection bias. Search terms were identified based on influential papers in the field. Given that privacy requirements are treated in a narrow perspective as security requirements [13], and to determine the extent privacy is addressed in SE literature, we focused only on the perspective of "privacy by design" proposed by Cavoukian since it is recognized as an approach to address privacy in software systems [A5].

Databases used in this review are recommended for conducting mapping studies in software engineering [17] and only peer-reviewed articles, including conference proceedings that belong to grey literature [21], were selected. Since sound empirical studies about practices on software engineering were lacking, a literature review that considers both peer-reviewed and grey literature would provide a comprehensive view of issues that practitioners face [22]. In addition, snowballing procedures should be applied to enhance the completeness of the search process [17].

Human error is another aspect that can impact any paper selection. Thus, search and selection procedures were kept in a log to avoid potential issues. Two authors participated in selecting primary papers, while a third verified the selection of a subset of primary papers. Selection inconsistencies were discussed among all researchers. Finally, a template was built to extract verbatim data from each primary paper. The extraction data was verified by the third and fourth authors in a subset of selected primary papers. Obtained data let us develop a classification approach, derived from data, to aggregate data in order to answer the research questions.

5 Conclusions and future work

This paper presents a mapping study that has been conducted in order to determine the State of the Art as regards PbD in software development. –We found little support for embed privacy during software development. Majority of proposals deal with privacy requirements, but they lack of methodological support for dealing with all stages of software development.

We perceived in the results of the SMS that the two types of systems that appeared more frequently in the primary results were social networks and health-care systems. Further research focused on the empirical results of using PbD practices or techniques in industry is needed in order to provide an idea of the real presence of practices in industry.

Moreover, PbD is related not only to developing systems, but also to processes and physical features [23], signifying that privacy regulations and laws oriented toward information systems should be created and disseminated between users and the developers' community. We believe that a well-informed community will create a better understanding of the fact that considering privacy in the whole development process as an inherit aspect, rather than a characteristic, brings a direct benefit to the system.

As a further work, we propose to develop a conceptual framework to address both privacy concerns and provide support for developing privacy-aware systems. In addition, practices for incorporating privacy into software system should be surveyed in companies to identify those practices considered most relevant in the context of privacy. Moreover, a validation of these proposals should be carried out in industrial settings.

Acknowledgements

This work has been developed within the SEQUOIA Project, funded by Fondo Europeo de Desarrollo Regional FEDER and (Ministerio de Economía y Competitividad, (TIN2015-63502-C3-1-R) (MINECO/FEDER).

The authors would like thank the Postgraduate Program of the Medical Faculty (DEP-FM) at the National Autonomous University of Mexico (UNAM).

References

1. Warren, S. and Brandeis, L.: *The Right to Privacy*. Harvard Law Review, Vol. 4, No. 5, pp. 193-220 (1890)
2. Altman, I.: *Privacy: A Conceptual Analysis*. Environment and Behavior, Vol. 8, No. 1, pp.: 7-29 (1976)
3. Nissenbaum, H.: *Privacy in Context: technology, Policy, and the Integrity of Social Life*. Stanford University Press, ISBN: 978-0-8047-5236-7 (2010)
4. Palen, L. and Dourish, P.: *Unpacking "Privacy" for a Networked World*. In Proceedings of CHI, ACM, Ft. Lauderdale, Florida, USA, ISBN: 1-58113-630-7/03/0004 (2003)
5. Hildebrandt, M. and Koops, B-J.: *The challenges of ambient law and legal protection in the profiling era*. Mod Law Rev 73(3):428–460 (2010)
6. Cavoukian, A.: *Privacy by Design: The 7 Foundational Principles*. Information and Privacy Commissioner of Ontario (2009)
7. Klitou, D.: *Privacy-Invading Technologies and Privacy by Design*. Information Technology and Law Series, Vol. 25, pp 27-45, 978-94-6265-026-8 (2014)
8. Cavoukian A.: Privacy by Design: Leadership, Methods, and Results. In: Gutwirth S., Leenes R., de Hert P., Poullet Y. (eds) European Data Protection: Coming of Age. Springer, Dordrecht, pp. 175-202 (2013)
9. Cavoukian, A.: *Operationalizing privacy by design: A guide to implementing strong privacy practices*. Information and Privacy Commissioner, Ontario, Canada. Retrieved on Dec, 6, 2017 from: http://www.ontla.on.ca/library/repository/mon/26012/320221.pdf (2012)
10. Loukil, F., Ghedira-Guegan, C., Benharkat, A. N., Boukadi, K., and Maamar, Z.: *Privacy-Aware in the IoT Applications: A Systematic Literature Review*. In OTM Confederated International Conferences" On the Move to Meaningful Internet Systems" (pp. 552-569). Springer, Cham (2017)
11. Hansen M.: *Top 10 Mistakes in System Design from a Privacy Perspective and Privacy Protection Goals*. In: Camenisch J., Crispo B., Fischer-Hübner S., Leenes R., Russello G. (eds) Privacy and Identity Management for Life. Privacy and Identity 2011. IFIP Advances in Information and Communication Technology, Vol. 375, pp. 14-31 (2012)
12. Meis, R., and Heisel, M.: *Computer-Aided Identification and Validation of Intervenability Requirements*. Information, Vol. 8, No. 1, 30 (2017)
13. Gharib M., Giorgini P. and Mylopoulos J.: *Towards an Ontology for Privacy Requirements via a Systematic Literature Review*. In: Mayr H., Guizzardi G., Ma H., Pastor O. (eds) Conceptual Modeling. ER 2017. Lecture Notes in Computer Science, Vol. 10650, pp. 193-208 (2017)
14. Azarm-Daigle, M., Kuziemsky, C. and Peyton, L.: *A Review of Cross-Organizational Healthcare Data Sharing*. Procedia Computer Science, Vol. 63, pp. 425-432, DOI: https://doi.org/10.1016/j.procs.2015.08.363 (2015)
15. Sajid, A. and Abbas, H.: *Data Privacy in Cloud-assisted Healthcare Systems: State of the Art and Future Challenges*. Journal of Medical Systems archive, Vol. 40, No. 6, pp. 1-16, DOI: 10.1007/s10916-016-0509-2 (2016)
16. Rahim, F., Ismail, Z. and Samy, G.: *Privacy Challenges in Electronic Medical Records: A Systematic Review*. In Proceedings of the Knowledge Management International Conference (KMICe) 2014, pp. 12-15 (2014)

17. Petersen, K., Vakkalanka, S. and Kuzniarz, L.: *Guidelines for conducting systematic mapping studies in software engineering: An update*. Information and Software Technology, Vol. 64, pp. 1-18, (2015)
18. Kitchenham, B.A. and Charters, S.: *Guidelines for Performing Systematic Literature Reviews in Software Engineering*. Technical Report EBSE-2007- 01, School of Computer Science and Mathematics, Keele University (2007)
19. Kalloniatis, C., Kavakli, E. and Gritzalis, S.: *Addressing privacy requirements in system design: the PriS method*. Requirements Eng. 13(3), 241–255 (2008)
20. Deng, M., Wuyts, K., Scandariato, R., Preneel, B. and Joosen, W.: *A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements*. Requirements Eng. Vol. 16, No. 1, pp. 3–32 (2011)
21. Adams, R.J., Smart, P. and Huff, A.S.: *Shades of Grey: Guidelines for Working with the Grey Literature in Systematic Reviews for Management and Organizational Studies*. International Journal of Management Reviews, Vol. 19, pp. 432-454, doi:10.1111/ijmr.12102 (2017)
22. Garousi, V., Felderer, M. and Mäntylä, M.: *The need for multivocal literature reviews in software engineering: complementing systematic literature reviews with grey literature*. In Proceedings of the 20th International Conference on Evaluation and Assessment in Software Engineering (EASE), 26 (2016)
23. Schartum, D.: *Making privacy by design operative*. International Journal of Law and Information Technology, No. 24, 151–175, DOI: 10.1093/ijlit/eaw002 (2016)