Privacy Champions in Software Teams: Understanding Their Motivations, Strategies, and Challenges

Mohammad Tahaei
mohammad.tahaei@ed.ac.uk
School of Informatics
University of Edinburgh

Alisa Frik
afrik@icsi.berkeley.edu
ICSI
University of California, Berkeley

Kami Vaniea
kami.vaniea@ed.ac.uk
School of Informatics
University of Edinburgh

ABSTRACT

Software development teams are responsible for making and implementing software design decisions that directly impact end-user privacy, a challenging task to do well. Privacy Champions—people who strongly care about advocating privacy—play a useful role in supporting privacy-respecting development cultures. To understand their motivations, challenges, and strategies for protecting end-user privacy, we conducted 12 interviews with Privacy Champions in software development teams. We find that common barriers to implementing privacy in software design include: negative privacy culture, internal prioritisation tensions, limited tool support, unclear evaluation metrics, and technical complexity. To promote privacy, Privacy Champions regularly use informal discussions, management support, communication among stakeholders, and documentation and guidelines. They perceive code reviews and practical training as more instructive than general privacy awareness and on-boarding training. Our study is a first step towards understanding how Privacy Champions work to improve their organisation's privacy approaches and improve the privacy of end-user products.

CCS CONCEPTS

• **Human-centered computing** → *Empirical studies in collaborative and social computing*; • **Security and privacy** → **Usability in security and privacy**; • **Social and professional topics** → *Software management*.

KEYWORDS

software development, privacy champions, user privacy

ACM Reference Format:
Mohammad Tahaei, Alisa Frik, and Kami Vaniea. 2021. Privacy Champions in Software Teams: Understanding Their Motivations, Strategies, and Challenges. In *CHI Conference on Human Factors in Computing Systems (CHI '21), May 8–13, 2021, Yokohama, Japan.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3411764.3445768

CHI '21, May 8–13, 2021, Yokohama, Japan

ACM ISBN 978-1-4503-8096-6/21/05…$15.00
https://doi.org/10.1145/3411764.3445768

1 INTRODUCTION

With the rise of technologies that collect data about every moment of peoples' lives, user data has become the economy's new oil [58] making it valuable for businesses but potentially privacy-harmful for consumers. Regulations, consumer education, and privacy-preserving technologies are often seen as the main strategies for addressing online privacy issues. However, regulations are by nature less agile than businesses, especially in a highly innovative field like technology. Regional differences in laws also make it hard to reconcile the privacy protection questions that spill across the borders of a single state or country. The effectiveness of consumer education is limited by users' bounded rationality and other human factors, such as memory, attention, and beliefs [1]. The lack of transparency about data flows in user interfaces further diminishes users' ability to make informed privacy choices [22, 28]. Oftentimes the only choice available to the users is to avoid or limit using the technologies altogether, as many systems do not offer usable and effective privacy-preserving options, resulting in "learned helplessness" among the users [23, 26]. Therefore, privacy-preserving technologies and product features are one of the most immediate and effective solutions for supporting consumer online privacy.

Software developers play a central role in the data economy. Software development teams can decide which libraries, tools, and platforms to use, what data to collect, and how to present information to users, which means that their choices directly impact user privacy [40]. Prior work has suggested that the success of implementing privacy engineering in organisations predominantly depends on the organisational culture around user privacy in software development and product design teams [4, 29, 76]. Therefore, it is important to promote privacy-preserving principles, such as "Privacy by Design" [15], which aim at including privacy considerations into design and development processes from the early stages [37]. Yet, shifting organisational culture is not a trivial task. While organisations increasingly recognise *security* values and try to improve security posture [18, 71], there are still few examples and little guidance on how to build *privacy* culture in the organisations. However, lessons from prior successes of building organisational culture around security might be useful.

One promising approach for inducing organisational change is to promote ideas through enthusiastic early adopters willing to put ideas into practice. Such enthusiasts who have a special interest, and often expertise, in a subject are called innovation "champions" (or "advocates"). They encourage others and aid with overcoming barriers that a new idea could face [56]. This approach has been explored in software teams with Security Champions [33, 68, 72]. Security Champions play an intermediary role to facilitate conversations between security and development teams [70].

Our study leverages the literature on Innovation Champions and Security Champions, to study the role and experiences of *Privacy Champions* in software teams. We believe that we can learn from these people about effective and ineffective strategies and communication channels they use to promote privacy values on the ground. This information and empirical evidence contributes to understanding best practices and forming recommendations for promoting privacy values in software teams and product design.

We conducted 12 semi-structured interviews with Privacy Champions who are part of software teams to understand their motivations, challenges, strategies, and communication channels for promoting user privacy within their teams and organisations. Our results suggest that negative privacy culture and attitudes, tensions between privacy and business priorities, lack of standardisation, evaluation metrics and automated privacy tools, and technical complexity are common barriers for implementing privacy in software design. Most Privacy Champions agree that regular privacy-focused meetings, informal discussions, management support, facilitation of communication among stakeholders (e.g. between legal and product teams), appropriate privacy documentation and guidelines are particularly useful in promoting user privacy, while shaming or punishing the developers for not implementing privacy features are ineffective. Privacy Champions' experience demonstrates that incorporating privacy considerations into design reviews has a bigger impact on the end-user privacy in the final decisions and products and yields better educational effects on developers, than company-wide awareness programs or on-boarding privacy training for new hires. We conclude that similar to Security Champions' programs aimed at facilitating security practices [33, 68, 72], Privacy Champions' efforts, when supported by management and a critical mass of other developers, can be effective in promoting organisational privacy culture, and implementing Privacy by Design principles.

2 RELATED WORK

Privacy regulations, such as the General Data Protection Regulation (GDPR) [51] in the EU and California Consumer Privacy Act (CCPA) [48] in the US, have forced companies to modify their services and products to comply with them [6, 17, 24, 44]. Those privacy regulations introduce such concepts as the "right to be forgotten," the "right to data portability," and the "right to restriction of processing," with the implementation of them left to developers. Such frameworks as "Privacy by Design" [15] are intended to bridge regulations with technical implementations. Yet, there are still gaps in developers' understanding of privacy and privacy frameworks [29, 76]. For example, developers' opinions about privacy are limited by security vocabulary and compliance requirements, and privacy is rarely considered in the design process [76]. In addition to regulations, developers are also having to contend with requirements set by software platforms like the Android App store, these platforms require even independent developers to engage in privacy-related activities like writing privacy policies, declaring permission usage, and getting consent from users [69].

Security Champions. One way to support company innovations in general, and privacy innovations specifically, is to have a "champion" who advocates for these innovations and is willing to promote it actively [56]. "Where radical innovation is concerned, the emergence of a champion is required . . . the new idea either finds a champion or dies" [59, p. 8]. Prior research acknowledges the role of champions in software teams for promoting the use of software technologies such as Java generics [52, 53], usability [46], and security practices [31–33].

Security Champions in development teams have an interest in security but they are not necessarily security experts or have a formal Security Champion title [33, 57, 68, 70, 72, 79]. They can positively influence the security practices of others [19–21] often with a bottom-up approach instead of a top-down approach [8, 19, 55]. Such behaviours and attitudes are valuable in organisations that prioritise security [35]. Peer developers view Security Champions as essential players in software security [70, 77, 78]. They can be an experienced hacker who helps testers in finding vulnerabilities [74], an intermediary between the security and development teams [25, 70], or the leader in threat modelling activities [10, 63]. They are involved in several security-related activities such as educating other developers [31, 33, 34, 38, 73], increasing awareness [19, 33, 34], and promoting the adoption of technologies [31, 32, 34].

Security Champions' motivations are primarily internal (e.g., sense of duty and evidence of impact), but also external (rewards and punishments) [27, 34]. Broadly, Security Champions are hierarchists who follows the security policies [8, 9], have personality traits such as good imagination, altruism, morality and openness to experience [27] with good communication and soft skills [31], understand the balance between security and business processes [9], and have a thorough understanding of risks associated with actions and outcomes [9].

Our study builds on the importance of having a champion for new ideas and innovations in companies to make them successful. We explore how *Privacy Champions* in software teams promote privacy, what motivates them, what strategies they use, and what feedback they receive while playing this role.

3 METHOD

We conducted 12 semi-structured interviews with members of software development teams who actively promote user privacy in their teams and organisations, who we refer to as "Privacy Champions." Our interview script was designed to address the following research questions: (1) what Privacy Champions find motivating, rewarding, challenging, and frustrating in promoting user privacy in their organisations, (2) what strategies and channels do they find least and most effective in achieving their goals, and (3) what resources do they use to keep up with the latest in privacy. The study received approvals from the ethics boards of the authors' respective institutions. All participants provided informed consent to participate in the study and be audio recorded.

3.1 Recruitment

Prior research identified innovation and Security Champions using such methods as screening surveys [56], and nomination by peers [36], executives [41], and self-nomination [33, 34]. We believe that the role of successful Privacy Champions need to be recognised by their community, not only by themselves. Hence, we used the referral and snowballing techniques for recruiting participants. In

our recruitment messages, we asked the recipients to nominate someone in their organisation or network, who can be described in at least one of the following ways: (1) they formally or informally promote best practices for users' privacy, educate others, persuade, and advocate for privacy adoption throughout the software development process, and (2) they have an official or unofficial role within their team acting as the "voice" of users' privacy for the product or team, for example by giving privacy-related advice that can influence decisions and privacy practices.

