Working Paper: WU_MIS_1_2018

Engineering Privacy by Design: Are engineers ready to live up to the challenge?

Kathrin Bednar, Institute for MIS, WU Vienna

Sarah Spiekermann, Institute for MIS, WU Vienna

Marc Langheinrich, University of Lugano

ABSTRACT

Organizations struggle to comply with legal requirements as well as customers' calls for better data protection. Yet, information privacy depends on system engineers putting effort into the matter. We interviewed six seniors in system engineering, who work for globally leading IT corporations and research institutions in order to investigate their motivation and ability to comply with privacy expectations. The results of our in-depth interview study point to a lack of perceived responsibility, control and autonomy and to a struggle with the legal world. The information society may be facing the dilemma of asking engineers to live up to a challenge they are currently not ready to embrace.

Introduction

Privacy is hardly a new topic. Over the years, a plethora of research and review articles as well as books on ethics and IT have pointed to the importance of privacy (Johnson 2009; Baase 2008; Vermaas et al. 2008; Culnan and Armstrong 1999; Acquisti, Brandimarte, and Löwenstein 2015; Bélanger and Crossler 2011; Smith, Dinev, and Xu 2011). Other literature discusses how privacy can be undermined as well as protected by an appropriate system design (Friedman, Kahn Jr., and Borning 2006; Cavoukian 2009; Spiekermann 2012; Spiekermann and Cranor 2009). Core privacy regulation has been passed and adopted since the 1980s (see, e.g., the privacy guidelines of the Organisation for Economic Cooperation and Development, OECD, 1980, and the Directive 95/46/EC of the European Parliament and Commission, 1995). Privacy technologies were already launched in the 1990s (e.g., Pretty Good Privacy, PGP, proposed by Zimmermann in 1995, or Privacy by Design, introduced as privacy-enhancing technology by Hes and Borking 2000). Privacy by Design pushes respect for user privacy while maintaining full system functionality. It stands for proactive and preventative measures that embed privacy in system design, set privacy as a default and ensure consent-based transparency of the processing, transfer and storage of personal data throughout the data lifecycle (Cavoukian 2010; Spiekermann 2012; Spiekermann and Cranor 2009). Therefore, Privacy by Design "requires the guts and ingenuity of engineers" (Spiekermann 2012, 39) as it is the system engineers who have to find a competent and creative way to realize privacy implementations. The question of this paper is: Are engineers ready to live up to this challenge?

More than twenty years ago, Smith (1994) investigated privacy management in the corporate landscape of the United States. He found issues with all three societal mechanisms that influence corporate decisions. First, he found that the individual consumer cannot exert pressure through the market system, as consumers are often not informed about privacy intrusions, or it is not even clear what a privacy intrusion is. Second, management lacks time and resources to proactively initiate corporate behaviours that are in accordance with societal expectations. And third, U.S. legislators lag behind with privacy regulations and target privacy issues in a too narrow way, if they do so at all. For a successful future management of information privacy, Smith therefore asked for a systemic fix, rather than a regulatory one.

What is the situation today? With the increasingly important role that the Internet and new information technologies (IT) play in our everyday lives, concerns about information privacy are growing. Consumer studies reveal that unease is spreading among citizens, as people fear to lose control over their personal data. In the United States (Pew Research Center 2014) as well as in Europe (TNS Opinion & Social 2015), the majority of consumers feel that they have lost control over their personal data and are concerned that third party companies or the government access their personal information. At the same time, digital privacy breaches abound all over the world. Recent reports have revealed hundreds of data breaches in different sectors (such as banking, business, or healthcare), which amounted to tens of millions of exposed records (Identity Theft Resource Center 2016; Verizon 2017). Regulators have started to react to these developments. In the U.S., new privacy regulations have been called for (The White House 2015) in addition to several sectorial privacy regulations (for a good overview, see the Privacy Bridges 2015 report). In Europe, the new "General Data Protection Regulation" (GDPR; The European Parliament and the Council of the European Union 2016) enforces the protection of personal data. At the same time, personal data markets

flourish more than ever before (Christl 2017) and personal data is considered the "new oil" of the digital economy (Schwab et al. 2011). Against this background, corporations find themselves torn between a rising call for more privacy-friendliness on one hand and the pressure to participate in the data economy on the other hand (Spiekermann et al. 2015). How does this situation influence the behaviours and attitudes of system engineers? Have engineers become more aware of privacy issues? Have they assumed their responsibility and acquired the competences they need to build privacy-friendly systems? And are they provided within their corporations with the resources they need?

Very little is known about the subjective attitudes of system engineers towards ethical behaviours such as Privacy by Design. Scholars have presented a holistic model of software engineers' general job motivation (Sharp et al. 2009) and have looked at personality types of software engineers (Cruz, da Silva, and Capretz 2015; Varona et al. 2012). But when it comes to the study of practical ethics by design, the literature is sparse. Berenbach and Broy (2009) have recently presented a practical analysis showing how organizational constraints impede engineers to behave ethically on the job and in line with the code of ethics and professional conduct of the Association for Computing Machinery (ACM)[3]. This is countered by Szekely (2011), who studied a broader group of IT professionals and found that IT people live up to ethical demands if they are asked to do so by their organizations. They normally comply with decisions taken by their employers, regardless of whether these are in line with ethical conduct or not. However, none of these studies focus on information privacy specifically.

Fifteen years ago, Langheinrich and Lahlou (2003) studied engineers' privacy behaviour to gather best-practice methods of researchers with regard to the incorporation of information privacy in system design. Their empirical study revealed that engineers were rarely aware of their responsibility at the time. For the interviewed researchers, privacy was "not yet necessary" as they first wanted to build prototypes, but at the same time privacy often turned out to be "no problem for prototypes". They saw privacy as "too abstract of a problem" that was "not necessary anymore" as security mechanisms like firewalls could take care of it. Langheinrich and Lahlou (2003) also reported that researchers were "not feeling morally responsible" – they felt it was "not up to them", e.g., because they lacked expertise. In some cases it was mentioned that privacy issues were simply "not part of deliverables" and therefore the necessary time had not been reserved for it by their organizations. What is more, Birnhack, Toch, and Hadar (2014) point out that standard textbooks used in computer science education (e.g., Sommerville 2011) do not teach engineers any timely knowledge on Privacy by Design. Instead, they reinforce the idea of maximizing data collection and minimizing the engineering effort regarding non-functional requirements.

More recent research seems to indicate that system engineers' concern for privacy and their users has grown over the past few years. For example, computational modellers have stressed the importance of being faithful to reality and to users' values, as expressed in this statement of one modeller: "If we're going to produce models, they need to be accurate and they need to be useful. I don't want to lead people along the wrong path... They need to be grounded in a code of ethics. I think it's essential." (Fleischmann, Wallace, and Grimes 2010, 3). Similar results were presented by Greene and Shilton (2017, 8), who found that an "ethic of care" for users is common among app developers. They concluded that developer forums such as the iPhoneDevSDK forum and the Android XDA forums act as quasi-regulators, setting privacy expectations for applications to be published on their platform stores and thereby guiding app developers' privacy efforts. Complementary research showed that certain work practices, such as navigating the platform's approval or user requests, can act as levers for privacy

discourse, triggering larger debates on privacy and ethical requirements in general (Shilton and Greene 2017).

Hence, we begin to understand some factors that determine engineers' ethical motivations, but we have hardly any understanding of system engineers' subjective attitudes toward ethical system design. We know little about their attitudes and beliefs regarding information privacy, their knowledge, skills and their true degrees of freedom in organizations. This gap in research calls for a comprehensive study of system engineers' privacy engineering behaviour, which we are presenting in this article.

We conducted two complementary studies [1] to investigate engineers' privacy engineering behaviours and intentions. First we conducted an in-depth qualitative study. We conducted 7.5 hours of semi-structured interviews with a small sample of senior system engineers working for some of today's largest global software companies and renowned research institutions, the results of which will be presented hereafter. These interviews were complemented by a larger-scale survey-based study with 124 system engineers (see working paper 2: Spiekermann, Korunovska, and Langheinrich 2018). Our qualitative and quantitative investigations were guided by the Theory of Planned Behaviour (TPB; Ajzen 1985, 1991, 2002) as well as Jonas's work on the imperative of responsibility (Jonas 1984). This paper focuses on the in-depth learnings we gathered from our interviews, which provide a deep and nuanced understanding of the views engineers hold towards privacy engineering. We also report selected results obtained from the survey (Spiekermann, Korunovska, and Langheinrich 2018) to underline that our interviews revealed issues that can be confirmed from a larger perspective.

We chose a mixed methods approach for the analysis of the interview data. We first applied a qualitative content analysis to inductively construct a system of categories and subsequently assessed how often a category was found within the interviews, thereby gaining a quantitative representation for each of the categories. Our investigations were guided by the Theory of Planned Behaviour (TPB; Ajzen 1985, 1991, 2002) as well as Jonas's work on the imperative of responsibility (Jonas 1984). We used the TPB as theoretical framework for our empirical research in order to understand system engineers' ethical thinking within their organizational settings. Two consecutive review papers that cover the empirical ethical decision-making literature from 1996 to 2011 pointed out that the relationship between moral intent and moral behaviour has not been sufficiently studied and needs further empirical exploration (O'Fallon and Butterfield 2005; Craft 2013). As Ajzen's TPB predicts this link between intent and act, it seems especially fitting as theoretical framework to explain system engineers' ethical decision-making. Other theories, such as the organizational legitimacy theory (Suchman 1995), also describe the relationship between an organization and its stakeholders. However, while organizational legitimacy focuses solely on attitudes, Ajzen's TPB models how attitudes are translated into behaviours.

In the following, we first review the literature on engineers' privacy attitudes, beliefs and work contexts as well as work autonomy. We then present the results from our interviews with four senior system engineers and two heads of academic software groups as well as complementary evidence gathered from our survey. Our literature review and empirical results offer a deep insight into system engineers' attitudes, emotions and beliefs as well as their latitude regarding ethical decision-making within their organizational context.

[1] See our two working papers: https://www.wu.ac.at/ec/research/

Literature review on issues relevant for privacy engineering

The TPB states that the intention to engage in a specific behaviour is generally caused by three core factors: (1) people's instrumental and experiential attitudes towards a behaviour, (2) people's subjective norms, and (3) their perceived behavioural control. For our study context, this translates into engineers' intention to engage in Privacy by Design as a result of their attitudes towards information privacy, their personal and professional environment, and their degree of control over their systems' design. We defined privacy engineering as any activity undertaken by an engineer (i) to reduce the collection and storage of *personal* data (e.g., through data minimization or anonymization), (ii) to limit the sharing of personal data with third parties not explicitly authorized by the data subject, (iii) to give users full information about what happens to their personal data (i.e., transparency), and (iv) to give users real choice whether they consent to the processing of their personal data or not. We used the TPB to systematically review the literature on ethical engineering and structure our findings accordingly.

Attitudes and beliefs

Attitudes towards a behaviour are experienced in two forms: instrumental attitudes determine if we find a behaviour useful and sensible; experiential attitudes determine if we find a behaviour enjoyable and pleasant. Both forms of attitudes are typically driven by beliefs (Ajzen 1991). For instance, if an engineer believes that "any system can be hacked", this belief tends to negatively influence his attitude to invest his time in Privacy by Design.

