Empir Software Eng (2018) 23:259–289
DOI 10.1007/s10664-017-9517-1

Privacy by designers: software developers' privacy mindset

Irit Hadar[1] · **Tomer Hasson**[1] · **Oshrat Ayalon**[2] · **Eran Toch**[2] · **Michael Birnhack**[3] · **Sofia Sherman**[1] · **Arod Balissa**[3]

Published online: 30 April 2017

Abstract Privacy by design (PbD) is a policy measure that guides software developers to apply inherent solutions to achieve better privacy protection. For PbD to be a viable option, it is important to understand developers' perceptions, interpretation and practices as to informational privacy (or data protection). To this end, we conducted in-depth interviews with 27 developers from different domains, who practice software design. Grounded analysis of the data revealed an interplay between several different forces affecting the way in which developers handle privacy concerns. Borrowing the schema of Social Cognitive Theory (SCT), we classified and analyzed the cognitive, organizational and behavioral factors that play a role in developers' privacy decision making. Our findings indicate that developers use the vocabulary of data security to approach privacy challenges, and that this vocabulary limits their perceptions of privacy mainly to third-party threats coming from outside of the organization; that organizational privacy climate is a powerful means for organizations to guide developers toward particular practices of privacy; and that software architectural patterns frame privacy solutions that are used throughout the development process, possibly explaining developers' preference of policy-based solutions to architectural solutions. Further, we show, through the use of the SCT schema for framing the findings of this study, how a theoretical model of the factors that influence developers' privacy practices can be conceptualized and used as a guide for future research toward effective implementation of PbD.

Keywords Data protection · Privacy · Privacy by design · Qualitative research · Grounded analysis · Social cognitive theory · Organizational climate

Communicated by: Tim Menzies

✉ Irit Hadar
hadari@is.haifa.ac.il

[1] Department of Information Systems, University of Haifa, 199 Aba Khoushy Ave. Mount Carmel, 3498838 Haifa, Israel

[2] Faculty of Engineering, Tel Aviv University, P.O. Box 39040, 6997801 Tel Aviv, Israel

[3] Faculty of Law, Tel Aviv University, P.O. Box 39040, 6997801 Tel Aviv, Israel

1 Introduction

Privacy is a dynamic concept, contingent upon changing social norms and technology. Privacy concerns, namely the access to individually identifiable personal information (Smith et al. 2011), are triggered in an ever-expanding landscape with new applications and architectures, such as online social networks, big data analytics, and location-based services. Recent legal research identified the shortcomings of current legal instruments (Ohm 2010; Tene and Polonetsky 2013) and their limited effect in shaping users' privacy experience online (Birnhack and Elkin-Koren 2011). Accordingly, legal authorities suggested an approach called privacy by design (PbD), an initiative that expands privacy solutions from the legal and social realms to the technological realm (van Lieshout et al. 2011). PbD calls for embedding privacy into the design of technologies at early stages of the development process and throughout the lifecycle of their development. PbD principles ask, for example, to design systems with minimal data collection processes and proper notice and consent interactions. Long advocated by computer scientists and regulators (Langheinrich 2001), PbD has recently attracted policy makers' attention both in the U.S. (FTC 2012) and in the EU's proposed General Data Protection Regulation (GDPR 2012). However, despite the apparent simplicity of the idea of PbD, a major challenge for its successful deployment is translating the general abstract notion and the meaning of informational privacy (or, in its European term, data protection) into concrete guidelines for software developers (Birnhack et al. 2014; Gürses et al. 2011; van Rest et al. 2014).

Since PbD wishes to introduce privacy considerations into the technological design, it delegates responsibility over privacy to those in charge of the design, namely software developers who design information technologies (hereafter called developers); thus, their perceptions and point of view are essential when implementing PbD. PbD is contingent on the extent to which developers impact the privacy outcome of a system. As software systems are developed within a particular technological framework, in a particular technological culture, developers play an important role in determining how issues such as trust and security are handled by the system (Mathew and Cheshire 2017). Accordingly, to successfully deploy PbD projects, we need to understand how developers think of privacy, perceive it, and eventually design it.

Privacy perceptions and concerns among software *users* have been widely studied (Ackerman et al. 1999; Fienberg 2006; Gross and Acquisti 2005; Madejski et al. 2011; Resnick and Montania 2003). User-centric research led to well-used models that portray users' privacy decision making (Ackerman et al. 1999; Dinev and Hart 2006; Awad and Krishnan 2006; Gross and Acquisti 2005). However, less attention has been given thus far to the context and the process in which privacy is built into (or missing from) software – or specifically information – systems, and the role developers play in the privacy engineered into the system. Several studies investigated the perceptions toward surveillance by Webmasters (Shaw 2003) and IT administrators (Székely 2013). Recent studies focused on specific segments of technology developers, mostly mobile application developers (Balebako et al. 2014; Jain and Lindqvist 2014, Van Der Sype and Maalej 2014), acknowledging the influence of the developers on data processing and their potential contribution to the protection of user privacy by taking privacy-friendly decisions in the early development stages (Van Der Sype and Maalej 2014). However, it is still unclear how privacy plays into the system design process, in which requirements are understood and an appropriate solution for meeting the requirements is designed, which in this case determines how it collects and manages personal data. Specifically, our understanding – and the understanding of policy makers who advocate PbD – is quite limited with respect to the way developers understand and attend to

informational privacy. While several recent studies have tackled the topic of privacy requirements, especially in the context of mobile applications, acknowledging that traditional requirements elicitation methods do not provide effective means for representing and analyzing privacy requirements in the frequently changing contexts of application usage (Omoronyia et al. 2013; Thomas et al. 2014), the software engineering community still lacks "systematic studies to find out what privacy requirements are and how these requirements should be addressed by developers" (Sheth et al. 2014).

The objective of this research is to fill this gap in understanding how developers interpret privacy. Our main research question is: What are the perceptions of privacy among developers involved in the design of software systems? More specifically, we examined two sub-questions: First, how do developers interpret the concept of privacy in their daily work and working environment, in light of the privacy concept as explained by the regulators? Second, given that developers typically work within organizations, and are evidently influenced by them, how are the organizational characteristics and procedures translated into the developers' privacy decisions? While others, notably Bamberger and Mulligan (2010), studied how the public's demand for privacy affects organizations, we draw attention to the developers themselves, and query their perceptions of privacy, so to assess the viability of PbD.

As this topic is a relatively new area of research, offering no rigor models and theories, we chose a qualitative, interpretive approach (Walsham 2006), using in-depth interviews with developers as a means to study their privacy perceptions and practices, and their interpretations of their work environment in this context. We conducted interviews with 27 software developers who practice software design in various domains, and analyzed the data according to the principles of the grounded theory methodology (Strauss and Corbin 1994, 1998). The findings shed a new light onto developers' privacy perceptions, interpretations and practices when designing new technologies and the interplay between the different forces affecting and affected by their privacy decision making. These findings indicate, among other things, that developers hold a partial understanding of privacy, mostly limited to security concerns, prefer policy-based solutions to architectural solutions, and are highly influenced by organizational privacy climate – a powerful force guiding developers toward particular practices of privacy. The latter finding points to existing obstacles for applying PbD, but at the same time suggests potential avenues to improve privacy practices. Based on the research findings and the classification of the data according to the schema of Social Cognitive Theory (SCT) (Bandura 1986), we propose a conceptualization of the factors that influence, and are influenced by developers' privacy practices, which can be used as a guide for future research toward effective implementation of PbD.

The paper is organized as follows: The next section reviews related literature. Next, we present the research method and findings. We then discuss the findings, framed and analyzed via the schema of SCT, and propose potentially beneficial future strategies. Finally, we list and discuss the limitations and implications of our research, and conclude with some thoughts about the prospects of PbD.

2 Related Research

This section presents the background for contextualizing the current research. It starts by explaining the notion of privacy from the point of view of the regulators, which could be viewed as the desired situation, namely the requirements for privacy in software-based

information technologies. Next, engineering approaches for privacy, designed for translating the legal regulations to engineering terminology and practices are presented. Finally, research on privacy perceptions and practices in the software industry is reviewed, as a basis for reflecting on the existing situation, and for positioning the current research.

2.1 Fair Information Practice Principles for Privacy

Over the years, various legal systems converged around a rough set of principles, known as Fair Information Practice (or sometimes Privacy) Principles (FIPPs), which attempt to translate the rather abstract concept of privacy into more concrete and workable guidelines. (As an example of their articulation, see Gellman (2013).) FIPPs originated in the United States, in a governmental report following Watergate, which is known as the Ware Report (US Dept. of Health 1973). While these principles are not binding or obligating, they are considered as the common grounds between different approaches to informational privacy, namely the U.S. and European approaches (Birnhack et al. 2014).

Although there are some variations, as a general matter, FIPPs require that data subjects are notified about the collection of their personal data (notice), that they are given the option to agree to the collection and processing (consent, sometimes called choice), that data controllers, i.e., the party that collects the data and processes it, is subject to a series of duties as to the data: that only the minimal data needed for the legitimate purpose of the business or the technology is collected and processed (data minimization), and that the data is not used for other, incompatible purposes, to which the subject has not consented (purpose specification). The data controller is also under the duty of secrecy as to the data, namely, not to hand over the data to unauthorized parties (confidentiality), and is required to prevent malicious third parties from obtaining the data (data security). The data subject has correlative rights, as well as a right to access the data held by the controller about her (access) and if the data is inaccurate, to require that it is rectified (rectification).

FIPPs serve us as a theoretical basis for the legal and social requirements for privacy in software-based information technology. In the current research, when examining developers' perceptions of privacy, we compare these perceptions to the core FIPPs. In the results section below, we elaborate on each of the FIPPs and discuss related findings.