We posted the recruitment messages on Twitter, and in security, privacy, and software development-related LinkedIn, Reddit, and Slack groups, mailing lists, and public fora. We also sent direct messages to LinkedIn users with privacy and security-related titles, and reached out to the employees of software companies in our personal networks. The interviewer did not personally know any of the participants, and the resulting sample is diverse in terms of participants' characteristics and background.

We included in the message a link to a short screening survey and our contact details for questions. Based on the screening survey results, we sent the eligible candidates a link to the interview booking system, where they could select the date and time for a 30-60 minute interview. We thanked survey respondents who did not meet our selection criteria for their interest in our research and asked them, and selected interview respondents, to share information about our study with other potential candidates.

3.2 Procedures

Screening survey. After reading the consent form and providing consent to participate, respondents answered questions about demographics, employment status, job title and role, industry sector they work in, and language proficiency (see Appendix A). We excluded participants who were students or were not working in software teams, and invited the eligible participants for an interview.

Interview. Before starting the interview, we first read aloud the consent form's key information, as a reminder. We started the audio recording and the interview upon receiving participants' verbal consent. Due to the similarities in research goals, our questions were partially inspired by an interview study with Security Champions [33, 34]. We asked participants about definition of privacy in their work context, motivations, frustrating and rewarding aspects, strategies and communication channels and their (in)effectiveness, feedback they receive from others, and resources to keep up with the latest in privacy (Appendix B includes the interview script). After conducting two pilot interviews with Privacy Champions from our personal networks to validate the interview script and timing (not included in our analysis), we slightly modified the script to improve clarity. All the interviews were conducted virtually using participant's preferred online calling service, audio-recorded, and transcribed by professional GDPR-compliant services.

3.3 Analysis

Two of the authors independently built initial codebooks based on two interviews, while continuing the recruitment. Then they merged the initial codebooks, discussing and resolving disagreements and differences. After applying the merged codebook to two additional interviews, they added and merged some of the codes to reach a comprehensive structure. After applying the modified (final) codebook to the rest if the available interviews, they found that all raised themes fit within the codebook structure, suggesting that saturation was reached. Thus, they stopped the recruitment, and, using the final codebook, re-coded the interviews used for the initial codebook development and validation (see Appendix C for the final codebook). All themes were mentioned by multiple participants, signalling that they are recurring. All interviews were coded by both researchers resulting in an inter-rater agreement rate of 55% (calculated as Brennen and Prediger Kappa [11]). Most disagreements were related to minor differences in coding policy (e.g., applying high-level codes to an excerpt that contains multiple lower-level codes) and due to similarities between the related groups of codes (e.g., "conversations and discussions" can be a strategy and a communication channel, but the coders might have applied just one of the two codes). The researchers together discussed, resolved disagreements, and re-coded the excerpts for the groups of codes with the Kappa below 60%. They achieved the final agreement rate of 75% (with the agreement rate on individual groups of codes between 60% and 100%), which is considered satisfactory [42, 43]. The quantified insights in the results section are based on this final analysis[1]. These numbers are reported to show the frequency of occurrences and should not be interpreted for generalisation purposes. We used MaxQDA software for qualitative analysis and calculation of the agreement rates.

3.4 Limitations

While the variety of channels we used for recruitment resulted in sufficiently diverse sample, it does not represent the software industry and cannot be generalised to all companies and software teams. Our study was limited by the availability of participants, which are hard to recruit and incentivise, given their busy schedules and high incomes, in comparison to previously-used broader populations that included people advocating to managers and end-users [33, 34]. We suspect that finding a Privacy Champion is particularly challenging because it is not a well-defined role, usually informal, and many developers blend the concepts of privacy and security [29, 54, 76]. Moreover, our study was conducted during the COVID-19 pandemic when most businesses were closed or working remotely; hence, minimising the chances of in-person networking and recruitment in workshops, meetings, and conferences.

We made a particular effort in increasing gender diversity by posting in 18 LinkedIn groups, Slack channels, and forums specifically directed at women in tech, and encouraged participation of women, and representatives of gender and ethnic minorities in other channels. Despite our efforts, the sample is still male-dominated, which is in line with Stack Overflow's 2020 Developer Survey [49].

Although prospective participants working in the big tech companies acknowledged that non-disclosure agreements prohibited them from discussing the details of their work, our research does not rely on obtaining such details, as our analysis focuses on higher-level patterns. Moreover, by nature, Privacy Champions may be privacy protective, concerned about sharing contact details, using

[1] In evaluating the inter-rater agreement, we did not consider the codes on which we did not intend to report quantified results (i.e., warm-up questions Q1 and Q2 about participants' jobs and beliefs about why they were nominated for the interview).

the interview booking system, online calling services, and limit active participation in the social media and online forums. Our transparency in the recruitment materials, consent mechanism, use of various recruitment strategies, and offering alternative choices was focused on mitigating those concerns.

4 RESULTS

In this section, we describe our participants, their conceptualisations of privacy, motivations to be Privacy Champions, challenges, and the strategies and resources that they use.

4.1 Participants

Recruitment was done during July and August 2020. We received 29 complete responses to the screening survey, which on average took 5 minutes (SD = 3 minutes) to complete, excluding one participant who completed the survey in over 24 hours. We screened out 7 respondents because they were students or were not working in software teams. We reached out to 22 eligible candidates, of which 14 participants signed up for an interview, one later cancelled, and one did not show up and did not reschedule. In total, we conducted 12 interviews, which on average took 36 minutes each (SD = 10 minutes). Participants received a 20 USD (or equivalent in their local currency) gift card for their time.

While participants hold different job titles, they all work full-time in software teams and interact with other developers, and are proficient or fluent in English. They are employed in the business sector except for one from the non-profit sector. Six are employed in North America, five in Europe, and one in Asia. On average, they have 10 years of experience (SD = 6 years), and work in a team size of 10 (SD = 13 members). Nine participants identify as male, two as female, and one preferred not to identify their gender. The average age is 33 years old (SD = 7 years). Eight participants hold an official title or a role related to privacy or security, and one (P8) holds an informal Security Champion role. P11 previously worked as a privacy architect working with developers, and most of our conversation with him was about his previous role. Table 1 shows a summary of participants' demographics.

During the recruitment we received a number of interesting informal comments from the people who saw the recruitment message. First, they acknowledged that it would be easier for them to nominate a Security Champion than a Privacy Champion, suggesting that the latter role is not yet as well defined or common as the former one. Second, they often asked if a privacy officer or another privacy expert from a legal department would qualify for the study, as those are the only people who directly address privacy issues in their company, to the best of their knowledge. Moreover, the official titles of most of our participants are primarily related to security, while their actual formal responsibilities and informal activities often include privacy as well. These observations align with the insights from the interviews regarding the overlap of privacy considerations with security engineering and legal perspectives on data protection (see more details in Section 4.2).

When we asked participants why they believe their colleagues nominated them for the interview, they attributed it to either formal responsibilities (such as being a member of a special interest group focused on privacy, or being a point of contact for user data protection), or informal aspects of their advocacy (e.g., being vocal about privacy, and having a reputation of privacy enthusiast).

4.2 Privacy conceptualisations

We asked participants to define the term "privacy" as they normally use it in their work context, and describe what are the differences between security and privacy. In line with privacy literature [47, 50, 64], the majority of Privacy Champions (7/12) acknowledged that **privacy is a broad, complex, and contextual term**: "*Privacy is really hard to define, because it's so contextual*" (P9).

4.2.1 Privacy as data protection. Almost all (11/12) Privacy Champions, in the context of their work, refer to privacy as protection of personal data from unauthorised access: "*Privacy really means . . . that we're going to do our utmost not to leak their [users'] data, that we're going to protect their data and that we're going to do our best to secure it*" (P9). Among data protection techniques and approaches, participants mentioned: anonymisation (6/12), data minimisation (5/12), encryption (4/12), differential privacy (3/12), and Privacy by Design (1/12). We discuss participants' opinions about the relative effectiveness of these approaches in Section 4.5.

4.2.2 Privacy as transparency and trust. Privacy Champions (9/12) also referred to privacy as ensuring transparency about data practices and respecting users' trust, by meeting their expectations, and respecting their preferences. Less often, they referred to privacy policies as an instrument for ensuring transparency. Some even openly criticised using legal documents for communicating privacy information to the users: "*These ridiculous legal terms, terms of service pages that continue to get more lengthily and more complex and smaller font and basically aren't able to provide humans with an intuition of what's exactly happening*" (P7).

4.2.3 Privacy as data management and control. Many participants (8/12) conceptualise privacy as users' ability to manage and control their personal data, for example, through consent mechanisms:

> *Privacy . . . means that I as a user can give my consent to someone to process my data in a controlled manner . . . and if at any point I wish to be forgotten, I should have this right preserved, and that should be mandatory.* (P5)

4.2.4 Privacy as legal compliance. Some participants (7/12) mentioned legal compliance, but few rely on it as the primary working concept: "*You need to make sure that the data you store complies with regulations and the intent that the user supplies the data with*" (P2).

4.2.5 Privacy as human right and ethical value. Several participants (5/12) acknowledge a broader, non-technical, view on privacy as a fundamental human right and ethical value, enabling personal freedom: "*I think privacy is important for freedom, democracy*" (P6). While not necessarily used as a working concept in their daily job, as we discuss in Section 4.3, this conceptualisation is a common driver for Privacy Champions to advocate for privacy in their work.

4.2.6 Comparisons between privacy and security. Many participants recognised the close relationship between privacy and security, to the point where a few mixed the two terms or found the boundaries between them blended or *"blurry"* (P4). Many participants (8/12) saw the **reinforcing relationship** between these

Table 1: Summary of participants' demographics.

ID	Role	Job title	Sector	Current continent	Gender	Number of employees	Team members	Years of experience	Age
P1	Privacy and/or security eng.	Sr. Security Engineer	Business	North America	M	1,000-9,999	13	9	30–34
P2	Privacy and/or security eng.	Contractor Cryptographer	Business	Europe	M	100-999	4	8	25–29
P3	Software development	R&D Software Engineer	Business	Europe	M	+10,000	6	15	35–39
P4	Privacy and/or security eng.	Privacy Officer	Business	Asia	M	+10,000	50	2	18–24
P5	Privacy and/or security eng.	Head of R&D	Business	Europe	M	1-9	5	10	25–29
P6	Privacy and/or security eng.	Sr. Product Security Engineer	Business	North America	M	10-99	4	15	35–39
P7	Managing software develop.	Sr. Manager Research Engineer	Business	North America	NA	1,000-9,999	6	10	35–39
P8	Software development	Software Engineer	Business	Europe	F	1,000-9,999	6	2.5	25–29
P9	Privacy and/or security eng.	Research Engineer	Non-profit	North America	F	1,000-9,999	3	5	25–29
P10	Research: new features	Sr. Privacy Researcher	Business	North America	M	100-999	10	14	35–39
P11	Research: telecom security	Technical Staff	Business	Europe	M	+10,000	8	25	45–49
P12	Software development	Software Engineer	Business	North America	M	100-999	4	7	30–34

concepts, whereas security enables privacy: "*I think privacy is a subset of security*" (P10). Others (7/12) viewed **privacy as a broader concept** where "*privacy goes further than security*" (P6).

However, two participants acknowledged potential **tensions and contradictions between privacy and security**: "*Even though security and privacy often get lumped together in terms of the technical underpinnings of what is required to achieve these systems they can often be at odds in terms of how to accomplish them*" (P7).

Some participants (5/12) mentioned that **security values are more widely recognised** than privacy values, and that security is a more mature field with more defined terms, taxonomies, metrics, and established best practices, which may create a useful benchmark for privacy: "*With privacy, it feels a lot more abstract, when you're trying to argue for it*" (P2).

P1 emphasised the value of differentiating between the user-focused privacy roles (e.g., usable privacy researchers or ethics experts) and technical security roles and having "*someone whose job is explicitly to be the privacy advocate for the users, whose job is not to know what cryptography is . . . who has a little bit more of that social scientist in them*" (P1).

While the official job titles of the majority of our participants are shaped around security, their conceptualisations of privacy are not limited to security concepts, as it is typical among software developers [29]. Broad understanding of privacy reassures the Privacy Champions' potential in promoting privacy values in their organisations beyond the common security and legal frameworks.

4.2.7 Socio-cultural differences in approaches to privacy. Three Privacy Champions acknowledged **country-level differences in privacy cultures**. P12 believes that people in Europe are more concerned about privacy than people in the US and "*that privacy is much more of a first-class concern there than here*" (P12).

Moreover, P1 highlights the socio-political differences between the US and Europe, which lead to diversity in their approaches to addressing privacy issues, and recommend a more unified approach that brings together the perspectives of different stakeholders:

> *America has been very American about it and said, . . . 'Let's let the corporations solve the problem for us.' Europe is very European about it and says, . . . 'Let's have the government just solve the problem for us.' Frankly what we need is a much more multi-stakeholder conversation.* (P1)

Similarly, findings from Bamberger and Mulligan show that US privacy is based on "risk management to avoid harm to consumer expectations" and the European privacy culture is formed "as an individual human right and eschewed the language of risk and consumer" [5, p.12].

4.3 Motivations

We asked Privacy Champions about what motivates them to promote privacy, what they find rewarding in that process, and what positive feedback they receive from their colleagues. We found that participants are driven by both personal and organisational motivators. Prior work has seen similar trends that these two factors are complimentary and affect individual performance at work [3]. Motivation is important for Privacy Champions because one of their main tasks is motivating others [39, 56].

4.3.1 Personal motivations. Most participants (10/12) mentioned personal motivations for promoting privacy in the organisation, such as **strong personal privacy attitudes**, human rights and **societal benefits**, and **empathy towards users**: "*I always put myself in the other person's shoes. I would not like my data to be tampered with*" (P4). Thus, Privacy Champions (6/12) find it rewarding to see the **impact of their efforts** on end-users and society.

Interestingly, a few people admitted that **personal experience with privacy violation**, or big **media stories** (e.g., Snowden revelations) inspired them to become Privacy Champions in their organisations: "*The Snowden revelations came out and I felt extremely strongly that what he did was heroic and that I should figure out a way to support that kind of effort*" (P10).

Experiences and expertise gained during school and work projects also inspired some of our participants (3/12), and contributed to the perceived **sense of personal responsibility** (6/12) for building products and services that protect user privacy:

> *It's not like one day I woke up and said, 'I want to be a champion of privacy.' It's just that my project required me to use this data . . . I saw how important it is to keep this data safe and so I tell everyone else . . . how they should also handle this type of data.* (P3)

Finally, some Privacy Champions **enjoy solving technically challenging tasks**, and find it rewarding when they discover privacy-preserving solutions for real-world problems (3/12):

> *It can be a bit of a fight sometimes to get people to . . . go through the pain of adding this extra . . . [privacy-preserving] feature . . . but it's very satisfying to come out of this with something that is much better than the way that the average company does it.* (P6)

4.3.2 Organisational motivations. Organisational motivations (8/12) also drive Privacy Champions' work in promoting user privacy. Participants see the respect of user privacy as a **competitive advantage** or even **existential requirement** for a company that wants to have a successful software product on the market: "*If we are perceived as an organisation that doesn't care about user privacy, then that will harm us. If we are perceived as an organisation that does care, that will benefit us*" (P1). It highlights the value of privacy as a central attribute of the company brand and corporate identity. Addressing privacy issues is especially important to the success of the companies working on emerging technologies, due to potential lack of users' familiarity with and trust in such technologies and their data practices: "*We are in emerging technology . . . so there's this business understanding that we will freak people out, and we will ruin our business, if we don't respect people's privacy*" (P9).

Strong corporate privacy culture attracts people with positive privacy attitudes, and offers an opportunity to align the professional goals with personal values. "*I have developed my professional trajectory in order to create opportunities to work on things that matter . . . the promotion and development of privacy-enhancing technologies . . . is very much aligned with the goals of the organisation* " (P7).

Privacy Champions (5/12) find it encouraging and rewarding also when they notice an **improvement in company' privacy culture and values**: "*The awareness I create through this process, that's the most rewarding thing*" (P5).

Recognition by peers and managers, their requests for advice, further encourage Privacy Champions: "*The most implicit form of a reward system is from leadership, who aren't usually bothered by these small things, when they come down to your level and are like, 'We have a problem, and we need help with so-and-so problem'*" (P4).

In contrast, weak privacy culture not only inhibits their enthusiasm but may also turn Privacy Champions away from the company entirely: "*I actually left a previous job because I disagreed with the privacy aspect of the project I was asked to work on*" (P12).

Only one participant mentioned tangible incentives contributing to their motivation to promote privacy. Most of the participants are not advocating for privacy in exchange for rewards. However, while Privacy Champions find positive feedback, and recognition of the value of their work intrinsically rewarding, they also appreciate more formal rewards, such as **career promotions or additional compensation** (2/12): "*It's not part of my job, so when it comes to career advancement, getting recognition, getting compensation, there are some shortcomings*" (P12).

4.4 Challenges

We asked Privacy Champions about challenges and frustrations in promoting privacy, instances when they felt their efforts were not appreciated, and negative feedback received from colleagues.

4.4.1 Indifferent or negative attitudes. Privacy Champions perceive mixed privacy attitudes from their teams and organisation. In Section 4.3 we discussed how positive culture, attitudes, and feedback encourage Privacy Champions. Conversely, indifference, **"I've Got Nothing to Hide"** mentality [65], or even openly **negative privacy attitudes**, such as annoyance and push back **from the team members**, make it challenging for Privacy Champion (11/12) to advocate for privacy values: "*'I have nothing to hide,' people are really difficult to deal with. When you run into people with that mindset, it can be very difficult to engage with them*" (P9). The indifference and unawareness of the privacy benefits **among clients and users** circles back and also negatively affects the attitudes of engineering teams: "*When I would argue for privacy, I would get push back from people that was, 'Users don't care, nobody cares, why are you bothering me about this? I have a job to do, just let me get my job done'*" (P1).

However, some participants noted that engineers' attitudes have been shifting to the positive direction over time, thanks to the changes in social norms, emergence of privacy regulations and requirements, and efforts of the Privacy Champions, which we discuss in more details in Section 4.5:

> *Right now, privacy's become . . . the priority, before you move on to anything else. People have started to act upon it faster . . . because they understand the impact of not handling data privacy in the right way.* (P4)

4.4.2 Tensions between priorities. Engineers' push back is related to the tension between privacy features and other, technical or business, priorities (9/12), such as **primary technical features and performance**, or additional **time**, **efforts**, and **financial resources** it takes to address privacy, postponing deadlines, and increasing the costs: "*If you want to . . . have these techniques that retain privacy, usually this translates into a cost. That could be performance. That could be money. That could be user experience*" (P5).

4.4.3 Lack of standardisation and evaluation metrics. Privacy Champions agreed (8/12) that "privacy is hard to measure," for two main reasons. First, privacy lacks **standardised definitions and taxonomies**: "*There's no national law or agreement on what privacy standards should be. There are things like the NIST [National Institute of Standards and Technology] privacy framework, but there's no consensus, it's not widely known, widely shared*" (P12).

Second, there is a lack for **metrics for evaluating privacy risk, harm, and penalties for violating privacy** and **metrics for evaluating the effectiveness** of privacy protection approaches. The ambiguity of the existing frameworks leave engineering teams in uncertainty about the privacy status of their products and whether the deployed protective measures are adequate and sufficient:

> *What is, for example, the minimum anonymity set that we can have in our products? . . . Is it enough to put people in buckets of 3 people, or should we be looking at 100 people? . . . can we do it even if there's only 100 people in that particular country? Those are numbers that we've been asked to formalise . . . We haven't been able to do that yet.* (P6)

Without being able to quantify the benefits and extent of improved privacy and costs of its violation, it is hard for Privacy Champions

and engineering teams to advocate the business impact of privacy, or argue for the project timeline extension or budget increase necessary for addressing privacy concerns.

Additionally, there are practical challenges with standardisation of privacy due to high context-dependency, and heterogeneity of users' preferences and needs: "*GDPR, it was definitely trying to answer the question of what I hear is the right answer for all EU citizens, as if all EU citizens were exactly the same with the exact same desires for privacy*" (P1).

4.4.4 Technical complexity. Privacy Champions (6/12) mentioned that building privacy features is **technically difficult**: "*How can we enable applications like procreated rendering and other really important product directives . . . while still protecting privacy? That's been really difficult*" (P9). Sometimes the technical complexity relates to the **lack of knowledge** in the development team: "*Typically we can identify a risk, but the developer may not be aware of privacy preserving techniques that might be used to mitigate that risk*" (P6). However, more often it just translates into extra effort and time, creating the tensions described in Section 4.4.2.

The complexity can also arise from the fact that broad privacy-related goals and vague **guidelines are difficult to translate** into specific technical requirements and then practices, especially when they are: "*generated from the legal documents . . . They were all very, very fuzzy . . . There's very, very little of the how we should do things, how we should integrate this for the engineering processes*" (P11).

4.4.5 Communication issues between stakeholders. Ensuring privacy in a product requires involvement of various stakeholders, to consider the multitude of conflicting interests. Given that developer, manager, and lawyer stakeholders come from **different backgrounds**, are members of separate teams, and hold various places in the corporate hierarchy, the communication between them can be challenging (5/12), due to discrepancies in terminology and conceptualisations. Similar to the difficulty of translating privacy goals into technical requirements (see Section 4.4.4), the conversation between developers and legal departments demanding compliance without taking into consideration technical limitations may be frustrating for both parties: "*Having this engineering background is very, very different to how the lawyers perceive the system . . . there was no understanding of the engineering process*" (P11).

A female Privacy Champion, brought up a communication issues specifically associated with **gender biases**. She had to seek her manager's support to convey her ideas and prove herself as a female Privacy Champion and engineer to teammates: "*I can be overlooked in meetings sometimes. I think it is more because of my gender than anything else . . . I've had to Slack my opinions through my director, who has then raised them in meetings for me* " (P9). She emphasised the positive impact of gender diversity on the breadth of ideas and considerations of privacy implications: "*Sometimes men are like, 'Why would you need to protect a phone number more?' Women are like, 'Because sharing your phone number gets you harassed.' It does give you a different perspective on privacy*" (P9).

This is in line with the literature suggesting that cybersecurity needs to be more inclusive and diverse [31, 45]. These observations highlight the importance of increasing gender diversity in privacy community specifically and tech companies in general, and the importance of management support in overcoming gender bias. However, delivering all the female employees' opinions through a team manager is not the most effective way of communication, and also not the most fair to the women who do not get credit for their ideas. Therefore, it is important that management encourages women to speak up and independently express their opinions in meetings and company's communication channels. This will increase the diversity of perspectives, and breadth of ideas, eventually leading to better privacy solutions.

4.5 Strategies

Privacy Champions mentioned a variety of strategies and techniques that help promote privacy in teams and organisations; these range from formal documentation and policies, and specific libraries and tools to informal *"water-cooler conversations"* (P12).

In general, our participants emphasised the effectiveness of a "***collaborative tone***" (P7) when promoting privacy values. On the other hand, participants' opinions about the effectiveness of **enforcement of the policies** regarding privacy are mixed. For instance, some Privacy Champions think that enforcing policies signals management's serious intentions about it, and makes developers recognise the importance of addressing privacy issues and put extra effort in it: "*These kinds of decisions need to be enforced by upper management . . . Developers always go for the easy solution, and having privacy in mind when dealing with users' data, unless it's enforced, it's just extra work*" (P5). Others believe that without explanations of reasoning behind mandatory processes, those mandates do not reach the full potential and developers may treat the processes as a *"box-ticking exercise"* (P7) and hence ineffective.

4.5.1 Improving company culture. All participants (12/12) acknowledged that improving company culture regarding privacy is essential in promoting end-user privacy values in software development teams. Privacy Champions suggest to encourage regular formal and informal **discussions about privacy** to not only shape individuals' mindsets or educate about certain practices but also to build the collective organisational privacy culture: "*It's less about individual features, but more about bending the arc of the organisation over time, to value privacy more highly, by simply engaging with it publicly a lot*" (P12). Privacy Champions suggest encouraging in product teams **general empathy towards users'** needs and expectations and **sense of personal responsibility** to make them "*feel that they both can be and should be thinking about the implications for the users*" (P7) and reflect on "*What are the kinds of user harms that are occurring because we did privacy wrong in our product, and how can we design our product to be more privacy friendly*" (P1).

In those discussions, to help justify additional costs, time or work load required by privacy engineering, Privacy Champions find it especially effective to **emphasise risks and potential costs** associated with not addressing privacy issues and also pointing out the benefits and competitive advantages of privacy-friendly products: "*Acknowledge and accept that it is extra work to do things in a privacy-conscious manner but it's worthwhile work. It is to the benefit of the company, . . . of the user, . . . of the society*" (P12).

Privacy Champions also find **management support** important in promoting privacy culture, by talking about it in company wide speeches *"to inspire people"* (P1), and explaining the value of privacy:

> *The CEO, chief legal officer and head of product all stand up and say 'Look, from a product perspective . . . from a legal perspective . . . from the perspective of doing the right thing for our users, this is super important.'* (P1)

Facilitating communication between teams improves the overall culture of privacy in the company as well. Our participants recognised the benefits of forming special interest groups focused on privacy and integrating Privacy Champions into various teams, to have at least one or two privacy expert in every team and to help different stakeholders and teams understand each other's perspectives, terminology, requirements, and needs. **Integrating Privacy Champions** into engineering teams helps to make the process of addressing privacy considerations and implementing Privacy by Design principles more straightforward, fast, and less bureaucratic, reducing the tensions between privacy and time (see Section 4.4.2): "*We'll work with your design, we'll point out places where it could be tightened up and so on, and we will reduce the amount of documentary evidence required in order to pass a privacy audit*" (P11).

Communication channels. Privacy Champions use various channels for promoting privacy values and organisational culture, including verbal (10/12) and written (4/12) communications, productivity and communication platforms (4/12), and special events (3/12).

One-on-one discussions and group meetings are the main verbal channels that Privacy Champions deploy for promoting privacy. Among written materials, while Privacy Champions find guidelines and documentation generally useful (see Section 4.5.3), P8 brought up an issue with keeping them updated and navigating through them: "*Searching content on Confluence [wiki] is quite hard, and most of the documentation is quite old . . . Or there's a lot of archives documentation that when you search you can't really find it*" (P8). P1 further warns about the trade-off between the informativeness of detailed documentation and educational materials and its poor fit for lifting motivation to implement privacy in product design: "*Those detail-heavy classes and detail-heavy instruction material are very bad at inspiration but very good at education*" (P1). Personal or company blogs, and books were mentioned only by a few participants as resources that can be shared with colleagues as a point of reference.

Among productivity platforms, Slack is commonly used by Privacy Champions to answer specific questions about privacy or communicate with peers about privacy less formally: "*I keep an eye out for when people are talking about security and privacy things and will try to tactfully insert my opinions without steamrollering everything*" (P12). GitHub is used not only to discuss, but even to document identified privacy issues: "*A GitHub issue. That's where we do our security reviews. If you want to do security reviews, you raise that as a GitHub issue, and then we ask questions*" (P6).

Finally, special events like workshops, seminars, hackathons, and lightning talks provide additional opportunities to Privacy Champions to promote privacy values and share knowledge: "*That's how I share with the company what's new, and what we're doing to promote user privacy*" (P9).

4.5.2 Design and code reviews. Privacy Champions find a good opportunity to promote privacy values during **design and code review** process (10/12), prior and after development: "*Much like many companies have security reviews early in product scoping sessions, data management and privacy reviews can go a long way*" (P7). These processes help to "block off" time for privacy, and think through practical challenges and applied solutions: "*When someone has to take in some feedback and then actually think through proposed mitigation and have a discussion around how we can change that mitigation to make it more workable. They're actually deeply involved into the particular problem*" (P6).

Echoing the Privacy by Design philosophy, some participants believe that privacy reviews are **more effective when conducted before development** (at the requirements stage) than after: "*Whether or not there are more privacy-preserving ways to build that feature. Those ways never get implemented after the fact, because at that point, the feature's done and the team's moved on to something else*" (P12).

Moreover, Privacy Champions suggest that **open-ended questions** are more helpful than compliance checklists or privacy impact assessment scales in triggering a more profound discussion about the privacy implications of a software product: "*What user data goes through your service? What can you learn about the user from this? Very basic questions give a lot of the leverage*" (P1). Some participants mentioned that it's beneficial if everyone in the company, in addition to the developers and data protection experts, can engage in the reviews of requirements and specifications of the new features.

4.5.3 Documentation and guidelines. Many Privacy Champions (8/12) believe that documentation and guidelines are helpful in promoting implementing privacy in product design and software development. Our participants frequently mentioned internal documentation, organisational policies, formalised processes, and internalised risk management strategies. Less often, participants mentioned external guidelines and standards, such as: "*General guidelines, like GDPR, you can get some stuff from the ISO 27000*" (P5).

Lack of **formalised and standardised policies** may lead to product incompatibilities, inconsistencies, and engineers' frustrations about time wasted on implementing sub-optimal privacy mitigation solution. The value of formal processes is especially critical in reconciling the disagreements among experts about best practices and advice: "*We recognised the value of having the standard . . . to synchronise our thoughts on something before we provide someone with a recommendation*" (P6). Formal procedures and policies also leverage Privacy Champions' ability to advocate privacy features.

On the other hand, preparing documentation and reviews takes time and creates friction between teams: "*Nobody wants to be audited or write documentation that much if they could write code instead*" (P8). Therefore, **combining formal procedures with informal roles** of Privacy Champions or other privacy experts offers a balanced solution to promoting privacy: "*That was seen as the advantage of this role. That this dissemination of knowledge that was the goal would happen organically rather than formally*" (P2). At the end of the day, some participants believe that documentation cannot substitute human involvement and expertise in providing customised guidance and help, emphasising the benefits of moderating role of Privacy Champions or other privacy experts: "*There are tonnes of documents, but basically, they point you to the right people to talk to . . . you have to talk with someone who understands . . . your problem better*" (P3).

4.5.4 Training and mentoring. Privacy Champions (8/12) talked about the role of training and mentoring in promoting privacy values, however, their opinions about its effectiveness were nuanced. For instance, in addition to shifting attitudes and raising sensitivity to privacy issues, Privacy Champions believe that training should provide **practically useful** information on how to implement privacy principles to be a valued resource for developers: "*If I talk to someone out of blue about this . . . maybe they're not so interested, but when they actually have to use this data they are more receptive into what I have to tell them about it*" (P3). For the same reason, design and code reviews can have a better educational effect than formal training, due to their practical relevance: "*The developer education seems to be more effective once they've had a review and they see how we think about things, and they start to change*" (P6). Similarly, delivering information about organisational privacy documentation *"that includes the security and privacy checklist"* during on-boarding training for new hires may be "*the wrong time to do that*" (P6).

Moreover, training **targeted to the specific audience or topic** that is "*relevant to those people's technical jobs*" (P11) is more effective and motivating for the engineers than general privacy awareness programs: "*It was better to have a subject matter expert come in and teach people within the team or within close by teams, rather than have everyone know everything*" (P2).

On the other hand, mandatory training applied selectively to the teams can be perceived as punishment, e.g., for the mistakes they made in implementing privacy. To mitigate this, P1 recommends to change the tone of the purpose for training assignment, approach the team lead and offer a privacy session tailored specifically for the target team with the examples relevant to their product, rather than positioning it as a behaviour correction measure: "*They're likely to show up to that anyway because you made it exciting to them*" (P1). Even more generally, P1 believes that **punishing and shaming** developers for not being concerned about users' privacy **are not effective** approaches for instruction and behaviour change in the organisations; instead it may make developers defensive and secretive about privacy issues: "*They go into this, 'How do I make sure my team doesn't get in trouble with the privacy team?'*" (P1).

Additionally, **mentoring** can be effective in educating developers about privacy: "*We do have a strong internal mentorship programme both formal with expectations or pairing junior developers with more senior developers and senior managers*" (P7).

4.5.5 Tools and libraries. Privacy Champions use or build tools and libraries to assist others in developing privacy-preserving products, testing, and vulnerability discovery (7/12), in addition to using such common approaches as cryptography, k-anonymity, and differential privacy. For instance, **libraries** can offer choices that are privacy-preserving by default, and built in the best data protection practices hence, minimising the chances of making mistakes for developers:

> *Give people libraries, tools etc that are already built in a way that tries to minimise data . . . You're limiting the choices that are available, to only the choices that are deemed to provide enough privacy or enough security* (P2).

Data flow modelling and data annotation techniques further assist developers in thinking about privacy implications:

> *I have seen people look at designs for how they're planning to store data and go, 'Oh, we actually don't need all this sensitive data. Dealing with sensitive data is annoying, we can design this feature so that we use public data to solve this problem.'* (P1)

Our participants mentioned some **automated tools** that detect vulnerabilities: "*There is a lot of automated systems in the company and most of them work when you push a code to GitHub . . . It would prevent you from merging code if it said 'really high vulnerability'*" (P8). However, most of the mentioned automated tools are focused on security; indeed, P6 expressed the need *"to have more automation"* (P6) for discovering *privacy vulnerabilities* and provided an example how *"to prevent other third-parties from learning about our users, we proxy all requests to third-party services, like for example, Google Safe Browsing"* (P6).

4.5.6 External factors. External factors, outside of the company, may influence the adoption of privacy principles within the organisations (8/12). One if these factors is **political and regulatory support** (e.g., EU GDPR, CCPA, FERPA): "*Because you had that soft power and influence and buy in from people that comes from not just inside the company but from the whole society*" (P1).

Privacy champions believe that **academic work** also influences organisational privacy practices, however, academic research is not always practically applicable: "*They are the kinds of things that people publish papers about in web privacy are mostly often tales and novel and not actually useful*" (P10). Finally, **public critique** in mass media or through the open-access and public-facing documentation encourages *"transparency and accountability"* (P7).

4.5.7 Criteria for assessing the effectiveness of a strategy. We asked Privacy Champions to tell us how they know if a strategy or a communication channel is effective or ineffective. Many Privacy Champions often mentioned **practical usefulness** (8/12): "*We were able to do these [data flow modelling] and come back with very, very definite, very concrete requirements which were really appreciated by the engineering staff*" (P11); especially if the proposed privacy approach can **save developers' time**: "*Developers really want to have code in production as soon as possible, so, any kind of benefit to that is a massive win for them*" (P2); or **reduce the tension between teams**: "*We started to be more consistent about doing spec reviews and inviting people to publish their specs earlier, and we've had a lot less fights with people at the implementation level*" (P6).

Positive impact on end-users and developers' decisions and attitudes, or lack of that impact, is another factor that Privacy Champions use to estimate the effectiveness of a privacy-promoting strategy (8/12). Given the lack of standardisation and evaluation metrics, discussed in Section 4.4.3, **the ability to measure** the impact of a strategy or approach, or define the minimum requirements is especially appreciated by Privacy Champions (4/12): "*I and a couple of other people are working on some equipment privacy metric and I think that will be enormously useful in prioritising and motivating the development of certain features*" (P10).

Finally, **relevance** of a strategy or information, e.g., training content (see Section 4.5.4), to a particular audience is another criteria Privacy Champions (3/12) suggest considering when defining

its effectiveness. For example, broadcasting messages or company-wide training may not be as effective as information targeted to a certain audience "*because people tend to read it and then quickly forget about it*" (P6).

4.6 Information resources

We asked Privacy Champions how they keep up with the latest in privacy. **Online resources**, including articles on the Internet, general media, news, and blogs are the most common online resource about privacy among our participants (9/12): "*Knowing what they're saying about privacy on NBC and CNN and Fox News and the New York Times can really give me a sense of what the general population is seeing*" (P1). Online social networks, such as Twitter and LinkedIn groups, Reddit, other fora, and newsletters are also popular sources of information. Half of our participants (6/12), in positions related and not related to research, read **academic papers** and attend conferences to keep up with the latest in privacy. Privacy Champions also learn about latest achievements, best practices, and mistakes in privacy domain from the **experiences of other companies** (4/12). Some even have "*shared channels with other companies*" (P6) to exchange information.

In-person communications with peers, attending industry events, workshops, and working groups help Privacy Champions (3/12) stay tuned as well: "*A series of workshops, I went to one where they were gathering feedback on their privacy framework, and learned a ton there, and also got to contribute to that conversation*" (P12). **Internal organisational channels**, such as Slack, are common and useful resources for both finding and promoting information about privacy (2/12): "*We have a Slack channel, where everybody shares articles that they've encountered*" (P6).

5 DISCUSSION

Privacy engineering is a challenging task for developers [29, 60, 66, 69]. Our interviews demonstrate that, similarly to Innovation Champions in other domains, including cybersecurity [31, 33, 34], Privacy Champions are promising facilitators of the privacy transition in software teams. However, they need support from organisations and peers to succeed in their efforts.

5.1 How to motivate Privacy Champions?

Given the promising role of Privacy Champions, the logical question arises: how to find, retain, and support motivation of Privacy Champions? We found that self-motivated Privacy Champions seek employment in companies with strong privacy culture and like-minded colleagues, and avoid companies with weak privacy values (see Section 4.3.2). This finding suggests that Privacy Champions may be especially concentrated in a handful of privacy-focused companies and be rather rare or muted in other companies. Therefore, **putting privacy values at the forefront of the company's mission** would not only strengthen the competitive advantage at the user market, but also help attract and retain Privacy Champions.

Privacy Champions are motivated by personal and organisational values, similar to other champions of innovation [39, 56]. Like security advocates [9], Privacy Champions' attitudes often form from personal experience with privacy risks. In contrast to the security domain [34], privacy has a strong connection to social norms and ethical values; Privacy Champions see privacy as a fundamental human right and feel personal responsibility to protect it and satisfaction from creating benefits for society. This passion explains why many of our participants continue being the voices of privacy despite their efforts not being officially recognised or compensated. Therefore, the recruitment efforts (within or outside of the organisation) directed at Privacy Champions need to **emphasise their positive impact on users and society**, possibly with the supporting examples from media, creating a sense of purpose and mission, which has been proved as effective driver in psychology and management [13, 14, 80].

Privacy Champions, like other engineers [30], enjoy solving challenging tasks and appreciate the recognition of their efforts (see Section 4.3.1). Thus, organisations and peers should stimulate their curiosity, encourage them to use their unique expertise to find privacy-preserving solutions for technical issues, provide **intellectual freedom and resources** for exploring new approaches and ideas [7], and **acknowledge their efforts** not only via explicit positive feedback, but also via career promotions and fair compensation for the additional (often voluntary) work they do.

5.2 Support the motivations

Privacy Champions often face developers' low motivation to address privacy issues in software design due to indifference and negative privacy attitudes (see Section 4.4.1). Similarly, Security Champions often have to overcome apathy towards security by making it tangible and relatable using stories and analogies to help team members understand [33]. While security has objective tangible benefits, the value of privacy is hard to measure thus it is more subject to diverse personal attitudes (see Section 4.4.3).

To address such negative privacy attitudes among members of software development and product design teams, it is important to **improve organisational privacy culture**. To achieve that, Privacy Champions in our study recommend encouraging **formal and informal discussions** about privacy implications for end-users. The discussions about privacy can take a variety of forms, from seminars and lightning talks, specialised channels (e.g. Slack groups or message threads) dedicated to discussing privacy questions and exchanging resources on the topic, to motivational speeches during all-hands company meetings, where **management can show their support and recognition** of the importance of privacy values and leverage "social influences" [12].

The technical complexity associated with designing and implementing privacy-preserving solutions (Section 4.4.4), can be leveraged to increase the motivation of engineers, who find solving difficult challenges rewarding (see Section 4.3.1). Companies could **emphasise the prestige of privacy engineering work** due to the level of expertise is requires, and **praise developers** and provide them with **tangible rewards**, e.g. career promotions or additional compensation, for improving privacy in their products.

Moreover, it is important to **improve communication between teams**, aligning priorities of different stakeholders, and **increase diversity** in the teams to invite the variety of opinions to the table. Similarly to Security Champions [68], Privacy Champions can leverage their multidisciplinary knowledge and skills to facilitate

the communications between legal and development teams. Participants acknowledged the value of special interest groups that focus on privacy and are comprised of members of different teams to facilitate the transfer of knowledge between teams and ensure that each team has an expert they can consult about privacy matters. In contrast to findings about Security Champions [34], Privacy Champions in our interviews did not find it useful to punish or shame developers for not addressing privacy concerns (see Section 4.3), and recommend employing a rather **collaborative approach**.

External influence, e.g. **media stories, public critique and privacy regulations**, can also increase developers' awareness of users' concerns, reinforce privacy norms and social values, and provide basis for judging privacy-related misconduct. Privacy regulations also establish penalties for privacy violations, motivating companies to include this aspect in the cost-benefit analysis. **Open-source documentation** further supports the corporate and individual developers' accountability and responsibility over designing privacy-preserving systems and solutions that respect privacy norms.

5.3 Support the opportunities

Privacy Champions in our study reported that software developers are more likely to push back the engineering goals related to privacy when their opportunity to work on these issues competes with other technical or business priorities (e.g., primary product functionalities, performance, and revenue), and is limited by time and financial resources (see Section 4.4.2). Similarly, security also doesn't receive as much developers' attention as functional requirements [68].

To provide developers an opportunity to think about the privacy implications of their software throughout the development, privacy considerations should become an integral part of software development process, so that the project timelines and deadlines account for the additional time required to address privacy concerns, and project headcounts include engineers whose responsibilities involve such work. The principles of **Privacy by Design** (PbD) [15] provide a useful framework and a starting point for incorporating privacy considerations throughout the software development life cycle. In line with PbD, our participants repeatedly mentioned the importance of thinking about privacy impact early in the process, starting from the design reviews during the requirements stage. **Design and code reviews** offer a good opportunity to supervise the progress on a project, check the quality of implemented safeguards, and detect vulnerabilities. Moreover, opportunity to comment on design should be offered to all employees, instead of limiting it to a specific team, to check in with the interests of other stakeholders, take advantage of the diversity of perspectives, and further encourage strong privacy culture.As security reviews are already common, privacy reviews can piggyback on them by adding to their templates a block of criteria for evaluating privacy.

Finally, companies could organise **privacy-focused hackatons**, which could encourage engineers to both identify the current issues and compete for finding the best and novel solutions for them.

5.4 Support the capabilities

Our participants acknowledged that they and engineers they work with sometimes lack the knowledge about privacy and how to implement it. To overcome the technical challenges of privacy engineering, we propose to increase developers' knowledge, awareness, and skills around privacy and facilitate the task itself.

Increase the knowledge, awareness, and skills. Prior work has shown the value of University-type education in improving security and privacy skills of software developers [2, 62, 67]. In most computer science programs, computer security is not a mandatory course [2] and privacy engineering programs are rare [16]. However, modern software developers need to think not only about the functionalities but also about the ethics of their products, encouraging to **include the topics of privacy and ethics in the curriculum**. This does not mean that every software developer needs to be an *expert* in privacy; if most developers in a team have at least a basic understanding of privacy requirements and ethical values, Privacy Champions and other privacy experts can assist with the nuances of its implementation.

At the workplace, when deploying privacy training, our participants recommend teaching engineers **practical skills** relevant to building privacy-preserving systems and **targeted to their roles** rather than raising their general privacy awareness and concerns. In terms of timing, our participants find privacy training to be rather ineffective during the on-boarding process for new hires, as new employees lack the familiarity with the specifics of the product they will be working on to properly contextualise their knowledge. Instead, they recommend integrating it directly into into the development work. For instance, in addition to advantages discussed in Section 5.3, **design and code reviews** can educate developers about the company's values and the concept of privacy using practical examples from their own work.

Mentoring programs is an alternative way to integrate practical privacy education throughout the development process. However, to be effective, mentors need certain guidance themselves on how to best supervise someone's work, deliver critique and advice, and encourage critical thinking of their apprentices.

As Privacy Champions often rely on **online resources and academic work** for learning about privacy, we encourage researchers to share their work not only in academic venues, but also in blogs, online social networks (e.g., Twitter and LinkedIn), professional newsletters, and general media outlets and news sites (see Section 4.6). Privacy Champions may be instrumental in sharing this knowledge with the development teams. Companies can also create more opportunities to exchange their experiences, success stories, and mistakes in addressing privacy issues, for example, through newsletters, meetup groups, workshops, and company blogs.

Alleviate the complexity of privacy engineering. In addition to design and code reviews, to incorporate privacy considerations into formal processes, our findings suggest using **verified libraries** that do not contain privacy threats as well as tools that help to **annotate data sets**, **map data flows**, and **automate the detection of privacy threats**. Such tools should be practically useful and effective, and save developers' time without introducing additional burden [61]. Since security tools are already commonly used in the organisations, the new privacy features can be incorporated into those existing tools to further facilitate adoption.

Providing developers with **regulation-compliant and user-friendly privacy consent templates**, and code samples for its

integration could help follow the best compliance and user consent practices and avoid mistakes. Our participants acknowledged that **recommendations that help interpret legal documentation** and **translate it into technical requirements** would also help developers incorporate privacy in software design, and facilitate communication between different stakeholders, including engineers, regulators and lawyers, and business management.

Several participants find it difficult to measure privacy risks, and effectiveness of mitigation strategies. Over 80 privacy metrics to measure privacy aspects of a system were proposed in academic research, such as, time that it takes an attacker to violate user privacy or how much information an attacker can gain [75]. Nevertheless, only a few metrics (e.g. k-anonymity and differential privacy) were mentioned by our participants. Increasing awareness of the existing metrics and developing new practical and robust **privacy metrics** could provide reliable tools for demonstrating the benefits of addressing and costs of not addressing a specific privacy issue, and aligning various conflicting corporate priorities.

6 CONCLUSIONS AND FUTURE WORK

We show that Privacy Champions play an important role and have strong personal and organisational motivations to promote privacy values in software development teams, despite the challenges they face. We discuss the main strategies and communication channels that Privacy Champions use to overcome those challenges, and resources they use to learn about privacy matters. We discuss how organisations and team members could assist Privacy Champions by providing organisational support, resources, and simply acknowledging their efforts.

Future research is called for to quantify the prevalence of identified challenges to adoption of privacy practices in organisations, evaluate the effectiveness of strategies, develop robust and standardised taxonomies of privacy risks, detailed practical guidelines and privacy engineering recommendations on how to technically address privacy issues, explore the reasons why existing privacy metrics are not widely adopted in software development industry, and propose solutions to those issues.

ACKNOWLEDGMENTS

We thank all the participants for their time and valuable inputs, Julie M. Haney for sharing materials from their study on cybersecurity advocates and helping with the recruitment, Mary Ellen Zurko for helping with the recruitment, and Adam Jenkins for his feedback on earlier versions of this paper. We also thank the anonymous reviewers whose comments helped improve the paper greatly. This work was supported by the Center for Long-Term Cybersecurity at UC Berkeley, National Science Foundation grants CNS-1514211 and CNS-1528070, Microsoft Research through its PhD Scholarship Program, and a Google Research Award.

REFERENCES

[1] Alessandro Acquisti and Jens Grossklags. 2007. What can behavioral economics teach us about privacy. *Digital privacy: theory, technologies and practices* 18 (2007), 363–377. https://doi.org/10.1201/9781420052183.ch18

[2] Majed Almansoori, Jessica Lam, Elias Fang, Kieran Mulligan, Adalbert Gerald Soosai Raj, and Rahul Chatterjee. 2020. How Secure Are Our Computer Systems Courses?. In *Proceedings of the 2020 ACM Conference on International Computing Education Research* (Virtual Event, New Zealand) *(ICER '20)*. Association for Computing Machinery, New York, NY, USA, 271–281. https://doi.org/10.1145/3372782.3406266

[3] Teresa M. Amabile. 1993. Motivational synergy: Toward new conceptualizations of intrinsic and extrinsic motivation in the workplace. *Human Resource Management Review* 3, 3 (1993), 185–201. https://doi.org/10.1016/1053-4822(93)90012-S

[4] Oshrat Ayalon, Eran Toch, Irit Hadar, and Michael Birnhack. 2017. How Developers Make Design Decisions about Users' Privacy: The Place of Professional Communities and Organizational Climate. In *Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (Portland, Oregon, USA) *(CSCW '17 Companion)*. Association for Computing Machinery, New York, NY, USA, 135–138. https://doi.org/10.1145/3022198.3026326

[5] Kenneth A Bamberger and Deirdre K Mulligan. 2015. *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe*. MIT Press. https://mitpress.mit.edu/books/privacy-ground

[6] Catherine Barrett. 2019. Are the EU GDPR and the California CCPA becoming the de facto global standards for data privacy and protection? *Scitech Lawyer* 15, 3 (2019), 24–29. https://search.proquest.com/docview/2199825726

[7] Cynthia Mathis Beath. 1991. Supporting the Information Technology Champion. *MIS Quarterly* 15, 3 (1991), 355–372. https://doi.org/10.2307/249647

[8] Ingolf Becker, Simon Parkin, and M. Angela Sasse. 2017. Finding Security Champions in Blends of Organisational Culture. In *Proceedings 2nd European Workshop on Usable Security*. Internet Society, Paris, France, 11 pages. https://doi.org/10.14722/eurousec.2017.23007

[9] Odette Beris, Adam Beautement, and M. Angela Sasse. 2015. Employee Rule Breakers, Excuse Makers and Security Champions: Mapping the Risk Perceptions and Emotions That Drive Security Behaviors. In *Proceedings of the 2015 New Security Paradigms Workshop* (Twente, Netherlands) *(NSPW '15)*. Association for Computing Machinery, New York, NY, USA, 73–84. https://doi.org/10.1145/2841113.2841119

[10] Karin Bernsmed and Martin Jaatun. 2019. Threat modelling and agile software development: Identified practice in four Norwegian organisations. In *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. IEEE, 1–8. https://doi.org/10.1109/CyberSecPODS.2019.8885144

[11] Robert L Brennan and Dale J Prediger. 1981. Coefficient Kappa: Some Uses, Misuses, and Alternatives. *Educational and psychological measurement* 41, 3 (1981), 687–699. https://doi.org/10.1177/001316448104100307

[12] Fei Bu, Nengmin Wang, Bin Jiang, and Huigang Liang. 2020. "Privacy by Design" implementation: Information system engineers' perspective. *International Journal of Information Management* 53 (2020), 102124. https://doi.org/10.1016/j.ijinfomgt.2020.102124

[13] Andrew Campbell and Sally Yeung. 1991. Creating a sense of mission. *Long Range Planning* 24, 4 (1991), 10 – 20. https://doi.org/10.1016/0024-6301(91)90002-6

[14] Susan Cartwright and Nicola Holmes. 2006. The meaning of work: The challenge of regaining employee engagement and reducing cynicism. *Human Resource Management Review* 16, 2 (2006), 199 – 208. https://doi.org/10.1016/j.hrmr.2006.03.012 The New World of Work and Organizations.

[15] Ann Cavoukian. 2009. Privacy by Design: The 7 Foundational Principles. *Information and privacy commissioner of Ontario, Canada* 5 (2009), 5 pages. https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

[16] Lorrie Cranor and Norman Sadeh. 2013. A Shortage of Privacy Engineers. *IEEE Security & Privacy* 11, 2 (2013), 77–79. https://doi.org/10.1109/MSP.2013.25

[17] Maria da Conceição Freitas and Miguel Mira da Silva. 2018. GDPR Compliance in SMEs: There is much to be done. *Journal of Information Systems Engineering & Management* 3, 4 (2018), 30. https://doi.org/10.20897/jisem/3941

[18] Adéle Da Veiga and Jan HP Eloff. 2010. A framework and assessment instrument for information security culture. *Computers & Security* 29, 2 (2010), 196–207. https://doi.org/10.1016/j.cose.2009.09.002

[19] Duy Dang-Pham, Siddhi Pittayachawan, and Vince Bruno. 2017. Applications of social network analysis in behavioural information security research: Concepts and empirical analysis. *Computers & Security* 68 (2017), 1–15. https://doi.org/10.1016/j.cose.2017.03.010

[20] Duy Dang-Pham, Siddhi Pittayachawan, and Vince Bruno. 2017. Applying network analysis to investigate interpersonal influence of information security behaviours in the workplace. *Information & Management* 54, 5 (2017), 625–637. https://doi.org/10.1016/j.im.2016.12.003

[21] Duy Dang-Pham, Siddhi Pittayachawan, and Vince Bruno. 2017. Investigation into the formation of information security influence: Network analysis of an emerging organisation. *Computers & Security* 70 (Sept. 2017), 111–123. https://doi.org/10.1016/j.cose.2017.05.010

[22] Linda Di Geronimo, Larissa Braz, Enrico Fregnan, Fabio Palomba, and Alberto Bacchelli. 2020. UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376600

[23] Nora A Draper and Joseph Turow. 2019. The corporate cultivation of digital resignation. *New Media & Society* 21, 8 (2019), 1824–1839. https://doi.org/10.1177/1461444819833331

[24] Pietro Ferrara and Fausto Spoto. 2018. Static Analysis for GDPR Compliance. In *Proceedings of the Second Italian Conference on Cyber Security (ITASEC 2018), Milan, Italy (CEUR Workshop Proceedings, Vol. 2058)*. CEUR-WS.org, 10 pages. http://ceur-ws.org/Vol-2058/paper-10.pdf

[25] Rita Francese, Carmine Gravino, Michele Risi, Giuseppe Scanniello, and Genoveffa Tortora. 2017. Mobile App Development and Management: Results from a Qualitative Investigation. In *Proceedings of the 4th International Conference on Mobile Software Engineering and Systems* (Buenos Aires, Argentina) *(MOBILESoft '17)*. IEEE Press, 133–143. https://doi.org/10.1109/MOBILESoft.2017.33

[26] Alisa Frik, Leysan Nurgalieva, Julia Bernd, Joyce S. Lee, Florian Schaub, and Serge Egelman. 2019. Privacy and Security Threat Models and Mitigation Strategies of Older Adults. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security* (Santa Clara, CA, USA) *(SOUPS'19)*. USENIX Association, USA, 21–40. https://www.usenix.org/conference/soups2019/presentation/frik

[27] Trevor Gabriel and Steven Furnell. 2011. Selecting security champions. *Computer Fraud & Security* 2011, 8 (2011), 8–12. https://doi.org/10.1016/S1361-3723(11)70082-3

[28] Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L. Toombs. 2018. The Dark (Patterns) Side of UX Design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3173574.3174108

[29] Irit Hadar, Tomer Hasson, Oshrat Ayalon, Eran Toch, Michael Birnhack, Sofia Sherman, and Arod Balissa. 2018. Privacy by designers: software developers' privacy mindset. *Empirical Software Engineering* 23, 1 (Feb. 2018), 259–289. https://doi.org/10.1007/s10664-017-9517-1

[30] Tracy Hall, Helen Sharp, Sarah Beecham, Nathan Baddoo, and Hugh Robinson. 2008. What Do We Know about Developer Motivation? *IEEE Software* 25, 4 (2008), 92–94. https://doi.org/10.1109/MS.2008.105

[31] Julie M Haney and Wayne G Lutters. 2017. Skills and Characteristics of Successful Cybersecurity Advocates. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, 7. https://www.usenix.org/conference/soups2017/workshop-program/wsiw2017/haney

[32] Julie M. Haney and Wayne G. Lutters. 2017. The Work of Cybersecurity Advocates. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI EA '17)*. Association for Computing Machinery, New York, NY, USA, 1663–1670. https://doi.org/10.1145/3027063.3053134

[33] Julie M. Haney and Wayne G. Lutters. 2018. "It's Scary...It's Confusing...It's Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Baltimore, MD, 411–425. https://www.usenix.org/conference/soups2018/presentation/haney-perceptions

[34] Julie M. Haney and Wayne G. Lutters. 2019. Motivating Cybersecurity Advocates: Implications for Recruitment and Retention. In *Proceedings of the 2019 on Computers and People Research Conference* (Nashville, TN, USA) *(SIGMIS-CPR '19)*. Association for Computing Machinery, New York, NY, USA, 109–117. https://doi.org/10.1145/3322385.3322388

[35] Julie M. Haney, Mary Theofanos, Yasemin Acar, and Sandra Spickard Prettyman. 2018. "We make it a big deal in the company": Security Mindsets in Organizations that Develop Cryptographic Products. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Baltimore, MD, 357–373. https://www.usenix.org/conference/soups2018/presentation/haney-mindsets

[36] Michael S.H Heng, Eileen M Trauth, and Sven J Fischer. 1999. Organisational champions of IT innovation. *Accounting, Management and Information Technologies* 9, 3 (1999), 193–222. https://doi.org/10.1016/S0959-8022(99)00008-9

[37] Jaap-Henk Hoepman. 2019. *Privacy Design Strategies (The Little Blue Book)*. Radboud University. https://cs.ru.nl/~jhh/publications/pds-booklet.pdf

[38] Christopher Horn and Anita D'Amico. 2019. Measuring Application Security. In *Advances in Human Factors in Cybersecurity*, Tareq Z. Ahram and Denise Nicholson (Eds.). Vol. 782. Springer International Publishing, Cham, 44–55. https://doi.org/10.1007/978-3-319-94782-2_5

[39] Jane M Howell and Christine M Shea. 2001. Individual differences, environmental scanning, innovation framing, and champion behavior: key predictors of project performance. *Journal of Product Innovation Management* 18, 1 (2001), 15–27. https://doi.org/10.1016/S0737-6782(00)00067-9

[40] Shubham Jain, Janne Lindqvist, et al. 2014. Should I Protect You? Understanding Developers' Behavior to Privacy-Preserving APIs. In *Workshop on Usable Security (USEC'14)*. Internet Society, 10 pages. https://doi.org/10.14722/usec.2014.23045

[41] Donna Kelley and Hyunsuk Lee. 2010. Managing Innovation Champions: The Impact of Project Characteristics on the Direct Manager Role*. *Journal of Product Innovation Management* 27, 7 (2010), 1007–1019. https://doi.org/10.1111/j.1540-5885.2010.00767.x

[42] J. Richard Landis and Gary G. Koch. 1977. The Measurement of Observer Agreement for Categorical Data. *Biometrics* 33, 1 (1977), 159–174. https://doi.org/10.2307/2529310

[43] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. 2017. Chapter 11 - Analyzing qualitative data. In *Research Methods in Human Computer Interaction* (second edition ed.), Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser (Eds.). Morgan Kaufmann, Boston, 299–327. https://doi.org/10.1016/B978-0-12-805390-4.00011-X

[44] He Li, Lu Yu, and Wu He. 2019. The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management* 22, 1 (2019), 1–6. https://doi.org/10.1080/1097198X.2019.1569186

[45] Xenia Mountrouidou, David Vosen, Chadi Kari, Mohammad Q. Azhar, Sajal Bhatia, Greg Gagne, Joseph Maguire, Liviana Tudor, and Timothy T. Yuen. 2019. Securing the Human: A Review of Literature on Broadening Diversity in Cybersecurity Education. In *Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education* (Aberdeen, Scotland UK) *(ITiCSE-WGR '19)*. Association for Computing Machinery, New York, NY, USA, 157–176. https://doi.org/10.1145/3344429.3372507

[46] Deborah Mrazek and Michael Rafeld. 1992. Integrating Human Factors on a Large Scale: Product Usability Champions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Monterey, California, USA) *(CHI '92)*. Association for Computing Machinery, New York, NY, USA, 565–570. https://doi.org/10.1145/142750.142989

[47] Helen Nissenbaum. 2009. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press. http://www.sup.org/books/title/?id=8862

[48] State of California Department of Justice. 2018. California Consumer Privacy Act (CCPA). Retrieved August 2020 from https://oag.ca.gov/privacy/ccpa

[49] Stack Overflow. 2020. Developer Survey Results. Retrieved August 2020 from https://insights.stackoverflow.com/survey/2020

[50] Leysia Palen and Paul Dourish. 2003. Unpacking "Privacy" for a Networked World. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Ft. Lauderdale, Florida, USA) *(CHI '03)*. Association for Computing Machinery, New York, NY, USA, 129–136. https://doi.org/10.1145/642611.642635

[51] The European parliament and the council of the European union. 2018. General Data Protection Regulation (GDPR). Retrieved August 2020 from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[52] Chris Parnin, Christian Bird, and Emerson Murphy-Hill. 2011. Java Generics Adoption: How New Features Are Introduced, Championed, or Ignored. In *Proceedings of the 8th Working Conference on Mining Software Repositories* (Waikiki, Honolulu, HI, USA) *(MSR '11)*. Association for Computing Machinery, New York, NY, USA, 3–12. https://doi.org/10.1145/1985441.1985446

[53] Chris Parnin, Christian Bird, and Emerson Murphy-Hill. 2013. Adoption and use of Java generics. *Empirical Software Engineering* 18, 6 (Dec. 2013), 1047–1089. https://doi.org/10.1007/s10664-012-9236-6

[54] Mariana Peixoto, Dayse Ferreira, Mateus Cavalcanti, Carla Silva, Jéssyka Vilela, João Araújo, and Tony Gorschek. 2020. On Understanding How Developers Perceive and Interpret Privacy Requirements Research Preview. In *Requirements Engineering: Foundation for Software Quality*, Nazim Madhavji, Liliana Pasquale, Alessio Ferrari, and Stefania Gnesi (Eds.). Springer International Publishing, Cham, 116–123. https://doi.org/10.1007/978-3-030-44429-7_8

[55] Hiep Cong Pham, Linda Brennan, Lukas Parker, Nhat Tram Phan-Le, Irfan Ulhaq, Mathews Zanda Nkhoma, and Minh Nhat Nguyen. 2019. Enhancing cyber security behavior: an internal social marketing approach. *Information & Computer Security* 28, 2 (Oct. 2019), 133–159. https://doi.org/10.1108/ICS-01-2019-0023

[56] Jaco Renken and Richard Richard. 2019. Champions of IS Innovations. *Communications of the Association for Information Systems* 44 (2019), 811–851. https://doi.org/10.17705/1CAIS.04438

[57] SAFECode. 2019. *Software Security Takes a Champion - A Short Guide on Building and Sustaining a Successful Security Champions Program.* Technical Report. SAFECode. http://safecode.org/wp-content/uploads/2019/02/Security-Champions-2019-.pdf

[58] Gabe Scelta, Hamid Rashid, Hoi Wai Jackie Cheng, Marcelo LaFleur, Mariangela Parra-Lancourt, Alex Julca, Nicole Hunt, S. Islam, and Hiroshi Kawamura. 2019. Data Economy: Radical transformation or dystopia? *Frontier Technology Quarterly* 1 (Jan. 2019). https://www.un.org/development/desa/dpad/wp-content/uploads/sites/45/publication/FTQ_1_Jan_2019.pdf

[59] Donald A. Schon. 1963. Champions for Radical New Inventions. *Harvard Business Review* 41 (1963), 77–86. https://id.lib.harvard.edu/ead/c/bak00203c02144/catalog

[60] Awanthika Senarath and Nalin A. G. Arachchilage. 2018. Why Developers Cannot Embed Privacy into Software Systems? An Empirical Investigation. In *Proceedings of the 22nd International Conference on Evaluation and Assessment in Software Engineering 2018* (Christchurch, New Zealand) *(EASE'18)*. Association for Computing Machinery, New York, NY, USA, 211–216. https://doi.org/10.1145/3210459.3210484

[61] Awanthika Senarath, Marthie Grobler, and Nalin Asanka Gamagedara Arachchilage. 2019. Will They Use It or Not? Investigating Software Developers' Intention to Follow Privacy Engineering Methodologies. *ACM Transactions on Privacy and Security* 22, 4, Article 23 (Nov. 2019), 30 pages. https://doi.org/10.1145/3364224

[62] Katie Shilton, Donal Heidenblad, Adam Porter, Susan Winter, and Mary Kendig. 2020. Role-Playing Computer Ethics: Designing and Evaluating the Privacy by Design (PbD) Simulation. *Science and Engineering Ethics* PP, PP (July 2020), 16 pages. https://doi.org/10.1007/s11948-020-00250-0

[63] Daniela Soares Cruzes, Martin Gilje Jaatun, Karin Bernsmed, and Inger Anne Tondel. 2018. Challenges and Experiences with Applying Microsoft Threat Modeling in Agile Development Projects. In *2018 25th Australasian Software Engineering Conference (ASWEC)*. IEEE, Adelaide, SA, 111–120. https://doi.org/10.1109/ASWEC.2018.00023

[64] Daniel J Solove. 2005. A taxonomy of privacy. *University of Pennsylvania Law Review* 154 (2005), 477–560. https://ssrn.com/abstract=667622

[65] Daniel J Solove. 2007. "I've Got Nothing to Hide" and Other Misunderstandings of Privacy. *San Diego Law Review* 44 (2007), 745. https://ssrn.com/abstract=998565

[66] Sarah Spiekermann, Jana Korunovska, and Marc Langheinrich. 2019. Inside the Organization: Why Privacy and Security Engineering Is a Challenge for Engineers. *Proc. IEEE* 107, 3 (2019), 600–615. https://doi.org/10.1109/JPROC.2018.2866769

[67] Mohammad Tahaei, Adam Jenkins, Kami Vaniea, and Maria K. Wolters. 2020. "I Don't Know Too Much About It": On the Security Mindsets of Computer Science Students. In *Socio-Technical Aspects in Security and Trust* (first ed.), Thomas Groß and Tryfonas Theo (Eds.). Springer International Publishing. https://www.springer.com/book/9783030559571

[68] Mohammad Tahaei and Kami Vaniea. 2019. A Survey on Developer-Centred Security. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 129–138. https://doi.org/10.1109/EuroSPW.2019.00021

[69] Mohammad Tahaei, Kami Vaniea, and Naomi Saphra. 2020. Understanding Privacy-Related Questions on Stack Overflow. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376768

[70] Tyler W. