The privacy aware transmission highway framework

Alfredo Pérez Fernández* and Guttorm Sindre

Department of Computer Science,
Norwegian University of Science and Technology,
NO-7491 Trondheim, Norway
Email: alfredo.perez.fernandez@ntnu.no
Email: guttorm.sindre@ntnu.no
*Corresponding author

Comment [P1]: Author: Please confirm if A.P. Fernández is the corresponding author.

Abstract: Handling users' privacy in ubiquitous systems is a difficult challenge. Many frameworks have been proposed to analyse the problems of privacy in a world with computers resembling typewriters. However, as the world evolves towards a proliferation of invisible computers, we see that the classical approaches are insufficient. Designers and developers need tools to help them better understand how to mitigate privacy threats in such complex systems. In our approach, the *privacy aware transmission highway* (PATH) framework, we address privacy threats originated as the result of the interaction between users and ubiquitous computing systems. We analyse the reasons why these privacy threats occur and propose a method to decompose the complex and abstract problem of privacy into more manageable sub-problems. An evaluation has been conducted with experts and students to validate the applicability of the framework.

Keywords: privacy, privacy-by-design, ubiquitous computing, HCI, PATH framework, evaluation process, design science research.

Reference to this paper should be made as follows: ~~Fernández, A.P.,~~ and Sindre, G. (xxxx) 'The privacy aware transmission highway framework', *Int. J. Information Privacy, Security and Integrity*, Vol. X, No. Y, pp.xxx–xxx.

Biographical notes:

Comment [P2]: Author: Please provide the biographical details of each author (not more than 100 words for each author).

~~This paper is a revised and expanded version of a paper entitled [title] presented at [name, location and date of conference].~~

Comment [t3]: Author: If a previous version of your paper has originally been presented at a conference please complete the statement to this effect or delete if not applicable.

1 Introduction

Privacy was early defined as "the right to be left alone" [Warren and Brandeis, (1890), p.205], and later as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" [Westin, (1967), p.7]. It is an important aspect of life in society that has quickly become more relevant due to the evolution into the *information society* (Introna, 1997). Several reasons are given for the importance of privacy by Rachels (1975), generally because the person whose information is exposed is put at disadvantage in a competitive environment. However, an important aspect not mentioned by Rachels is that individuals can also benefit from providing as much information as possible if the society is highly collaborative (Lunheim and Sindre, 1993). It is difficult to determine whether an environment is mainly collaborative or competitive, or rather somewhere in between, and in such cases it seems convenient to apply the principle of proportionality proposed by Iachello and Abowd (2005), judging the adequacy of the personal information exposure based on the proportional benefit obtained by the individual being exposed, or rephrased with the words of Palen and Dourish (2003, p.131) "the goal of privacy regulation is to modify and optimise behaviours for the situation to achieve the desired state along the spectrum of openness and closeness." In any case, trying to provide an adequate definition of privacy is a hard task and it should be done with a clear purpose in mind, since privacy issues "are fundamentally matters of values, interests, and power" [Gellman, (1997), p.194].

When designing and implementing ubiquitous computing applications (Lyytinen and Yoo, 2002), privacy related requirements are normally de-prioritised in favour of functional requirements. Developers consider it more important to implement a system that is working than one that is privacy-friendly. In the cases where privacy is taken into consideration, it is done only "ad hoc and specific to the system at hand" (Langheinrich, 2001). Even if the system designers and developers of these systems had privacy as a main focus, this task is complex enough to require a proper methodology.

In Section 2 of this paper, we provide an overall problem definition, justifying the importance of understanding privacy concerns in interactive ubiquitous computing systems. Section 3 discusses related work. Our proposed framework is presented in Section 4. The methods used to evaluate the framework with experts and students are described in Section 5. Finally, Section 6 provides some concluding remarks.

2 Problem definition

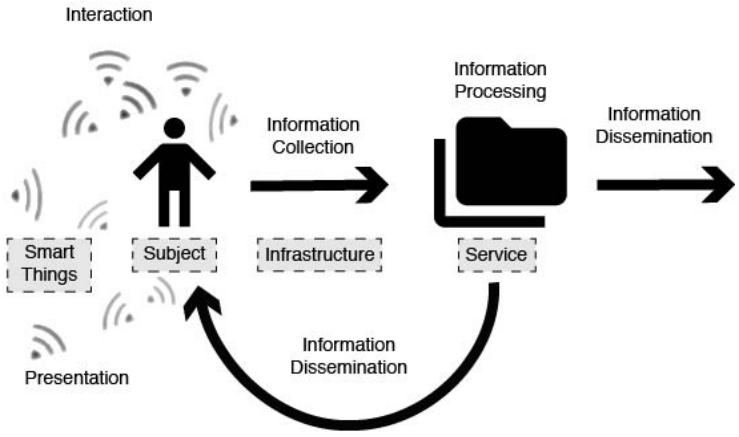
Improvements in technology allow flows of information that were impossible before. In 2003, the organisation *Consumers Against Supermarket Privacy Invasion and Numbering* (CASPIAN) called for a worldwide boycott against the razor manufacturer Gillette and the fashion firm Benetton, supposedly for using *RFID* to unobtrusively track customers behaviour (Ismail, 2009). The computer magazine PCWorld (2011) published an article in June 2011 warning mobile phone users about how scanning a malicious QR code could lead to disclosure of personal information. On December 2014, the Bluetooth Special Interest Group (SIG, 2014) released the core specification version 4.2 with support for the anonymisation of the Bluetooth MAC address as a mechanism to protect users' privacy at the link layer. Also on December 2014, Jan Krissler (a hacker from the Chaos

Computing Club) managed to clone the fingerprints of Ursula von der Leyen (The German Defence Minister) by processing pictures of her fingers (Kleinman, 2014). From Autumn 2012, the Norwegian chain store Bunnpris started using fingerprints at their stores as a way to prevent selling alcohol or cigarettes to minors, which initiated a dispute between the firm and the data protection inspector about the necessity of using biometrics for this purpose (Kisku et al., 2013).

These are a few examples that illustrate the relation between privacy concerns and ubiquitous computing. These concerns do not affect only the end users. Due to the incorporation of the General Data Protection Regulation (GDPR) in the European regulation, organisations that collect or process any personal information from EU residents, are required to apply *Privacy-by-design* (Cavoukian, 2009) as an integral part of their process model (Colesky et al., 2016) even if the term is still abstract and difficult to operate (Rubinstein and Good, 2013). This requirement also applies to developers of ubiquitous computing systems. This means that the efforts in protecting privacy should shift from *data protection* (DP) techniques towards *personal privacy* (PP) like *data minimisation*.

The reference model proposed by Ziegeldorf et al. (2014) (Figure 1) can be used to understand the implications of the new regulations in ubiquitous computing. Minimising the usage of data must take place in the *interaction phase*, before information is collected.

Figure 1 Adapted from the reference model for information flow in ubiquitous computing proposed by Ziegeldorf et al. (2014)



Ubiquitous computing system developers need conceptual models, process frameworks, and tools to understand the complexities of user interactions in ubiquitous computing systems and how these interactions impact users' privacy [Hachello, (2005), p.5].

The research question for this paper is: *What framework can be elaborated to assist a privacy-by-design process of ubiquitous systems at the interaction level?* To answer this question, we have opted to apply a design science research methodology (DSRM) (Peffers et al., 2007). The main motivation for applying DSRM is that our intention was to provide an answer to the research question in the form of an artefact (a framework). Our DSRM has a problem-centred initiation and aims at providing a better understanding of the privacy implications of the interaction in ubiquitous computing.

Comment [P4]: Author: Please be informed that Figure 2.1 was changed to Figure 1. The succeeding figures have been renumbered as well.

Comment [P5]: Author: Please be informed that Figure 2.1 was changed to Figure 1. The succeeding figures have been renumbered as well.

Comment [P6]: Author: Please provide full reference or delete from the text if not required.

3 Related work

There are several proposed frameworks and guidelines for the development of privacy-friendly information systems. Each of them has a trade-off between several needs in order to fit the purpose within the scope of the problem it was aiming to solve.

Probably the most well known of these frameworks is the fair information practices (FIPS) which has been widely applied in the industry for the development of systems that had as a main purpose the large-scale storage of sensitive personal information (Gellman, 2017). Bellotti and Sellen (1993) proposed an adaptation of the questions options criteria (QOC) (MacLean et al., 1991) to address the privacy threats that would be present in the RAVE media space. Another, more procedural, framework for the analysis and evaluation of systems is STRAP [Jensen et al., (2005), p.4] which has a different iterative approach compared to the others and focuses on the requirements related workflow. The approximate information flow framework proposed by Jiang et al. (2002) applies different concepts from economics and information theory to model the exchange of information among the actors (data owners, data collectors and data users) to minimise the asymmetry of information flow among them. Other authors propose a privacy-by-architecture approach. One example is the privacy awareness system (PawS) architecture (Langheinrich, 2001). PawS is an implementation of the FIPS and proposes the utilisation of privacy beacons as a helper mechanism to provide privacy policies for the interaction with services proxies from the user client. Other architectures that consider the privacy aspects in ubiquitous systems include the aura project (Garlan et al., 2002) and the home media space (HMS) privacy project (Neustaedter and Greenberg, 2003). Thomas et al. (2014) propose both a framework (privacy facets, or PriF) and a process (the privacy requirements distillation process) to elaborate the list of privacy requirements for the software development of a mobile app. There are some disadvantages of this proposal, including the complexity of the process when it comes to use it in real case scenarios, and the need for an initial phase of elaboration of qualitative user data. Spiekermann and Cranor (2009) provide an interesting model, the three-layer responsibility framework, which helps identifying the areas in which an engineer needs to focus when developing different types of systems. Corcoran (2016) elaborated an extension of Spiekermann and Cranor's framework after broadening its scope by applying the definitions of privacy from Finn et al. (2013).

These frameworks and architectures make an in depth analysis of privacy in different specified scenarios and at different levels.

One way of classifying these frameworks has been introduced by Iachello and Hong (2007) considering their characteristics, such as the *type* (guideline, process framework or modelling framework), *scope* (*general*, *specific*), *purpose* (*data protection* vs. *personal privacy*), *motivation* (*principled* vs. *communitarian*), *advantages* and *disadvantages* (for example, if the framework is difficult to use or not) (Table 1). All the frameworks proposed by Iachello plus eight other frameworks that we found relevant were evaluated in terms of their adequacy in the ambit of privacy in ubiquitous computing systems. As part of our research process and, following the DSRM, we observed that tasks such as performing a goal oriented analysis (GOA) or cost estimation have a positive impact on how effectively they can address privacy threats during the design and development of such systems. Additionally, understanding the development process that was followed in order to elaborate the different frameworks is interesting in the sense that it can be useful to compare them in terms of completeness and limitations.

Table 1 Frameworks comparison table

	Name	*Scope*	*GOA*	*Cost*	*DP/PP*	*Princ./comm*	*Advantages*	*Disadvantages*	*Elaboration*	*Reference*
Guidelines	FIPS	Basic personal data	no	no	DP	Principled	Simple popular	System-centred. Not applicable for personal privacy	Based on experience	Gellman (2017)
	FIPS for RFID	Specific to RFID	no	no	PP	Principled	Simple and specific	Too much focus on RFID	Framework extension	Garfinkel (2002)
	Design patterns	Ubiquitous computing	no	no	PP	Principled	Easy to learn	Mismatch with design	Pattern language (Alexander, 1979)	Junestrand et al. (2001) and Chung et al. (2004)
Process frameworks	UC guidelines	Ubicomp	no	no	Neutral	Principled	Simple popular	Too generic	Adapted from FIPS	Langheinrich (2001)
	QOC	Questions and criteria for evaluating designs	no	no	PP	Principled	Simple	Limited to VMS systems	Adapted from (MacLean et al., 1991)	Bellotti and Sellen (1993)
	Risk analysis	Ubiquitous computing	no	yes.	Neutral	Communitarian	Clear checklists	Difficult to evaluate risk	Adapted from (Hand, 1947)	Hong et al. (2004)
	Interface analysis	Web applications	no	no	DP	Principled	Good rationale	Complex to apply	Applied (~~Wickens, 1992~~)	Patrick and Kenny (2003)
	Proportionality	Value/prop balanced with privacy risk	no	no	Neutral	Communitarian	Lightweight. Used in related communities. Explicit balance	Demands in-depth analysis	Inspired on data protection principles.	Iachello and Abowd (2005)
	STRAP	Privacy analysis based on goal analysis	yes	no	Neutral	Neutral	Lightweight	Goal-driven May ignore non-functional issues	Combination/ adaptation of frameworks	Jensen et al. (2005)
Modelling	PnF	Mobile apps	no	no	PP	Communitarian	Structured and detailed	Needs obtention of qualitative data. Complex to use	Experience supported with theories	Thomas et al. (2014)
	PIA	Privacy impact assessment	no	no	Neutral	Principled	Promotes communication, adaptable to different organisation sizes	Too generic. It requires significant resources	Experience	Okoye (2017)
	APSIDAL	Operationalised GDPR	no	no	PP	Principled	Methodic and focused on GDPR	Too generic, it requires significant resources	DSRM	ElShekeil and Laoyookhong (2017)
	AIF	Model of information flows	no	no	DP	Principled	Comprehensive framework	Frail assumptions Incompatible with data protection law	Adapted from OM-AM	Jiang et al. (2002)
	Interaction model	Ubiquitous computing	no	no	DP	Principled	Accurate and realistic	Only descriptive, not process and highly generic	Extended from (Altmann, 1975)	Lehikoinen et al. (2008)
	Three-layer responsibility	General model	no	no	Neutral	Principled	Simple and practical	Highly generic	Based on experience	~~Spiekermann (2009)~~
	IoT framework	Internet of things	no	no	Neutral	Principled	Simple and Broad	Only descriptive, not process	Spiekermann and Cranor (2009)	Corcoran (2016)

Notes: ■ = extended by the authors, GOA = goal oriented analysis, Cost = cost estimation, DD = data protection, PP = personal privacy.

Comment [P7]: Author: Please provide full reference of Spiekermann (2009) or delete from the text if not required.

For these reasons, the original comparison table by Iachello and Hong (2007) has been extended with three new columns:

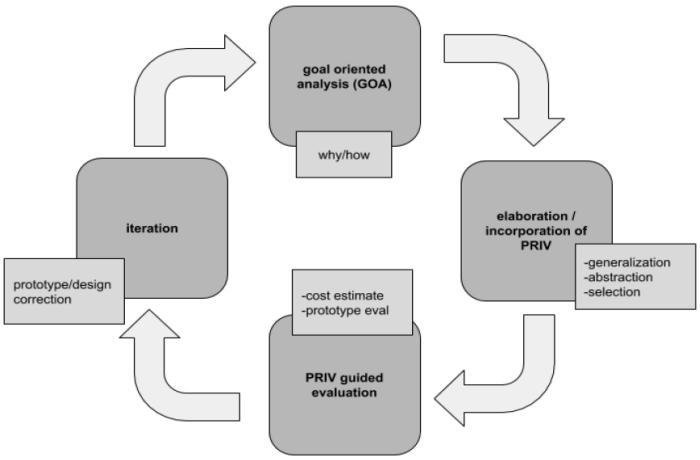
- *GOA based:* if the framework proposes a GOA during the development process.
- *Cost estimation method:* if the framework proposes a method to estimate the costs of developing or compensating the impact on users' privacy by the system.
- *Development process:* what process was followed to obtain the framework? This could be based on *experience* (applying lessons learned and mistakes while developing systems and applications that have exposed the privacy of the users), *extension* (use an already existing framework as a starting point and adapt it to the privacy domain), *methodical process* (apply an already existing framework or process to obtain the resulting framework in a systematic way).

None of the frameworks address in detail the impact of ubiquitous interactions on users' privacy. Rather, they focus on more traditional systems where data is explicitly provided by input, rather than sometimes harvested automatically. With the advent of ubiquitous computing and big data, it is important to cover also the latter, which is the purpose of this paper. Thus, the next section will present a framework that also takes systems with ubiquitous data harvesting into account.

4 The PATH framework

We propose a process framework to guide the stages of development of interactive ubiquitous computing applications. We consider that this framework needs to be iterative and adapted to the different phases of the software development lifecycle. According to Jensen et al. (2005), "changes to one part of a system's design may affect multiple other parts in terms of privacy." Our framework consists of four iterative steps: GOA; privacy related interaction vocabulary (PRIV) elaboration and PRIV guided evaluation and iteration (Figure 2). These phases are described in Sections 4.1 to 4.4.