2.2 Engineering Approaches to Privacy

Spiekermann and Cranor (2009) reviewed engineering approaches toward implementing privacy in a wide variety of software-based information technologies. Several authors proposed design frameworks meant to assist designers in addressing privacy during the development process. These include, for example, a privacy risk model as an approach to the design of privacy-sensitive ubiquitous computing systems (Lahlou et al. 2005), models for incorporating privacy in the early stages of requirements engineering and system design (Kalloniatis et al. 2008; Gürses et al. 2011), and an analysis of privacy risks and privacy-preserving technologies associated with personalization systems (Toch et al. 2012). In recent years, we have witnessed the first steps of a process in which privacy principles and patterns that originated in academia have been introduced into development practices. For example, in "The Privacy Engineer's Manifesto", published in 2014, the authors offer comprehensive guidance through technologies and architectures to design privacy (Dennedy et al. 2014).

Several recent studies demonstrate the growing importance of privacy in software engineering literature, highlighting the privacy challenges in various software engineering processes, such as software testing (Grechanik et al. 2010), bug reporting (Castro et al. 2008), and sharing information about software defects (Peters and Menzies 2012; Peters et al. 2013). Grechanik et al. (2010) define the following main problem in software testing, which is also typical to other processes: realistic data is needed in testing information systems and often contains sensitive information, whereas existing methods for faking or anonymizing data reduce test coverage. Several research works propose ways to anonymize testing data by selectively changing data records according to the tested program properties (Grechanik et al. 2010; Taneja et al. 2011). For example, implementations of the k-Anonymity method, which aims to make the data of an individual indistinguishable from other k-1 individuals, have been proposed for software testing (Budi et al. 2011; Lucia et al. 2012). While these research works focus on addressing privacy concerns during the processes of development and maintenance of software, it is important to examine how the developed software will function and manage private data after its deployment, throughout its usage lifecycle.

Empirical evidence of the actual impact of privacy technologies implemented in software systems is mostly evaluated by looking at end users (Ackerman et al. 1999; Fienberg 2006; Gross and Acquisti 2005; Madejski et al. 2011; Resnick and Montania 2003; Smith et al. 2011). Several studies measured the privacy risks and decision-making in domains such as electronic commerce (Dinev and Hart 2006), and online social networks (Ayalon and Toch 2013; Stutzman et al. 2013). These studies reveal that, in practice, developers are willing to tradeoff the level of privacy offered to end users in order to achieve better usability of the system. In many types of systems, once built, privacy-related requirements impose additional burdens on the end users, such as limiting the ability of the system to offer personalized features through detailed user modeling (Awad and Krishnan 2006). As in many other cases of value-sensitive design, implementing values such as privacy requires a thorough analysis of complex tradeoffs (Friedman et al. 2006).

Privacy design frameworks and technologies serve as potential bridges between software designers and policy makers. However, to the best of our knowledge, it is still unclear how effective these design frameworks are, and what are the possible limitations for their utilization in everyday engineering practices. Evidence shows that in several important domains, such as the adoption of P3P (Platform for Privacy Preferences Protocol), privacy-oriented design solutions gained only modest success (Reay et al. 2009). Indeed, there are very few cases of successful implementation of PbD. The exception seems to be cases in which the government applied PbD to its own systems, or worked closely with regulated industries, such as the Ontario Lottery and Gaming Corporation, which implemented facial recognition technology with the assistance of the Ontario Privacy Commissioner (Cavoukian 2009, 2011; Cavoukian et al. 2014).

Several critics have described PbD as vague, with regard to the way it could be applied in engineering scenarios (Gürses et al. 2011; van Rest et al. 2014). Rubinstein and Good (2013) pointed out the inherent tension between privacy and business models based on surveillance and personalization. Another tension is described by Birnhack et al. (2014) pointing to the tension between the privacy mindset of data-intense software systems and the technological mindset of privacy legislation and regulation. Analyzing the way in which privacy and data-utilization thinking is embedded in today's design processes is important for understanding how privacy can be effectively implemented by engineering practices. Developing PbD frameworks that do not take the current organizational processes into account might result in

practices that would not be adopted by engineers. From the technological point of view, it is necessary to understand how privacy considerations fit into software design decisions, in order to innovate and design privacy-preserving solutions.

2.3 Software Developers and Privacy

As the awareness about the need to consider privacy in software design increases, research has recently emerged on the perceptions and interpretations of software development professionals regarding privacy. An investigation of attitudes of Webmasters toward privacy in Web services revealed that social influence from others in the organization explains a significant part of the former's moral attitude toward privacy (Shaw 2003). This influence increases with the sense of belonging, common identity and shared values with the organization. Another investigation, focusing on the attitudes of IT system administrators toward surveillance, portrays a complex picture in which most IT administrators do not object to Internet usage surveillance, such as monitoring Internet browsing, although they do object to the use of surveillance for specific objectives such as employee assessment (Székely 2013). Culnan and Williams (2009) demonstrated, through a series of case studies, how an infrastructure of moral responsibility is essential for helping IT companies to successfully handle privacy breach of trust. They emphasize that security and privacy are two distinct concepts and that securing the stored personal information is not enough to ensure users' privacy.

Sheth et al. (2014) investigated developers' perceptions of privacy, comparing them to those of users. They found that developers perceive data anonymization to be more effective for reducing privacy concerns than privacy laws and policies. They also found significant differences between the beliefs of users and developers. For example, developers are more willing than users to accept less privacy for added or intelligent system functionality. These differences may suggest that the users' privacy preferences are not reflected in the developed systems.

In the context of mobile applications, factors such as the size of the development company and its revenue model were found to impact its organizational privacy and security practices, including usages of security protocols (i.e., SSL), and the existence of privacy policy and a chief privacy officer (CPO) (Balebako et al. 2014). Programmers can be nudged into using privacy-preserving choices by highlighting the privacy benefits of an application-programming interface (Jain and Lindqvist 2014).

In an article exploring how privacy law views technology and how technology views privacy, Birnhack et al. (2014) found deep, ideological differences between the law's technological mindset and technology's privacy mindset. More specifically, they revealed that canonic literature regarding data analytics in IT systems handling private data proposes uses of data in ways which are not always compatible with privacy principles. It seems that PbD is doomed to fail unless some means to bridge the gap between the law and the technology mindsets are introduced (Birnhack et al. 2014).

In this research, we seek to learn more about privacy-related perceptions and behaviors of developers and their interrelations with the developers' work environment, but with some considerable differences compared to the literature detailed above. First, we focus on developers who serve as software architects, namely the people making the high-level design decisions in large-scale systems in different domains in which private data is dealt, including telecommunications, healthcare, and other enterprise software systems. By turning to this population, we aim to investigate the mindset of the people responsible for technologies'

design, namely those whom the regulators expect to consider and mitigate privacy risks within this design. Second, we take an exploratory approach, as no theory is currently available, as far as we know, for conceptualizing privacy perceptions and practices of developers and their interrelations with their work environment. Such theory would not only assist in explaining the gap between the privacy requirements and the privacy perceptions and interpretations of developers found in the above reviewed and the current research works, but could also point to means for bridging this gap.

3 Research Method

The main objective of this study is to identify privacy perceptions and interpretations of developers with regard to informational privacy. We took a qualitative research approach, which has advantages when aiming to explore and understand complex socio-technical processes (Myers 1997) and has been found to contribute to software engineering and information systems research (e.g., Seaman 1999; Lacity and Janson 1994; Chan 2000). As the research in this field is in its initial stage, a grounded approach has the potential of identifying and understanding phenomena related to developers' perceptions and interpretation of privacy in their full complexity, including factors that may play a role in forming, and be formed by, these perceptions and interpretations, and influence privacy-related practices. We followed the principles of grounded theory methodology (Strauss and Corbin 1998), iterating between data and literature throughout the data collection and analysis processes, constantly assessing and interpreting theoretical constructs against the iteratively elicited and analyzed data.

3.1 Sample Context and Selection of Participants

Participant sampling was performed according to the theoretical sampling principles (Strauss and Corbin 1990). To be eligible to participate in the study, a participant had to be a software developer, practicing software design and/or architecture.[1] In order to reflect variations within our data, we aimed to achieve a diverse sample of participants, with different levels of experience and from different domains. In order to meet these criteria, the main tool for participants' recruitment was LinkedIn, where users publish detailed proficiency information and participate in interest groups. Several additional participants were recruited directly by the researchers based on professional acquaintance.

Participants were characterized according to their domain and experience. The classification to domains was done according to the organization or the environment in which they work, as well as their previous experience and expertise. Participants from three main domains were included in our sample: seven participants from the telecom domain (communication via electronic transmission of impulses, cable, telephone, radio, television, or internet); eleven participants from general enterprise systems (CRM/ERP/Integration platforms); and three participants from the healthcare domain (health information systems). In addition, we had six participants, each from a different domain: shipping, defense, retail, mobile applications, insurance, and an IT research organization, developing privacy enhancing technologies. The

[1] High-level design of the software system, with emphasis on the system's structure and the non-functional requirements it needs to meet.

professional experience of the participants varied from four to 30 years of experience, with the average of 12 years. Detailed information about each of the participants is presented in Appendix Table 4.

3.2 Data Collection

The main tool of data collection was semi-structured interviews. We decided to use interviews rather than surveys, despite the inevitable result of a lower number of participants, as we were interested in in-depth exploration of developers' perceptions and interpretations of privacy and related concepts, and interviews are considered a key way of accessing the interpretations of informants in the field (Walsham 2006). This exploration would not have been possible to conduct and navigate using a closed set of survey questions with no interaction with the participants. This was also the reason for preferring semi- over fully-structured interviews. This structure enabled the scrutiny of interesting answers provided by the interviewee, without being limited to a pre-defined script of a question set. Our preference of interviews over observation stemmed from the following reasons: While field observations have the advantage of direct access to developers' actual behavior, conducting such observations was not practical – privacy issues are usually not dealt with on a daily basis in most domains, and access to direct observations by researchers from outside the companies is highly restricted. Finally, merely observing developers' behavior does not provide access to developers' cognitive processes and perceptions.

Following Myers and Newman (2007), the interviews included situating the interviewer within the context of the interview, reducing social dissonance and building trust by introducing the interviewer and the research topic and describing procedures for ensuring anonymity and security of data, eliciting background about the participant, mirroring the verbal posture and the vocabulary of the participant, and allowing for flexibility in the interview to follow directions the participant found interesting. The interview questions focused on privacy definitions, awareness to privacy concerns, familiarity with privacy laws, practices that revolve around privacy, and the work environment of the participants, namely the organization in the which they operate. The research group, which includes researchers from the disciplines of software engineering, information systems and law, composed the question set. Following pilot interviews with five developers, the initial question set was refined and improved to its final version (see interview guide in Appendix 2).

Only the data elicited with the final version of the question set were included in the analysis. The interviews were conducted by the second author between March 2013 and February 2014 iterating between data elicitation and analysis, directing the next interviews (Strauss and Corbin 1990). More specifically, the early (pilot) interviews directed us toward a complete set of questions, whereas the later interviews directed our attention and sensitivity to recurring phenomena, and emphases and examples used in the non-structured parts of the interviews. Some of the interviews were conducted using Skype (video conversations) and others were conducted in face-to-face meetings. The interviewees were encouraged to answer freely and with as many examples as possible (where relevant). In addition, an unstructured conversation took place, usually at the end of the interview. This enabled the participants to express themselves freely, indicating additional examples, knowledge, opinions and perceptions, beyond the ones discussed in the context of the questions. The interviews were recorded and later transcribed by the interviewer.

3.3 Data Analysis

The principles of the grounded theory methodology were used for data analysis (Strauss and Corbin 1994) in conjunction with interpretive research principles (Walsham 2006). "[I]nterpretive methods of research start from the position that our knowledge of reality, including the domain of human action, is a social construction by human actors. Our theories concerning reality are ways of making sense of the world, and shared meanings are a form of intersubjectivity rather than objectivity" (Walsham 2006). This corresponds with our aim to unveil the meaning and sense-making of privacy and related concepts as interpreted by developers. Grounded theory offers a possible analysis method for interpretive research to learn from the data itself (Walsham 2006), and was chosen in this research due to its systematic guidance for analyzing people's perceptions and actions while considering the full complexity of the social context (Strauss and Corbin 1998).

When using the grounded theory approach, consideration of literature is allowed for guiding data analysis (Suddaby 2006). In order to examine developers' perceptions of privacy, we analyzed them in light of existing data protection principles, namely the set of FIPPs (Gellman 2013). This enabled us to capture strengths and gaps in developers' perceptions as viewed through the lens of the legal concept of informational privacy (or data protection). Similarly, we used the taxonomy by Spiekermann and Cranor (2009) to categorize privacy engineering solutions reported by participants. These were suited to analyze the applicability of PbD, which expects system developers to embed legal privacy protective measures into the technological design. The rest of the data analysis was done based on concept analysis, according to the inductive analysis approach in which categories emerge from the data and are validated and refined throughout the analysis process (Strauss and Corbin 1990, 1994).

The purpose of inductive analysis is to identify recurring themes, which serve as the basis for the categories, and to define their properties and dimensions, in our case, developers' privacy perceptions, interpretations and practices. The data-analysis procedure included open, axial, and finally selective coding (Strauss and Corbin 1994, 1998) to determine the categories regarding the tension between developers' perceptions and interpretations of privacy and the law. The open coding was conducted iteratively with the continuation of data collection, and included exploration for recurring themes. The axial coding was conducted after the completion of the data collection, iterating between new patterns identified in the axial coding and revisiting the open coding, as well as consultation with literature, finally leading to categories, subcategories and the relations between them. Finally, after identifying a *central* code (Strauss and Corbin 1998), namely, the interplay between developers' perceptions of privacy, characteristics of their work environment, and their actual practice, we selectively re-coded the data focusing on the schema of SCT and on the theory of organizational climate. This approach of integrating an existing theoretical construct with the principles of grounded theory methodology has been applied and accepted in similar areas of research (e.g., Berente and Yoo 2012).

4 Findings

4.1 Conceptualization of the Findings

The findings of the research included aspects related to the cognitive processes of the participants, namely their perceptions and interpretations of the concept of privacy, the

characteristics of the organization in which they work, and their actual practices, with apparent interplays between these different aspects. Social cognitive theory (SCT) proposes a structure of bidirectional causation relationships between: cognitive and other personal factors, environmental influences, and behavior (Bandura 1986). The influences of the different sources do not have to be of equal strengths nor are they expected to occur simultaneously: "It takes time for a causal factor to exert its influence and to activate reciprocal influences. Because of the bidirecitonality of influence, people are both products and producers of their environment." (Wood and Banduar 1989, p. 362).

In the process of analyzing and making sense of the data, we borrowed this schema, abstracting and adapting it for the purpose of this research. In cognitive and personal factors (P) reside the findings related to developers' perceptions of privacy and their interpretation of this concept. In the external environment (E) reside the findings related to the work environment of the developers, namely the organization in which they operate, with its privacy-related characteristics. Specifically, we identified organizational climate as a central force representing the influence of the environment on developers' cognitive factors and behavior related to privacy. This allocation of organizational climate to the category of external environment in SCT has been proposed before; for example, in the context of knowledge sharing perceptions and behavior of programmers (Tsai and Cheng 2010). In behavior (B) reside the findings related to the developers' (self-reported) behavior when encountering informational privacy concerns during software development. We further examined available technological solutions and architectural patterns that the developers reported they used in practice. We believe that developers' use of such available technologies also plays an important role in shaping their mindset by introducing axiomatic thinking about the capabilities and constraints of technology.

4.2 Developers' Privacy Perceptions and Interpretation (P)

We asked the participants direct questions regarding the definition of informational privacy. In addition, several other questions and discussions during the interviews, indirectly reflecting these topics, further contributed to our understanding of how the developers perceive informational privacy. The answers indicated that there was a substantial gap between the legal norms as to privacy, and privacy as perceived by the participants.

In order to contextualize the participants' privacy perceptions, we analyzed them in light of the FIPPs, as described earlier, including: notice, consent, data minimization, purpose specification, subjects' access and rectification rights, confidentiality, and data security. Accordingly, we classified participants' relevant quotes into these FIPPs. Although qualitatively analyzed, we decided to count the text segments classified to each FIPP, as an indication regarding the extent of familiarity of the different FIPPs among the participants of the research. Tables 1 and 2 present our qualitative observations accompanied with example quotes for the different FIPPs as referred to by the participants (each quote is referenced to the interviewee's serial number). The FIPPs are listed in the tables according to decreasing frequency of participants' statements. Figure 1 presents the number of participants' quotes classified to each FIPP.

When examining how the participants responded to privacy-related scenarios, in addition to further analysis of their definition of informational privacy, we found that their interpretation of the concept of privacy also plays an important role. A recurring phenomenon was participants' interpretation of privacy as a theoretical, abstract, and impractical – perhaps even naïve – concept.

Table 1 FIPPs reflected in the privacy definitions of the participants

FIPP	Definition (Gellman 2013)	Observation	Examples
Security	Personal data should be protected by reasonable security safeguards.	Most participants defined privacy by referring to and highlighting security related terms, and found it hard to differentiate between privacy and security. Their definitions reflect a view of privacy as security or a subset thereof, referring to protecting information that resides in the system from external malicious agents. The use of terms such as passwords, hackers, and securing information was highly frequent.	*Privacy means keeping the information at its appropriate location and doing the best you can in order to prevent data leakage. (I8)* *[Privacy is] to make sure that other users, hackers, will not access the client's [data subject] data. (I16)*
Confidentiality	Personal identifiable information should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality.	Defining privacy as a framework for confidentiality was also relatively common, but did not take as central of a role as security.	*Privacy is a control mechanism – who is authorized to see the information. (I1)* *Privacy means that the data actually belongs to the client [data subject], and others can view it only after the client [data subject] agreed. Like a doctor [who can see the patient's data only if the patient agrees]. (I13)*
Purpose specification	Information should be regarded as collected and held for a specific purpose and not to be used, without appropriate authorization, for other purposes.	Purpose specification was mentioned by about half of the participants, at times in the form of not sharing the data with a third party.	*[Privacy means] not to share information between companies without the client's [data subject] consent. (I3)* *I'd expect that if I buy something online, this information would be used only for receiving and executing my order. (I17)*
Consent	Organizations should involve the individual in the process of collecting personal data and seek individual consent for its collection, processing, use, and further transfer.	Consent was reflected in the definitions of privacy only by a small number of participants.	*When the owner of the information [data subject] controls to whom the information is revealed. (I1)* *It is forbidden to share private information without the user's [data subject] consent. (I3)*

Table 2 FIPPs generally not reflected in the privacy definitions of the participants

FIPP	Definition (Gellman 2013)	Observation
Notice	Informing the data subject about the data collection.	Each of these FIPPs was mentioned by a single participant.
Data subject's access	Enabling an individual to access their personal data, held by the data processor.	
Data minimization	Limiting the types of information an organization may collect about an individual	
Rectification	Allowing the data subject to require that the data is rectified if it is inaccurate	Rectification was not mentioned by any of the participants.

