Sarah Spiekermann-Hoff and Jana Korunovska and Marc Langheinrich

Understanding Engineers’ Drivers and Impediments for Ethical System Development: The Case of Privacy and Security Engineering

Original Citation:

This version is available at: http://epub.wu.ac.at/6339/
Available in ePub\textsuperscript{WU}: May 2018

epub\textsuperscript{WU}, the institutional repository of the WU Vienna University of Economics and Business, is provided by the University Library and the IT-Services. The aim is to enable open access to the scholarly output of the WU.
Sarah Spiekermann-Hoff and Jana Korunovska and Marc Langheinrich

Understanding Engineers’ Drivers and Impediments for Ethical System Development: The Case of Privacy and Security Engineering

Original Citation:

This version is available at: http://epub.wu.ac.at/6339/
Available in ePub^WU: May 2018

ePub^WU, the institutional repository of the WU Vienna University of Economics and Business, is provided by the University Library and the IT-Services. The aim is to enable open access to the scholarly output of the WU.
Abstract— Machine ethics is a key challenge in times when digital systems play an increasing role in people’s life. At the core of machine ethics is the handling of personal data and the security of machine operations. Yet, privacy and security engineering are a challenge in today’s business world where personal data markets, corporate deadlines and a lag of perfectionism frame the context in which engineers need to work. Besides these organizational and market challenges, each engineer has his or her specific view on the importance of these values that can foster or inhibit taking them into consideration. We present the results of an empirical study of 124 engineers based on the Theory of Planned Behavior and Jonas’ Principle of Responsibility to understand the drivers and impediments of ethical system development as far as privacy and security engineering are concerned. We find that many engineers find the two values important, but do not enjoy working on them. We also find that many struggle with the organizational environment. They face a lack of time and autonomy that is necessary for building ethical systems, even at this basic level. Organizations’ privacy and security norms are often too weak or even oppose value-based design, putting engineers in conflict with their organizations. Our data indicate that it is largely engineers’ individually perceived responsibility as well as a few character traits that make a positive difference.
I. INTRODUCTION

The rapid diffusion of machines into all spheres of human life is increasing the call for more ethical reflections in their development. When autonomous cars carry passengers, robots serve the elderly, and personal agents speak with people about their most intimate life details, questions of ethical baselines for such technologies become inevitable. In his 2006 essay on “The Nature, Importance, and Difficulty of Machine Ethics” James Moor outlines how machines should be designed to avoid unethical outcomes (implicit ethical agents) and even encode and learn ethics where this is feasible (explicit ethical agents) [1].

With his 2006 call for implicit ethical agents, Moor was early to tap into a strand of research that aims to respect human values in the design of systems [2-4]. He talked about “machine virtues” at the time, naming issues like safety and reliability. Since then, many values have been recognized as vital for machines; in fact, phenomenologically each machine can bear unique values depending on its use context [5]. But there are some values that seem to be particularly relevant in system design because they relate to the very way in which data is handled across technologies and contexts. These include privacy and security, which have consequently been subject to long-term academic efforts [see for e.g. 6, 7-9] and have been recognized in technology regulation all over the world [10-12]. In fact, scholars have made a tremendous effort to develop privacy-enhancing solutions at least since the 1990s [9, 13-15] and the security engineering field has proposed major design standards [16, 17].

Yet, apart from some success stories such as SSL/HTTPS, the widespread use of proposed solutions and standards is still lagging behind (the exception being security-related application areas such as wireless payment systems). Even the NSA ignored baseline security measures that would have protected them against Edward Snowden’s revelations [18]. Not surprisingly, data breaches abound all over the world: in 2017, in the US alone, over 178 million records of personal data were exposed in over 1500 data breaches and 4200 security attacks, a 45 percent increase over the already record high figures reported for 2016 [19, 20]. Such breaches and attacks are said to lead to billions in losses for corporations [21]. Consumer studies reveal that unease is spreading among citizens, as people fear losing control over their personal data and see their privacy being compromised [22]. This situation is troubling. What will happen if soon robots serving people are hacked and turned into competitive and aggressive robots as Vanderelst and Winfield outline in their article on “The Dark Side of Ethical Robots” [23]? Who is responsible when personal agents like Alexa or Siri betray the trust of their owners, because privacy awareness has not been properly designed into them?

If ordinary people were asked as to who is responsible for this situation, they would probably point at the engineering world. Historically, engineers have always been held responsible for their products. The Babylonian Code of Hammurabi (1750 BC), one of the oldest deciphered writings of significant length in the world, says: “If a builder has built a house for a man and has not made his work strong enough and the house he has made has collapsed and caused the death of the owner of the house, that builder shall be killed. If it destroyed possessions, he shall make recompense for whatever he destroyed. Moreover, since the house he had built collapsed because he had not made it strong enough, he shall rebuild the house which collapsed from his own resources.” [24, p. 109]

Yet, today we know that engineers are not independent craftsmen, but often work in teams where they face an organizational environment that is not always easy. Pressed for time, many have difficulties to even live up to their associations’ code of ethics (i.e. ACM, IEEE), which only ask for minimum value standards, such as the quality and reliability of products [25]. It has been reported that organizations see value conflicts arise within development teams, which need to be actively managed [26]. Is the current situation of privacy and security “nightmares” a testament to such organizational challenges, which can be fixed given better incentive structures? Or are we witnessing a deeper personality and socio-cultural issue that hinders privacy and security engineering at a deeper level?

Unfortunately, we know very little about privacy and security behavior of engineers in their development work [26-30]. Only four studies have looked at this issue [27-30]. Particularly noteworthy is the study by Lahlou, Langheinrich, & Röcker who found in 2003 that engineers were very reluctant to embrace privacy: Privacy “was either an abstract problem [to them], not a problem yet (they are ‘only prototypes’), not a problem at all (firewalls and cryptography would take care of it), not their problem (but one for politicians, lawmakers, or, more vaguely, society), or simply not part of the project deliverables” [28, p. 60]. The only quantitative study that exists on privacy and security behavior focuses on smartphone app developers [30] and largely confirms these insights. It shows that many app developers lack awareness of privacy and security measures and make engineering decisions in an ad hoc manner, especially when working in smaller organizations. They are also conflicted on privacy due to current economic trends that support personal data markets [31]. None of these existing studies have developed a systematic model that would identify drivers and impediments of privacy and security engineering behavior across technologies. We therefore lack an important piece of research in our efforts to build ethical machines: We know hardly anything about the people who build them.
To address this gap in research we studied 124 software and system engineers working for a wide spectrum of companies and research institutions around the world and at various hierarchical levels. The study is based on the Theory of Planned Behavior (TPB) and Jonas’ Principle of Responsibility as baseline behavioral models [32-34]. In addition, we report on six interviews with senior engineers at globally leading IT companies and research centers. We believe that our findings strongly contribute to our understanding of privacy and security engineering, because it looks into the practical realities, conflicts and challenges we need to confront in organizations to build more secure and private systems. If we succeed in doing this, then we will have taken a major step towards more ethical systems in general.

II. THEORETICAL BACKGROUND

A. Privacy and Security Behavior and the Theory of Planned Behavior

We define security engineering behavior as any activity undertaken by an engineer that fosters the confidentiality, integrity, availability, authenticity and non-repudiation of the data collected or services created. We define privacy engineering behavior as any activity undertaken by an engineer that (1) reduces the collection and storage of personal data (i.e. through data minimization or anonymization), (2) limits the sharing of personal data with third parties not explicitly authorized by the data subject, (3) gives users full information about what happens to their personal data (transparency) and (4) gives users real choice whether to consent to the processing of their personal data. With these definitions, we consider privacy and security as relevant dimensions for implicit ethical agents [1].

When we use the term “engineer” hereafter, we refer to both software engineers and systems engineers. While there is no clear-cut definition of the two roles, they are usually differentiated by the scope of system issues on which they focus [35]. In this classification, a software engineer would mostly design and write code, while a systems engineer looks more holistically across multiple aspects and technologies (software, hardware, human factors, and processes). We refer to both forms of engineering because ethical issues such as the privacy and security design of an information technology are typically addressed at various technical levels, including the architecture of a system, its hardware and software design, and the way these are embedded in organizational processes.

According to the issue-contingent model of ethical decision-making behavior in organizations [36], any moral issue first needs to be recognized and judged upon by a person. Only following this moral awareness phase, moral intent is formed and people behave (hopefully) in line with their intent. For the present context of privacy and security engineering, recognizing the moral issue is not a given. When privacy or security are not recognized in IT product design, there are normally no immediate sanctions from users, sometimes not even in the long-term. In the absence of effective legal sanctions (and hence any reasonable applicability of expected-utility theory [37, 38]) the question arises as to whether engineers will be aware of privacy and security issues at all. Some research doubts this [28, 30]. So what could drive engineers’ motivation to consider privacy and security in their systems?

We chose TPB as our primary behavioral model because it circumvents the limits of expected-utility theory for our context. It is also widely used in the ethical decision-making literature [39] and was successfully applied to understand unethical programming behavior [40]. TPB states that planned human behavior is generally caused by three core factors: (1) people’s (instrumental and experiential) attitudes towards a behavior, (2) people’s subjective norms for that behavior, and (3) their perceived behavioral control to perform the behavior [41]. In the following section, we take a close look into these main constructs of the TPB in relation to our context of privacy and security engineering behavior and derive our hypotheses.

1) Engineers’ Privacy and Security Attitudes and Beliefs

Ajzen’s TPB, as well as other psychological theories [42, 43], emphasize peoples’ attitudes as key to understanding why and how they act. Attitudes towards behaviors can be instrumental (how a person rationally values a behavior), or they can be experimental (how a person values the experience of the behavior) [41]. For example, instrumental attitudes determine if we find a behavior useful, valuable, important or sensible. Experiential attitudes, on the other hand, determine if we find a behavior enjoyable, pleasant or frustrating. Both these attitudes are typically driven by beliefs held by an individual. For instance, if an engineer believes that “privacy is dead” or that “any system can be hacked”, these beliefs can negatively influence their attitude towards investing time in privacy-preserving and secure systems. So what are common beliefs related to privacy and security?

It is well known that the values of privacy and security are ambivalent. Many voice the belief that privacy is outdated at a time of ubiquitous computing, when people share so much of their data on social network platforms [44] and when more data seems to promise more knowledge [45, 46]. Developer platforms see both discussions on “human privacy whiners”, as well as mutual touting of privacy-enhancing mechanisms [47, p. 9]. Some authors regard privacy as a value that needs to be traded off for more transparency [48, 49] or knowledge creation [46], presuming that these cannot co-exist with privacy. Moreover, embracing privacy engineering costs time and money, while at the same time undermining business models that rely on personal data as a property on sale [29, 47]. Such negative beliefs have been countered by privacy advocates, who argue that the respect for privacy in system design
creates business advantages [50], reduces corporate liability [51] and risks [52], and does not need to undermine security [53, 54]. Advocates argue that privacy is a fundamental right [55, 56], which is essential to balancing power in functioning democracies [56], especially vis-à-vis corporates [47].

Security beliefs and attitudes see similar contradictory dynamics. Some feel that the importance of (national) security is overstated [57], while others use it extensively to justify investments in a security infrastructure [58]. The business impact of security is highly related to the risk inherent in systems' infrastructures, which are easily underestimated by those who have to pay for the technical investments [59] and potentially overstated by those who earn money from these [60]. The practicability of security is doubted by those who believe that any system can be hacked anyways, while others feel confident that cryptography can sufficiently protect security [61] and that, in principle, we can build error-free and hence fully secure systems.

If we take all of these contradictory beliefs together, it is reasonable to expect that engineers have equally mixed attitudes towards privacy and security. In our interviews with senior engineers, we found that experiential attitudes towards privacy were often negative. They argued that it is difficult to implement effective privacy mechanisms and that users could still be tricked into disclosure. That said, the instrumental attitudes were more positive. Almost all interviewees agreed to the necessity of protecting users' privacy somehow (undisclosed reference).

Based on these insights, as well as the direction of influence postulated by TPB, we hypothesize:

Hypothesis 1a: Experiential attitudes towards privacy and security are positively related to privacy and security engineering behavior.

Hypothesis 1b: Instrumental attitudes towards privacy and security are positively related to privacy and security engineering behavior.

According to the TPB, the beliefs that are the base for the attitudes towards certain behaviors are always context and behavior specific, so we are dissuaded from hypothesizing a relationship between every privacy and security belief and the engineers' attitudes towards building privacy and secure systems. However, we did explore which beliefs relate to these attitudes (see below).

2) The Role of the Professional Environment for Privacy and Security Engineering

Recent studies provide support for the claim that IT professionals comply with organizational expectations when it comes to privacy engineering or ethical system design at large. Shaw [62, p. 314] has shown that webmasters seek "organizational consensus" when deciding if an action related to privacy is ethical or unethical: "Webmasters do not make ethical decisions in a vacuum, but instead look to their co-workers for guidance". In a large-scale study in Hungary and the Netherlands, Szekely [63] has shown that the majority of IT professionals usually agree with the organizational decisions made about the handling of personal data throughout a project. If they happened to disagree with a decision, they would definitely let it be known, but the great majority would still go along with the organizational decision. Only 12 percent of the respondents in Szekely's study stated that they would refuse to implement the decision in such a situation. Considering the generally positive relationship between organizational norm and engineering behavior, we hypothesize:

Hypothesis 2: Engineers' subjective norm for privacy and security engineering is positively related to privacy and security engineering behavior.

3) Perceived Behavioral Control over Privacy and Security Engineering.

In the TPB, next to attitudes and social norm, the final determinant of behavior is the perceived behavioral control [64]. It determines how easy or difficult it is for individuals to perform a behavior, based both on their abilities and on the context in which they operate. Organizational teams operate in a highly competitive, cost-minimizing, and hype-driven rush towards technical upgrades [3]. As a result, software engineering teams often work in a climate that can be hostile to non-functional system requirements such as privacy and security. A good description of such an environment can be found in Berenbach and Broy’s account of professional and ethical dilemmas in software engineering [25]. The authors describe how the rush towards system delivery can lead to organizationally induced problematic ethical behavior, the difficulty to honor agreements, the lack of comprehensive and thorough evaluation of computer systems, a promotion of “fictionware”, and the tendency to sweep lack of quality under the rug.

Against this background, software engineers might simply not have enough time or autonomy, and consequently control, to engage in privacy and security engineering behavior. On the other hand, Schaefer [65, p. 3] observes that engineers are the ones “closest to the work” and therefore often get from their managers the freedoms to pursue what is necessary. That said, plans and processes are still a non-negligible part of the professional engineers' surrounding. The organizational set-up, staffing, sales deals, delivery dates or external funding set limits to the length
of development efforts and, by extension, engineers’ ability to engage in privacy and security engineering. Our interviews revealed that even senior engineers do not hold positive control perceptions (undisclosed reference). They state that privacy issues are technically difficult to solve and that the concept of privacy is unclear. These issues, found in other studies as well [27, 30], point to an issue of knowledge and education that could lead engineers to not perceive sufficient control over privacy and security engineering. The corresponding hypothesis to these practical challenges is:

**Hypothesis 3:** The perceived behavioral control over privacy and security engineering is positively related to privacy and security engineering behavior

**B. The Role of Perceived Responsibility for Privacy and Security Engineering**

In addition to using the TPB for our research, we also explored the relevance of perceived personal responsibility of engineers in our work. Virtue ethics sees people acting ethically just for the sake of doing the right thing [66]. Some scholars trace virtuous awareness or consciousness of values and ethics back to a cognitive moral development that some people have more than others [67] and that is one of the core individual characteristics prohibiting unethical intentions and choices in organizations [68]. In his famous 1976 book on “Principles of Responsibility”, Hans Jonas called for more engineering responsibility, as otherwise the future would have no seat at technology design tables [69].

In contrast to this, Schaefer asked “Should the programmer be the one solely held accountable for the software faults?” [65]. Lah lou and colleagues [28] found that engineers felt that privacy was not their problem, but one for politicians, lawmakers, or, more vaguely, society at large. Greene and Shilton report that developers believe users are responsible for their privacy by simply not accepting usage terms or using privacy-enhancing tools [47], but they also see developers touting good privacy-enhancing solutions [27]. In our own interview study with senior engineers in corporate and university research, we found support for the perception that someone else is responsible for privacy, especially corporate lawyers, but not so much the engineers themselves (undisclosed reference). This finding is also present in a larger quantitative study of IT professionals [63, p. 209], which 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”.

Along these lines, it might be that it is low perceived responsibility for privacy and security that has led to limited engagement in respective design efforts, leading to the following hypothesis:

**Hypothesis 4:** The perceived responsibility for privacy and security engineering is positively related to privacy and security engineering behavior

Figure 1 summarizes the hypothesized relationships and gives an overview of the model we explored empirically.

---

Besides establishing and testing this hypothesized model, we controlled for the potential belief structures described above and potentially explaining the instrumental and experiential attitudes. On theoretical grounds and in accordance with Ajzen, we did not include these beliefs in our model, since they are not expected to be internally consistent [41]. We also included concrete organizational context variables in our investigations, which might influence the subjective norm. Furthermore, we controlled for individual characteristics, which were shown relevant in earlier studies of unethical managerial choices. These studies suggest that individual’s perceived locus of control [68], their motivation [70-72], and their personality traits (extraversion, agreeableness, conscientiousness, emotional stability and openness to experience) [73] might influence engineers’ behavior. Finally, we included religiousness, because an extensive literature study on the frequent failure of software projects identified religious views as a moderating factor [74] and many ethical decision-making studies in organizations have revealed religiousness to be a significant predictor of good behavior [39].

### III. Method

**A. Sampling**

We used an online questionnaire to investigate the drivers and impediments of privacy and security engineering. Participants were recruited through a mailing list from the “UbiComp” Conference (containing 252 e-mail addresses), which is a conference on new and avant-garde technologies. We used this mailing list to ensure that we reached engineers in the highly dynamic field of software and system design, that is, engineers who develop new prototypes and architectures and not legacy systems or corporate infrastructures for which privacy and security designs may
have been decided long ago. In addition, we advertised our survey in relevant social network groups and with a few innovative software companies in our surrounding (including a start-up and a major retailer’s IT department).

B. Measures

When starting the survey, participants received a briefing of our privacy and security engineering definitions (see above) to ensure a common understanding of the behavior under study. The battery of questions that followed was structured in line with the TPB. We took Ajzen’s conceptual and methodological considerations for the design of a TPB questionnaire [41]. We adapted his scales for the privacy and security engineering context, measuring behavior, attitudes, subjective norm and perceived behavioral control as described in the following. Relevant Behavioral Predictors of Privacy and Security Engineering

To measure reported behavior, we asked participants whether they had incorporated privacy and/or security mechanisms into the systems that they had built in the past 4 to 5 years. Answers ranged between never and always on a 5-point Likert scale. To measure engineers’ attitudes towards privacy and security engineering, we used a 5-point semantic differential scale with twelve bipolar adjective pairs that describe the instrumental component (e.g. privacy engineering is worthless - valuable) as well as the experiential qualities (e.g. security engineering is annoying - pleasing) of incorporating privacy and security mechanisms. For the subjective norm we used 5-Point Likert scale items ranging from 1 — “I should not” to 5 — “I should”. The items have “injunctive quality, consistent with the concept of social norm” [41, p.6]. Example item is “Regardless of my organization, people who I have a lot of respect for probably think that I should/shoud not incorporate privacy mechanisms into the systems I build”. For perceived behavioral control we used questions that measure the perceived capability of performing the behavior (whether engineers could incorporate privacy/security mechanisms if they wanted to), as well as controllability of the behavior (whether it is up to them to incorporate the mechanisms). Both sets of items were measured on 5-Point Likert scales ranging from definitely false to definitely true, and strongly disagree to strongly disagree, respectively. In addition to the constructs derived from the TPB, we asked participants an additional self-developed question about their perceived responsibility: “To what extent do you feel you have responsibility for the privacy/security characteristics of the systems you build?”. The item was measured on a 5-point Likert scale ranging from no responsibility to full responsibility.

In addition to the direct predictors of engineering behavior we hypothesized, and in accordance with Ajzen, we included additional items that measured a number of beliefs related to privacy and security engineering [41]. Specifically, we included six political beliefs and six technical beliefs held by engineers about privacy and security. These were revealed as important in the qualitative expert interviews as well as in the literature review. Examples are “more data is more knowledge” or value tradeoffs such as “transparency is more important than privacy”. Additionally, we included questions about normative beliefs (i.e. what engineers believe is expected of them from their organizations) and their motivation to comply with those expectations. The interplay between normative beliefs (organizational norm) and motivation to comply is assumed to influence the subjective norm of individuals [41].

Finally, we included measures of engineers’ control beliefs, specifically related to the knowledge they have and the autonomy and time given to them by their organizations to incorporate privacy and security mechanisms.

Finally, we controlled for demographic and personality variables, as well as engineers’ organizational context. Specifically, we collected information on an engineer’s hierarchical position in the organization and employment status (hierarchical rank, self-employed, employed), the type of organization (industry, academia, government, etc.), as well as age, sex and country of residence. We measured locus of control with scales by Levenson [75], motivation with scales from Sokolowski, Schmalt, Langens, and Puca [76], and the Big-5 personality traits with Gosling, Rentfrow, and Swann’s instrument [77]. We controlled for religiousness with a scale developed by Wilkes, Burnett, and Howell [78].

C. Procedure

In order to test our hypotheses, that is, to understand why engineers did or did not incorporate privacy and security designs into their systems in the past 4 to 5 years, we calculated separate models for privacy and for security in line with Figure 1 and our hypotheses. For each value we conducted a step-wise regression analysis with all TPB predictors entered in the first step, and responsibility added to the model in the second step. We chose this method in order to highlight the potential incremental validity of perceived responsibility over and above the predictors postulated by the TPB. In addition, we calculated the overall structural fit of the models in AMOS [79].

After the initial analysis we tried to modify the initial model in order to increase its predictive validity. We also looked into significant differences and relationships between the control variables and all relevant model variables (predictor and outcome variables) using t-tests, analysis of variance and simple correlations, depending on the type of control variable. In the results section we report only the significant differences and relationship between the control variables and the model variables.
A. Sample and Descriptive Analysis

In total, 292 engineers started to answer the survey and 43 percent completed it, resulting in a final sample of 124 completed questionnaires. On average, it took participants 38 minutes to complete the questionnaire. As compensation for participants’ effort, we offered a lottery-participation for an iPhone, an iPod, as well as Amazon vouchers (1 x 100 EUR, 1 x 50 EUR, and 5 x 20 EUR).

The respondents in the sample were 81 percent male and on average 36 years old. Thirty-three percent (N = 39) of them were from German-speaking countries, 13 percent (N = 16) engineers were from the US, and 10 percent (N = 12) were from Italy. The rest had 29 different nationalities from across the world. In terms of work position and environment, 77 percent (N = 96) of the respondents were professional engineers and 23 percent (N = 28) were PhD students. Sixty-two percent (N = 73) work in a research-related environment (i.e. university, corporate R&D or research institutes), 48 percent (N = 46) in product development for an IT company, two for NGOs, and three for governments. Hierarchically, 25 percent (N = 29) engineers indicated that they were in leadership positions.

Just under two-thirds of the engineers indicated that they incorporated privacy and security preserving features into the systems they built in the past 4 to 5 years. This means that in more than one third of the cases privacy and security-preserving features were not built into the systems. Specifically, 36 percent (N=44) of the engineers stated that they had rarely or never incorporated privacy mechanisms into the systems that they built, and 35 percent (N=43) said that they have rarely or never incorporated security mechanisms.

The great majority of engineers, however (91 percent for both privacy and security), think that privacy and security engineering is useful, valuable and important. A lot less (60 percent for privacy and 63 percent for security) find incorporating these values pleasing, exciting, or interesting. On the 5-point scales, mean values for the instrumental evaluations were $M_{hr} = 4.19 \ (SD_{hr} = 0.76)$ for privacy and $M_{sec} = 4.24 \ (SD_{sec} = 0.75)$ for security; for experiential evaluation, they were $M_{exr} = 3.32 \ (SD_{exr} = 0.82)$ for privacy and $M_{exc} = 3.31 \ (SD_{exc} = 0.82)$ for security.

The subjective norm for incorporating privacy mechanisms was also very high ($M_{sr} = 4.13, SD_{sr} = 1.10$). Only 13 engineers (11 percent) indicated that the people, for whom they have a lot of respect, expect them not to incorporate privacy mechanisms. The same goes for security: 99 engineers (80 percent) have a high subjective norm for security engineering ($M_{sec} = 4.21, SD_{sec} = 1.02$). Only 10 engineers (8 percent) do not subscribe to this positive norm.

The behavioral control perceptions of privacy and security engineering were mixed. A substantial proportion of engineers (37 percent or N = 46 for privacy and 40 percent or N = 50 for security) do not feel that they have sufficient control over implementing privacy and security mechanisms ($M_{pr} = 3.58, SD_{pr} = 1.09; M_{sec} = 3.61, SD_{sec} = 1.00$). This is not due to their capability (66 percent or N = 82 for privacy and 72 percent or N = 89 for security state that if they wanted to, they could design these values into systems), but due to controllability: 51 percent (N = 63) pointed out that (in their organization) it is not (solely) up to them whether they will pursue privacy and security engineering. The degree of perceived behavioral control over privacy and security engineering is positively correlated with the hierarchical position: managers have the highest perceived behavioral control, followed by independent (self-employed) coders, followed by employees in the lower ranks ($F_{pr} (2,114) = 12.27 \ p<.001; F_{sec} (2,114) = 12.63 \ p < .001$). Finally, the majority of engineers (63 percent for privacy and 62 percent for security) also feel responsible for the two values ($M_{pr} = 3.63 \ (SD_{pr} = 1.04), M_{sec} = 3.66 \ (SD_{sec} = 1.07)$). Here, too, engineers in management positions (including the self-managing independent coders) report more responsibility ($F_{pr} (2,114) = 3.10, p<.05; F_{sec} (2,114) = 2.74, p = 0.69$).

B. Predictors of Privacy and Security Engineering

The hypothesized TPB models explained 36 percent of the variance in past privacy engineering and 37 percent of the variance in past security engineering (Table 1). Furthermore, they both had a good structural fit ($\chi^2_{93} = 140.39, CFI_{pr} = .947, RMSEA_{pr} = .064; \chi^2_{102} = 166.12, CFI_{sec} = .944, RMSEA_{sec} = .064$) [80]. However, few of the postulated predictors of the TPB seem to play a role in explaining privacy and security engineering behavior. For privacy, neither experiential attitude ($\beta = .11, p > .05$), subjective norm ($\beta = .02, p > .05$), nor perceived behavioral control ($\beta = .07, p > .05$) could successfully predict the implementation of privacy mechanisms. The only successful predictors for privacy engineering were instrumental attitude ($\beta = .33, p < .001$) and perceived responsibility ($\beta = .36, p < .001$). Perceived responsibility alone explained 10 percent of the variance in past privacy engineering. Perceived responsibility is hence more important than any of the TPB predictors. Thus, for privacy engineering our results support only hypotheses H1a and H4 (but not H1a, H2 and H3). However, it should be noted that the distribution of subjective norm among the engineers was so skewed to the positive side and had so little variance (almost all engineers had high subjective norm for privacy and security engineering) that this could be a reason for its low predictive power.

For security engineering we found that both instrumental ($\beta = .19, p < .01$) and experiential attitudes ($\beta = .26, p < .01$) play a role, lending support for hypothesis H1a, and H1b. However, both subjective norm ($\beta = -.03, p > .05$) and perceived behavioral control ($\beta = .07, p > .05$) were not significant predictors of security engineering. We therefore have to reject hypotheses H2 and H3 for security engineering. Here, too, the distribution of subjective norm was
skewed and lacked variance. Perceived responsibility was positively related to security engineering ($\beta = .46, p < .001$) and by itself explains as much as 19 percent of the variance in security engineering. Thus, our results strongly support hypothesis H4. Table 1 summarizes the regression results for both privacy and security engineering.

---

**Table 1**

---

1) **The (Indirect) Influence of Beliefs on Privacy and Security Engineering**

In the next steps, we wanted to explore why some of the predictors established by the TPB are doing so poorly in explaining privacy and security engineering behavior. We started by looking into engineers’ political and technical beliefs. We studied all beliefs separately to uncover the relevant ones, because beliefs are not theorized to be internally consistent [41].

As can be seen from the decreasing order of agreement with the beliefs in Table 2, engineers in our sample varied substantially in their beliefs about privacy and security. It is noteworthy that political beliefs see much more agreement than technical beliefs.

---

**Table 2**

---

Three of these beliefs stick out as significant attitude predictors, most prominently the belief in a necessary power-balance between corporations and citizens. Engineers who believe in the importance of this power-balance find both privacy and security engineering more useful and valuable than engineers who do not. The experiential attitude towards privacy and security engineering suffers especially for those engineers who value transparency more than they value privacy ($r_{pr} = .29, p < .05$). Moreover, engineers who call for this balance also find privacy engineering to be more enjoyable ($r_{pr} = .22, p < .01; r_{sec} = .14, p > .05$) and they were more likely to engage in privacy and security engineering in the past ($r_{pr} = .31, p < .001; r_{sec} = .21, p < .05$). Surprisingly, a power balance between *governments* and citizens is not significantly correlated with for engineers’ attitudes even though it rates high in importance.

The second relevant belief (on which engineers’ opinions are divided) is that there is a trade-off between transparency and privacy. Engineers who prefer transparent systems over private ones hold less favorable attitudes towards privacy and security engineering than engineers who do not. The experiential attitude towards privacy and security engineering suffers especially for those engineers who value transparency more than they value privacy ($r_{pr} = -.41, p < .001; r_{sec} = -.29, p < .05$), as does the instrumental attitude towards privacy ($r_{pr} = -.36, p < .05$). Finally, we find that engineers who believe that they can build zero-fault systems have a higher probability to enjoy security engineering ($r_{sec} = .20, p < .05$).

2) **The Role of Organizational Norms and Compliance Motivation**

The *normative belief (organizational norm)* that engineers should incorporate privacy and security mechanisms into their systems varied among study participants. Sixty-two percent (N = 77) of the engineers in our sample work for organizations that expect them to consider privacy mechanisms ($M_{pr} = 3.80; SD_{pr} = 1.09$) and 69 percent (N = 86) for organizations that expect security mechanisms ($M_{sec} = 4.00; SD_{sec} = 1.04$). While on average, the organizational norms of our engineers tend to supports privacy and security practices, still 31 percent (N = 38, for security) to 38 percent (N = 47, for privacy) of the engineers work for organizations without clear or even negative norms on these values. This is especially true for research institutions when it comes to security engineering. Namely, engineers who work in the industry report higher normative beliefs for security than their colleagues who work in research. Whereas 89 percent (N = 37) of the engineers who work in industry report very high normative beliefs on security, this is true only for 56 percent (N =40) of the engineers who work in research environments ($t_{sec}(112) = 3.03, p < .01$).

The motivation to comply with these norms is not a given. Even though the majority of engineers say that they want to comply with their organizations’ norms ($M_{pr} = 3.73; SD_{pr} = 1.04; M_{sec} = 3.86; SD_{sec} = 1.03$), there is a substantial share of respondents in our sample (for privacy, 42 percent or N =51; for security, 36 percent or N = 43) who are not very motivated to comply. We investigated whether this lack of compliance motivation is different for engineers working in industry versus research organizations. For privacy, there is no significant difference ($t_{pr}(118) = 1.87, p < .10$), but for security there is. In research and academic work environments, 47 percent (N = 33) of engineers do not want to comply with security norms, while this is the case for only 16 percent (N= 7) in industry ($t_{sec}(115) = 3.10, p < .01$). How do these ambiguous normative beliefs and compliance motivations interact with subjective norm and engineering behavior? We find that normative beliefs are related to motivation to comply in that the weaker the norms in an organization, the lower the motivation to comply with these (weak) norms. In fact, the share of engineers who want to comply with strong norms is two to three times higher than the share of engineers willing to comply with weak norms (Figure 2).

This interaction between normative beliefs (organizational norms) and motivation to comply with these norms is posited by the TPB to drive subjective norm. However, in our study, this interaction explains only 19 percent of the variance in subjective norm for privacy. When controlling for the main effects of normative belief and compliance motivation, none of the three factors (normative belief, compliance motivation and the interaction term between them)
is a significant predictor for subjective norm (F(3,119) = 9.27, p < .001, R² = .19). Instead, we find that normative beliefs (organizational norms) coupled with compliance motivation are actually a significant direct predictor of privacy engineering (F(4,118) = 5.45, p < .08, R² = .16). This means that an organization’s privacy expectations are more important for privacy design behavior than the engineer’s own (subjective) norms. However, the importance of the organizational norms only hold true when engineers are also highly motivated to comply with them (βsec_mtc = 1.33, p < .01). If they do not have this motivation, as is the case for as much as 42 percent (N=51) of engineers in our sample, the impact of the organization is lost. Figure 2a illustrates these dynamics: the dotted line left shows that the high portion of engineers (57 percent or N=27) who do not want to comply with the weak privacy norms of their organizations actually have the courage to ignore their organizations’ norms and sometimes implement privacy mechanisms despite their organizations’ lack of support. In other words, there seem to be “activist privacy engineers” in some organizations with weak norms that stick to their privacy convictions regardless of the organization. Unfortunately, this activism does not always materialize. Frequent privacy engagement can only be found in organizations with strong privacy norms and high compliance motivation. The care for privacy mechanisms against organizational norm is unique to privacy. In security engineering, weak organizational norms lead to a respectively rare incorporation of security mechanisms, regardless of the fact that 60 percent of engineers do not like to comply when working for organizations with weak security norms (Figure 2b). Organizational norm (β = .81, p < .001) is the only significant predictor of the subjective norm here, explaining almost half of its variance (F(3,117) = 34.20, p < .001, R² = .47). Compliance issues come in for security only when organizations have strong security norms. In such security-focused organizations, the problem is that 25 percent (N = 43) of engineers (Figure 2b) have low compliance motivation and actually prefer to not engage in security engineering.

---

3) Drivers of Perceived Behavioral Control

Engineers’ control beliefs, that is, their belief that they believe to have the autonomy, the time and the knowledge to incorporate privacy and security mechanisms — vary greatly and indicate mixed levels of perceived control (Mpr = 3.36, SDpr = 1.20; Msec = 3.42, SDsec = 1.21). About half of the respondents in our sample say that they do not have the autonomy to implement privacy and security mechanisms (52 percent or N = 64 for privacy and 47 percent or N = 58) for security. Moreover, the time required for privacy and security design makes implementation difficult for the majority (Mpr = 2.68, SDpr = 1.09; Msec = 2.59, SDsec = 1.06). Only one in five engineers believes that time is not a problem and it is religiousness that is related to this belief (rpr = .25; rsec = .17, p = .075). Trust in their own knowledge is well distributed among engineers (Mpr = 3.10, SDpr = 1.03; Msec = 2.95, SDsec = 1.05). Twenty-six percent (N = 32) believe that their knowledge makes incorporating privacy mechanisms difficult, for 35 percent (N = 43) it makes it easy. The same is true for 33 percent (N = 41) and 34 percent (N = 42) respectively, when it comes to security engineering. Our regression analysis (Table 3) confirms TPB’s assumption that the three control beliefs successfully predict perceived behavioral control. For privacy engineering, all three predictors play a significant role for control perceptions. For security engineering only knowledge does not. Knowledge does, however, influence privacy and security engineering directly (βpr = .51, p < .001; βsec = .24, p < .05).

---

However, against expectations, time is negatively related to perceived behavioral control. This means that limited time leads engineers to think that it is (solely) up to them to incorporate privacy and security mechanisms or not to do so. Coupled with the fact that many indicate that their organizations do not give them enough time, it could be that we are witnessing an organizational conflict. It is therefore important to understand the interplay between the normative beliefs (organizational norms) and perceived behavioral control. We find that the weaker the norms for privacy and security in organizations, the more engineers feel that it is (solely) up to them to implement the values (rpr = -.19, p < .05; rsec = -.24, p < .01). Two-thirds of those who work in organizations with weak norms (i.e., about a third of the organizations in our sample) have high control perceptions for privacy and security engineering (Table 4).

---

C. The Role of Perceived Responsibility

This interaction between organizational norm and perceived behavioral control is closely related to engineers’ perceived responsibility. Figures 3a to 3d show the interaction between responsibility, control perceptions and the organizational norms in relation to privacy and security engineering behavior, visualizing a significant three-way interplay between the three factors.

---

Figures 3a to 3d around here
What we can see in Figures 3b and 3d (see solid lines), is that only engineers with high responsibility and high control implement privacy and security frequently - and they do so regardless of the organizational norms. When the organizational norms are weak and either control (dotted lines) or responsibility (Figures 3a and 3c) are weak as well, then the engineers’ implementation of privacy and security mechanisms drops. Similarly, when the norms are high but responsibility is low, the implementation drops regardless of perceived control. The important role of perceived responsibility is further shown in Table 5, where we can see that even when we control for the interactions, the main effect of responsibility remains strong. For security, it is the single most important predictor ($\beta_{\text{pr}} = .42$, $p < .001$; $\beta_{\text{sec}} = .60$, $p < .001$). It also shows that the inclusion of the interaction factors (illustrated in Figures 2a, 2b, and 3a to 3d) distinctly improves the predictive power of our original model to $R^2 = .42$ and $R^2 = .43$ for privacy and security engineering respectively (compared to $R^2=.36$ and $R^2=.37$, Table 1). In the model we see that for privacy engineering, it is the interplay between organizational norms and compliance motivation that is particularly relevant - the “activist spirit” ($\beta_{\text{pr}} = .88$, $p < .05$; $\beta_{\text{sec}} = .19$, $p > .05$.). For security engineering it is the three-way interaction between organizational norms, perceived behavioral control and responsibility that counts ($\beta_{\text{pr}} = -.30$, $p < .10$; $\beta_{\text{sec}} = -.40$, $p < .01$). Privacy and security therefore seem to be driven by slightly different motivational shades.

-----

V. DISCUSSION

At the outset of our study we asked the question whether today’s privacy and security nightmares are testimony of a systemic failure that can be fixed with the right organizational and legal incentives, or whether we are witnessing a deeper socio-cultural issue that could impede our long-term hopes for more value-driven, privacy-friendly and secure machine designs. Our empirical results hint towards some issues beyond the influence of individual organizations.

First of all, it must be noted that the vast majority of engineers are aware that they should be pursuing privacy and security by design. Our subjective norm as well as instrumental attitude measures clearly proved this awareness of the matter. Only a small fraction of around 10 percent of the engineers in our sample find privacy or security engineering useless or ignored by respected peers. While these few ‘black sheep’ will contribute to insecure and privacy-invasive systems, they probably do not explain the scale of privacy and security issues we witness in today’s organizations. Instead, it seems that we are dealing with a fundamental responsibility issue: perceived responsibility is the single most influential factor that explains past privacy and security engineering. Unfortunately, almost 40 percent of our sample does not feel responsible for integrating the two values into their systems, which is a dark outlook for ethical machines. The finding is in line with what Lahlou and colleagues found over a decade ago [28]. In addition, many engineers do not find pleasure in working on the two values (on average 40 percent). Thus, for a substantial amount of engineers it seems a lack of perceived responsibility and ‘lack of zest’ that leads them to neglect the two values. Lack of zest is a particular issue for academic institutions and R&D departments. Security and privacy engineering is perceived as unpleasant by almost half of the engineers working in research institutions. Only one in ten of the engineers working in industry feel this way when it comes to security engineering, whereas one in three industry engineers share a lack of zest when working on privacy. Looking into correlations between attitudes and beliefs, we find that it is particularly the political belief to create a power balance between corporates and citizens that drives positive privacy as well as security attitudes; a finding mirrored in other studies [47, 63]. But also the belief that transparency is more important than privacy negatively correlates with privacy and security efforts. These correlations suggest that there are some drivers and impediments at work here at the individual level, which can hardly be influenced by a single organization and which might play out in many ethical machines. It seems that the political environment in terms of governmental and corporate trust as well as tech-cultural beliefs underlie vital engineering attitudes across technologies.

That said, some of our findings point to the role organizations have to play in ensuring more value-based and ethical machine designs. First of all, we observe that 38 percent of the organizations in our sample have weak norms for privacy and 31 percent weak norms for security. Some even explicitly instruct their employees to ignore privacy (11 percent) and/or security design (8 percent). This is the case for all organizational types we investigated. Such weak norms cannot be due to a lack of legal requirements for privacy or security or a lack of available technical strategies. Instead, we believe that they are due to the time cost associated with security and privacy design, as well as organizational conflict caused by today’s personal data markets, which promise that personal data is “the oil of the digital economy” [81]. As far as time investment is concerned, 45 percent (N = 56) of engineers stated that it is the time required to incorporate privacy design that makes it difficult or even very difficult for them to take care of the value. For security, this goes up to 50 percent (N = 62) of engineers. Conflicts over time have been reported by other scholars as well [25, 82], as is the case with conflicts resulting from revenue models in the app space, which depend on data collection and sharing [30]. Almost two thirds of engineers in our sample (64 percent) believe that personal information has become just another form of property that people can buy and sell. Organizations have the power to
change such perceptions. They can strengthen and sharpen their organizational norms around privacy and security, including transparency on their aspirations in personal data markets. They can also reserve more time for value-based engineering and invest in privacy and security training (see Table 3).

That organizations should act in this way is underlined by another one of our findings: We observe that secure system design suffers significantly from the interplay between weak organizational norms (normative beliefs), low engineering control (time, autonomy, knowledge) and limited perceived responsibility. Even if 60 percent of our engineers, who work for organizations with weak norms, are not motivated to comply with these weak organizational norms they face, they still remain passive and rarely engage in security engineering. If they do engage in security engineering — which happens rather rarely — they seem to be driven mainly by two particular character traits, namely, when they have high locus of control \( (r = .37, p < .05, N = 37) \) and when they are not motivated by the fear of failure \( (r = - .40, p < .05, N = 38) \).

The dynamics are slightly different for privacy engineering. Here 43 percent of the engineers who face weak organizational norms dare to sometimes ignore these. This non-compliance for the good or "activist engineering" is much higher than what Szekely [63] observed in 2011.

Finally, there are few personality variables that organizations might want to test for when recruiting engineers, which independently correlate to privacy and security engineering. The most important one is the engineer’s locus of control. Both privacy and security practices are positively influenced by the degree of engineers’ internal locus of control. This character trait may well be relevant for ethical engineering in general. Large scale reviews in ethical decision-making in organizations suggest it is [39]. Finally, we find that engineers with lower fear of failure, higher emotional stability and those who are religious are more likely to engage in the kind of ethical engineering we studied here.

A. Limitations and Future Outlook

Before closing we want to recognize some limitations of our study. Firstly, the cross-sectional design does not allow for causal interpretations, even though the TPB posits them. Secondly, a segment of our sample are engineers that work in research institutions rather than industry-based product manufacturing. We would argue that universities as well as corporate research departments are at the outset of the software supply-chain, determining major technical drivers of privacy and security design. Thirdly, we are aware that many scholars judge the use of single-item measures as unacceptable. However, recent studies have shown that single-item measures have the same predictive validity as multiple-item measures and contribute less to the common method bias [83, 84]. This is particularly true when it comes to very mature scales, such as those we used here for the TPB.

What we did not cover here, but find extremely important for future studies on engineers’ value engineering, is the role which SDKs (System Development Kits) and APIs (Application Programming Interfaces) play in engineers’ ability to truly control their work. A fascinating 2017 study by Greene and Shilton shows how engineers complain in developer forums about privacy design limitations already embedded in the APIs and SDKs for Android and iOS. Their findings point to limited development control at the technical level in highly monopolized technical platform environments [47]. If we want to do practically relevant IS research on engineering behavior, we may need to add such a technical-level view to empirical studies that complement drivers and impediments at the individual and organizational level.

Furthermore, as perceived responsibility has turned out to be such an important predictor for both values, it would be important to understand it better. We only captured the construct with one item, which is a clear limitation of our research. Is perceived responsibility for value engineering a result of an engineer’s cognitive moral development? Or, can it be learned through education or fostered through a certain organizational climate? Our study shows that some personality traits, such as locus of control, hope of affiliation and hope of success are positively related to responsibility, whereas agreeableness, fear of failure and religiousness are negatively related to it. Further research may want to investigate this further.

VI. CONCLUSION

We investigated 124 engineers in a detailed study to understand drivers and impediments of privacy and security engineering—two core components of machine ethics. We find that the Theory of Planned Behavior does not allow us to fully understand the reasons for low privacy and security engagement in today’s organizations. Instead, it seems to be engineers’ individually perceived responsibility that determines most of their engagement with ethics and the two values we investigated here, privacy and security. Perceived responsibility is not always a given. Too many engineers—that is, 40 percent of our sample — show limited responsibility for the two values, even though one would think them to be closest to the design of a system. As it turns out, organizations give engineers too little time and autonomy to dedicate themselves to these matters and many fail to provide their engineering staff with appropriate norms to follow.
FIGURES AND TABLES

A. Figures

**Fig. 1.** Research Model and Hypotheses

(a) Privacy Engineering

(b) Security Engineering

Fig. 2a-b. Normative beliefs (organizational norms) and motivation to comply with these norms as direct predictors of
(a) privacy and (b) security engineering

(a) Privacy Engineering/Low Responsibility

(b) Privacy Engineering/High Responsibility
Fig. 3a-b. Normative beliefs (organizational norms) and the perceived behavioral control as direct predictors of privacy engineering by engineers (a) with low responsibility and (b) high responsibility.

(c) Security Engineering/Low Responsibility

(d) Security Engineering/High Responsibility

Fig. 3c-d. Normative beliefs (organizational norms) and the perceived behavioral control as direct predictors of security engineering by engineers (a) with low responsibility and (b) high responsibility.
### TABLE I

**PREDICTORS FOR PRIVACY AND SECURITY ENGINEERING (BASED ON TPB)**

<table>
<thead>
<tr>
<th>Dependent variable</th>
<th>Privacy engineering in the past 4-5 years</th>
<th>Security engineering in the past 4-5 years</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Predictor variables</strong></td>
<td>B SE ß</td>
<td>B SE ß</td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
<td>B SE ß</td>
<td>B SE ß</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>B SE ß</td>
<td>B SE ß</td>
</tr>
<tr>
<td><strong>Constant</strong></td>
<td>-1.56 0.72</td>
<td>-2.05 0.68</td>
</tr>
<tr>
<td>Instrumental attitudes</td>
<td>0.66 0.16 0.38***</td>
<td>0.59 0.15 0.33***</td>
</tr>
<tr>
<td>Experiential attitudes</td>
<td>0.18 0.13 0.12</td>
<td>0.18 0.13 0.11</td>
</tr>
<tr>
<td>Subjective norm</td>
<td>0.10 0.08</td>
<td>0.03 0.10 0.02</td>
</tr>
<tr>
<td>Perceived behavioral control</td>
<td>0.23 0.10 0.19*</td>
<td>0.09 0.10 0.07</td>
</tr>
<tr>
<td>Responsibility</td>
<td>0.45 0.10</td>
<td>0.35***</td>
</tr>
</tbody>
</table>

R² change: .28***

Adjusted R²: .26***

---

**Notes.** B=estimated coefficient; SE = standard error; ß = standardized coefficient. Significance *p<.05; **p<.01. ***p<.001. N=121

### TABLE II

**MEANS, STANDARD DEVIATIONS AND BINOMINAL CORRELATIONS BETWEEN POLITICAL AND TECHNICAL BELIEFS ABOUT PRIVACY AND SECURITY AND ATTITUDES TOWARDS PRIVACY AND SECURITY ENGINEERING**

<table>
<thead>
<tr>
<th>Political (PB) and Technical Beliefs (TB) about Privacy and Security</th>
<th>M</th>
<th>SD</th>
<th>Privacy</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Instrumental attitudes</td>
<td>Experiential attitudes</td>
</tr>
<tr>
<td>1. PB: Designing user-privacy systems into systems is important to enable a power balance between CORPORATIONS and citizens</td>
<td>4.12</td>
<td>0.98</td>
<td>.28***</td>
<td>.22*</td>
</tr>
<tr>
<td>2. PB: Designing user-privacy into systems is important to enable a power balance between GOVERNMENTS and citizens</td>
<td>3.94</td>
<td>1.02</td>
<td>0.16</td>
<td>0.05</td>
</tr>
<tr>
<td>3. PB: I think that more data means more knowledge</td>
<td>3.60</td>
<td>1.10</td>
<td>0.06</td>
<td>0.02</td>
</tr>
<tr>
<td>4. PB: I think that personal information has become just another form of property that people can sell or buy</td>
<td>3.41</td>
<td>1.33</td>
<td>0.03</td>
<td>0.00</td>
</tr>
<tr>
<td>5. PB: I think that freedom of speech is more important than privacy</td>
<td>3.09</td>
<td>1.07</td>
<td>-0.22</td>
<td>-0.15</td>
</tr>
<tr>
<td>6. PB: I think that transparency is more important than privacy</td>
<td>3.00</td>
<td>1.11</td>
<td>-.36*</td>
<td>-.41**</td>
</tr>
<tr>
<td>7. TB: Ensuring user-privacy in a system is a legal issue rather than a technical one</td>
<td>2.95</td>
<td>1.27</td>
<td>-0.12</td>
<td>0.07</td>
</tr>
<tr>
<td>8. TB: I think that technology is neutral</td>
<td>2.88</td>
<td>1.43</td>
<td>-0.05</td>
<td>-0.08</td>
</tr>
<tr>
<td>9. TB: Efforts to fully secure a system are often futile, because good hackers can circumvent any security.</td>
<td>2.81</td>
<td>1.31</td>
<td>-0.10</td>
<td>-0.04</td>
</tr>
<tr>
<td>10. TB: I think that with the right cryptographic mechanisms most privacy problems can be solved</td>
<td>2.44</td>
<td>1.24</td>
<td>-0.01</td>
<td>-0.07</td>
</tr>
</tbody>
</table>
11. TB: As Ubiquitous Computing systems inherently rely on the collection of large amounts of data, privacy and UbiComp is a contradiction.

12. TB: I think that it is possible, in principle, to build error-free systems.

Notes. The beliefs are ordered by average agreement, i.e., disagreement; Beliefs in bold are significant predictors of attitudes towards privacy and/or security engineering; M = mean SD = standard deviation. Significance *p < .05; **p < .01; ***p < .001; PB = political belief, TB = technical belief.

### TABLE III
PERCEIVED BEHAVIORAL CONTROL AND PRIVACY AND SECURITY ENGINEERING PREDICTED BY CONTROL BELIEFS ABOUT KNOWLEDGE, TIME AND AUTONOMY

<table>
<thead>
<tr>
<th>Dependent variable</th>
<th>Perceived behavioral control</th>
<th>Engineering behavior in the past 4-5 years</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Privacy</td>
<td>Security</td>
</tr>
<tr>
<td>Predictor variable</td>
<td>B    SE   β   B    SE   β   B    SE   β   B    SE   β</td>
<td></td>
</tr>
<tr>
<td>Constant</td>
<td>1.86 0.29 2.50 0.28 0.29 0.42 1.82 0.44</td>
<td></td>
</tr>
<tr>
<td>Perceived behavioral control</td>
<td>/     /    /     /    0.07 0.11 0.06 0.12 0.12 0.12</td>
<td></td>
</tr>
<tr>
<td>Knowledge</td>
<td>0.26 0.10 0.25 0.07 0.10 0.07 0.67 0.13 0.51*** 0.30 0.14 0.24*</td>
<td></td>
</tr>
<tr>
<td>Time</td>
<td>-0.25 0.09 -0.25** -0.20 0.10 -0.22* 0.08 0.12 0.07 0.15 0.13 0.13</td>
<td></td>
</tr>
<tr>
<td>Autonomy</td>
<td>0.48 0.07 0.54*** 0.42 0.07 0.53*** 0.07 0.11 0.06 -0.17 0.12 -0.16</td>
<td></td>
</tr>
<tr>
<td>Adjusted R²</td>
<td>.35*** .25*** .34*** .11*</td>
<td></td>
</tr>
</tbody>
</table>

Notes. B = estimated coefficient; SE = standard error; β = standardized coefficient. Significance *p < .05; **p < .01. ***p < .001. N = 121. Dependent variables: left: perceived behavioral control; right: privacy and security engineering behavior in the past 4-5 years.

### TABLE IV
PROPORTION OF ENGINEERS’ WITH HIGH AND LOW PERCEIVED BEHAVIORAL CONTROL (PBC) OVER THE IMPLEMENTATION OF PRIVACY AND SECURITY DESIGN IN ORGANIZATIONS WITH WEAK AND STRONG NORMATIVE BELIEFS (ORGANIZATIONAL NORMS) FOR PRIVACY AND SECURITY ENGINEERING

<table>
<thead>
<tr>
<th>Organizations with:</th>
<th>Privacy</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Engineers with:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Low PBC</td>
<td>High PBC</td>
</tr>
<tr>
<td>Weak norms</td>
<td>N 17</td>
<td>30</td>
</tr>
<tr>
<td>Strong norms</td>
<td>% 36%</td>
<td>64%</td>
</tr>
<tr>
<td></td>
<td>N 45</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td>% 59%</td>
<td>41%</td>
</tr>
<tr>
<td></td>
<td>N 62</td>
<td>61</td>
</tr>
<tr>
<td></td>
<td>% 50%</td>
<td>50%</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>% 50%</td>
<td>50%</td>
</tr>
</tbody>
</table>

### TABLE V
ADJUSTED MODELS FOR PRIVACY AND SECURITY ENGINEERING

<table>
<thead>
<tr>
<th>Dependent variable</th>
<th>Privacy engineering in the past 4-5 years</th>
<th>Security engineering in the past 4-5 years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Predictor variables</td>
<td>B    SE   β   B    SE   β   B    SE   β   B    SE   β</td>
<td></td>
</tr>
<tr>
<td>Constant</td>
<td>-2,100,69 -2,100,69 -1,66 -1,74 -.68 -2,84 1,34</td>
<td></td>
</tr>
<tr>
<td>Instrumental attitudes</td>
<td>0,56 0,15 0,32*** 0,49 0,15 0,28** 0,32 0,14 0,19* 0,30 0,13 0,18*</td>
<td></td>
</tr>
<tr>
<td>Experiential attitudes</td>
<td>0,23 0,12 0,15 0,25 0,12 0,16 0,28 0,12 0,18* 0,24 0,12 0,16*</td>
<td></td>
</tr>
<tr>
<td>Subjective norm</td>
<td>-0,020,10 -0,020,10 -0,10 -0,03 -0,16 0,12 -0,12 -0,13 0,12 -0,10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>B</td>
<td>SE</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>Normative belief (organizational norm)</td>
<td>0.25 0.11 0.20*</td>
<td>0.25 0.33 0.20 0.28 0.13 0.23* 0.31 0.31 0.25</td>
</tr>
<tr>
<td>Motivation to comply</td>
<td>0.170 0.11 0.13</td>
<td>-0.84 0.35 -0.64* 0.11 0.11 0.09 -0.02 0.34 -0.01</td>
</tr>
<tr>
<td>Perceived behavioral control</td>
<td>0.10 0.10 0.08</td>
<td>0.27 0.16 0.22 -0.04 0.10 -0.03 0.25 0.14 0.19</td>
</tr>
<tr>
<td>Responsibility</td>
<td>0.40 0.10 0.31***</td>
<td>0.54 0.13 0.42*** 0.50 0.09 0.43* 0.70 0.11 0.60***</td>
</tr>
<tr>
<td>Normative belief × motivation to comply</td>
<td>0.01 0.01 -0.30†</td>
<td>-0.02 0.01 0.40**</td>
</tr>
<tr>
<td>Normative belief × perceived behavioral control × responsibility</td>
<td>0.00 0.00 0.00</td>
<td></td>
</tr>
</tbody>
</table>

R² change | 0.42*** | 0.04* 0.44*** 0.04*** |
Adjusted R² | 0.38*** | 0.42*** 0.40*** 0.43*** |

Notes: B=estimated coefficient; SE = standard error; ß = standardized coefficient. Significance *p<.05; **p<.01. ***p<.001; N=121

REFERENCES


Sarah Spiekermann (M’16) received the masters’ degree in economics from the European Business School ESCP-EAP (Paris- Berlin - Oxford) in 1997 and completed the Ph.D. in business informatics at the Humboldt University Berlin, Germany in 2001.

She chairs the Institute for Management Information Systems at Vienna University of Economics and Business (WU), Vienna, Austria. Before being tenured in Vienna in 2009, she was Assistant Professor at the Institute of Information Systems at Humboldt University Berlin (Germany), where she headed the Berlin Research Centre on Internet Economics (2003-2009). She was Adjunct Visiting Research Professor with the Heinz College of Public Policy and Management at Carnegie Mellon University (Pittsburgh, USA) (2006-2009). Her main research interest is electronic privacy, disclosure behavior and ethical system design.

Prof. Dr. Spiekermann is author of the textbook Ethical IT Innovation: A Value-based System Design Approach (Taylor & Francis, 2016) and co-chair of IEEE’s first standardization effort on ethical engineering (IEEE P7000). She has published in leading IS and CS Journals including the Journal of Information Technology, IEEE Transactions on Software Engineering, Communications of the ACM, the European Journal of IS (where she served as editor until 2013).

Jana Korunovska received the masters’ degree in psychology from the University of Vienna, Austria, in 2014 (main subject work and organizational psychology, minor subject research methods and evaluation). She is currently pursuing the Ph.D. degree in socio-economics at the Institute for Management Information Systems at Vienna University of Economics and Business (WU), Vienna, Austria.

Since 2015 she is a Research and Teaching Associate at the Institute for Management Information Systems at Vienna University of Economics and Business (WU), Vienna, Austria where she was a Research Assistant since 2011. Her research on privacy and personal data has been published at the Journal of Information Technology and presented at the ICIS and ECIS conferences.

Ms. Korunovska, together with Prof. Dr. Sarah Spiekermann and Dr. Christine Bauer won the CPDP 2013 Multidisciplinary Privacy Research Award (Computers, Privacy & Data Protection CPDP 2013).

Marc Langheinrich (M’10) ) received the masters’ degree (Diplom) in computer science from the University of Bielefeld, Germany, in 1997, and his PhD (Dr. sc.) from the ETH Zürich, Switzerland, in 2005.

He is a Full Professor for Computer Science at the Università della Svizzera italiana (USI) in Lugano, Switzerland, where he heads the Research Group for Ubiquitous Computing since September 2008. His main research interest lies at the intersection of privacy and ubiquitous computing. He has authored over 100 journal, magazine, and conference publications, and has been Program Chair or General Chair of most major conferences in the field of pervasive and ubiquitous computing, such as Pervasive, PerCom, and UbiComp.

Prof. Dr. Langheinrich is member of ACM and IEEE and serves on the steering committees of The Joint Conference on Ubiquitous and Pervasive Computing (UbiComp), the International Symposium on Pervasive Displays (PerDis), and the International Conference on the Internet of Things (IoT-Conference). He received the very first 10-year impact award from ACM UbiComp in 2011. As of 2018, he is the Editor-in-Chief of IEEE Pervasive Computing Magazine.