Figure 2 The PATH framework



4.1 Goal-oriented analysis

One of the most significant observations from our evaluations, also supported by literature, is the high probability of introducing over-specifications in the system during the design or development process of the system (Shmueli et al., 2015). Over-specification are a type of cognitive-bias (Mohanani et al., 2017) caused by an emotional or irrational attachment or preference for one specific alternative over other alternatives that might be more suitable or that might be less privacy intrusive.

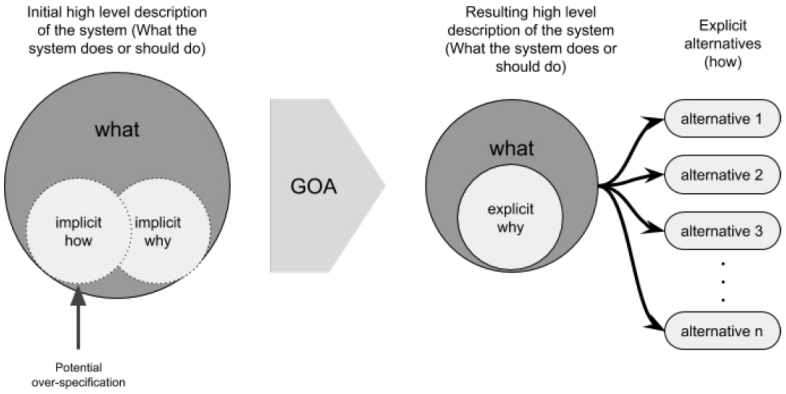
Dealing with over-specification is a challenging problem because "in general, cognitive biases do not disappear just because people know about them." [Stacy and MacMillan, (1995), p.62] and de-biasing can be either ineffective or too expensive (Mohanani et al., 2017). De-biasing is somewhat easier when the process promotes it, for example, as planning poker promotes the minimisation of biased estimation (Haugen, 2006). Performing GOA helps preventing system over-specifications by forcing engineers to move from the traditional way of thinking of what the system should do towards how and how-else (Yu and Mylopoulos, 1998) and, even more important, why the system should do that. This can help preventing over-specifications because a requirement that is not derived from a justified why can be questioned as valid. The majority of the analysed privacy frameworks do not consider the incorporation of a GOA phase in the development process. One exception is the STRAP framework (Jensen et al., 2005), that recommends the use of a Goal analysis method like ScenIC (Potts, 1999) or GRAIL/KAOS (Darimont et al., 1997). Kalloniatis et al. (2008) take one step further and propose a method to identify technological solutions to privacy vulnerabilities during the implementation phase. The problem with such methods is that they strongly rely on formal textual representations of the requirements making it less convenient for agile processes. Our proposal is to apply a simplified GOA (Figure 3) at a higher level, and more focused on the interaction mechanism. The simplified GOA phase is applied over a high level description of the system (normally provided by the stakeholders to the system developers). This description of *what* the system is supposed to do contains, implicitly, a motivation of *why* the system needs to be developed (e.g., raise profits or improve the performance of an already existing system). There is a possibility that the high level description imposes an unjustified limitation on *how* the system should be implemented which can lead to the introduction of *over-specifications* in the system requirements (examples of over-specifications in ubiquitous computing are imposition of certain interaction mechanisms like RFID, QR codes or fingerprint readers). The simplified GOA phase consists of modifying the high-level description so that the motivation is made explicit and the implementation details are presented in a separate document with a list of alternatives.

A benefit of keeping the analysis at a higher level is that it can be used in early stages of conceptualisation, before there is a more formalised list of requirements. Maintaining the focus of analysis on the interaction mechanism allows the simplification of the GOA into a two-level hierarchy without requiring identifying obstacles, objectives, tasks, and actors as proposed in ScenIC. The output of the GOA should be a more refined description of the system and a list of alternatives that can be subsequently evaluated.

In many cases, the whole project is driven by the development of one specific interaction mechanism, without having a unique user-centred scenario to guide the process. This type of project can be identified if the initial GOA results in a high level description of the project that contains a highly defined *explicit-how* and an ambiguous,

unspecific or unclear *explicit-why*. In such cases it is important to identify the reasons why that alternative is the only possibility (for example*: required by a stakeholder*, *reduced cost* or *already familiar to the development team*). For technology-centred design projects, it is necessary to guide the process with one (or more) user-centred scenarios, since the problem of privacy is fundamentally user-centred (Iachello and Abowd, 2005) (Section 3.4).

Figure 3 Lightweight GOA, (a) implicit decisions on the initial system description are made explicit and (b) alternatives found



(a) (b)

4.2 Elaboration of the PRIV

Privacy is a highly complex and multidimensional construct. To facilitate the management of privacy in the development of ubiquitous systems, it is necessary to divide it into more manageable and understandable sub-problems. Our proposal is to do this by identifying the attributes of the interaction mechanisms that have a potential impact on users' privacy. Making use of a PRIV has a number of advantages that can be grouped into three categories: *communication*, *evaluation* and *composition.*

- *Communication:* sharing a common vocabulary across development team members helps reducing ambiguity during the discussions about the suitability of a specific interaction mechanism in a project. There is no restriction on how abstract a term should be.
- *Evaluation: t*he evaluation of the suitability of an interaction mechanism can be divided into the evaluation of each of its attributes separately. For example, the intentionality (Table 2) can be estimated by performing surveys during the conceptualisation phase and, when a prototype is available, a user test can be performed with real users applying the perceived control (PC) (Spiekermann, 2005) extension of the technology acceptance model (TAM) (Venkatesh, 2000).
- *Composition: i*f an interaction mechanism is found to be unsuitable to the project due to one or more of its attributes, it can be replaced or combined with other interaction mechanisms that do not have that limitation.

Table 2 Proposed initial PRIV

Term	*Question for practitioners*	*Description*
		Customer attributes (CA)
Intentionality	Can the interaction take place if the user does not intend it?	Describes the degree of consciousness and willingness that is required for the interaction to take place. As an example, the exchange of information through a barcode or QR code is much less likely to happen if there is not an intention from the user than with RFID or NFC. Interaction mechanisms with a lower degree of intentionality have a higher probability of impacting users' privacy negatively (Spiekermann and Cranor, 2009).
Visibility	Does the user see that the interaction happened or will happen?	The term visibility is a pragmatic simplification of a more general and complex concept: perceivability. Before and after the interaction takes place, the user might or might not (in the case of unintentional interactions) perceive that the interaction is possible or what is the result of that interaction. The degree of visibility of an interaction mechanism in ubiquitous computing is a trade-off between the requirement of invisibility (Weiser and Brown, 1997) and the requirement of providing notice of the activities of the system (Gellman, 2017). This term is related to the definition of unobtrusiveness proposed by Langheinrich (2005).
Precision	Is the information precise?	As Langheinrich (2005) indicates, a higher "level of detail" of an interaction has a higher probability of impacting negatively in the users privacy. An example would be a fall detection system (Noury et al., 2007; Mashiyama et al., 2014) (why-level) implemented with two interaction mechanisms: video capture and infrared array sensor (how-level) similar in principle but with different degrees of precision. The infrared array sensor is expected to have a lower negative impact than video processing in the users privacy.
Understandability	Is the interaction easy to understand or to use?	A larger deviation between the users' mental model with respect to its actual behaviour leads to a higher probability of a negative impact in the users' privacy (Liginlal et al., 2009). This is regardless of the perceived ease-of-use. A user might find an RFID card easy to use while having a mistaken idea of what information it contains.

Table 2 Proposed initial PRIV (continued)

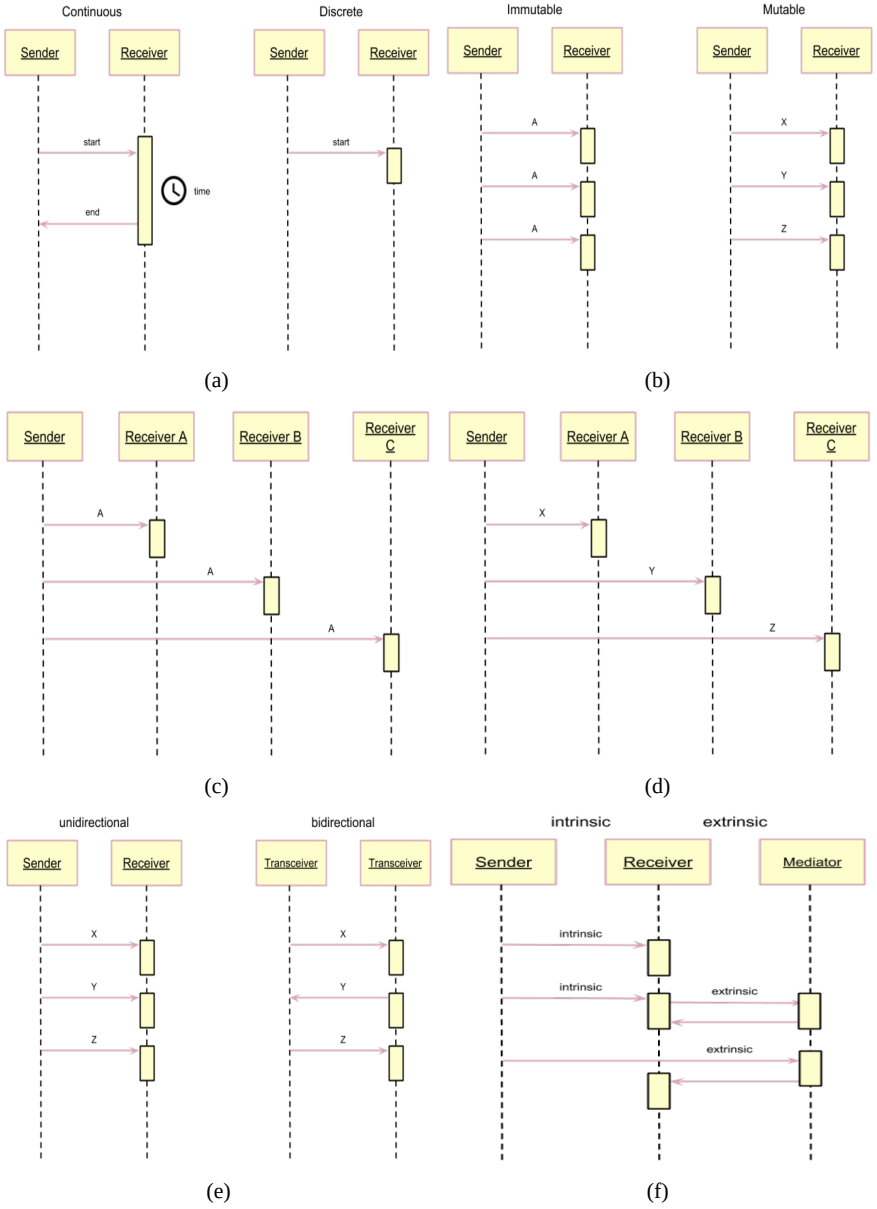
Term	*Question for practitioners*	*Description*
		Non-customer attributes (NCA)
Continuity	Is it possible for the system to measure how long the interaction is taking?	Specifies whether the interaction takes place only at a specific point in time (discrete) or instead it has a clear beginning and end (continuous). A location based system with real-time tracking (Schiller and Voisard, 2004) (Chapter 1) (continuous interaction) captures information about where the user is and for how long, while a system that notifies only about changes in the location within specific conditions (discrete interaction) does not reveal the duration. The continuity attribute of an interaction mechanism can also be exploited to impact positively in the users' privacy if it is used for example to terminate an ongoing session and hide personal information (Fernández and Sindre, 2014).
Mutability	Does the transmitted information change or is it always the same?	Specifies the capability of the interaction mechanism to modify the information that is transmitted. An example of typical immutable interaction mechanism is the use of different forms of biometrics such as fingerprints or retina. An RFID tag, on the other hand, has a higher degree of mutability. It is possible to implement a mechanism for identification obfuscation such as Variable MetaID's to prevent traceability (Weis et al., 2004). Immutable interaction mechanisms are subject to become an identifier of the user on mobile or wearable devices (i.e., mac address)
Segmentation	Is it possible to send different parts (segments) of information to different receivers or is it always the same?	Describes the possibility of the interaction mechanism to divide the information into smaller segments of information. This is a generalisation of more concrete cases of segmentation like speech segmentation (Adriaans, 2011) o r image segmentation (Chouhan et al., 2018) into information segmentation. As an example, an ID card based on a magnetic band, most probably will only transmit the holder's ID to all the receivers. On the opposite side, an RFID or Chip based ID cards with privacy features like the european eID card (Naumann and Hogben, 2008) is able to transmit independently service related information (authorisation) or personal information (age, name and address).
Directionality	Can the information flow in both directions or only in one direction?	Specifies the possibility of the interaction mechanism to transfer information in a bi-directional or uni-directional way. Uni-directional interactions present a limitation in terms of segmentability of the information. In the example of the European eID cards, the reason why the information can be customised is because the flow is bidirectional.
Mediation	Does the transmission of information require of a third party mediator?	The nature of the communication provided by the interaction mechanism can be categorised either as intrinsic or extrinsic. The communication is intrinsic when all the information is transported using exclusively the interaction mechanism as communication channel. Opposed to this, the communication is extrinsic when it is necessary an external communication channel to transmit the information. As an example, a QR code tag that is encoding a url to a webpage would be extrinsic, but another QR code tag encoding a plain text with a message would be intrinsic. The main complication that arises when analysing privacy implications is that it becomes necessary to analyse the privacy threats that could be incorporated to the system by the external channel.

The elaboration of the *PRIV* is a complex task and requires previous experience working with different types of interaction mechanisms, an unbiased mind-set with special focus on privacy and a good capability for generalisation and abstract thinking. Our observations show that it requires less effort for practitioners to decide if a term is applicable to their system and interaction mechanisms than to identify a new term themselves. For this reason, our framework proposes the use of an initial PRIV (Table 2) with a list of terms that have been identified through the iterations of analysis of our case studies and with the incorporation of feedback from the literature. These attributes can be grouped into *customer attributes* (CA) and *non-customer attributes* (NCA) (Chung and do Prado Leite, 2009) depending on whether they are easily identified and perceived by an end user or not.

The NCA are more difficult to understand only with a textual description. For this reason, we found it convenient to use sequence diagrams to illustrate the concepts. These diagrams are schematic representations proposed as part of the unified modelling language (UML) Specification as a mechanism to simplify the description of behavioural aspects of the interactions (http://www.omg.org/spec/UML/2.4.1/Superstructure/PDF/). (Figure 4) shows an example of the sequence diagrams for each of the five NCA:

- *Continuity* [Figure 4(a)]: the diagram on the left indicates that the interaction mechanism permits the system to determine the ending of the interaction, meaning that the interaction mechanism is continuous. The diagram on the right indicates that the start of the interaction can be determined but not the end, meaning that the interaction mechanism is discrete.
- *Mutability* [Figure 4(b)]: the diagram on the left indicates that the information sent by the interaction mechanism never changes, meaning that the interaction mechanism is immutable. The diagram on the right indicates that the information transmitted by the sender can be different in different transmissions, meaning that the interaction mechanism is mutable.
- *Segmentation* [Figure 4(c–d)]: Figure 4(c) indicates that the information transmitted by the sender is the same independently of the receiver, meaning that the interaction mechanism has a low segmentation. Figure 4(d) indicates that the information transmitted by the sender can be different depending on the receiver, meaning that the interaction mechanism has a high segmentation.
- *Directionality* [Figure 4(e)]: the diagram on the left represents the interaction between a sender and a receiver where the information flows only in one direction, meaning that the interaction mechanism is unidirectional. The diagram on the right represents an interaction mechanism that permits a bidirectional transmission of information. In this case, sender and receiver can be referred to as transceivers, since both can transmit and receive information.
- *Mediation* [Figure 4(f)]: this diagram represents the two different types of interaction with respect to the mediation aspect. The exchange of information between a sender and a receiver is considered intrinsic so interaction mechanisms that only support this type of information exchange are also considered intrinsic. If any information is transmitted to an external third party (mediator), be it because it is indirectly forwarded from the receiver or directly from the sender, the interaction is considered extrinsic.

Figure 4 Sequence diagrams corresponding to the NCA, (a) continuity (b) mutability (c) low segmentation (d) high segmentation (e) directionality (f) mediation (see online version for colours)



4.3 Evaluating the impact of the interaction mechanisms on users' privacy

The evaluation phase we proposed in our framework has as an objective to identify threats to users' privacy originating from the incorporation of one or more interaction mechanisms to the system. It is recommended for the development team to face the evaluation process with a critical mind-set and with an understanding of how complex privacy is (Solove, 2008). A potential pitfall is to constrain the analysis towards a convenient definition of privacy. For example, privacy definitions within *adversarial models*, i.e., that require the presence of an adversary (Hermans et al., 2011) ignore scenarios in which the system works correctly and securely but the *anonymity* or *pseudonymity* of the user is not guaranteed (Langheinrich, 2005). The privacy-friendliness of a system does not only depend on which interaction mechanism is used, it also depends of what is it used for (*application*), how is it implemented, and the situation of the user – e.g., is the user especially concerned about privacy or member of a privacy sensitive group? Any change in the design or implementation of the system can potentially introduce a privacy threat. For this reason, the evaluation has to be done in an iterative and continuous way. Cohn (2011) identifies the double nature of non-functional requirements with respect to validation: *initial compliance* (before the system or a usable prototype is present) and *ongoing compliance* (when a system is already implemented and needs to be evaluated or modified).

4.3.1 Initial compliance evaluation

When the system is in an early stage of design or conceptualisation and the implementation choices have not been set, using the *PRIV* as analytical guide has two purposes: divide the problem of privacy into more manageable sub-problems and expand conceptual alternatives in an exercise of lateral thinking. In the same way as in *planning poker* (Grenning, 2002) the team initiates a discussion of how much impact on users' privacy each interaction mechanism will have. The team does that by iterating over each attribute of each interaction mechanism. One of the simplest forms of evaluation would consists of requesting each member to provide an estimation for the impact of privacy on the system (example in Table 3).

In some cases, it might be difficult for the team to predict the impact without prior knowledge on the details of the system. In these cases, the team can start discussing the degree of each attribute as they perceive it in a scale from 1 to 5 (Table 4). Strong disagreements (*very high* values against *low* or *very low* values) in attributes estimations are interesting starting points because they can represent either a misunderstanding of the meaning of the term or a different understanding of how the interaction mechanism works. In both cases, the team has to clarify the reason and evaluate how it can impact on the project.

In Table 4 here are two types of significant disagreements. *Member 1* and *member 2* understand the term *visibility* in a different way. *Member 2* considers that NFC has a high degree of *visibility* because she thinks that the user needs to be able to see the NFC tag to exchange information with the system. *Member 1*, on the other hand, considers that the degree of *visibility* is low because NFC itself does not provide enough feedback to the user of what information has been transmitted. With respect to how the interaction mechanism works, there is also another disagreement. *Member 1* is assuming an NFC that is implemented as an RFID, meaning that the NFC tags are only capable of sending a

read only unique ID in one direction, making the interaction *immutable*, *not-segmental* and *unidirectional*. *Member 2* interprets NFC as a more flexible interaction mechanism capable of storing random pieces of information (Want, 2006).

Table 3 Example of costs estimated to remediate the impact of the interaction mechanism

Cost estimation – impact on privacy per attribute		
Application: BCC Shopping		
Interaction mechanism: Body Coupled Communication (BCC)		
Attribute	*Description*	*Estimated cost*
Intentionality	*Accidental interactions need to be prevented*	*20 hours*
Visibility		
Precision		
Understandability	*Users need to be educated on how the system works*	*40 hours*
Continuity		
Mutability		
Segmentation		
Directionality		
Mediation		

Note: The text in italics is introduced by a development team member.

Table 4 Example of result of the evaluation of NFC as an interaction mechanism for the museum visitors' tracker application performed by two different members

Attributes Estimation for Interaction Mechanism			
Application: Museum Visitors Tracker			
Interaction Mechanism: Near Field Communication (NFC)			
Attribute	*Member 1*	*Member 2*	...
Intentionality	*5*	*4*	...
Visibility	***2***	***4***	...
Precision	*4*	*4*	...
Understandability	*5*	*4*	...
Continuity	*4*	*5*	...
Mutability	***4***	***1***	...
Segmentation	***4***	***1***	...
Directionality	***4***	***1***	...
Mediation	*1*	*1*	...

Notes: Bold entries reflect a disagreement on the attributes of NFC. The text in italics is introduced by a team member.

Table 5 Evaluation of the privacy threats based on the interaction mechanism

Attribute	*Determine degree of attribute*	*Determine impact on privacy*	*Observations/potential trade-offs*
Intentionality	• TAM-PC (Spiekermann, 2005) • Observation (Mancini et al., 2009) • Field studies (Anderson and Dourish, 2005) • Conceptual models (Norman, 2013)	Higher impact on unintentional or erroneous disclosure of personal information	Ubicomp promotes low user intentionality (Weiser and Brown, 1997; Rogers, 2006; Marsden and Hollnagel, 1996). Evaluate users intentionality is complex and expensive. Requires tracking analytical data.
Visibility	• -Direct: user studies, interviews • Indirect: monitoring, sensoring, statistical analysis	Low visibility of the interaction result implies higher impact.	Requires special consideration for blind users
Precision	Margin of error: • Spatial: gps (km, m) (Lederer et al., 2003), touchscreen (cm), camera (pixels, blur radius) • Temporal: date (timestamp, day), period (fps), duration (seconds, minutes) • Identity: ambiguous, unambiguous	Low precision generally benefits users privacy	Disclosure of controversial imprecise information about the user needs to be avoided. Most designers would tend to increase the precision of their systems as much as possible.
Understandability	• -Conceptual models (Norman, 2013) • GEMS (Liginlal et al., 2009) • Questionnaires (Fernández, 2014)	Asymmetries between designer's model and user's model lead to erroneous behaviour of the user.	Evaluate users' understandability is complex and expensive. Requires tracking analytical data.
Continuity	• Technology centred evaluation: protocols, physical characteristics • User centred evaluation: statistical analysis	Continuity reveals users' session duration.	Can expose the preference of the user over a certain service, object or location if the time spent is recorded.
Mutability	• Technology centred evaluation	Immutable components of a wearable or mobile interaction mechanism can be used to identify the user (RFID, mac address, IP)	Mutability as a mechanism to promote obfuscation and pseudonymity complicates the design.
Segmentation	• -Technology centred evaluation • 'Need to know' principle • Ontology based analysis (Ye et al., 2007)	Unsegmentable interaction mechanisms (i.e. biometrics) expose collateral information (i.e. identity) (Kisku et al., 2013) (9.5.1.1)	It is more complicated to exploit the segmentability of information in unidirectional interaction mechanisms, since the information receiver needs to inform of what data is required.
Directionality	Technology centred evaluation: • -Bidirectional • Unidirectional	Directionality impacts segmentation	Bidirectional interaction mechanism increases the cost of the design.
Mediation	• Technology centred evaluation	Privacy analysis requires considering all the parts of the system involved in the mediation	Mediated interaction mechanisms simplify the design of each of them.

4.3.2 Ongoing compliance evaluation

Evaluating potential privacy threats in a system is done differently if a functional prototype is available. Each attribute of a specific interaction mechanism is evaluated applying techniques that are appropriated to the attribute (Table 5). The NCAs can be evaluated by expert developers while the CAs need to be evaluated with the participation of end-users. Since CAs are, by definition, more easily identified and perceived by the end-users, there is a possibility that a change in a CA makes users consider an interaction mechanism as privacy unsafe even when that is not the case. For this reason, CAs can be used for evaluations that are triggered by a *communitarian* motivation.

4.4 Iteration

Changes in the design and implementation are made to mitigate or eliminate the effects of the detected privacy threats. These changes can be at the conceptual level, education of the user, implementation of the interaction mechanism and selection of different interaction mechanism or composition of interactions.

5 Evaluation of the framework

As part of each iteration of our DSRM process, several groups of people, such as computer science students, researchers, ubiquitous computing developers and interaction designers have participated in workshops and evaluations, applying the framework to their own projects or given mock assignments. Apart from the feedback of these experts, the Privacy Aware Transmission Highway (PATH) framework also incorporates methods, concepts and techniques identified as useful in the analysis of privacy in other areas of application. Table 6 shows a list of projects in which usage of the PATH framework was proposed to the development team. The research methods used were: usability inspection method (UIM) (Nielsen, 1994), method evaluation model (MEM) (Moody, 2003), controlled experiment (Sjøberg et al., 2005), semi-structured interviews (DiCicco-Bloom and Crabtree, 2006) and case study research (Zainal, 2007).

It was found useful to have such variety of research methods to cover as many aspects of the framework as possible. We found this selection necessary due to the strength and weaknesses of each method:

- *UIM*: one important limitation that emerges during the empirical evaluation of a framework is to communicate all the details of the framework to the practitioner, including the steps that need to be followed and in which order, the concepts that need to be applied and the results that can be expected from applying the framework. Differences in the way these details are communicated to the practitioner can lead to variations in the results of the evaluation. To avoid these variations, a software assistant was developed to guide the practitioner through the process of applying the PATH framework to their own projects. This method is more expensive, in terms of resources needed to implement the software, compared to simply giving a presentation to the practitioners and requesting them to perform a certain task. However, the usage of software simplifies and automates the collection of data from the evaluation. A possible criticism is that, through this method, the usability of the

framework is not being directly evaluated, only the usability of the software. We consider that this is not a real problem since it is more likely to obtain false negative results due to a software malfunction or unimplemented features than to obtain false positive results that do not correspond to the framework.

- *MEM*: Moody (2003) presents the theoretical foundations that need to be considered for the evaluation of methodological knowledge (know how) in information systems. Validating a method is not done in terms of whether a method is 'correct' or not, but in terms of its pragmatic success, defined as the improvement in efficiency and effectiveness which is reflected in the adoptability of the method. Measuring the actual adoption of the PATH framework would be difficult since that would require a long-term analysis of the actual behaviour of the practitioners. Instead of that, MEM focuses on evaluating the perceived ease-of-use and the perceived usefulness. The main limitation we have experienced while applying MEM to evaluate our framework is that practitioners should have a clear motivation and a well-defined objective to perform a task so that it is possible to evaluate if the framework improves the performance. From all the experts that participated in the evaluation, none of them had previous experience, interest, motivation or need to identify privacy threats that could be caused by their projects. This fact could have a negative impact in the perceived usefulness but not necessarily in the perceived ease-of-use.
- *Case study*: as Zainal (2007) points out, case studies research is considered controversial due to the lack of robustness and the limited generalisation of the results. However, case studies can be useful to improve the understanding of complex problems where qualitative data is not sufficient. The museum visitors tracker project was used as a long-term scenario to frame and guide the research to inform the design of the PATH framework.
- *Controlled experiment*: research using controlled experiments is the standard method to identify cause-effect relationships. The approach has been to compare the PATH framework with other privacy framework, in this case Bellotti and Sellens' (1993) question option criteria (QOC), considered as a benchmark since it was introduced (Jensen et al., 2005). Two groups of bachelor students were assigned the task of analysing the Museum Visitor Tracker scenario with respect to privacy threats and elaborating a report with a list of privacy-friendly alternatives, each of the groups using a different framework. Although controlled experiments are interesting because they are normally easier to reproduce and validate, they are somehow limited when the research problem is complex, abstract, not understood completely and the sample size is limited, which is the case of privacy in ubiquitous computing.
- *Semi-structured interviews*: in conjunction with the controlled experiment, a semi-structured interview was conducted with both groups independently (PATH and QOC). The interview was guided by a set of open-ended questions related to the process followed, the difficulties, the decisions and the rationale behind the decisions, since those details are not captured in the final report delivered by the students.

Table 6 Projects used to evaluate PATH

Project name	*Description of the project*	*Participants*	*Evaluation method*
BCC shopping	A project where capacitive body coupled communication (BCC) is used as an alternative to barcodes in the shopping centre prototyped at Linköping University. (Kazim, 2015) (Chapter 4.2)	2 researchers in modelling body coupled communication	• UIM • MEM
Adressa Park	Public interactive media space with support for storytelling promoted by the newspaper Adresseavisen.	• 2 interactive media spaces researchers • 2 interaction designers	• UIM • MEM
Location based sound player	Mobile application that reproduces different sounds depending on the location of the user. The expert was 1 DIY practitioner.	1 DIY practitioner	• UIM • MEM
Museum visitors tracker	Smart system for the Science Museum (Vitensenteret) in Trondheim to track visitors and capture analytic information such as *age, gender or nationality* so that it can be matched with the level of engagement during the visit. The expert was an electronics engineer.	1 researcher 2 electronics engineers 14 bachelor students in informatics	• UIM • MEM • Case study • Controlled experiment • Semi-structured interview

The findings obtained from the experiments are grouped into benefits of GOA and use of PRIV:

- *GOA*: in the controlled experiment, the group that used PATH was able to elaborate a list of alternative designs including more interaction mechanisms (using RFID or NFC tag beacons or multiple selection buttons) than the QOC group. The alternatives proposed by the QOC group were more centred towards different ways to provide choice and consent to the visitors but constrained to video recording. The advantage of the alternatives proposed by the group that used PATH is avoidance of the over-specified requirement of using video recording, which was deliberately introduced in the problem description.
- *PRIV*: six of the eight experts that participated in the evaluation of the PATH framework stated that they found the method useful. With respect to the other two experts, one found the method complex and difficult to follow while the other remained neutral (neither agree nor disagree). They could use the PRIV as a way to find unknown privacy threats and to facilitate the communication among the team. The experts provided a total of 216 estimations for 24 different interaction mechanisms. The disagreements on the estimations by different members were used to spot the uncertainties with respect to privacy in their projects.

Table 7 Classification of the PATH framework

Framework name	*Scope*	*GOA*	*Cost*	*DP/PP*	*Motivation*	*Advantages*	*Disadvantages*	*Development process*
				Process framework				
PATH	Interaction Mechanisms in Ubicomp systems	simplified/ assisted through PRIV	Assisted through PRIV	personal privacy	neutral	Avoids privacy threats caused by over-specification. Decomposes the problem of privacy analysis in more manageable sub-problems.	Not applicable in desktop paradigm applications. Should be used in combination other frameworks for data protection. Applying a process requires extra effort from the practitioner compared to simply following guidelines.	DSRM (Peffers et al., 2007)

The UIM evaluations were assisted by a software tool, the *path assistant*, a web application that guides the experts through the analysis of their systems. This prototype served us as a proof-of-concept that it is possible to partially automate the PATH process.

Given the framework classification system from Table 1, it is possible to situate our proposal so that it can be compared to other frameworks (Table 7). The scope of the PATH framework is to identify privacy threats associated to interaction mechanisms in ubiquitous systems. The main difference with respect to the existing frameworks in Table 1 is the incorporation of a simplified GOA phase to reduce the appearance of over-specified requirements that may have an impact on users' privacy. Another difference of the PATH framework is that, a cost estimation approach is presented to facilitate the evaluation of alternatives with respect to their potential impact on users' privacy. Both phases, GOA and cost estimation are assisted through the utilisation of a PRIV. PATH is applied at the level of personal privacy, since the objective is to prevent personal information to be exposed through the utilisation of ubiquitous interaction mechanisms and it remains neutral with respect to the motivation of the practitioner whether it is principled or communitarian, as described by Iachello and Hong (2007). Compared to the existing frameworks, PATH has the advantage that it helps avoiding privacy threats caused by over-specification, however, this framework is not useful in classical desktop based application scenarios and when data protection is required it is necessary to combine PATH with other frameworks that take that aspect into consideration. PATH is the result of applying a DSRM to the problem of privacy in interactive ubiquitous computing systems.

6 Conclusions and future work

In this paper, we have presented the PATH framework, a novel approach that addresses the analysis of privacy threats in ubiquitous computing systems from the perspective of user interaction. We incorporate the utilisation of a semiotic approach, the PRIV as a way to decompose the analysis of privacy issues in more manageable and understandable subtasks. An evaluation of the framework has been conducted through different research methods, involving experts, practitioners, and informatics students. This evaluation shows that our proposal is a promising approach that can be adopted by practitioners in a variety of disciplines to simplify the analysis of privacy implications in ubiquitous systems. Future improvements on the framework are under consideration. We intend to extend our evaluation phase with privacy heuristics present in the literature, like the seven types of privacy (Finn et al., 2013), or other heuristics derived from the GDPR. It is possible that this extension complicates the application of the framework. However, it seems beneficial for practitioners to avoid relying only on their own definition of privacy. This work represents an overview of the whole PATH framework. Some of the results from the different evaluations are still pending publication.

References

Adriaans, F. (2011) *The Induction of Phonotactics for Speech Segmentation: Converging Evidence from Computational and Human Learners*, Netherlands Graduate School of Linguistics, Netherlands.

Alexander, C. (1979) *The Timeless Way of Building*, Oxford University Press.

Comment [P8]: Author: Please provide the place of publication.

Altman (1975) *The Environment and Social Behavior*, Brooks/Cole Publishing, Monterey.

Anderson, K. and Dourish, P. (2005) 'Situated Privacies: do you know where you mother [trucker] is', in *Proceedings of the 11th International Conference on Human-Computer Interaction*, Las Vegas.

Bellotti, V. and Sellen, A. (1993) 'Design for privacy in ubiquitous computing environments', in *Proceedings of the Third European Conference on Computer-Supported Cooperative Work, ECSCW'93*, Springer, 13– 17 September, Milan, Italy, pp.77–92.

Cavoukian, A. (2009) 'Privacy by design', *Take the Challenge*, Information and Privacy Commissioner of Ontario, Canada.

Chouhan, S.S., Sharma, U. and Singh, U.P. (2018) 'Soft computing approaches for image segmentation', in *Soft-Computing-Based Nonlinear Control Systems Design*, IGI Global, pp.286–310.

Chung, E.S. et al. (2004) 'Development and evaluation of emerging design patterns for ubiquitous computing', in *Proceedings of the 5th Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques*, ACM, pp.233–242.

Chung, L. and do Prado Leite, J.C.S. (2009) 'On non-functional requirements in software engineering', in *Conceptual Modeling: Foundations and Applications*, pp.363–379, Springer.

Cohn, M. (2011) *Estimating Non-Functional Requirements*, *Mountain Goat* Software [online] https://www.mountaingoatsoftware.com/blog/estimating-non-functional-requirements (accessed 20 February 2018).

Colesky, M., Hoepman, J-H. and Hillen, C. (2016) 'A critical analysis of privacy design strategies', in *2016 IEEE Security and Privacy Workshops (SPW)*, IEEE, pp.33–40.

Corcoran, P.M. (2016) 'A privacy framework for the internet of things', in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pp.13–18, DOI: 10.1109/WF-IoT.2016.7845505.

Darimont, R. et al. (1997) 'GRAIL/KAOS: an environment for goal-driven requirements engineering', in *Proceedings of the 19th International Conference on Software Engineering*, ACM, pp.612–613.

DiCicco-Bloom, B. and Crabtree, B.F. (2006) 'The qualitative research interview', *Medical Education*, Vol. 40, No. 4, pp.314–321.

ElShekeil, S.A. and Laoyookhong, S. (2017) *GDPR Privacy by Design*, Master's thesis, Stockholm University.

Fernández, A.P. (2014) 'Towards the tangible hyperlink', in *ACHI 2014, The Seventh International Conference on Advances in Computer-Human Interactions*, pp.17–20.

Fernández, A.P. and Sindre, G. (2014) 'Protecting user privacy when sharing mobile devices: research in progress', in *Norsk informasjonssikkerhetskonferanse (NISK)*.

Finn, R.L., Wright, D. and Friedewald, M. (2013) 'Seven types of privacy', in *European Data Protection: Coming of Age*, pp.3–32, Springer.

Garfinkel, S. (2002) 'Adopting fair information practices to low cost RFID systems', in *Privacy in Ubiquitous Computing Workshop*.

Garlan, D. et al. (2002) 'Project aura: toward distraction-free pervasive computing', *Pervasive Computing*, IEEE, Vol. 1, No. 2, pp.22–31.

Gellman, R. (1997) *Technology and Privacy*, in Agre, P.E. and Rotenberg, M. (Eds.), pp.193–218, MIT Press, Cambridge, MA, USA.

Gellman, R. (2017) *Fair Information Practices: A Basic History*, SSRN Scholarly Paper ID 2415020, Social Science Research Network, Rochester, NY.

~~Grenning, J. (2002) 'Planning poker or how to avoid analysis paralysis while release planning', *Hawthorn Woods: Renaissance Software Consulting*~~, Vol. 3.

~~Hand, J.L. (1947) *United States v. Carroll Towing Co.*~~, p.159, Carroll Towing Co.

Haugen, N.C. (2006) 'An empirical study of using planning poker for user story estimation', in *AGILE 2006 (AGILE'06)*, pp.9–34, DOI: 10.1109/AGILE.2006.16.

Comment [P9]: Author: Please provide the place of publication.

Comment [P10]: Author: Please provide the place of publication.

Comment [P11]: Author: Please provide the issue number and page numbers.

Comment [P12]: Author: Please provide the place of publication.

Hermans, J. et al. (2011) 'A new RFID privacy model', in *Computer Security – ESORICS 2011*, European Symposium on Research in Computer Security, Springer, Berlin, Heidelberg *(Lecture Notes in Computer Science)*, pp.568–587, DOI: 10.1007/978-3-642-23822-2_31.

Hong, J.I. et al. (2004) 'Privacy risk models for designing privacy-sensitive ubiquitous computing systems', in *Proceedings of the 5th Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques*, ACM, pp.91–100.

Iachello, G. and Abowd, G.D. (2005) 'Privacy and proportionality: adapting legal evaluation techniques to inform design in ubiquitous computing', in *Proceedings of the SIGCHI Conference on Human factors in Computing Systems*, ACM, pp.91–100.

Iachello, G. and Hong, J. (2007) 'End-user privacy in human-computer interaction', *Foundations and Trends in Human-Computer Interaction*, Vol. 1, No. 1, pp.1–137.

Introna, L.D. (1997) 'Privacy and the computer: why we need privacy in the information society', *Metaphilosophy*, Vol. 28, No. 3, pp.259–275.

Ismail, N. (2009) 'Radio frequency identification technology (RFID): is legal risk management relevant in consumer privacy?', *International Journal of Technology Transfer and Commercialisation*, Vol. 9, No. 3, pp.268–279.

~~Jensen, C. et al. (2005) 'STRAP: a structured analysis framework for privacy',~~

Jiang, X., Hong, J.I. and Landay, J.A. (2002) 'Approximate information flows: socially-based modeling of privacy in ubiquitous computing', in *Ubicomp 2002: Ubiquitous Computing*, Springer, pp.176–193.

Junestrand, S., Keijer, U. and Tollmar, K. (2001) 'Private and public digital domestic spaces', *International Journal of Human-Computer Studies*, Vol. 54, No. 5, pp.753–778.

Kalloniatis, C., Kavakli, E. and Gritzalis, S. (2008) 'Addressing privacy requirements in system design: the PriS method', *Requirements Engineering*, Vol. 13, No. 3, pp.241–255, DOI: 10.1007/s00766-008-0067-3.

Kazim, M.I. (2015) *Variation-Aware System Design Simulation Methodology for Capacitive BCC Transceivers*, PhD thesis, Linköping University Electronic Press.

Kisku, D.R., Gupta, P. and Sing, J.K. (2013) *Advances in Biometrics for Secure Human Authentication and Recognition*, CRC Press.

Kleinman, Z. (2014) 'Fingerprint 'cloned from photos'', *BBC News*, 29 December [online] http://www.bbc.com/news/technology-30623611 (accessed 19 February 2018).

Langheinrich, M. (2001) 'Privacy by design-principles of privacy-aware ubiquitous systems', in *Ubicomp 2001: Ubiquitous Computing*, Springer, pp.273–291.

Langheinrich, M. (2005) *Personal Privacy in Ubiquitous Computing*, ~~Citeseer.~~

Lederer, S. et al. (2003) *Towards Everyday Privacy for Ubiquitous Computing*, Technical Report: UCB/CSD-03-1283, EECS Department, University of California, Berkeley.

Lehikoinen, J.T., Lehikoinen, J. and Huuskonen, P. (2008) 'Understanding privacy regulation in ubicomp interactions', *Personal and Ubiquitous Computing*, Vol. 12, No. 8, pp.543–553, DOI: 10.1007/s00779-007-0163-2.

Liginlal, D., Sim, I. and Khansa, L. (2009) 'How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management', *Computers and Security*, Vol. 28, No. 3, pp.215–228, DOI: 10.1016/j.cose.2008.11.003.

Lunheim, R. and Sindre, G. (1993) 'Privacy and computing: a cultural perspective', in *Proceedings of the IFIP TC9/WG9, 6th Working Conference on Security and Control of Information Technology in Society on Board M/S Illich and Ashore*, North-Holland Publishing Co., pp.25–40 [online] http://dl.acm.org/citation.cfm?id=760241 (accessed 27 February 2015).

Lyytinen, K. and Yoo, Y. (2002) 'Ubiquitous computing', *Communications of the ACM*, Vol. 45, No. 12, pp.63–96.

MacLean, A. et al. (1991) 'Questions, options, and criteria: elements of design space analysis', *Human-Computer Interaction*, Vol. 6, No. 3–4, pp.201–250.

Comment [P13]: Author: Please provide the issue number.

Comment [P14]: Author: Please provide the place of publication.

Comment [P15]: Author: Please provide the place of publication.

Mancini, C. et al. (2009) 'From spaces to places: emerging contexts in mobile privacy', in *Proceedings of the 11th International Conference on Ubiquitous Computing*. ACM, pp.1–10.

Marsden, P. and Hollnagel, E. (1996) 'Human interaction with technology: the accidental user', *Acta Psychologica, (Usage of Modern Technology by Experts and Non-professionals)*, Vol. 91, No. 3, pp.345–358, DOI: 10.1016/0001-6918(95)00061-5.

Mashiyama, S., Hong, J. and Ohtsuki, T. (2014) 'A fall detection system using low resolution infrared array sensor', in *2014 IEEE 25th Annual International Symposium on Personal, Indoor, and Mobile Radio Communication (PIMRC)*, pp.2109–2113, DOI: 10.1109/PIMRC.2014.7136520.

Mohanani, R. et al. (2017) *Cognitive Biases in Software Engineering: A Systematic Mapping and Quasi-Literature Review*, arXiv preprint arXiv:1707.03869.

Moody, D.L. (2003) 'The method evaluation model: a theoretical model for validating information systems design methods', *ECIS 2003 Proceedings*, p.79.

Naumann, I. and Hogben, G. (2008) 'Privacy features of European eID card specifications', *Network Security*, Vol. 2008, No. 8, pp.9–13, DOI: 10.1016/S1353-4858(08)70097-7.

Neustaedter, C. and Greenberg, S. (2003) 'The design of a context-aware home media space for balancing privacy and awareness', in *UbiComp 2003: Ubiquitous Computing*, Springer, pp.297–314.

Nielsen, J. (1994) 'Usability inspection methods', in *Conference Companion on Human Factors in Computing Systems*. ACM, pp.413–414.

Norman, D. (2013) *The Design of Everyday Things: Revised and Expanded Edition*, Basic Books ~~(AZ)~~.

Noury, N. et al. (2007) 'Fall detection-principles and methods', in *29th Annual International Conference of the Engineering in Medicine and Biology Society, EMBS 2007*, IEEE, pp.1663–1666.

Okoye, J.N. (2017) *Privacy by Design*, Master's thesis, NTNU.

Palen, L. and Dourish, P. (2003) 'Unpacking privacy for a networked world', in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, pp.129–136.

Patrick, A.S. and Kenny, S. (2003) 'From privacy legislation to interface design: implementing information privacy in human-computer interactions', in: *Privacy Enhancing Technologies*, pp.107–124, Springer.

PCWorld (2011) *Cautions: Beware of Malicious QR Codes - Media Releases*, PC World Australia, 28 June [online] https://www.pcworld.idg.com.au/mediareleases/12655/avg-aunz-cautions-beware-of-maliciousqr-codes/ (accessed 19 February 2018).

Peffers, K. et al. (2007) 'A design science research methodology for information systems research', *Journal of Management Information Systems*, Vol. 24, No. 3, pp.45–77.

Potts, C. (1999) 'ScenIC: a strategy for inquiry-driven requirements determination', in *Proceedings of the IEEE International Symposium on Requirements Engineering*, IEEE, pp.58–65.

Rachels, J. (1975) 'Why privacy is important', *Philosophy and Public Affairs*, pp.323–333.

Rogers, Y. (2006) 'Moving on from Weiser's vision of calm computing: Engaging Ubicomp experiences', in *International Conference on Ubiquitous Computing*, Springer, pp.404–421.

Rubinstein, I.S. and Good, N. (2013) 'Privacy by design: a counterfactual analysis of Google and Facebook privacy incidents', *Berkeley Tech. L.J.*, Vol. 28, ~~p.1333~~.

Schiller, J. and Voisard, A. (2004) *Location-Based Services*, Elsevier.

Shmueli, O., Pliskin, N. and Fink, L. (2015) 'Explaining over-requirement in software development projects: an experimental investigation of behavioral effects', International Journal of Project Management, 33(2), pp. 380–394.

SIG (2014) *Core Specification 4.2 | Bluetooth Technology Website*, 2 December [online] https://www.bluetooth.com/specifications/bluetooth-core-specification/legacyspecifications (accessed 19 February 2018).

Comment [P16]: Author: Please provide the place of publication.

Comment [P17]: Author: Please provide the place of publication.

Comment [P18]: Author: Please provide the volume number and issue number.

Comment [P19]: Author: Please provide the issue number.

Comment [P20]: Author: Please provide the place of publication.

Sjøberg, D.I. et al. (2005) 'A survey of controlled experiments in software engineering', IEEE *Transactions* on *Software Engineering*, Vol. 31, No. 9, pp.733–753.

Solove, D.J. (2008) *Understanding Privacy*, p.420, Harvard University Press.

Spiekermann, S. (2005) 'Perceived control: scales for privacy in ubiquitous computing', in *Proceedings of Conference on User Modeling – UM'05*, pp.24–29.

Spiekermann, S. and Cranor, L.F. (2009) 'Engineering privacy', *IEEE Transactions on Software Engineering*, Vol. 35, No. 1, pp.67–82.

Stacy, W. and MacMillan, J. (1995) 'Cognitive bias in software engineering', *Communications of the ACM*, Vol. 38, No. 6, pp.57–63.

Thomas, K. et al. (2014) 'Distilling privacy requirements for mobile applications', in *Proceedings of the 36th International Conference on Software Engineering*, ACM, pp.871–882.

Varian, H.R. (1997) 'Economic aspects of personal privacy', ~~*Privacy and Self-Regulation in the Information Age*~~.

Venkatesh, V. (2000) 'Determinants of perceived ease of use: integrating control, intrinsic motivation, and emotion into the technology acceptance model', *Information Systems Research*, Vol. 11, No. 4, pp.342–365.

Want, R. (2006) 'An introduction to RFID technology', *IEEE Pervasive Computing*, Vol. 5, No. 1, pp. 25–33.

Warren, S.D. and Brandeis, L.D. (1890) 'The right to privacy', *Harvard Law Review*, pp.193–220.

Weis, S.A. et al. (2004) 'Security and privacy aspects of low-cost radio frequency identification systems', in Hutter, D. et al. (Eds.): *Security in Pervasive Computing*, Springer Berlin Heidelberg *(Lecture Notes in Computer Science, 2802)*, pp.201–212.

Weiser, M. and Brown, J.S. (1997) 'The coming age of calm technology', in *Beyond Calculation*, pp.75–85, Springer.

Westin, A. F. (1967) *Privacy and Freedom*, Atheneum, New York.

~~Wickens, C.D. (1992) *Engineering Psychology and Human Performance*, HarperCollins Publishers.~~

Ye, J. et al. (2007) 'Ontology-based models in pervasive computing systems', *The Knowledge Engineering Review*, Vol. 22, No. 4, pp.315–347.

Yu, E. and Mylopoulos, J. (1998) 'Why goal-oriented requirements engineering', in *Proceedings of the 4th International Workshop on Requirements Engineering: Foundations of Software Quality*, pp.15–22.

Zainal, Z. (2007) 'Case study as a research method', *Jurnal Kemanusiaan*, ~~Vol. 5, No. 1~~.

Ziegeldorf, J.H., Morchon, O.G. and Wehrle, K. (2014) 'Privacy in the internet of things: threats and challenges', *Security and Communication Networks*, Vol. 7, No. 12, pp.2728–2742.

Comment [P21]: Author: Please provide the place of publication.

Comment [P22]: Author: Please provide the publisher and the place of publication.

Comment [P23]: Author: Please provide the volume number and issue number.

Comment [P24]: Author: Please provide the place of publication.

Comment [P25]: Author: Please provide the place of publication.

Comment [P26]: Author: Please provide the page numbers.