The following set of quotes demonstrates the general discomfort the participants expressed when discussing privacy. They are not only unsure as to what privacy means, but the mere feasibility of its implementation is questioned. For example: *Wow, this [defining privacy] calls for philosophizing… (I8); In most systems it [privacy] is unrealistic [to implement]. (I1).*

Moreover, business considerations are interpreted as being of a higher priority over preserving end users' informational privacy: when the data subject's privacy conflicts with business needs, the latter overrides the former in the real (rather than the "idealistic") world. For example, the following quotes are answers to a question about what should be the default setting defined in an application regarding collecting personal information (consent or not): *Default consent for data collection [is preferable]. With all due respect to the idealistic world, people keep the defaults (I1); Default consent for data collection [is preferable], of course. We make a living by it (I12).*

Finally, participants tended to discuss privacy as a social concern, based on norms of morality and ethics, rather than a technological, engineering concern. For example: *Privacy is the moral aspect of keeping [private] information. (I9); It [privacy] is about the norms of interpersonal relations (I19).* This tendency implies that privacy decisions depend on social norms and individual values rather than the law or engineering guidelines and solutions.

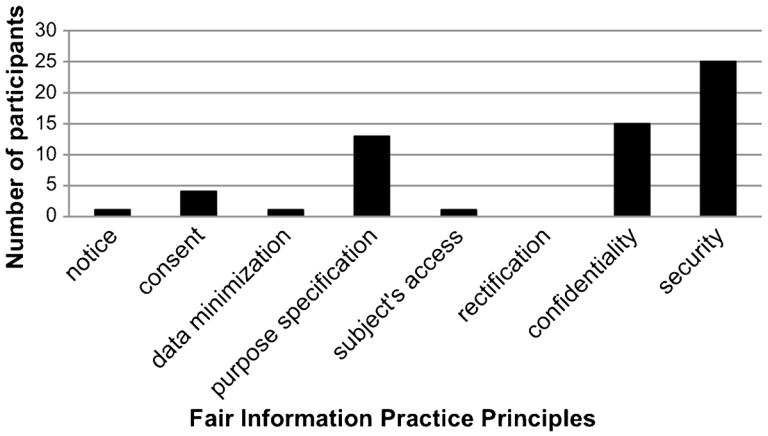

Fig. 1 Participants' quotes classification in the context of accepted FIPPs

4.3 Organizational Privacy Climate (E)

The organization is the immediate environment within which the vast majority of software developers operate. This environment and its characteristics may influence, and be influenced by, developers' privacy-related perceptions, interpretations and decisions. Data analysis revealed several aspects of this environment in this context.

We found in the interviews frequent references to organizational privacy policy. However, policy draws only part of the picture; its interpretation and dissemination within the organization is what really counts. We borrow the term *climate* from the organizational behavioral research domain in order to reason about how privacy-related design decision-making is affected by organizational norms, practices and beliefs. Organizational climate is the "perceptions of the events, practices, and procedures, and the kinds of behavior that are rewarded, supported, and expected in settings" (Schneider et al. 2013). Therefore, to understand how the organization affects developers in our context, we examine the *organizational privacy climate*. The term, *privacy climate*, has recently appeared in privacy literature (Ammori and Pelican 2013; Bamberger and Mulligan 2013; Ozer 2012; Sánchez Abril et al. 2012). We explore a specific type of privacy climate, an organizational privacy climate that resonates in the actions of developers. Reverse-engineering the term, we can refer to *organizational privacy climate* as a shared perception of the way behavior with regard to privacy is rewarded, supported and expected.

Table 3 provides our observations regarding organizational privacy climate, differentiating between positive and negative climates toward privacy, and accompanied with example quotes demonstrating both types of climate. Ten of the participants provided examples and statements

Table 3 Organizational privacy climate

Privacy climate	Observations	Examples
Positive	10 of the 27 participants referred explicitly to organizational procedures governed by organizational policy. In some organizations, a designated position is responsible for privacy concerns and/or organizational education of developers regarding privacy. Most notably, two participants described how their organizations systematically enforce rigor privacy policy via multiple workshops, memos and other information distribution channels for communicating and educating employees as to how to handle privacy.	*There are very clear guidelines [we need to follow] regarding privacy. For example, there are guidelines for the duration of keeping the information in the system. (I13)* *We had an in-house workshop that deals with privacy and protection of information. (I13)*
Negative	17 participants felt they were expected to comply with organizational norms and practices which do not conform with privacy concerns, and in many cases were in contradiction with the declared organizational privacy policy as well as their own moral values. However, these norm and practices de-facto determine the developers' behavior. Some of these participants did not refer to organizational policy. This implies that such policy either does not exist, or that employees are unaware of it.	*We use business data, which after 4–5 years may no longer be relevant. We should delete data when they become obsolete. We do not delete [data]. Ever. (I3)* *[Answering the question: Do you ever ask yourself if a specific purpose of collecting personal information is legal?]: Yes. But once I'm told to leave it, I go along with the organization. (I4)*

reflecting a positive organizational privacy climate, including organizational procedures governed by organizational policy, and in some cases additional strategies, such as a designated position within the organization responsible for privacy concerns, namely a Chief Privacy Officer (CPO), or means for educating developers to handle privacy concerns.

These means for promoting, distributing information, and educating developers about the privacy policy of the organization were evident in organizations where privacy is a core value, for example, in the healthcare and financial domains. In other cases, such as the telecommunication domain, the organizational policy, even where it clearly existed, was much less salient. Moreover, while the role of organizational privacy policy is to guide behavior within the organization regarding privacy concerns, we found a pattern of statements reporting on organizational norms and practices that led to participants' impression that they were expected by their organization to overlook privacy concerns, including the organization's own privacy policy and regulations. One participant even explicitly referred to the difference between organizations: "*The difference between Company X and Company Y is that Y emphasizes privacy more than X. In Y there are people leading the privacy concern, so you [the developer] have no choice but to treat it. It depends on the nature of the organization*" *(I15).* The "the nature of the organization", a murky definition indeed, points to the complex and indirect ability of privacy climate to affect the engineering culture.

Negative organizational privacy climate, while perceived as stemming from the organization's interests or simply due to omission of designated resources to implement privacy, was found in some of the instances to have substantial detrimental consequences, as demonstrated in the following example: "*There are plenty of organizational procedures regarding what to do about privacy. Each company has its own procedures. Many of these procedures are defined and clarified with time. For example, there was a situation in which we were sued as a company because we gave call details to a wife, who found that her husband was cheating on her because she could see who he was calling. Following this lawsuit, a procedure was defined on which identification details are needed in order to ensure that we are talking with the person authorized to receive this information. There is no law in this regard that we need to comply with, we need to understand how we – as a company – protect ourselves by ensuring that we do not provide information to the wrong person.*" *(I12).*

To summarize, it is clear that in many cases the organizations' privacy policies and their broader privacy climate are not always aligned. In some organizations, the organizational climate allows, and even promotes, behavior that is inconsistent with the official, defined policy or regulations, despite the risks of future losses in terms of money and reputation. Yet, in other organizations, the organizational climate promotes its privacy policy; supervision, communication and educational measures are taken to ensure that employees are aware of, and adhere with, the organizational privacy policy.

In both cases, we found that organizational climate is a powerful factor, almost inclusively determining the developers' behavior, regardless of whether it is aligned with policy, regulations, laws, or even the developers' own values and beliefs. In our study, most of the participants' reports demonstrate how the organizational privacy climate hinders privacy-preserving behavior. Yet, at the same time, acknowledging organizational climate as a decisive force affecting developers' behavior also points to a potentially promising and effective solution. We elaborate further on this direction in the discussion section.

4.4 Developers' Privacy Practices (B)

Looking into developers' privacy practices, we grounded our exploration in two aspects: (1) the privacy-related technologies they use in practice, and (2) their responses to privacy concerns.

Many kinds of privacy-related technologies are available for use. The participants were asked about this topic in two occasions: First, they were asked to describe examples from their past experience of using technological solutions for handling privacy concerns. Second, they were presented with a list of known technological privacy solutions and were asked to note, about each of them, whether they are familiar with it and whether they use it (see Appendix 2, question 6). This list of technological solutions was based on the list of FIPPs. We also made sure that there were enough examples of technologies following the two categories of the taxonomy proposed by Spiekermann and Cranor (2009) that differentiates between two types of solutions: *privacy-by-architecture* practices, in which the architecture of the system is designed in order to preserve privacy, and *privacy-by-policy* solutions, in which the system is configured (rather than designed) to support privacy. In privacy-by-architecture, the privacy of users cannot be violated even if the system operators wish to do so, because the architecture of the system itself prevents privacy risks. In privacy-by-policy, the users' privacy depends on the way the system is managed and on the policies of the system operators. Generally speaking, the privacy-by-architecture is a pure manifestation of privacy-by-design concepts, even though privacy can be enhanced through implementing privacy-by-policy solutions. We included in the list privacy-by-architecture choices that limit personal identifiability, including encryption, anonymization and decentralization, as well as privacy-by-policy options that include user control, access, and limitations on data collection.

In the open question, the participants were encouraged to provide examples from their own experience, in which they actually implemented or designed privacy solutions within a system. Eleven (11/27) participants did not have any experience of implementing such a solution and could not recall any privacy strategy they were familiar with. The rest of the participants (16/27) each described a single technological strategy. We followed the aforementioned taxonomy (Spiekermann and Cranor 2009) for classifying the noted solutions to the two privacy categories: by-architecture and by-policy. In addition, a third category of solutions stemmed from the data analysis: security solutions that protect the system from malicious third parties that attack the system from the outside. The participants' answers distributed as follows: three examples of privacy-by-architecture solutions, seven examples of privacy-by-policy, and six examples of security solutions.

Overall, analyzing the solutions the participants described reflects the limitations of the developers' privacy solution toolbox. The architectural changes were relatively basic, with heavy reliance on access control mechanisms. None of the participants questioned the fundamental architecture of the system to support privacy, or described situations in which the architecture was altered to support privacy. Rather, the existing architectures and framework were configured or adjusted to support policies.