The call for information privacy is met with scepticism and pessimism. Many voice the belief that "privacy is dead" in an age where people share so much of their personal data on social network platforms (Heller 2011). Also, privacy is regarded as a value that needs to be traded off for more (national) security (Pavone and Esposti 2012; Bowyer 2004), for more transparency (Cochrane 2000; Mayes 2010) or knowledge creation (Land, Nolas, and Amjad 2004). Studies have found that privacy-friendly system designs can undermine functionality as well as convenience of a system for users (Nakayama, Chen, and Taylor 2016) as well as service administrators (Ciocchetti 2007). Embracing a Privacy by Design approach for a system costs time and money, while at the same time it undermines business models that rely on personal data analysis and sales (Krumay and Oetzel 2011). Furthermore, considering values in the modelling process can create conflicts between the goals and needs of the user, the client and the organization, between system engineers' honesty and their obedience, as well as between (fast) product innovation and publication and the product's reliability and completeness (Fleischmann and Wallace 2010).

Privacy advocates are countering these negative observations by arguing that Privacy by Design can create business advantages (Hoffman 2014), reduce corporate liability (Ponemon Institute LLC 2011) and risks (Acquisti, Friedman, and Telang 2006) and does not necessarily undermine system security (Camenisch et al. 2005; Cavoukian 2009). They argue that privacy is a "fundamental right" (Solove 2008; Rouvroy and Poullet 2009), which is essential for functioning democracies (Rouvroy and Poullet 2009) and trustworthy online environments in the future (Clarke 2001). Regulators have tended to follow this latter view by overhauling the OECD Privacy Guidelines (Organisation for Economic Cooperation and Development 2013), passing the General Data Protection Regulation law in Europe (The European Parliament and the Council of the European

Union 2016) and trying to build political privacy bridges; especially between the US and Europe ("Privacy Bridges: EU and US Privacy Experts in Search of Transatlantic Privacy Solutions" 2015).

All in all, ambiguous privacy beliefs and attitudes revolve around the value of privacy itself, its business impact, its technical practicability, its legal feasibility in a globalized IT world, and its potential conflict with other values. Even though the insights into engineers' individual thoughts are sparse (see above), we must presume that - as part of a wider population - they are in the midst of this contradictory spectrum of views.

Professional environment and subjective norm

Regardless of attitudes and beliefs, engineers are not as autonomous in their decisions regarding system design as they would like to be (Wallenstein 1974). The majority of systems are built in teams today, which can sometimes comprise more than 50 people. Therefore, the norms of behaviour reigning in such teams and the importance of team norms for the individual software engineer could play a role in his or her propensity to consider privacy aspects. "Unless we look at and understand the social and institutional environment in which programmers work, attempts to hold the programmer solely accountable will be misguided", asserts Schaefer (2006, 1).

Ajzen (1985) referred to a social environment's influence on individuals as the *subjective norm*. He showed that the subjective norm or, more precisely, engineers' perceptions of what others expect of them, is a direct consequence of normative beliefs as well as an individual's motivation to comply with the norms and expectations that are common in the social environment. In our study context, this translates to whether or not the software engineers believe that their employers and peers expect them to implement privacy requirements in their systems. These beliefs are weighted by the engineers' individual motivations to comply with these perceived norms and expectations.

Studies have provided support for IT professionals complying with the (ethical) requirements of their organizations. Shaw (2003) showed how IT professionals seek "organizational consensus" when deciding if an action relating to privacy is ethical or unethical. They "do not make ethical decisions in a vacuum, but instead look to their co-workers for guidance" and also consider the organizational effects of privacy engineering (such as additional cost expenditure) in their moral attitude towards privacy (Shaw, 2003, 314). Szekely (2011) interviewed twelve IT professionals on their privacy engineering behaviour and surveyed 1,076 professionals in Hungary and the Netherlands. He found that the majority of them usually agree with the decisions made about the handling of personal data throughout a project. Almost all of the participants claimed that if they happened to disagree with a decision, they would definitely let it be known. However, three quarters of them also said they would go along with the decision, even if they disagreed with it. Only 12% stated that they would refuse to implement the decision in such a situation.

So what kind of normative beliefs dominate in organizations? Do they encourage and/or enforce privacy-sensitive design? It seems reasonable to expect that today's organizations embrace privacy as a design value, seen the increasing global legislation and frameworks. However, many organizations are operating in a highly competitive, cost-minimizing, as well as hype-driven rush towards technical upgrades (Spiekermann 2016). As a result, software engineering teams often operate in a climate that can be hostile to non-functional system requirements such as privacy and security (Berenbach and Broy 2009).

Perceived behavioural control

Perceived behavioural control deals with the "perceived ease or difficulty of performing the behaviour" (Ajzen 2002, 671). In our context, perceived behavioural control stands for the extent to which software engineers feel that they have the freedom and capability to embed privacy mechanisms into a system. Control is determined by the form of IT governance in an organization (Webb, Pollard, and Ridley 2006). For official governance structures, Schaefer (2006, 3) observes that engineers are those "closest to the work" and therefore often get the freedoms from their managers to pursue what is necessary. That said, plans and processes are still a non-negligible part of the professional engineers' surroundings. The organizational set-up, staffing, sales deals, delivery dates and external funding set limits to how long a development effort is allowed to last. As a result of time and budget constraints, "the institutional workplace operates under the pressure of efficiency" (Schaefer 2006, 2). When engineering teams are put under pressure to deliver some software, they often do not have the time necessary to follow up on ethical requirements (Berenbach and Broy 2009). In a more recent study, Balebako and colleagues (2014) investigated privacy and security decision-making by app developers and found that smaller companies, which are constrained in time and resources, engage less in activities that promote information privacy and security, while larger companies advocate privacy or legal experts.

Responsibility

Were ordinary people on the streets to be asked who is responsible for the design of IT systems, they would probably point their fingers to the engineers: "Engineers can influence the possible risks and benefits more directly than anybody else", asserts Roeser (2012, 105). As long as human societies have engaged in tool-making and construction, there has been a recognition of the responsibility of the toolmaker for his creations. But this responsibility is not unambiguously accepted by engineers. Already in 1974, Wallenstein wrote in IEEE Spectrum: "We engineers may not appreciate being likened to slaves and prisoners, but where is our spirit of free men? Are not most of us slaves to job opportunities and pay checks, and prisoners of a system in which responsibilities are shouldered by others?" (Wallenstein 1974, 78). In 2006, Schaefer asked the question "Should the programmer be the one solely held accountable for the software faults?" (Schaefer 2006, 1). In fact, when it comes to privacy engineering, Langheinrich and Lahlou (2003) found that engineers felt that this was not *their* problem but one that politicians, lawmakers, or, more vaguely, society has to deal with. Szekely (2011) found that IT professionals ultimately see the users responsible for safeguarding their own privacy by using privacy-enhancing (protection) tools. He also found that "the majority of the respondents think that they bear no responsibility in ensuring the legality of the system they help to develop or run: the responsibility lies with either the management or the clients, but in any case outside their competency" (Szekely 2011, 209). These findings are not in line with the imperative of responsibility that engineers have been called to live up to by philosophers such as Hans Jonas (1979), nor do they match the code of ethics of major professional engineering associations such as the ACM[3] or the Institute of Electrical and Electronics Engineers (IEEE)[4].

Method

We conducted six extensive interviews, spending roughly 7.5 hours with seniors in system engineering from renowned companies and research institutions. We assume that the totality of our interview partners have amassed more than 60 years of experience working for global software houses like Google, IBM, Alcatel Lucent, and Microsoft or doing research for leading ubiquitous computing research labs. They were all in senior system engineering positions that are usually held only after many years of hands-on software and system engineering experience. One of the authors conducted and digitally recorded the interviews at a major IT conference (Ubicomp, which is a conference on new and avant-garde technologies) with the informed consent of the participating interview partners. The participants' names were fully anonymized. The interviews were conducted in English and German (three German interviews, three English interviews); German interviews have been translated into English by the authors.

In addition, 124 engineers answered an online survey that measured the scale of attitudes, subjective norm perceptions and control aspects found in the interview. Participants were recruited through a mailing list from the same IT Conference, ensuring to reach engineers who are developing new systems rather than maintaining corporate infrastructures for which privacy designs may have been decided long ago. It took them 38 minutes on average to answer, participating in a lottery for Apple products and Amazon vouchers in return. 81% of the respondents were male and on average 36 years old. 39% (n = 39) from German-speaking countries, 13% (n = 16) from the US, 10% (n = 12) from Italy. The rest was comprised of 29 different nationalities from across the world. In terms of work position and environment, 77% (n = 96) of the professional engineers and 23% (n = 28) were PhD students. 62% (n = 73) work in a research-related environment (i.e., university, corporate R&D or research institutes), 48% (n = 46) in product development for an IT company, two for NGOs, and three for governments. Hierarchically, 25% (n = 29) indicated to have a leadership position. In this paper we primarily focus on the results obtained from the interviews. That said, our qualitative findings are largely underlined in the trends found in the survey data, and where the two diverge we discuss these divergences are discussed.

Interview guide

The aim of our qualitative study was to better understand why system engineers take or do not take ethical considerations and in particular privacy considerations into account when they build applications. We operationalised privacy and security engineering with the definitions provided above. Sharing these with interviewees we asked them to think about concrete ethical design targets in the past when answering our questions.

As outlined above, we used the TPB and Jonas's imperative of responsibility as a framework of our semi-structured interviews (see Appendix for the full interview guide). The interview guide first targeted ethical decision-making in system design and development in general ("What is 'ethical computing' from your perspective?") and then focused on privacy and related security mechanisms in particular (e.g., "What are disadvantages and challenges of incorporating privacy mechanisms into your projects?"). It also included questions about our interview partners' (experiential) attitudes (e.g., "Do you find security problem solving more pleasing and enjoyable than privacy problems?"), their perceived social pressure or subjective norms (e.g., "What do most people who are important to you think about privacy and security?", "How much do you want to comply with what your environment thinks?") as well as their perceived

behavioural control (e.g., “Do you have the skill set?”, “Do you have the time?”). Inspired by works of Jonas (1979), we decided to also cover responsibility as an interview topic (e.g., “How do you see your own responsibility?”).

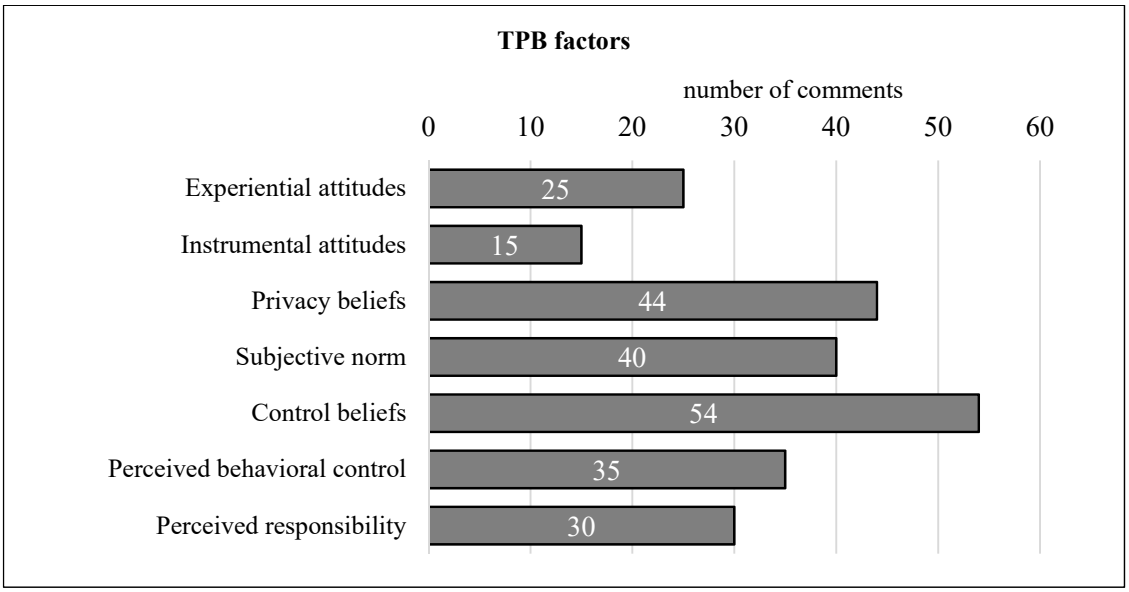
Analysis of interview data

Interview transcriptions yielded 63 pages of recordings from the six interviews, comprising 34,290 words. We analysed the transcribed text passages in two phases using NVivo software (version 11), starting with an explorative and inductive content analysis. Based on the results of this first analysis phase, we deployed a descriptive and deductive analysis method (Mayring 2014).

In the explorative analysis phase, we marked 588 text passages in the interview transcriptions (containing single words, phrases or sentences) as relevant. We then inductively generated themes from these text passages by identifying similarities and regularities. This first step yielded 14 *themes*. Ten of these 14 themes comprised less than 30 text passages each. In contrast, the theme “privacy” comprised 243 text passages, spanning almost half of the comments and statements (41%). In order to explore this manifold data in a focused way, we focused uniquely on privacy in the second and main phase of the analysis (presented below).

In the second phase, we chose a descriptive design for the content analysis (Mayring 2014). We categorized the pool of coded comments and statements that targeted privacy deductively, using the structure of the TPB as a guideline, and registered how often each category occurred in the interviews. In this process, we created six categories that correspond to TPB factors (privacy beliefs, instrumental attitudes, experiential attitudes, subjective norm, control beliefs, perceived behavioural control) and an additional category relating to responsibility, see Figure 1. As it combines qualitative and quantitative text analyses, our approach can be referred to as a mixed method approach (Mayring 2014).

Figure 1. Overview of comments categorized under TPB factors (*N*=243).



While some of the interview questions targeted TPB factors directly – for example, the question “How do you spontaneously feel about ethical requirements?” referred to

experiential attitudes – our interview partners did not always answer in a straightforward way. Often, our interview partners covered several TPB factors in one answer. Moreover, many statements that fit with a specific TPB factor did not come up with the according question but at other points in the interview. Therefore, we always took the whole interview as a basis for the interview analysis and did not only focus on the questions relevant for one TPB factor. We then systematically assigned the statements to specific categories, drawing on the definition of each of the factors of the TPB outlined above.

More precisely, *privacy beliefs* comprise all those comments and statements that express underlying convictions and generic beliefs about the nature of (information) privacy or related concepts (e.g., "consent"). It is important to understand that beliefs differ from other TPB factors in that they capture general statements rather than expressions of subjective experiences. Therefore, wherever a statement was generic and did not express the engineer's personal attitude or perception, we categorized it as belief – either as a general privacy belief or as a more specific control belief. We categorized all those comments and statements that targeted the importance of (information) privacy as *instrumental attitudes*. Whenever emotional adjectives were used by our interview partners, we categorized them within the range from positive to negative *experiential attitudes*. The *subjective norm* category – representing the perceived social pressure to behave in a certain way – subsumes all comments and statements that describe how system engineers perceive the importance of information privacy in their working environment as well as in the general population. We interpreted statements referring to the system engineers' own resources, time, knowledge, experience, capabilities or autonomy to solve privacy issues and implement privacy mechanisms as *perceived behavioural control*. *Control beliefs* on the other hand include general statements about privacy, related concepts and aspects that have an influence on whether one perceives it as possible to protect information privacy by means of system design. All comments in which the system engineers directly referred to their own or others' responsibility or tasks that they (or others) need to fulfil, as well as rules they need to comply with, were subsumed under the category *responsibility*.

Inter-coder agreement was secured by constant communication between a primary coder and a second coder who acted as supervisor. This second coder had access to and was familiar with the whole interview material, the definitions of TPB factors and the coding of the first coder. The supervising coder checked and confirmed the analyses of the first coder and wherever discrepancies were found, the two coders discussed the selection and interpretation of the respective text segments. While this kind of inter-coder agreement is described by Mayring (2014, 114) as a "'lighter' test", it enables two coders to agree completely on the final assignment of all text segments to the system of categories.

Results: Qualitative insights into privacy engineering behaviour and attitudes

A word frequency analysis of all the interviews showed that the ten key words that were most often mentioned in the interviews by the interviewer and the interviewees were, in descending order, "privacy", "people", "data", "system", "product", "security", "information", "design", "user" and "location". While initially the structure of the interview targeted ethical decision-making in system design and development in general as well as privacy and security mechanisms in particular, the actually conducted interviews focused heavily on privacy, security being less eagerly discussed.

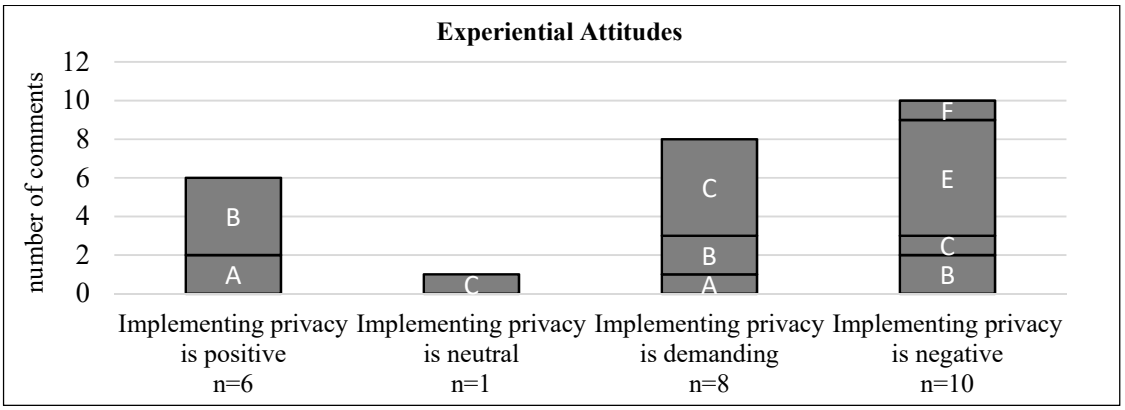
One of the main goals of the analysis presented hereafter was to explore the motivating factors that drive privacy engineering. While the small number of interview partners limits the level of generalizability of our findings, it also allows an in-depth analysis of the different subjective attitudes. Instead of testing how dominant one belief or attitude is within a representative sample, our study focuses on the different possible configurations of beliefs and attitudes and on what we can learn from them. For example, we illustrate how often several – even seemingly contradictory – attitudes, beliefs and perceptions are held by one single person. For this reason, our results do not only depict the number of statements that fall within each of the categories [indicated in squared brackets], but also indicate who made these statements, whereby interview partners are anonymously represented by the letters A to F in the figures presented hereafter.

The six seniors in system engineering interviewed expressed their attitudes towards information privacy and its consideration in system design in 40 comments, out of which 25 comments expressed their experiential attitudes and 15 comments revealed how they evaluate the importance of privacy (instrumental attitude). The most relevant questions from the interview guideline in this respect were “How do you spontaneously feel about ethical requirements?”, targeting experiential attitudes, and “What is your own thinking?” in the context of what is important, targeting instrumental attitudes. The categories that emerged comprise statements indicating positive, neutral and negative experiential attitudes towards the implementation of information privacy as well as positive and negative instrumental attitudes regarding its importance.

Experiential attitudes towards privacy

It is immediately apparent that the experiential attitudes tend to be rather negative, as our interview partners had more arguments for privacy being demanding, describing it even as outright negative. Figure 2 depicts the experiential attitudes that emerged from the engineers’ statements as well as the number of statements that fall within each category. The letters in the bars show which interview partner is represented in each of the categories.

Figure 2. The engineers’ experiential attitudes towards the incorporation of information privacy mechanisms as expressed in 25 comments; the interviewed engineers are anonymously represented within the bars by the letters A to F.



Four of the six system engineers interviewed considered the incorporation of information privacy mechanisms somewhat "*inconvenient*" (mentioned six times by one of the interview partners) or otherwise negative ("*not pleasing or enjoyable or exciting*", "*not enthusiastic*", "*it just becomes a nightmare*") [10 comments]. Furthermore, it is demanding or (intellectually) "*challenging*" [8 comments] – something that can be good or bad, according to one remark.

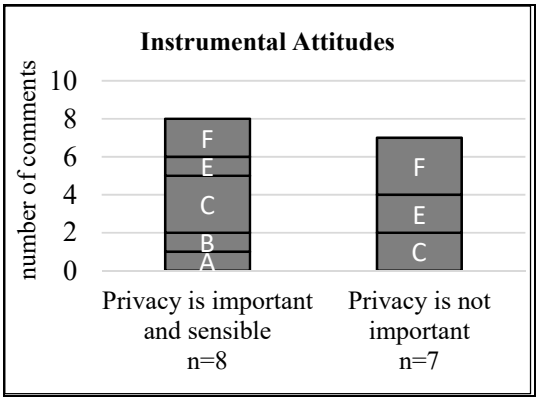
Two of the six interview partners found some positive words for the implementation of information privacy, expressing that implementing privacy mechanisms makes them happy ("*if it wants me to incorporate privacy I will be very much happy* [sic]") or mentioning that it is "*interesting*", "*exciting*" and "*satisfying*" [6 comments]. However, as the letters in Figure 2 indicate, even these two interviewees (A and B) had mixed feelings towards privacy, as they equally mentioned negative aspects or expressed how demanding it is. One interview partner associated it with "*neutral emotions*" [1 comment].

This rather negative experiential attitude towards privacy was confirmed in our quantitative study. We used a 5-point semantic differential scale with five bipolar adjective pairs to measure experiential attitudes (e.g., annoying – pleasing). The mean across adjective pairs was $M = 3.32$ ($SD = 0.82$). 40% of the engineers surveyed don't like to engage in privacy engineering. Experiential attitude towards privacy engineering was significantly correlated with an engineer's belief that transparency would be more important as a value than privacy ($r = -.41$; $p < .001$), pointing to a value conflict. Those, however, who believe that privacy engineering is important to enable a power balance between corporations and citizens were also more likely to enjoy privacy engineering ($r = .22$; $p < .05$).

Instrumental attitudes towards privacy

When it comes to instrumental attitudes, the views are much more balanced (see Figure 3). Eight comments pointed to privacy being important and sensible while seven comments questioned its importance. Again, we must recognize that within the same interview partners both views are represented.

Figure 3. Comments expressing the engineers' instrumental attitudes towards the incorporation of information privacy mechanisms, n=15.



Five out of six system engineers interviewed pointed to the importance of information privacy [8 comments], saying that it is "sensible", "*relevant*" or *"(very) important*", that "*design and human interaction issues are increasingly accepted as a critical aspect of*

any software that we develop" and that they are "*very concerned*" about it. However, three out of the five system engineers who mentioned the importance of information privacy at some other point of the interview, also made comments that expressed that privacy is not important nowadays ("*Now privacy is not as big as then*", "*and regarding up-to-date: this is more a general question, if we are going to see it a lot; and I believe while this will not be the all-determining topic in two, three years, it will yet be important*") and referred to information privacy as "*secondary*" or "*side part*", e.g., when compared to Internet connection or functionality [7 comments]. Thus, some of our interview partners effectively contradicted themselves, giving the impression that system engineers are split in their views.

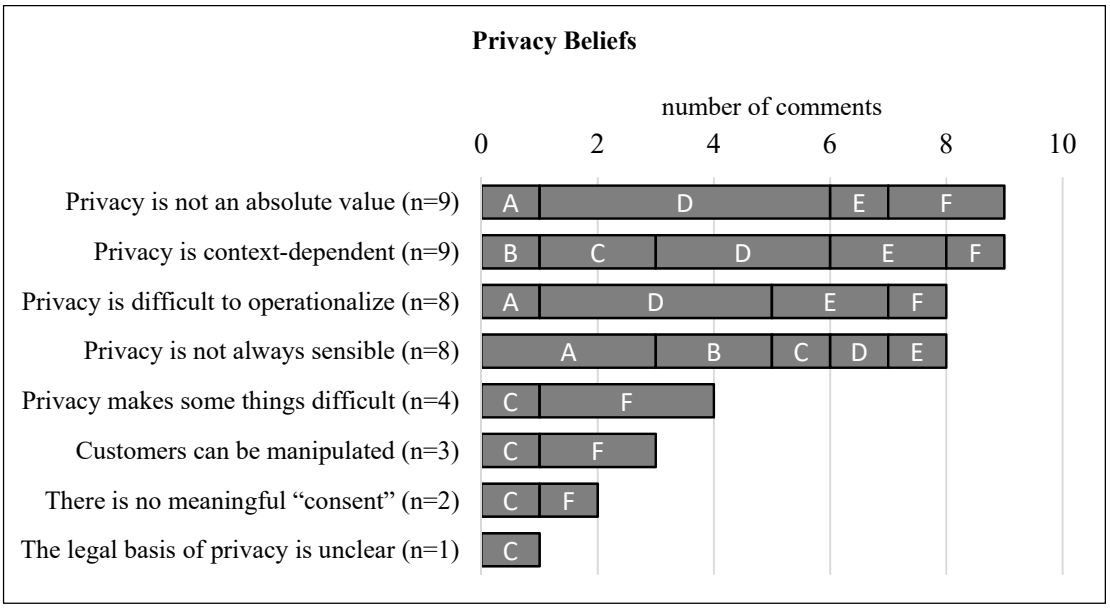
Our survey results underline the interview results that instrumental attitudes are much more positive. We used a 5-point semantic differential scale with six bipolar adjective pairs to measure instrumental attitudes (e.g., privacy engineering is worthless - valuable). The mean across adjective pairs was $M = 4.18$ ($SD = .76$) and hence much higher than with experiential attitudes. Only a small fraction of 10% of the engineers find privacy engineering useless. Again, the conflicting value of transparency ($r = -.36$, $p < 0.1$) and the belief in corporate-citizen power balance ($r = .28$; $p < .05$) influence the attitude held.

All in all, the results show that the system engineers' experiential attitudes towards information privacy are rather unfavourable and that their instrumental attitude is ambivalent.

Privacy beliefs

The system engineers interviewed revealed beliefs about (information) privacy in 44 statements and comments. These statements were often made in relation to the question "What is 'ethical computing' from your perspective?". Figure 4 displays the nine beliefs we found in their statements. All of these beliefs are critical, sceptic, or negative, thus pointing to challenging issues.

Figure 4. Engineers' beliefs regarding (information) privacy as expressed in 44 comments, ordered by the descending numbers of comments for each belief.



One of the most prominent beliefs that was expressed by four out of six interview partners is that privacy is not an absolute value [9 comments], as it has "*room for interpretation*" and a "*human element*". It is not equivocally perceived as a fundamental right ("*I cannot share the idea that privacy is a fundamental right that is just indefeasible*") as it is merely "*a perception to people* [sic]" that always changes, a "*commodity*" that can – and in certain contexts *should* – be traded or sold ("*if I own the data, I should sell the data*").

Another prominent belief is that privacy is context-dependent [9 comments], which was expressed by five out of six interview partners. Engineers expressed that in some contexts it is more important to consider privacy than in others; here they referred to companies making money with the data as opposed to the academic or research context ("*And I think in the academic environment it is not as critical as in the company environment, where you make money with the data"; "From a research point of view there's nothing stopping us from doing something. I think this question becomes a lot more relevant when you are making a product"*). They also believe that users assess their privacy differently in different contexts *("….who can see it and who cannot. We did that with a study and there it was very clear, that you have to decide that as the case arises. Well, for example, 'is the user on the toilet or not' - this is a moment where I do not want to call*"). The system engineers' view on the legitimacy of information privacy also influences their ethical perception of their own actions ("*I don't believe that collecting data per se violates privacy; there are many situations where we collect data*"; "*Well, it depends because if we are not misusing anything, if we are not selling this information to anybody…*").

The engineers do not always know how to operationalize privacy [8 comments]: "*One privacy question here is: is it the collection of data the problem or the exposure of the data?*", "*If we approach systematically what we do, we lack understanding: what then is the overall system that we call privacy?*". They expressed that privacy is "*not as well*

formalized and understood" and that different engineers have different ideas and solutions.

Furthermore, engineers point to the issue that it is not always sensible to implement privacy [8 comments]. They mentioned that data is often needed for systems to work ("*The system would need to collect data in order to do something meaningful*"; "*There are systems that only work when I have big data*") as well as for other purposes like advertising ("*on the other hand, you do want to use the mass of data for advertisement*"). Another argument that decimated the value of information privacy pointed out that it not only protects individuals, but also gives citizens and customers the power of misuse ("*maybe privacy is one thing, where the corporation is not misusing the data, but anonymity can let citizens misuse the corporation. What if I had anonymized phones, and I basically make a call and the corporation doesn't know who to bill?";* "*Transparency can of course go in both directions, you cannot forget about that. And transparency can be the opposite of privacy. Full transparency also stands for more power on the customer's side*").

In addition, two engineers interviewed pointed out that privacy makes things difficult [4 comments] as it can slow down processes ("*it could nevertheless be possible that decisions are delayed or processes slowed down at the code level*"), impede functionality and hinder research because less information is available ("*you can have an access control list ….that makes things very heavy, because in your data model you have to have meta data that describe your data*").

Two engineers mentioned issues related to users and customers. First of all, these engineers believe that the implementation of privacy becomes more tricky as customers can be manipulated and bribed by companies [3 comments]: "*If I, as a customer, agree with the collection of my data, I cannot do anything against it; that means I can be bribed*", "*if we look into different other* [sic] *systems, if you have a very bad user interface but a very good functional system, it will still not work*", "*that* [a bad user interface for privacy settings] *is intentionally done to make people just ignore it*".

Secondly, engineers are aware of the difficulty of giving and receiving meaningful consent [2 comments], pointing out that "*the biggest lie we do every day* [sic] *is when we click the 'I agree' button; you never read those privacy statements and agreements*" and "*You can do these consent-things, but then the question arises if that is enough. Do the people really read and understand that we collect these data and analyse it for research?*".

And lastly, one interview partner saw the legal basis of (information) privacy as unclear [1 comment]: *"…this is not at all acknowledged by the data protection law; there are also very few court decisions that said: 'in this case, there was enough anonymization and in that case, there was not'".*

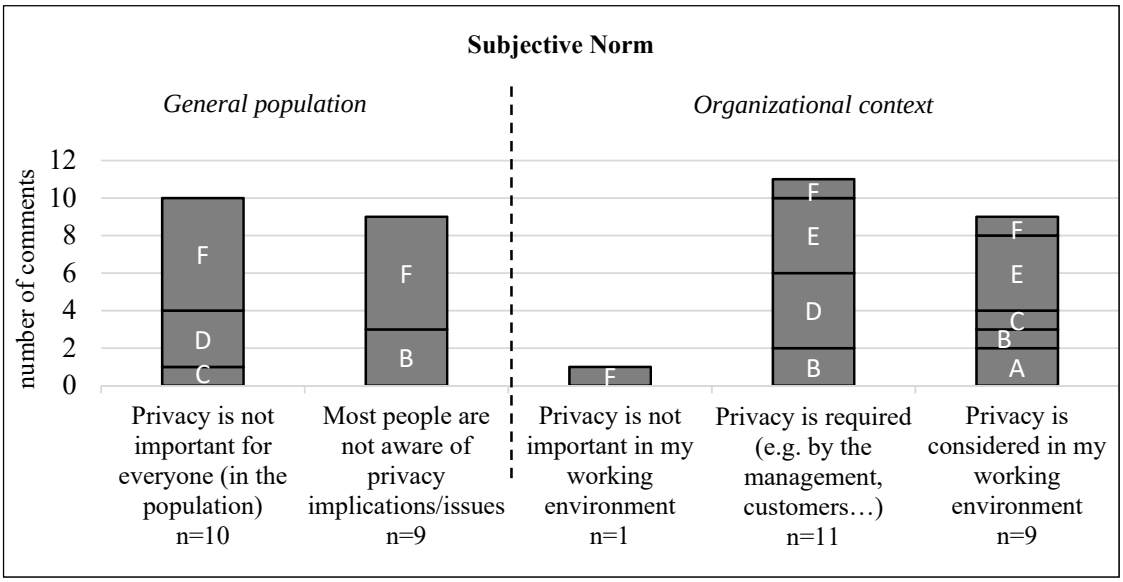
In our quantitative study, we tested for a bigger number of beliefs that we mostly retrieved from the literature. The full set of beliefs investigated as well as their correlations with privacy attitudes can be found in appendix 2. However, the beliefs in the value of transparency and in the necessity to balance the power of corporations with that of citizens were confirmed as highly relevant in our quantitative study.

Professional environment and subjective norm

Figure 5 displays the system engineers' subjective norms that emerged from 40 comments on their perceived social pressure from their working environment and the general population. In relevant questions from the interview guidelines engineers were asked about their assumption as to what their respective organization and people who

are important to them think and expect as well as their own motivation to comply with these norms. Results show that engineers do not perceive any pressure from the general population (assuming that they are not interested in or aware of privacy issues) and that information privacy is mostly required in their organizational context.

Figure 5. The engineers' perceived social pressure from the general population and their organizational context to incorporate information privacy mechanisms as expressed in 40 comments.



Three system engineers believe that privacy is not important for everyone in the population [10 comments] as "*people don't care*" if their privacy is breached and people think no one is interested in a "*nobody*" or a "*general person*" like them. One system engineer concluded that "*for the majority of the people privacy is not an issue*". The system engineers also mentioned user awareness issues and associated knowledge asymmetries [9 comments]. They believe that people are not fully aware of privacy implications and issues ("*I don't think that companies are not aware of the impact of these systems; it is the individual, sitting in front of it, who is probably not aware of it*"), that they "*have a very vague notion of what privacy means*" and find it difficult and painful to "*read and do all the stuff you don't care [about]".*

Most of our interview partners observed that information privacy matters more in their working environment. Only one engineer stated that developers and researchers from his working environment were not interested in privacy concerns [1 comment]: "*I have found in my particular role that sometimes it was very difficult to pass the message to the developers or even to the researchers, they were not interested in privacy, or to take those concerns* [sic]*; you need to have multiple conversation before they are willing to agree to compromise their design decisions to accommodate those privacy features*".

In nine remarks that referred to the importance of information privacy as perceived in their organizational context, system engineers recognized information privacy as something that is deliberately considered in their respective environment as "*there is certainly a lot of thinking about these issues*" and people in the companies are "*very concerned*", "*cautious*" and "*fairly careful*" about it [9 comments].

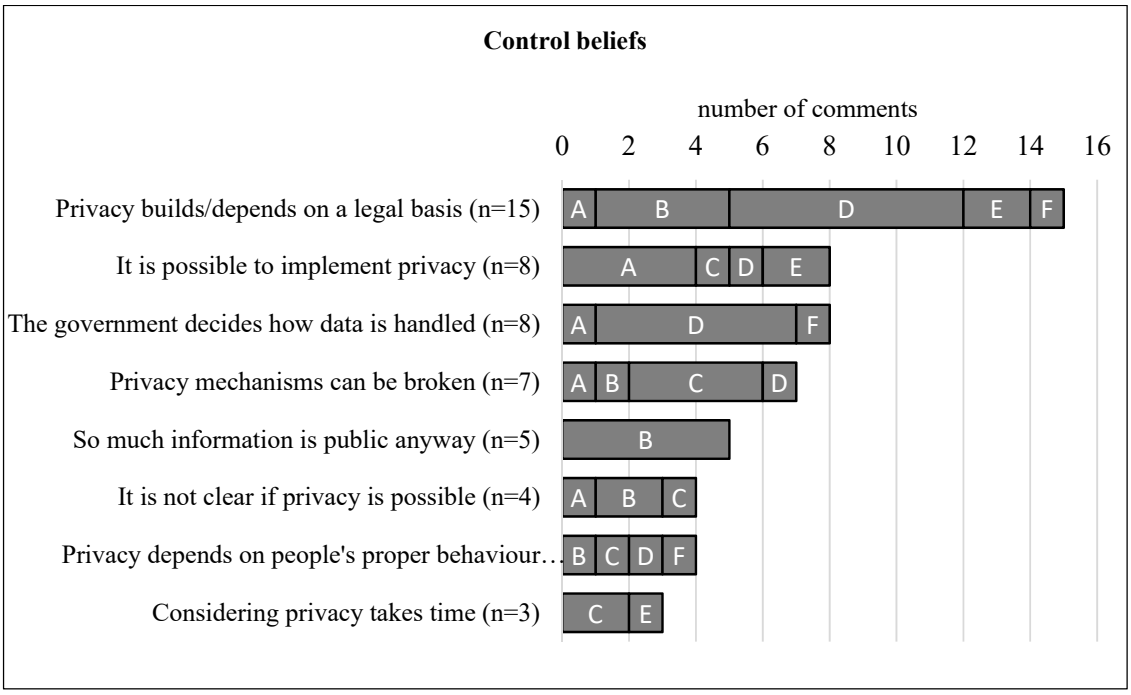
They also referred to information privacy as something that must be dealt with and that is somehow required [11 comments], saying that "*it is quite a serious matter*", "*it has to be there*" and that "*privacy is not an optional thing anymore*". For some, the reasoning behind the consideration of privacy issues is to avoid criticism and a negative public image ("*if there is something, if the press was taking* [it] *down the wrong pipe, then we're dead*"; "*in general you cannot get very far in collaborations and so on if you don't have that*" [this comment refers to "ethics" and "thinking about privacy"]).

In our survey we nuanced these insights with more detail. Subjective norm was measured with a 5-point differential scale asking engineers whether most *people who are important to them* think that they should (1) or should not (5) incorporate privacy mechanisms into the systems they build. It turned out that privacy engineering was expected of engineers (M_{pr} = 4.13, SD_{pr} = 1.10). Only 13 engineers (11%) indicated that the people who they find important would *no*t expect them to incorporate privacy mechanisms. That said, we used another item in our questionnaire, which queried engineers' organizational context; we asked about the strength of the normative privacy belief of the engineers' employers (see appendix 1). And here we found a picture that enriches our qualitative findings while challenging engineers' subjective norm: In fact, only 62% (n = 77) of the engineers in our sample work for organizations that expect them to consider privacy mechanisms (M_{pr} = 3.80; SD_{pr} = 1.09). 38% work for employers without clear or even negative privacy norms.

Control beliefs

In 54 comments, system engineers expressed their beliefs with regard to control over privacy implementations (see Figure 6). As with privacy beliefs in general, statements that were categorized as control beliefs were made at various points in the interview, for example in relation to questions about their interpretation of ethical computing or their skills and autonomy. While a few comments hinted at our interview partners believing that it is possible to implement privacy, they also pointed to several difficulties that could reduce their individual control. In particular, it turns out that there seems to be a conflict with the legal world with regard to data protection and information privacy.

Figure 6. The engineers' control beliefs regarding the incorporation of information privacy mechanisms as expressed in 54 comments, ordered by the descending numbers of comments for each belief.



According to their statements in the interviews, five out of six system engineers believe that privacy is a legal issue within a legal framework and that only after the legal issues being "*fixed*", the legalities being settled and laws being passed, we can talk about the technological implementations [15 comments]. Exemplary statements were as follows: "*without a legal framework there is no chance of getting privacy*" and "*the more liability your corporation has, the more careful it is*".

Four interviewees mentioned ways that allow to protect privacy technically ("*there are things that automatically check whether you follow these guidelines; and we also do privacy checks [too] which can be done automatically, for instance if no information should flow out of a program and things like that*"; "*but we will be able to solve many privacy problems*") [8 comments]. However, we can again observe that the same engineers who expressed optimism also express concerns at other points in the interview.

For one thing, they see privacy as entangled with national interests. Three out of six engineers interviewed perceive the government as an important power that always decides in the end as it has the sovereignty to tell corporations what to do and what data (not) to use ("*when corporates are collecting information about their customer base, you are kind of liable to give it to the government at some point, if they ask you to do so*"; "*as it were, if the government wants my data, then there is a law, that I have to give away my data*") [8 comments].

Furthermore, privacy mechanisms can be broken ("*there are so many ways of breaking privacy*"), overridden ("*and every mechanism, that you then build in, can somehow be levered out – and I think most often this will also happen*", "*it is quite obvious, when you have the right tools and the right data, it doesn't yield you anything*"),

overruled ("*because everyone can easily overrule privacy*") and that anonymized data can be de-anonymized with additional information sources ("*because everyone knows that maybe with clever tricks you can maybe again deanonymize if I bring in external sources*") [7 comments].

One software engineer expressed further concerns by referring to the amount of information that is already available, saying that "*everything is quite public*" and that "*there are so many ways of inferring about the person*", which makes the protection of privacy more difficult [5 comments].

Other comments passed the responsibility of control onto the users and their proper behaviour [4 comments], either because they have the choice ("*if you don't want to be known you switch off your cell phone*") or because they make mistakes ("*they don't know the trade-off; and at that point they make mistakes*").

Although they expressed the opposite at other points in the interview, some engineers even doubted the feasibility of privacy per se [4 comments] as "*the question of whether privacy is possible or not is still up in the air*" and they believe that companies will not easily let go of the data that they could otherwise use or sell.

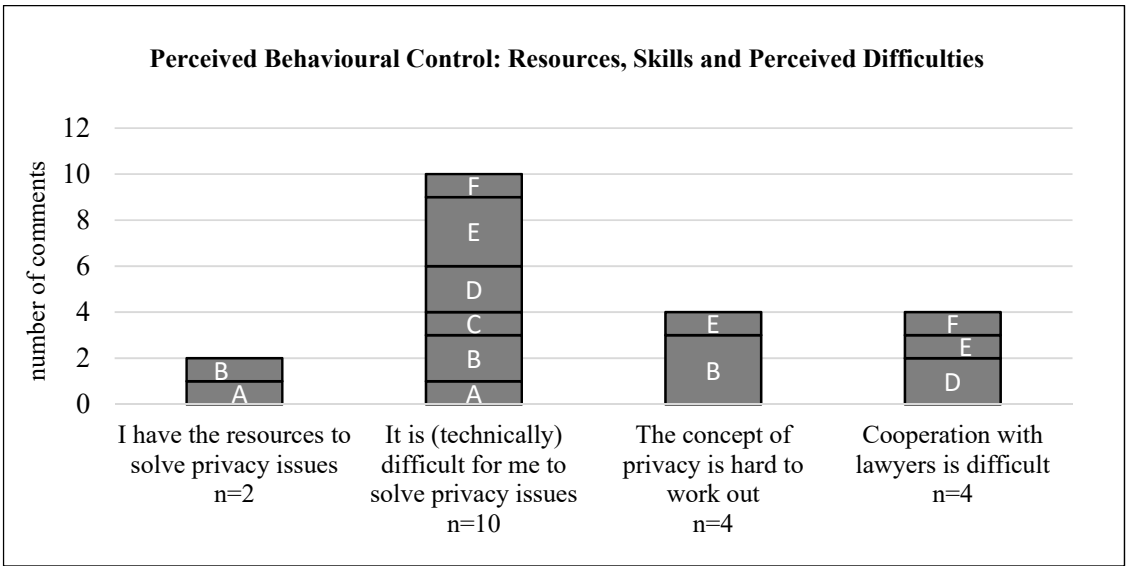
And lastly, taking privacy into consideration slows down the whole process [3 comments]: "*we have to think of the data protection mechanisms and develop them, it certainly would be easier, if we did not have to do that; then we would be faster done with the study and with the whole development of the systems*".

The control beliefs we found in our interviews largely point to the larger environment in which privacy is finally achieved or not. Only one external control belief was mentioned that is directly related to the engineers' working environment; that is the time required for building privacy-friendly systems. We tested for this aspect in our quantitative study asking engineers how difficult (1) or easy (5) it would be for them to incorporate privacy mechanisms into their systems in the immediate future (2-3 years). The mean result pointed to time difficulties (M_{pr} = 2.68, SD_{pr} = 1.09): only 22% of the engineers we asked believe that time is *not* a problem for them when it comes to privacy engineering.

Perceived behavioural control

Control beliefs, such as those presented in the section above on the implementation of privacy, influence a person's perceived individual control. That is, my belief regarding the control of a certain behaviour determines whether I feel that I have the power to successfully carry out this specific behaviour myself. For example, concerning the control belief, engineers pointed out that it is not clear whether privacy is possible. This belief then influences their perception of their own control over privacy engineering, i.e., whether it is possible for them to deal with privacy. The following questions in the interview guideline targeted engineers' skills and autonomy: "Could you do more if you really wanted to? Do you have the leeway? Do you have the skill set? Do you have the time?". They expressed their respective perception of their own behaviour control in 35 comments, which all pointed to a lack of control (see Figure 7). This was due to missing resources and skills as well as (technical) challenges in building privacy-sensitive systems.

Figure 7. The engineers' perceived resources, skills and difficulties to incorporate information privacy mechanisms as expressed in 20 comments.



Only two system engineers felt that they had the resources, that is, the experience or time to solve privacy issues [2 comments] ("*I have worked on privacy*"; Question*: "Are you considered as a privacy specialist in the organization, so that they give you the time specifically to think about privacy mechanisms?"* – Answer: *"Yes. I've written papers which discuss privacy, so of course*").

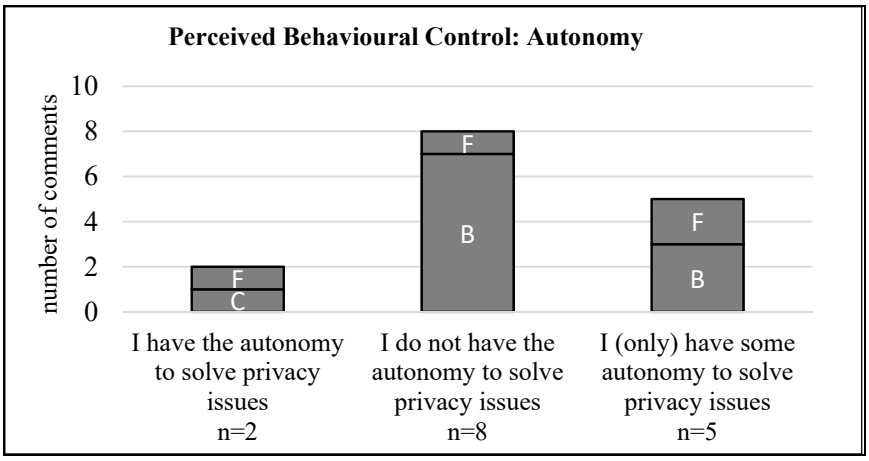
All of the engineers interviewed find it difficult to deal with privacy issues and solve them technically ("*it is by all means difficult to fulfil certain requirements regarding data storage*"; "*it's somewhat clumsy and blunt and anything else*"; "*the design itself is very hard*"; "*there are several implications in terms of just designing a system that will take privacy and security into concentration which makes it quite hard*") [10 comments].

Furthermore, the concept of privacy is hard to work out [4 comments]: "*it is just very hard to figure out when you want information to be revealed and when you do not want it to be revealed*", "*incredibly hard to define, what is meant by privacy, especially in location*", "*but there are increasingly some of these softer requirements where there should be humans in the loop to kind of check, those become quite hard to interpret by the developer or the engineer*".

What is more, working on privacy often requires cooperation with lawyers, which some of the engineers find tiresome and difficult [4 comments]: "*There are simply people who do not understand the technical realities and make definitions from a legal perspective, that essentially are not reasonable*", "*I was working with one of the lawyers of our company… it was a nightmare to explain to her certain things and also to know from her the regulations*".

A very similar picture can be found with regard to autonomy. Those engineers that commented on their autonomy mostly pointed to a lack of autonomy when it comes to deciding over privacy design. Autonomy is presented in Figure 8.

Figure 8. The engineers' perceived autonomy to incorporate information privacy mechanisms as expressed in 15 comments.



Two system engineers expressed that they have the autonomy to solve privacy issues [2 comments] ("*the decision was taken by myself*"). However, one of them (interview partner "F") also shared the perception of another engineer (interview partner "B") that they do *not* have the autonomy to solve privacy issues [8 comments], or have only some autonomy [5 comments]. They expressed that it "is not up to them" or that they have no final control ("*sometimes you get that kind of requests incorporating some of this features, then we have to do it*" [in this comment, the engineer referred to requests that he did "not agree with ethically", such as checking the location or age of users for market research], "*you don't really have a choice*", "*Autonomy exists and double thinking about the implications. But whether you incorporate it into a large scale system, there is no autonomy*") and they have only some autonomy ("*it's more in the middle*", "*that is not entirely up to me; there are some other elements too*").

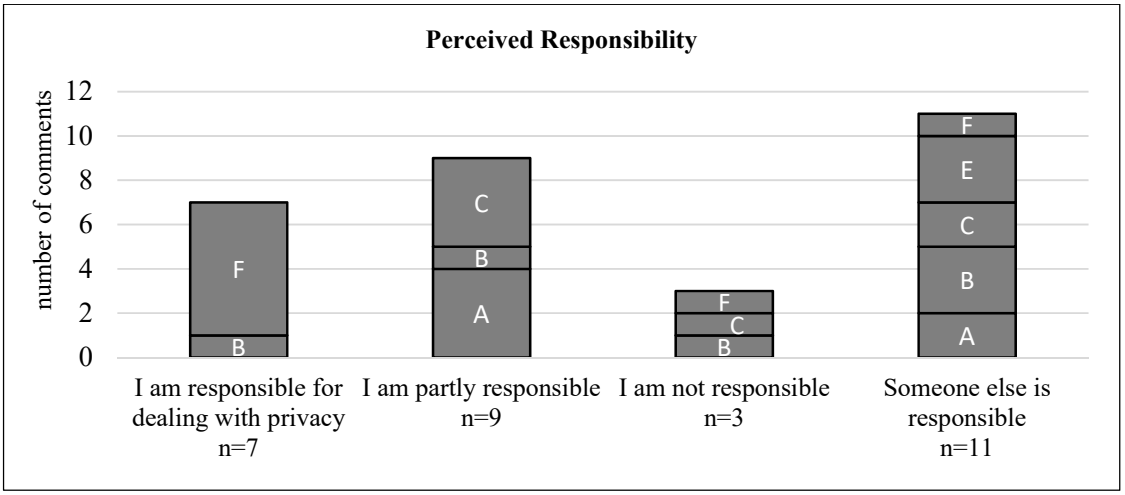
Our survey results confirm a control issue among engineers. 37% of the engineers (n = 46) do not feel that they have sufficient control over implementing privacy mechanisms (M_{pr} = 3.58, SD_{pr}= 1.09). This is *not* due to their capability. 66 % (n = 82) state that if they wanted to, they could incorporate privacy mechanisms. Only 26% (n = 32) of the engineers believe that they do not have sufficient knowledge to implement privacy. Instead, they face a controllability issue in their work context: Over half of our respondents (51 %; n = 63) pointed out that in their respective organization it is not (solely) up to them whether they will pursue privacy or not. As outlined above, many seem not to get the time required to implement privacy. But our quantitative study also confirms that autonomy is an issue. 52% (n = 64) say that they do not have the autonomy to implement privacy controls into their systems. Even though the degree of perceived behavioural control over privacy engineering is positively correlated with the hierarchical position: 7% in the higher ranks still express a low level of controllability (considering their mean perceived behavioural control), and 31% say that with the autonomy they are given it is difficult to incorporate privacy.

Beyond the TPB: Perceived responsibility

In addition to the predictors of behaviour proposed by the TPB, perceived responsibility was an important aspect in the interviews. Several questions in the interview guideline referred to the engineers' perceived responsibility, like for example "How do you see your own responsibility?" and "What was your role and responsibility in

the respective project?". The comments that expressed how responsible the seniors in system engineering felt are summarized in Figure 9, which clearly shows that the majority of interview partners do not feel responsible.

Figure 9. The engineers' perceived responsibility as expressed in 30 comments.



Only two out of the six interview partners stated that they feel responsible for incorporating privacy mechanisms into their systems [7 comments] ("*I have the sole responsibility*"; "*it's a choice I have to make*"), but at other points of the interview both of them stated that they are not responsible [3 comments] ("*but we are not responsible for the product*"; "*and it is not just me, if I did not develop this system, somebody else will; or at least there are other systems out there which are capable of doing something similar*").

Three engineers expressed that they feel only partly responsible [9 comments] ("*I admittedly have a certain responsibility*"; "*my part is a really small one in that scale*").

Most of the comments pointed to someone else who is responsible [11 comments], ranging from the user ("*the thigh responsibility lies with those that deploy it*") to the companies ("*it is really up to them*"), colleagues ("*but I certainly have colleagues; there is for instance a privacy person that works more on the technology side*") or the code ("*so when we do something like that with companies, we give them the code; so we give them the whole rights for the stuff, so we get rid of everything; then they can do whatever they want*").

Our quantitative study points to a similarly nuanced position towards responsibility. 63% (n = 77) of the engineers feel responsible for privacy engineering. We asked whether engineers agreed that privacy-friendliness is not *their* responsibility. They somewhat disagreed with this (M = 3.63; SD = 1.04). Notably, engineers in management positions (including the self-managing independent coders) report significantly more responsibility (F_{pr} (2,114) = 3.10, p < .05). That said, we would argue that seeing 37% of the engineers dismissing their responsibility somewhat confirms the mixed views found in interviews.

Discussion

We want to stress three core results of our analysis: First, many senior system engineers perceive privacy demands as a negative burden, even though they understand the necessity to take care of the value. Second, they are deeply divided with regard to their control and responsibility for the matter. And third, they find themselves in an ongoing struggle over information privacy with the legal world.

Privacy by Design as the engineers' burden

More than three fourths of all 243 comments on privacy (*n*=188, 77.4%) were negative, sceptical, or pessimistic, saw the responsibility with other people, or listed problems and difficulties associated with the implementation of information privacy mechanisms. When interpreted in light of the TPB, we found that almost all factors that predict the intention to meet privacy demands (privacy beliefs, experiential attitudes, subjective norm, control beliefs, perceived behavioural control, perceived responsibility) are mostly negative.

The reasons given by our interviewees for their negative beliefs regarding privacy and its implementation are manifold. First, they perceive privacy as a vague concept and its value as uncertain, not always legitimate, context-dependent, and not absolute. It seems that they do not know how to ensure privacy in different contexts in a proper way. Therefore, it is comprehensible that these beliefs could have a negative effect on engineers' motivation to implement privacy mechanisms. Already more than twenty years ago, the ambiguity of privacy was discussed as a "systemic disease" causing most of the problems surrounding privacy (Smith 1994, 167). More recently, the context-dependence of privacy has been taken up in the privacy discourse in a positive way, drawing on the term "contextual integrity", coined by Nissenbaum (2009). Contextual integrity emphasizes that the legitimacy of data use depends heavily on the context of use and is therefore dynamic. However, it is difficult to make sure that systems and data are not used out of context – and engineers know this.

Second, privacy makes things technically more difficult for system engineers. The system engineers interviewed mentioned resource difficulties in 90% (*n*=18) of their reflections on past experiences and anticipated obstacles. They say that considering privacy takes a lot of time and believe that privacy mechanisms can be broken, overridden or overruled. Furthermore, it is tricky to ensure information privacy as it also depends on the users' behaviour and whether they can easily be tricked into revealing personal data or not. This phenomenon of shifting responsibility onto the users had been observed before with app developers, with one developer proclaiming that "at the end of the day its [sic] up to the user" (Greene and Shilton 2017, 14).

Third, despite the senior positions of our interviewees, perceived behavioural control over privacy engineering turned out to be a negative motivational driver. When speaking about their autonomy to design privacy, 87% (*n*=13) of the statements hinted that they do not have the autonomy to deal with privacy issues. The reason for this lack of autonomy is not clear from our data. It may be that negative organizational conditions – business models favouring data collection, organizational strategy, time pressure in development, etc. – undermine engineers' degrees of freedom when developing privacy mechanisms (Balebako et al. 2014; Berenbach and Broy 2009). Further research into this issue is definitely called for. But for the time being, our interviews seem to signal a status of frustration around the privacy matter among engineers, an unconvinced

experiential attitude and the impression that the whole privacy effort is in vain and hardly feasible.

System engineers are in an inner conflict

Regardless of our interviewees' overall negative emotions and their frustration regarding privacy, they recognize that information privacy is important, sensible and fruitful. Half of the comments categorized as instrumental attitudes went into this rationally positive direction. Yet, this counting of positive instrumental arguments is misleading, as at the same time most interviewees contradicted their position at a later point in the interview. System engineers are not only undecided as to their instrumental attitudes, but also when it comes to their perceived behavioural control, which reflects the resources, skills and autonomy they have for privacy design, as well as their perceived responsibility. This is especially interesting as our interview partners are senior system engineers who (should) have the knowledge and resources to consider the protection of information privacy in their systems' design.

In one comment each, four out of our six engineers expressed that they believe to have the resources or the autonomy to solve privacy issues. However, all of them also expressed in roughly one third of their statements on control how difficult they find it to implement privacy (regarding technical aspects, privacy as a concept, and legal requirements). One of the two engineers who mentioned their design autonomy contradicted himself, mentioning later that he does *not* have the autonomy, or only has *some.* Another engineer mentioned at several occasions that he had neither the choice nor the final control. Such a lack of autonomy and control is especially startling as all interviewees hold senior roles and hence should be in the position to strongly influence (if not determine) how information privacy is dealt with in their teams and projects.

When it comes to perceived responsibility for privacy, 40% (n=12) of the comments indicated partial responsibility or none at all. Roughly 37% (n=11) of the comments pointed to other responsible parties. Most remarkably, our interviewees again made many self-contradictory remarks, feeling fully or partly responsible for the incorporation of privacy but at the same time mentioning someone else's responsibility or stating such things as "it is not up to me". Identical phrasing is found in the study of Langheinrich and Lahlou (2003) published fifteen years ago. Taken together, our findings show a deep division over privacy within engineers' own thoughts on the matter.

System engineers are fighting a battle with the legal world

At several points in the interviews, system engineers mentioned the legal basis for information privacy as well as the legal staff representing it in organizations. First of all, our engineers perceive privacy as a concept that is legally hard to define. They say that cooperating with lawyers is difficult and tiresome and that it is hard to reach a shared level of understanding with them. Most importantly, our interviewees believe that information privacy is dependent on a legal basis that has not been settled yet. In their opinion, privacy only makes sense once this "legal issue" is fixed and the legal situation has been clearly established: "without a legal framework there is no chance of getting privacy". Besides the interdisciplinary difficulties, these legal views of seniors in system engineering is alarming, since a decent framework for privacy regulation has been around since 1980 in the form of the OECD guidelines on the protection of privacy, reinforced in 1995 by the data protection directive 95/46/EC of the European Parliament and the Council of the European Union.

It may be that the EU's GDPR, which has just come into effect in May 2018, will create further clarity for engineers. Interestingly, while engineers pointed at lawyers in our interviews, the same finger-pointing can be observed in the legal world, which is frustrated over engineers' reluctance to embrace privacy. In a recent paper, legal scholars have presented an analysis of computer scientists' educational material and textbooks which continue to promote data collection maximization (instead of privacy-friendly data minimization) and ignore matters of data flow control and privacy (Birnhack, Toch, and Hadar 2014).

Taken together, our theoretical and empirical insights suggest that there may be an underlying conflict between the legal world and the engineering world, with lawyers imposing responsibility on engineers that the engineers do not want to embrace. We wonder whether this conflict can be resolved if engineers receive better legal education, learn more about privacy at university and confront the long list of hard requirements raining down on them due to new data protection regulations like the GDPR. We are not ready to exclude that the information society at large has not yet made up its mind on the right balance between privacy on the one side and openness on the other.

Conclusion: A 15 years' leap from non-awareness to inner disunity?

In this exploratory interview study, we wanted to gain an understanding for the way system engineers think about ethical values such as information privacy and data security. In our data analysis we shifted our focus to information privacy as one of the most important ethical values in IT design.

In summary, our findings suggest that system engineers deal with information privacy in their working environment, mostly because they are required to do so. However, regarding privacy engineering all of our interview partners saw difficulties, which are not only of a technical nature. Moreover, we identified only few clear expressions of responsibility, autonomy, and control in the system engineers' statements. Their mostly negative experiential attitude coupled with their awareness of many challenges related to information privacy as well as the lack in perceived social pressure from the general population result in an overly negative motivational stance towards Privacy by Design. Where they do not see responsibility for themselves, they see it with the legal world, which they do not like to deal with. These findings are very much in line with the findings in the 2003 Langheinrich and Lahlou survey. Even though their study is now 15 years old, we still see a lack the areas of researchers' and system engineers' perceived importance of privacy, their resources as well as their responsibility and autonomy to deal with privacy issues.

When confronted with a task that is time-intensive, makes things "clumsy" and "very heavy", entails technical difficulties and arduous co-operation with experts from another discipline, system engineers have to draw from a high degree of self-motivation. However, the results of our interview study point to a low motivation of system engineers to think about privacy issues and incorporate mechanisms that protect information privacy in their design in the long run. These findings are discouraging, seen the rapid rise of personal data markets, data-based discrimination, manipulation and ongoing privacy breaches (Christl and Spiekermann 2016).

If we want new technologies to respect human values, we need to find ways to motivate system engineers to incorporate values such as information privacy into their designs. Several approaches to including ethics into design have been suggested, such as ethics education for engineers, professional codes of ethics, external ethics experts

and ethical design practices within design teams. The educational approach (e.g., Ware, Ahlgren, and Silverman 2013) as well as incorporating ethical design practices in laboratories, thereby creating "values levers" (Shilton 2013), both seem promising. Professional codes of ethics have also been presented as influential aspects of engineers' ethical awareness (e.g., Fleischmann, Wallace, and Grimes 2010). However, the strong negative attitude of system engineers towards legal experts that we have observed in our interview study seems to weaken the potentials of the third approach – bringing in external ethical experts.

While the small sample of this interview study demands a cautious interpretation of results, we see the views we collected here as indicators for a resistance of system engineers to what society will increasingly demand in the future beyond functionality. The results of this study do not aim at generalizability and can only hint at explanations for the reluctance of system engineers to include privacy mechanisms in the products they design and develop. However, they clearly show that several factors have to be considered as substantial influences on the motivation of system engineers. So far, studies have focused too narrowly on single factors or aspects like personality and ethics of the profession as such. We hope to encourage more research into the fundamental issues at work in organizations that impede that privacy is positively, fully and truly embraced in system design, which would certainly be needed.

Notes

1. See https://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct
2. See https://www.ieee.org/about/ethics.html

References

Acquisti, Alessandro, L. Brandimarte, and G. Löwenstein. 2015. "Privacy and Human Behavior in the Age of Information." *Science* 347 (6221): 509–14.

Acquisti, Alessandro, Allan Friedman, and Rahul Telang. 2006. "Is There a Cost to Privacy Breaches? An Event Study Analysis." *Proceedings of the 3rd International Conference on Intelligent Systems (ICIS), Prague, Czech Republic* 94.

Ajzen, Icek. 1985. "From Intentions to Actions: A Theory of Planned Behavior." In *Action-Control: From Cognition to Behavior*, edited by Julius Kuhl and Jürgen Beckmann, 11–39. Berlin: Springer.

———. 1991. "The Theory of Planned Behavior." *Organizational Behavior and Human Decision Processes* 50: 179–211.

———. 2002. "Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior." *Journal of Applied Social Psychology* 32 (4): 665–83.

Baase, S. 2008. *A Gift of Fire: Social, Legal, and Ethical Issues for Computing and the Internet*. New Jersey: Pearson Prentice Hall.

Balebako, Rebecca, Abigail Marsh, Jialiu Lin, Jason I. Hong, and Lorrie Faith Cranor. 2014. "The Privacy and Security Behaviors of Smartphone App Developers." In *Proceedings 2014 Workshop on Usable Security (USEC)*. San Diego, CA: Internet Society. https://doi.org/10.14722/usec.2014.23006.

Bélanger, F., and R. E. Crossler. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems." *MIS Quarterly* 35 (4): 1017–

41.
Berenbach, Brian, and Manfred Broy. 2009. “Professional and Ethical Dilemmas in Software Engineering [Cover Feature].” *Computer*, 2009. https://doi.org/10.1109/MC.2009.22.
Birnhack, Michael, Eran Toch, and Irit Hadar. 2014. “Privacy Mindset, Technological Mindset.” *Jurimetrics: Journal of Law, Science & Technology* 55: 1–71. https://doi.org/10.2139/ssrn.2471415.
Bowyer, Kevin W. 2004. “Face Recognition Technology: Security versus Privacy.” *IEEE Technology and Society Magazine* 1: 9–19.
Camenisch, Jan, Abhi Shelat, Dieter Sommer, Simone Fischer-Hübner, Marit Hansen, Henry Krasemann, Ronald Leenes, and Jimmy Tseng. 2005. “Privacy and Identity Management for Everyone.” In *Workshop On Digital Identity Management (DIM), November 11, 2005, Fairfax, Virginia, USA*. ACM.
Cavoukian, Ann. 2009. *Privacy by Design: Take the Challenge*. Information and Privacy Commissioner of Ontario, Canada.
———. 2010. “Privacy by Design: The 7 Foundational Principles.” Toronto, Canada.
Christl, Wolfie. 2017. “Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions.” Vienna.
Christl, Wolfie, and Sarah Spiekermann. 2016. *Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy*. Vienna: Facultas Verlags- und Buchhandels AG.
Ciocchetti, Corey. 2007. “The Privacy Matrix.” *Journal of Technology Law & Policy* 12 (1): 245–329.
Clarke, Roger. 2001. “Privacy as a Means of Engendering Trust in Cyberspace Commerce.” *University of New South Wales Law Journal* 24 (1): 290–97.
Cochrane, Peter. 2000. “Head to Head.” *Sovereign Magazine, Spring*, 2000.
Craft, Jana L. 2013. “A Review of the Empirical Ethical Decision-Making Literature: 2004-2011.” *Journal of Business Ethics* 117: 221–59. https://doi.org/10.1007/s10551-012-1518-9.
Cruz, Shirley, Fabio Q. B. da Silva, and Luiz Fernando Capretz. 2015. “Forty Years of Research on Personality in Software Engineering: A Mapping Study.” *Computers in Human Behavior* 46: 94–113. https://doi.org/10.1016/j.chb.2014.12.008.
Culnan, M., and P. Armstrong. 1999. “Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation.” *Organization Science* 10 (1): 104–15.
Fleischmann, Kenneth R., and William A. Wallace. 2010. “Value Conflicts in Computational Modeling.” *Computer* 43 (7): 57–63.
Fleischmann, Kenneth R., William A. Wallace, and Justin M. Grimes. 2010. “The Values of Computational Modelers and Professional Codes of Ethics: Results from a Field Study.” *Proceedings of the 43rd Hawaii International Conference on System Sciences (HICSS)*, 1–10. https://doi.org/10.1109/HICSS.2010.400.
Friedman, Batya, Peter H Kahn Jr., and Alan Borning. 2006. “Value Sensitive Design and Information Systems.” In *Human-Computer Interaction and Management Information Systems: Foundations*, edited by Ping Zhang and Dennis Galletta, 348–72. Armonk, NY: M.E.Sharpe.
Greene, Daniel, and Katie Shilton. 2017. “Platform Privacies: Governance, Collaboration, and the Different Meanings of ‘Privacy’ in IOS and Android Development.” *New Media & Society*, 146144481770239. https://doi.org/10.1177/1461444817702397.
Heller, Christian. 2011. *Post-Privacy: Prima Leben Ohne Privatsphäre*. München:

C.H.Beck.
Hes, Ronald, and John Borking, eds. 2000. *Privacy-Enhancing Technologies: The Path to Anonymity*. Revised ed. The Hague: Registratiekamer. https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/av/av11.pdf.
Hoffman, David. 2014. “Privacy Is a Business Opportunity.” *Harvard Business Review, April 18*. https://hbr.org/2014/04/privacy-is-a-business-opportunity.
Identity Theft Resource Center. 2016. “Data Breach Reports.” 2016. http://www.idtheftcenter.org/images/breach/DataBreachReport_2016.pdf.
Johnson, Deborah G. 2009. *Computer Ethics: Analyzing Information Technology*. Upper Saddle River, NJ: Pearson Education.
Jonas, Hans. 1984. *The Imperative of Responsibility: In Search of an Ethics for the Technological Age*. Chicago & London: The University of Chicago Press.
Krumay, Barbara, and Marie Caroline Oetzel. 2011. “Security and Privacy in Companies: State-of-the-Art and Qualitative Analysis.” In *Proceedings of the 2011 6th International Conference on Availability, Reliability and Security, ARES 2011*, 313–20. https://doi.org/10.1109/ARES.2011.53.
Land, Frank, Sevasti-Melissa Nolas, and Urooj Amjad. 2004. “Knowledge Management: The Darker Side of KM.” *Knowledge, Organisations and Development Network (KODE) Working Papers Series* 9.
Langheinrich, Marc, and Saadi Lahlou. 2003. “A Troubadour Approach to Privacy.” *Ambient Agoras Report* 15.3.1.: 2–29.
Mayes, G. Randolph. 2010. “Privacy and Transparency.” In *The AAAI Spring Symposium: Intelligent Information Privacy Management, Paolo Alto, CA*, 125–29.
Mayring, Philipp. 2014. *Qualitative Content Analysis: Theoretical Foundation, Basic Procedures and Software Solution*. http://nbn-resolving.de/urn:nbn:de:0168-ssoar-395173.
Nakayama, Makoto, Charlie Chen, and Christopher Taylor. 2016. “The Effects of Perceived Functionality and Usability on Privacy and Security Concerns about Adopting Cloud Application Adoptions.” In *Proceedings of the Conference on Information Systems Applied Research, Las Vegas, Nevada, USA*, 1–8.
Nissenbaum, H. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford Law Books.
O’Fallon, Michael J., and Kenneth D. Butterfield. 2005. “A Review of the Empirical Ethical Decision-Making Literature: 1996–2003.” *Journal of Business Ethics* 59: 375–413. https://doi.org/10.1007/s10551-005-2929-7.
Organisation for Economic Cooperation and Development. 1980. “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.” OECD. 1980. http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.
———. 2013. *The OECD Privacy Framework*. OECD. http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.
Pavone, Vincenzo, and Sara Degli Esposti. 2012. “Public Assessment of New Surveillance-Oriented Security Technologies: Beyond the Trade-off between Privacy and Security.” *Public Understanding of Science* 21 (5): 556–72.
Pew Research Center. 2014. “Public Perceptions of Privacy and Security in the Post-Snowden Era.” https://doi.org/202.419.4372.
Ponemon Institute LLC. 2011. “The True Cost of Compliance: A Benchmark Study of Multinational Organizations [Research Report].” 2011. http://www.ponemon.org/local/upload/file/True_Cost_of_Compliance_Report_copy.pdf.

"Privacy Bridges: EU and US Privacy Experts in Search of Transatlantic Privacy Solutions." 2015. 37th International Privacy Conference Amsterdam 2015. 2015. http://privacybridges.mit.edu/sites/default/files/documents/PrivacyBridges-FINAL.pdf.

Roeser, Sabine. 2012. "Emotional Engineers: Toward Morally Responsible Design." *Science and Engineering Ethics* 18 (1): 103–15. https://doi.org/10.1007/s11948-010-9236-0.

Rouvroy, Antoinette, and Yves Poullet. 2009. "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy." In *Reinventing Data Protection?*, edited by Serge Gurwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne, and Sjaak Nouwt, 45–76. Dordrecht: Springer.

Schaefer, Robert. 2006. "A Critical Programmer Searches for Professionalism." *ACM SIGSOFT Software Engineering Notes* 31 (4): 1–17.

Schwab, Klaus, Alan Marcus, Justin Rico Oyola, and William Hoffman, eds. 2011. *Personal Data: The Emergence of a New Asset Class*. An Initiative of the World Economic Forum.

Sharp, Helen, Nathan Baddoo, Sarah Beecham, Tracy Hall, and Hugh Robinson. 2009. "Models of Motivation in Software Engineering." *Information and Software Technology* 51: 219–33. https://doi.org/10.1016/j.infsof.2008.05.009.

Shaw, Thomas R. 2003. "The Moral Intensity of Privacy: An Empirical Study of Webmasters' Attitudes." *Journal of Business Ethics* 46: 301–18. https://doi.org/10.1023/A:1025628530013.

Shilton, Katie. 2013. "Values Levers: Building Ethics into Design." *Science, Technology, & Human Values* 38 (3): 374–97. https://doi.org/10.1177/0162243912436985.

Shilton, Katie, and Daniel Greene. 2017. "Linking Platforms, Practices, and Developer Ethics: Levers for Privacy Discourse in Mobile Application Development." *Journal of Business Ethics*. https://doi.org/10.1007/s10551-017-3504-8.

Smith, H. Jeff, Tamara Dinev, and Heng Xu. 2011. "Information Privacy Research: An Interdisciplinary Review." *MIS Quarterly* 35 (4): 989–1015.

Smith, H Jeff. 1994. *Managing Privacy: Information Technology and Corporate America*. Chapel Hill, NC: The University of North Carolina Press.

Solove, Daniel J. 2008. *Understanding Privacy*. Cambridge, MA: Harvard University Press.

Sommerville, Ian. 2011. *Software Engineering*. 9th ed. Boston: Addison-Wesley. https://doi.org/10.1111/j.1365-2362.2005.01463.x.

Spiekermann, Sarah. 2012. "The Challenges of Privacy by Design." *Communications of the ACM*, 2012. https://doi.org/10.1145/2209249.2209263.

———. 2016. *Ethical IT Innovation: A Value-Based System Design Approach*. Boca Raton, FL: CRC Press.

Spiekermann, Sarah, Alessandro Acquisti, Rainer Böhme, and Kai-Lung Hui. 2015. "The Challenges of Personal Data Markets and Privacy." *Electron Markets* 25: 161–67. https://doi.org/10.1007/s12525-015-0191-0.

Spiekermann, Sarah, and Lorrie Faith Cranor. 2009. "Engineering Privacy." *IEEE Transactions on Software Engineering* 35 (1): 67–82. https://doi.org/10.1109/TSE.2008.88.

Spiekermann, Sarah, Jana Korunovska, and Marc Langheinrich. 2018. "Understanding Engineers' Drivers and Impediments for Ethical System Development: The Case of Privacy- and Security Engineering" (Working Paper 2). https://www.wu.ac.at/ec/research/. Retrieved from http://epub.wu.ac.at/6339/

Suchman, Mark C. 1995. “Managing Legitimacy: Strategic and Institutional Approaches.” *Academy of Management Review* 20 (3): 571–610. https://doi.org/10.5465/AMR.1995.9508080331.

Szekely, Ivan. 2011. “What Do IT Professionals Think about Surveillance?” In *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*, edited by Christian Fuchs, Kees Boersma, Anders Albrechtslund, and Marisol Sandoval, 198–219. New York: Routledge.

The European Parliament and the Council of the European Union. 1995. “Directive 1995/46/EC on Protection of Individuals with Regard to the Processing of Personal Data on the Free Movement of Such Data.” *Official Journal of the European Communities*.

———. 2016. “Regulation (EU) 2916/679 (General Data Protection Regulation).” *Official Journal of the European Union* 59: 1–88. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN.

The White House. 2015. “Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015.” Washington.

TNS Opinion & Social. 2015. “Special Eurobarometer 431: Data Protection.” European Union. https://doi.org/10.2838/552336.

Varona, Daniel, Luiz Fernando Capretz, Yadenis Piñero, and Arif Raza. 2012. “Evolution of Software Engineers’ Personality Profile.” *ACM SIGSOFT Software Engineering Notes* 37 (1): 1–5. https://doi.org/10.1145/2088883.2088901.

Verizon. 2017. “Data Breach Investigations Report.” http://www.verizonenterprise.com/DBIR/2014/insider/?utm_source=earlyaccess&utm_medium=redirect&utm_campaign=DBIR.

Vermaas, P. E., P. Kroes, A. Light, and S. A. Moore, eds. 2008. *Philosophy and Design: From Engineering to Architecture*. Springer Science + Business Media.

Wallenstein, Gerd D. 1974. “Engineers Are Supersnobs.” *IEEE Spectrum*, 78–79.

Ware, David K., David J. Ahlgren, and Harvey F. Silverman. 2013. “Educating Engineering Students about Ethics: Experiences at Brown University and Trinity College.” In *2013 American Society For Engineering Education Annual Conference*. Atlanta, Georgia. https://peer.asee.org/19463.

Webb, Phyl, Carol Pollard, and Gail Ridley. 2006. “Attempting to Define IT Governance: Wisdom or Folly?” In *Proceedings of the 39th Hawaii International Conference on System Sciences*, 1–10.

Zimmermann, P. 1995. *The Official PGP User’s Guide*. Boston: MIT Press.

Appendix 1 – Questionnaire Items

Experiential attitude	For me the prospect of actually incorporating privacy mechanisms or processes into my new systems in the immediate future (2-3 years) would be… *pleasing - - - - - - - - - annoying* *enjoyable - - - - - - - - - unenjoyably* *exciting - - - - - - - - - boring* *challenging - - - - - - - - - trivial*
Instrumental attitude	I find that incorporating privacy mechanisms into the design of my systems in the immediate future (2-3 years) *up-to-date - - - - - - - - - outmoded* *very useful - - - - - - - - - useless* *sensible - - - - - - - - - senseless* *fruitful - - - - - - - - - futile* *valuable - - - - - - - - - worthless*
Subjective Norm	Most **people who are important to me** think that *I should - - - - - I should not* incorporate privacy mechanisms into the systems I build
Normative Beliefs of the Organization	Against the background of your respective organizational context (company, university, research group), what is true for you? My **organization** thinks that *I should - - - - - I should not* incorporate privacy mechanisms into the systems I build
Perceived Behavioural Control	It is mostly up to me whether or not I incorporate privacy mechanisms into the systems I build in the immediate future (2-3 years). *strongly agree - - - - - - - - - strongly disagree* If I wanted to I could incorporate privacy mechanisms into the systems I build in the immediate future (2-3 years). *definitely true - - - - - - - - - definitely false*
Control Beliefs	**The knowledge** I need to have to incorporate privacy mechanisms into my systems would make it *very difficult - - - - - very easy* for me to do so in the immediate future (2-3 years). **The time** required to incorporate privacy mechanisms into my systems would make it *very difficult - - - - - very easy for me* for me to do so in the immediate future (2-3 years). **The autonomy** I need to have to incorporate privacy mechanisms

	into my systems would make it *very difficult - - - - - very easy* for me to do so in the immediate future (2-3 years).
Responsibility	Ensuring the privacy-friendliness of a system is not my responsibility. *strongly agree - - - - - - - - -strongly disagree*

Appendix 2 – Engineers' Beliefs and Correlations with Privacy Attitudes

Political (PB) and Technical Beliefs (TB) about Privacy	*M*	*SD*	Instrumental attitudes	Experiential attitudes
1. PB: Designing user-privacy systems into systems is important to enable a power balance between CORPORATIONS and citizens	4.12	0.98	0.28**	0.22*
2. PB: Designing user-privacy into systems is important to enable a power balance between GOVERNMENTS and citizens	3.94	1.02	0.16	0.05
3. PB: I think that more data means more knowledge	3.60	1.10	0.06	0.02
4. PB: I think that personal information has become just another form of property that people can sell or buy	3.41	1.33	0.03	0.00
5. PB: I think that freedom of speech is more important than privacy	3.09	1.07	-0.22	-0.15
6. PB: I think that transparency is more important than privacy	3.00	1.11	-0.36*	-0.41**
7. TB: Ensuring user-privacy in a system is a legal issue rather than a technical one	2.95	1.27	-0.12	0.07
8. TB: I think that technology is neutral	2.88	1.43	-0.05	-0.08
9. TB: Efforts to fully secure a system are often futile, because good hackers can circumvent any security	2.81	1.31	-0.10	-0.04
10. TB: I think that with the right cryptographic mechanisms most privacy problems can be solved	2.44	1.24	-0.01	-0.07
11. TB: As Ubiquitous Computing systems inherently rely on the collection of large amounts of data, privacy and UbiComp is a contradiction	2.43	1.11	-0.13	-0.12
12. TB: I think that it is possible, in principle, to build error-free systems	2.21	1.28	-0.06	0.06