The answers to the second question, regarding familiarity and use of technological solutions we presented to the participants, are presented in Fig. 2. The most familiar, as well as most frequently used solution was found to be encryption, which was reported to be familiar and used by *all* participants. Note that encryption is used in many security scenarios, highlighting once again that developers associate privacy with security. The second and third most used solutions refer to the *user access* privacy principle. This result is somewhat unexpected, since

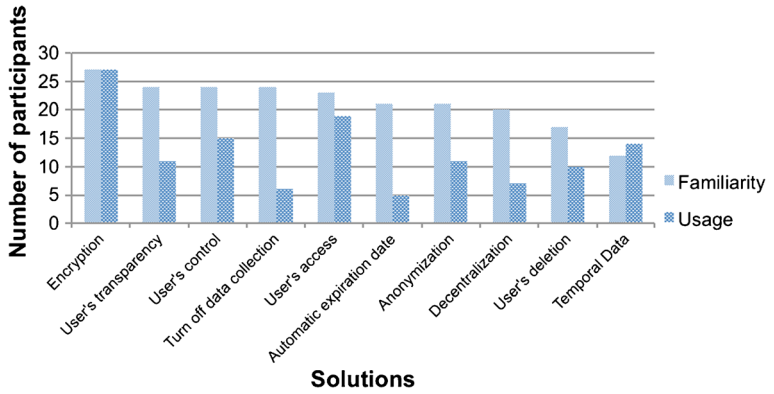

Fig. 2 Familiarity and usage of informational privacy solutions

the participants almost never mentioned access during the interviews in general, and in the privacy definitions in particular. Possibly, while most participants are familiar with these strategies, they do not necessarily associate them with privacy.

The fourth most used solution was temporal data, which refers to a strategy in which the collected data is regularly deleted after using it. For example, credit card numbers cannot be stored, and are deleted immediately after their use. This solution, again, is related to the *security* principle, as it limits the ability of malicious third-party agents to access and (mis)use sensitive information.

As Fig. 2 shows, most of the participants are familiar with most of these solutions. However, except for the case of encryption, the use of these strategies is less frequent than their familiarity. An obvious explanation for this difference could be report bias; participants may tend to report on familiarity of technological solutions even when they are only superficially familiar or even not familiar with them at all. However, we found an additional explanation in the participants' comments about these strategies. For example, see the following comments: the first in the context of decentralization, and the second in the context of automatic expiration date: "*I don't use it [decentralization] and I think it's a bad idea. Data decentralization should be considered according to the system's requirements, and not in order to protect the data.*" *(P2);* "*Information is valuable to the company and therefore is not deleted.*" *(I7).* These and similar comments participants made correspond with the previously identified developers' interpretation of business considerations being of a higher priority over informational privacy (see section 4.2).

The actual use in practice of existing technological strategies for privacy preservation may influence, as well as be influenced by, the developers' perceptions. For example, the perceived strong association of privacy and security may influence developers to use more security-based solutions to resolve privacy concerns, and vice versa, their high familiarity and experience with security-related solutions may form their tendency to use the security hammer to resolve any privacy concern.

In addition to the observations above, when examining how the participants responded when encountering privacy concerns, we found a tendency, demonstrated by many of the participants, of not taking responsibility over privacy: most of the participants (17/27) expressed a clear statement that handling privacy concerns is not within their responsibility; four participants were inconclusive whether this topic falls within their responsibilities; and the remaining six participants stated that they are responsible for informational privacy. The

tendency of not taking responsibility over privacy was manifested in quotes such as the following: *[If a privacy* concerns *arises] I would forward it to the relevant role to handle, either to the system owner, security department or my managers (I3); It [privacy] is not within my domain; we are not really doing anything about it (I18).* This adds another aspect to the one discussed above, namely that the tendency to use the security hammer is operationalized only in cases of developers who believe it is their responsibility to deal with the (privacy) nail to begin with.

5 Discussion

Privacy by Design (PbD) advocates the introduction of privacy considerations into the technological system design. Therefore, PbD delegates responsibility over privacy to those in charge of the design of information technologies, namely software developers. For PbD to be a viable option, it is essential to understand developers' point of view with regard to privacy. This study provides qualitative insights into the different factors formulating the mindset and behavior of developers regarding privacy, and proposes a model for classifying these factors and the relations between them based on the adoption and adaptation of the schema of SCT. The proposed theoretical model reflects the mechanisms unveiled in this qualitative research. Further quantitative research will enable substantiating and generalizing these categories and the relations between them.

Our findings indicate that developers use the vocabulary of data security to approach privacy challenges, and that this vocabulary limits their perceptions of privacy mainly to third-party threats. This perception is interestingly similar to perceptions that were previously identified in the context of users, rather than developers; specifically, that users often reduce the notion of privacy to security concerns only (Sheth et al. 2014). We detail the environmental mechanisms that influence, and are influenced by, developers when handling privacy concerns, identifying organizational privacy climate as a powerful means for organizations to guide developers toward particular interpretations of privacy, and specifically their perceptions as to how they are expected to act upon privacy concerns, which can either be aligned or conflict with the stated policy. In addition, we describe how software architectural patterns frame the privacy solutions that are used throughout the development process, and provide evidence that developers prefer policy-based solutions to architectural solutions.

These findings suggest a possible explanation for the slow acceptance of PbD in practice. While PbD is much hailed in policy circles, the way developers perceive privacy, the use of personal data by the organization and the stemming privacy ramifications differ to a great extent from the policy makers' view. As PbD relies on developers to incorporate privacy into the core architecture of the system, the narrow way developers interpret privacy may well be translated to the low implementation of PbD. Thus, for PbD to become a useful policy tool, this gap should be bridged. One way to do so turns to the causes of the gap. A recent study of discourse analysis based on engineering professional literature reveals one possible cause: the technology's privacy mindset, as reflected in leading engineering textbooks, and the legal mindset share little ground (Birnhack et al. 2014). For PbD to succeed, engineers should learn more about privacy (and of course, lawyers should learn more about technology). We suggest that there is an urgent need for a shift in technological education and literature that will teach concrete ways, in which a design can achieve both the technological goals of usability and functionality, and at the same time, cater for the privacy needs.

An additional important finding is the central role of organizational climate, and specifically the *organizational privacy climate,* in forming engineers' mindset and behavior. We found that developers' understanding of the way the organization expects them to behave when encountering privacy concerns dictates the way they behave, regardless of regulations they might be familiar with, their own beliefs, or even the organization's formal policy. This is strongly aligned with literature. Studies in different domains in the context of organizational climate suggest that organizational environment and organizational norms have a large impact on employees' perceptions and behavior (Stamper et al. 2000) and found significant effects of specific dimensions of organizational climate on employees' behavior (e.g., (Argyris 1960; Eisenberger et al. 1990; Nicholson and Johns 1985).

Several studies examining specific organizational characteristics and their effect on privacy-related behaviors were conducted thus far. For example, Balebako et al. (2014) observed that developers from smaller companies are less likely to demonstrate positive privacy and security behaviors. Our research further extends the relations between company characteristics and privacy decision-making, grounding characteristics in the concepts of organizational climate. We demonstrate that privacy climate differs between organizations, which may well be related to size and to other external characteristics such as the business domain, and can also be influenced by internal characteristics, such as management and specific roles within the company (to be further elaborated on below), all ultimately forming the organizational privacy climate. This finding not only reveals the situation in its current complexity, it opens a hatch to potential means for improvement.

The construct of a facet-specific organizational climate refers to "shared perceptions among members of an organization with regard to aspects of the organizational environment that inform role behavior, that is, the extent to which certain facets of role behavior are rewarded and supported in any organization" (Zohar and Luria 2005). Organizational climate's strength is determined via designated measures developed uniquely for a given facet. Special attention is given to facets that present competing operational demands to other, core facets; for example, caring for work safety reduces productivity. In such cases effective indicators are actual, enacted procedures and practices which should be distinguished from formally declared policies, thus reflecting the true priorities of the organization (Zohar 2000). The literature of organizational climate offers solidification of a focused climate approach to understanding organizational processes and outcomes, leading to survey approaches to culture and multi-level work on climate, climate strength, validity for a climate approach, and the relationship between leadership, climate and culture (Schneider et al. 2016). The development of climate strength measures requires development of designated surveys focusing on reported actual behavior and perceived expectations in the context of the measured facet of organizational climate. For example, Zohar (1980) describes the development of a focused safety climate measure including, e.g., employee perceptions of management attitudes toward safety and effects of safety behavior on promotion and status within the organization. This measure was significantly related to safety inspectors' rankings of organizations' safety practices and accident prevention programs. Luria (2008) proposes a measure for organizational quality climate, that is calculated based on a scale of quality behaviors of individual employees and their managers, as ranked by the employees, while accounting for management leadership. Similar measures have been developed for organizational climates relating to service, justice, leadership and more (Schneider et al. 2016).

The informational privacy facet in software systems development demonstrates similar characteristics to the facets mentioned above, by competing with other facets that are typically

perceived of higher priority, such as productivity and software usefulness. Since the topic of organizational privacy climate has thus far not been examined, we believe that valuable lessons can be learned from previous research examining the change of employees' behavior via organizational climate, such as in the context of work safety and ethics, two areas in which organizational climate was found to be highly influential. Studies on work safety found that organizations with strong safety climates report fewer injuries than organizations with weak safety climates (Brown and Holmes 1986; Cooper and Phillips 2004; Gershon et al. 2000; Gimeno et al. 2005; Grosch et al. 1999; Siu et al. 2004; Varonen and Mattila 2000; Zohar 2000). Mohamed (2002) corroborates the importance of the role of management commitment, communication, workers' involvement, attitudes, competence, as well as supportive and supervisory environments, in achieving a positive safety climate. Studies that investigated organizational ethics as an aspect of organizational climate similarly examined the effect of the ethical climate on employees' behavior. Organizations with stronger ethical climates were found to contribute to employees' ethical behavior and perceptions thereof (Bartels et al. 1998; Deshpande 1996; Jaramillo et al. 2013). Supervision was found to highly influence ethical climate and ethical behavior (Wimbush and Shepard 1994).

Based on the above, it is reasonable to infer that a climate of an organization in a certain area is quite predictive of its employees' behavior and is highly affected by the values and climate that management adopts. The components that were found to affect organizational climate, such as management commitment and communication with employees, need to be considered when forming a plan to change it. Specifically, an important factor repeatedly mentioned in the literature is internal supervision, which was found to significantly change organizational climate and employees' behavior. In the context of privacy, a Chief Privacy Officer (CPO) with high visibility and authority in the organization could successfully fulfill this role. Another interesting topic addressed in organizational literature is the importance of empowering employees to take initiative and serve the collective interests of the company as though they are its owners, without being micro-managed, in order to succeed in today's global business environment with its knowledge and creativity requirements (Spreitzer 2008 and the references therein). In software projects, where requirements are often under-maintained and under-managed, and different risks may present themselves in different products, developer disclosure is important for translating the general privacy policy or law to concrete software requirements.

Future research could focus on defining measures for organizational privacy climate, as done in previously investigated organizational climates. Such measures would be instrumental for managing and controlling different mechanism for increasing positive organizational privacy climate toward improving awareness, interpretation, and behavior of developers in the context of addressing privacy concerns in the developed software systems.

The contribution of this study is threefold. First, the research empirically unveiled the current privacy mindset of developers, namely that many of them hold a partial understanding of privacy, and interpret it as being of relatively low priority. Second, the analysis of the data led to insights regarding the forces forming and formed by this mindset, identifying existing technological solutions the developers use and organizational climate as highly influencing their mindset and vice versa. Finally, based on the findings and related research on organizational climate, we propose forming a strong positive organizational privacy climate and appropriate education to familiarize developers with privacy solutions beyond those addressing security concerns, as a future direction for improvement mechanisms.

The findings and their applicability as discussed in this paper are relevant to professionals involved in the development of any software system in which personal data are stored. The findings are also relevant to educators, as well as to researchers from different fields engaged in informational privacy (data protection) research, including the fields of information systems, software engineering, computer science, law, philosophy, and organizational studies. The theory presented in this paper and the identification of some of the sources of the phenomenon represented by the adapted SCT model, offers directions for bringing about change to the current situation, pointing to possible improvement mechanisms, starting with organizational privacy climate.

6 Limitations

Some limitations should be considered in interpreting the findings of this study. Examining how developers understand and behave upon informational privacy was not possible by direct observations of their work, due to relatively rare instances of handling privacy related concerns. Therefore, data collection was based on interviews, relying on retrospective data that may be biased due to memory error and self-serving bias. Moreover, in the settings of the interviews, time was pre-allocated and no time pressure or other kinds of stress were observed. This setting is different from real-life software development practice, presenting less time and performance pressure. While this can be considered a limitation as well, in the context of the findings of this study – when developers were specifically asked to discuss privacy and so were highly attuned to this topic – we expect their answers to reflect more attention and consideration of privacy than in the complexity and tight schedule of real-life situations. Thus, their actual behavior regarding privacy is expected to be *even less* considerate of privacy than the perceptions and attitudes found in this study indicate.

Our sample includes 27 software developers. While this list of participants was determined according to the theoretical sampling principles, and reflected varied domains, organization types and extent of experience, we cannot say that it provides a statistically representative sample of the population of developers. A point of strength is the theoretical saturation reached based on the analysis of the data collected from eighteen participants, further verified and validated with the data collected from the additional nine participants. Nevertheless, due to our limited, nonrandom sample, caution should be exercised in generalizing the findings. Future research in additional domains, and using quantitative research methods, could contribute to the generalization of these finding and the validation of the theoretical model, its components and the relationship between them, as identified in this study.

7 Conclusion

Privacy by *designers*? Well, not just yet. Examining the point of view of software developers, it seems that, except in the context of specific domains, software developers are actively discouraged from making informational privacy a priority, being expected to conform to norms and practices dictated by a negative organizational privacy climate. But the problem goes deeper than mere prioritization; many developers do not have sufficient knowledge and understanding of the concept of informational privacy (data protection), nor do they sufficiently know how to develop privacy-preserving technologies. If PbD is ever to become a viable practice, a considerable change is to be made for preparing the field for the wide implementation of this policy. The findings of this study suggest that *organizational privacy climate* highly influences developers' privacy interpretation and

behavior; thus, it may potentially serve as an effective mechanism to bring about the required change in the privacy mindset and practices as to informational privacy, starting with the adaptation of organizational policy to the principles of FIPPs and followed by the diffusion of this policy into the organizational climate. Other findings, notably developers' high familiarity with security solutions, as opposed to solutions of other privacy-related concerns, as well as developers' preference to use privacy-by-policy rather than privacy-by-architecture solutions, indicate that developers lack the required knowledge for effectively design privacy preserving technologies. A well-designed educational program would increase developers' knowledge and skills for designing privacy. Providing developers with knowledge, by means of education, as well as motivation, by means of positive organizational privacy climate, could potentially create the mindset required for designing privacy-preserving solutions. Future research may examine these and other means and their actual effect on developers' perceptions and attitudes toward informational privacy. If successful, this would be an important and necessary step toward wide and effective implementation of PbD.

Acknowledgement We acknowledge the support of the Israel Science Foundation, Grant 1116/12.

Appendix 1: Participants

Table 4 List of participants

ID	Role	Academic education*	Years of experience	No. of subordi-nates	Domain	Company size***
I1	Architect	None**	13	0	Healthcare	Large
I2	System analysts	Practical SE	11	0	Telecom	Large
I3	Architect	B.A.: Business admin.; MBA	4	0	Telecom	Large
I4	Architect	B.A.: Business admin.	12	0	Telecom	Large
I5	CTO	B.Sc. + M.Sc.: CS	8	4	Mobile Application	Small
I6	Architect	B.Sc.: CS	7	12	Enterprise systems	Small
I7	Architect	B.Sc.: CS	4	5	Telecom	Large
I8	Architect	B.Sc.: SE	4	0	Telecom	Large
I9	Architect	B.Sc.: CS; M.A.: Law	10	5	Enterprise systems	Small
I10	Architect	B.Sc. + M.Sc.: CS	30	15	IT Research -Privacy	Enterprise
I11	Team manager	B.Sc.: SE; M.Sc.: IS	15	0	Healthcare	Enterprise
I12	Chief Architect	None	15	5	Telecom	Large
I13	Chief Architect	Practical SE	23	45	Healthcare	Enterprise
I14	Chief Architect	B.Sc.: CS + Math M.Sc..: CS	14	0	Enterprise systems	Medium
I15	Chief Architect	B.Sc.: CS+ Criminology M.Sc..: CS	15	0	Enterprise systems	Small
I16	Architect	B.Sc.: IS	17	10	Retail	Large
I17	Architect	Military training in software development	8	7	Enterprise systems	Small
I18	Architect	Practical SE	17	8	Enterprise systems	Large
I19	Architect	None	13	12	Enterprise systems	Large
I20	Architect	B.Sc.: SE	10	0	Enterprise systems	Enterprise
I21	Architect	B.A.: Social sciences	7	0	Enterprise systems	Small

Table 4 (continued)

ID	Role	Academic education*	Years of experience	No. of subordi-nates	Domain	Company size***
I22	Department head	B.Sc.: SE; M.Sc.: CS	14	40	Defense systems	Enterprise
I23	Team leader	B.A.: Business admin.	10	8	Telecom	Enterprise
I24	Architect	B.Sc.: CS; MBA	10	25	Shipping	Large
I25	Architect	B.Sc.: SE	4	0	Enterprise systems	Enterprise
I26	Architect	B.Sc. + M.Sc.: CS	17	6	Enterprise systems	Enterprise
I27	Department head	B.Sc.: IS; MBA	10	12	Insurance	Large

*We use in this column the following abbriviations: SE (software engineering), CS (computer science), IS (information systems), MBA (masters in business adminstration),

**Most of the participants, and specifically the participants with no academic education (who define themselves self-educated), reported to have taken several non-academic technological courses over the years

***The size catgorizaiton was accoridng the no. of employees creteria, as follows: small <100, Meduim <1000, Large <10,000, Enterprise >10,000

Appendix 2: Interview Guide

1. Background information

    - Domain (of development), position, years of experience, number of subordinates, formal education, additional professional training
    - What sources of knowledge do you use beyond the requirements of the customer? (Colleagues? Friends outside the organization? Literature? Professional journals? Web? Other?)
    - Have you been involved in the development of information systems that handle information about users or other data subjects? If so, please describe your role in each project.
    - Have you acquired knowledge/education specifically related to privacy concerns in information systems? If so, please describe.
    - What development methodologies do you use?
    - Do you have direct communication with the customer?
    - When you take design decisions, do they affect others in the development team? If so, who is affected (and how many)? What are their roles?

2. Privacy definition

    - What is informational privacy?
    - What is the difference between security and privacy?

3. Information sources

    - What sources of information do you use in order to resolve privacy concerns?
    - (Internet / what sites? Organizational procedures? Managers? Other employees? Literature (which)?)

4. Guidelines

   - What laws are you familiar with, in the context of informational privacy?
   - What procedures are you familiar with, in the context of informational privacy?
   - What norms are you familiar with, in the context of informational privacy?

5. Cases and examples

   - When you encounter a privacy concern, what do you do about it?
   - In what cases do you consider or analyze privacy concerns, while designing a system?
   - When developing a system, what are the potential risks regarding privacy?
   - Describe three examples of projects you were involved in, in which privacy concerns were discussed. What aspects of privacy did you handle?
   - Are privacy concerns considered, in projects you are involved with, while designing user interfaces? If so, in what context?
   - Do you initiate discussions regarding privacy or require clarifications or additional privacy-related requirements when designing a system?
   - Is privacy taken into account when planning for future requirements?

6. Familiarity and use of privacy strategies

   - What strategies (presented in Table 5) are you familiar with as solutions for privacy concerns?
   - (Bring examples)
   - For each of the following strategies, please specify whether you are familiar with it, whether you use it, and why / in what cases do you decide not use it?

7. FIPPs

   - Does the organization inform its users about its privacy policy?
   - During your work, have you ever needed to address concerns of notifying users about ongoing operations or information theft? If so, how? At what stage?
   - In your opinion, to what extent is it important to receive consent from users prior to collecting private data about them?
   - In your opinion, to what extent do the users have the right to choose how, when and what information is gathered about them (that is, the freedom to design the information that is collected about them)?
   - Do you think that user consent for data collection should be opt-in (default is lack of consent, and requires active action to give consent) or opt-out (default is agreement, and requires active action to deny consent)?
   - Have you ever dealt with user consent in this context? In what stage of the development? Who raised the need? Is the topic of user consent discussed during projects?
   - Do you, or the customer (for whom the system is designed), define the purpose for which the information is collected by the system?
   - How do you decide what information is collected by the system? What are the considerations? Are they determined according to customer requirements? According to common practices? Some other criteria?

- Is the legitimacy of the purpose for which personal information is collected by the system discussed? Do you ever ask yourself if a specific purpose of collecting personal information is legal/problematic in any sense?
- In your opinion, should personal information accumulated about users in the system be deleted? If so, after how much time should it be deleted? (Immediately after the use of the information? after one month? three months? one year? two years? five years? ten years?)

8. Responsibility

- Is information privacy considered to be the responsibility of the architect?
- (If not): Whose responsibility is it?

9. Open discussion

- Do you have any other thoughts about informational privacy you would like to share?
- Why did you agree to be interviewed for this research?

Table 5 List of privacy strategies

Strategy	Familiar with	Uses
Decentralization of data so there is no central access point for all data		
Collected data is regularly deleted after usage		
Providing users control over privacy settings: What would be revealed to other users or system operators		
Optional "turn off" of overall data collection for a certain time frame		
Encryption technologies		
Data anonymization for management and analysis purpose		
User transparency about his/her information that is available in the system		
Systems that enable users to access personal information about them, which resides within the system		
Systems that enable users to delete personal information about them, which resides within the system		
Automatic expiration of personal information		

References

Ackerman MS, Cranor LF, Reagle J (1999) Privacy in e-commerce: examining user scenarios and privacy preferences. Proceedings of the 1st ACM conference on electronic commerce, Denver

Ammori M, Pelican L (2013) Media diversity and online advertising. Alb L Rev 76:665–696

Argyris C (1960) Understanding organizational behavior. The Dorsey Press, Oxford, England

Awad NF, Krishnan MS (2006) The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. MIS Q 30:13–28

Ayalon O, Toch E (2013) Retrospective privacy: managing longitudinal privacy in online social networks. Proceedings of the Ninth Symposium on Usable Privacy and Security

Balebako, R., Marsh, A., Lin, J., Hong, J., Cranor, L. F. (2014) The privacy and security behaviors of smartphone app developers. Workshop on Usable Security (USEC 2014), San Diego, 2014

Bamberger KA, Mulligan DK (2010) Privacy on the books and on the ground. Stanford Law Rev 63: 247
Bamberger KA, Mulligan DK (2013) Privacy in Europe: initial data on governance choices and corporate practices. Geo Wash L Rev 81:1529–1755
Bandura A (1986) Social foundations of thought and action: a social cognitive theory. Prentice-Hall, Englewood Cliffs
Bartels KK, Harrick E, Martell K, Strickland D (1998) The relationship between ethical climate and ethical problems within human resource management. J Bus Ethics 17(7):799–804
Berente N, Yoo Y (2012) Institutional contradictions and loose coupling: Postimplementation of NASA's enterprise information system. Inf Syst Res 23(2):376–396
Birnhack M, Elkin-Koren N (2011) Does law matter online? Empirical evidence on privacy law compliance. Michigan Telecommun Technol Law Rev 17:337
Birnhack M, Toch E, Hadar I (2014) Privacy mindset, technological mindset. Jurimetrics 55:55–114
Brown R, Holmes H (1986) The use of a factor-analytic procedure for assessing the validity of an employee safety climate model. Accid Anal Prev 18(6):455–470
Budi, A., Lo, D., Jiang, L., Lucia (2011) Kb-anonymity: a model for anonymized behaviour-preserving test and debugging data. PLDI 2011: 447–457
Castro M, Costa M, Martin JP (2008) Better bug reporting with better privacy. ACM Sigplan Notices 43(3):319–328
Cavoukian A (2009) Privacy by design: the 7 foundational principles. Information and Privacy Commissioner of Ontario, Toronto
Cavoukian A (2011) Privacy by design: origins, meaning, and prospects. Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards Information Science Reference (an imprint of IGI Global)
Cavoukian, A., Chibba, M., Stoianov, A., Marinelli, T., Peltsch, K., Chabanne, H., Despiegel, V. (2014) Facial recognition with biometric encryption in match-on-card architecture for gaming and other computer applications. eBook, York University, Toronto
Chan YE (2000) IT value: the great divide between qualitative and quantitative and individual and organizational measures. J Manag Inf Syst 16(4):225–261
Cooper MD, Phillips RA (2004) Exploratory analysis of the safety climate and safety behavior relationship. J Saf Res 35(5):497–512
Culnan MJ, Williams CC (2009) How ethics can enhance organizational privacy: lessons from the ChoicePoint and TJX data breaches. Manag Inf Syst Q 33(4):673–687
Dennedy MF, Fox J, Finneran T (2014) The privacy engineer's manifesto: getting from policy to code to QA to value. Apress, Berkeley
Deshpande SP (1996) Ethical climate and the link between success and ethical behavior: an empirical investigation of a non-profit organization. J Bus Ethics 15(3):315–320
Dinev T, Hart P (2006) An extended privacy calculus model for e-commerce transactions. Inf Syst Res 17(1):61–80
Eisenberger R, Fasolo P, Davis-LaMastro V (1990) Perceived organizational support and employee diligence, commitment, and innovation. J Appl Psychol 75(1):51
Fienberg SE (2006) Privacy and confidentiality in an e-commerce world: data mining, data warehousing, matching and disclosure limitation. Stat Sci 21(2):143–154
Friedman B, Kahn Jr PH, Borning A (2006) Value sensitive design and information systems. In: Human-Computer Interaction in Management Information Systems, M.E. S Sharpe Inc., pp 348–372
FTC (2012) Protecting consumer privacy in an era of rapid change: recommendations for businesses and policymakers. FTC Privacy Report
GDPR (2012) European Commission, Proposal for a regulation of the European Parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012PC0011. Accessed 14 Apr 2017
Gellman R (2013) Fair informaiton practices: a basic history http://bobgellman.com/rg-docs/rg-FIPShistory.pdf. Accessed 16 Aug 2013
Gershon RR, Karkashian CD, Grosch JW, Murphy LR, Escamilla-Cejudo A, Flanagan PA, Martin L (2000) Hospital safety climate and its relationship with safe work practices and workplace exposure incidents. Am J Infect Control 28(3):211–221
Gimeno D, Felknor S, Burau K, Delclos G (2005) Organisational and occupational risk factors associated with work related injuries among public hospital employees in Costa Rica. Occup Environ Med 62(5):337–343
Grechanik M, Csallner C, Fu C, Xie Q (2010) Is data privacy always good for software testing? In: 2010 I.E. 21st International Symposium on Software Reliability Engineering, IEEE, pp 368–377

Grosch JW, Gershon RR, Murphy LR, DeJoy DM (1999) Safety climate dimensions associated with occupational exposure to blood-borne pathogens in nurses. Am J Ind Med 36(S1):122–124
Gross R, Acquisti A (2005) Information revelation and privacy in online social networks. Proceedings of the 2005 ACM workshop on privacy in the electronic society, Alexandria
Gürses S, Gonzalez Troncoso C, Diaz C (2011) Engineering privacy by design. Comput, Priv Data Prot 14(3)
Jain S, Lindqvist J (2014) Should I protect you? Understanding developers' behavior to privacy-preserving APIs. Workshop on Usable Security (USEC'14)
Jaramillo F, Mulki JP, Boles JS (2013) Bringing meaning to the sales job: the effect of ethical climate and customer demandingness. J Bus Res 66(11):2301–2307
Kalloniatis C, Kavakli E, Gritzalis S (2008) Addressing privacy requirements in system design: the PriS method. Requir Eng 13(3):241–255
Lacity MC, Janson MA (1994) Understanding qualitative data: a framework of text analysis methods. J Manag Inf Syst 11:137–155
Lahlou S, Langheinrich M, Röcker C (2005) Privacy and trust issues with invisible computers. Commun ACM 48(3):59–60
Langheinrich M (2001) Privacy by design—principles of privacy-aware ubiquitous systems. International conference on ubiquitous computing. Springer, Berlin, Heidelberg
Lucia, Lo D, Jiang L, Budi A (2012) kbe-anonymity: test data anonymization for evolving programs. In: 2012 Proceedings of the 27th IEEE/ACM International Conference on Automated Software Engineering, Essen, 2012, pp 262–265
Luria G (2008) Controlling for quality: climate, leadership, and behavior. Quality Manangement Jounral 15(1): 27–40
Madejski M, Johnson ML, Bellovin SM (2011) The failure of online social network privacy settings. Department of Computer Science, Columbia University, tech. Rep. CUCS-010-11
Mathew A, Cheshire C (2017) Risky business: social trust and community in the practice of cybersecurity for internet infrastructure. In: Proceedings of the 50th Hawaii International Conference on System Sciences
Mohamed S (2002) Safety climate in construction site environments. J Constr Eng Manag 128(5):375–384
Myers MD (1997) Qualitative research in information systems. MIS Q 21:241–242
Myers MD, Newman M (2007) The qualitative interview in IS research: examining the craft. Inf Organ 17:2–26
Nicholson N, Johns G (1985) The absence culture and psychological contract—who's in control of absence? Acad Manag Rev 10(3):397–407
Ohm P (2010) Broken promises of privacy: responding to the surprising failure of anonymization. UCLA Law Review 57:1701
Omoronyia I, Cacallaro L, Salehie M, Pasqualie L, Nuseibeh B (2013) Engineering adaptive privacy: on the role of privacy awareness requirements. Proceedings of the 2013 International Conference on Software Engineering. IEEE Press, 2013
Ozer NA (2012) Putting online privacy above the fold: building a social movement and creating corporate change. NYU Rev L & Soc Change 36:215
Peters F, Menzies T (2012) Privacy and utility for defect prediction: experiments with MORPH. ICSE 2012:189–199
Peters F, Menzies T, Gong L, Zhang H (2013) Balancing privacy and utility in cross-company defect prediction. IEEE Trans Softw Eng 39(8):1054–1106
Reay, I., Dick, S., Miller, J. (2009) A large-scale empirical study of P3P privacy policies: stated actions vs. legal obligations. ACM transactions on the web (TWEB), 3(2), 6
Resnick ML, Montania R (2003) Perceptions of customer service, information privacy, and product quality from semiotic design features in an online web store. International Journal of Human-Computer Interaction 16(2): 211–234
Rubinstein IS, Good N (2013) Privacy by design: a counterfactual analysis of Google and Facebook privacy incidents. Berkeley Tech LJ 28:1333–1583
Sánchez Abril P, Levin A, Del Riego A (2012) Blurred boundaries: social media privacy and the twenty-first-century employee. American Business Law Journal 49(1):63–124
Schneider B, Ehrhart MG, Macey WH (2013) Organizational climate and culture. Annu Rev Psychol 64:361–388
Schneider B, González-Romá V, Ostroff C, West MA (2016) Organizational climate and culture: reflections on the history of the constructs in Journal of Applied Psychology. J Appl Psychol 102(3):468
Seaman CB (1999) Qualitative methods in empirical studies of software engineering. IEEE Trans Softw Eng 25(4):557–572
Shaw TR (2003) The moral intensity of privacy: an empirical study of webmaster' attitudes. J Bus Ethics 46(4): 301–318

Sheth S, Kaiser G, Maalej W (2014) Us and them: a study of privacy requirements across North America, Asia, and Europe. Proceedings of the 36th International Conference on Software Engineering. ACM, 2014

Siu O-L, Phillips DR, Leung TW (2004) Safety climate and safety performance among construction workers in Hong Kong: the role of psychological strains as mediators. Accid Anal Prev 36(3): 359–366

Smith HJ, Dinev T, Xu H (2011) Information privacy research: an interdisciplinary review. MIS Q 35(4):989–1016

Spiekermann S, Cranor LF (2009) Engineering privacy. IEEE Trans Softw Eng 35(1):67–82

Spreitzer GM (2008) Taking stock: a review of more than twenty years of research on empowerment at work. In: Handbook of organizational behavior. Sage, Thousand Oaks, pp 54–72

Stamper R, Liu K, Hafkamp M, Ades Y (2000) Understanding the roles of signs and norms in organizations-a semiotic approach to information systems design. Behav Inform Technol 19(1):15–27

Strauss A, Corbin J (1990) Basics of |qualitative research. Sage publications, Newbury Park

Strauss A, Corbin J (1994) Grounded theory methodology: an overview. In: Denzin NK, Lincoln YS (eds) Handbook of qualitative research. Sage, Thousand Oaks, pp 273–285

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

Stutzman F, Gross R, Acquisti A (2013) Silent listeners: the evolution of privacy and disclosure on Facebook. Journal of Privacy and Confidentiality 4(2):2

Suddaby R (2006) From the editors: what grounded theory is not. Acad Manag J 49(4):633–642

Székely I (2013) What do IT professionals think about surveillance? Internet and surveillance: the challenges of web 2.0 and social media, 16, 198

Taneja K, Grechanik M, Ghani R, Xie T (2011) Testing software in age of data privacy: a balancing act. Proceedings of the 19th ACM SIGSOFT Symposium and the 13th European conference on foundations of software engineering, ACM, pp 201–211

Tene O, Polonetsky J (2013) Big data for all: privacy and user control in the age of analytics. Northwest J Technol Intellect Prop 11(5):1

Thomas K, Bandara AK, Price BA, Nuseibeh B (2014) Distilling privacy requirements for mobile applications. Proceedings of the 36th International conference on software engineering. ACM, 2014

Toch E, Wang Y, Cranor LF (2012) Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems. User Model User-Adap Inter 22(1–2):203–220

Tsai MT, Cheng NC (2010) Programmer perceptions of knoweldge-sharing behavior under social cognitive theory. Expert Syst Appl 37(12):8479–8485

U.S. Dept. of Helath, Education & Welfare (1973) Record computers and the rights of citizens. REp. of Sec'y Advisory Comm. on Automated Pers. Data Sys. 41 (1973). http://www.justice.gov/opcl/docs/rec-com-rights.pdf

Van Der Sype YS, Maalej W (2014) On lawful disclosure of personal user data: what should app developers do? 7th International Workshop on Requirements Engineering and Law (RELAW), IEEE 2014

van Lieshout M, Kool L, van Schoonhoven B, de Jonge M (2011) Privacy by design: an alternative to existing practice in safeguarding privacy. Info 13(6):55–68

van Rest, J., Boonstra, D., Everts, M., van Rijn, M., van Paassen, R. (2014) Designing privacy-by-design. Privacy Technologies and Policy, Springer Berlin, Heidelberg

Varonen U, Mattila M (2000) The safety climate and its relationship to safety practices, safety of the work environment and occupational accidents in eight wood-processing companies. Accid Anal Prev 32(6):761–769

Walsham G (2006) Doing interpretive research. Eur J Inf Syst 15(3):320–330

Wimbush JC, Shepard JM (1994) Toward an understanding of ethical climate: its relationship to ethical behavior and supervisory influence. J Bus Ethics 13(8):637–647

Wood R, Banduar A (1989) Social cognitive theory of organizational management. Acad Manag Rev 14(3):361–384

Zohar D (1980) Safety climate in industrial organizations: theoretical and applied implications. J Appl Psychol 65:96–102

Zohar D (2000) A group-level model of safety climate: testing the effect of group climate on microaccidents in manufacturing jobs. J Appl Psychol 85(4):587

Zohar D, Luria G (2005) A multilevel model of safety climate: cross-level relationships between organization and group-level climates. J Appl Psychol 90(4):616–628

Irit Hadar is a tenured faculty member at the Department of Information Systems, University of Haifa, and the Head of the Software Architecture Laboratory at the Caesarea Rothschild Institute for Interdisciplinary Applications of Computer Science. She received her Ph.D. in Computer Science Education, from the Technion – Israel Institute of Technology. Her main research area is cognitive aspects of requirements analysis, software architecture and design. Hadar has been serving as an organizer and PC member in conferences and workshops (e.g., RE, CAiSE, ICIS), founded and organizes a workshop series on cognitive aspects of information systems engineering (COGNISE) and has served as an editorial board member of the ACM Transactions on Computing Education (2011-2015). Contact hadari@is.haifa.ac.il. More information at: is.haifa.ac.il/~hadari.

Tomer Hasson is an experienced software architect, mostly at the field of integration and process development (EAI and B2B), and has been working in the past 10 years as a Software Architect. Hasson received a MSc in Information Systems from the University of Haifa, and is also Alumni of Software Architecture Laboratory at Caesarea Rothschild Institute for Interdisciplinary Applications of Computer Science at the University of Haifa. He received his computer science degree from Ort Braude College. Contact: tomer.hasson@gmail.com.

Oshrat Ayalon is an information systems scientist with an interest in human computer interaction and usable privacy and security; she is a PhD candidate at the Department of Industrial Engineering of Tel Aviv University.

Eran Toch is a tenured faculty member at the faculty of Engineering at Tel-Aviv University, Israel. His research is in the field of usable security and privacy, human-computer interaction, and information systems. Eran's research group is working on various engineering challenges that revolve around computationally understanding human behavior, and applying this knowledge to solve real-world security and privacy challenges. The group is funded by grants from the Israel Ministry of Science, Israel Science Foundation, DARPA, EU Horizon 2020, and other resources. More information is available at http://toch.tau.ac.il.

Michael Birnhack is Associate Dean for Research at the Faculty of Law, Tel Aviv University, where he also directs the Parasol Foundation Trust International LLM Program and the S. Horowitz Institute for IP. His research interests are information law, and especially privacy, copyright and free speech, in dynamic settings. Birnhack served on the Israeli Public Council for the Protection of Privacy (three terms), and was a sub-contractor for the EU Commission for its evaluation of the adequacy of Israel's data protection law. He holds an LLB degree from TAU Law (1996), LLM from NYU School of Law (1998) and JSD (NYU, 2000). Contact: birnhack@tau.ac.il Personal Site: https://en-law.tau.ac.il/profile/birnhack.

Sofia Sherman is a research fellow at the Software Architecture lab in the University of Haifa. Her research interests include requirements engineering, architecture processes and the role of the architect in different development methodologies, and human aspects of software engineering. Sherman received her Ph.D. from the Department of Information Systems at the University of Haifa. She has recently started her postdoctoral fellowship at the Cheriton School of Computer Science, University of Waterloo.

Arod Balissa is an attorney and the Cyber & Health Sector Manager at Deloitte IL's Innovation Tech Terminal, specializing in Start-Up Consulting Services. He holds a Bachelor's and Master's (Magna Cumme Laude) Degrees in Law from Tel-Aviv University. His research experience includes the legal aspects of emerging technologies, Artificial Intelligence, International Law, Data Protection and Complex Adaptive Systems. Balissa serves as a director in several non-profits in Israel and is involved in several local social enterprises. Contact at arodba@gmail.com.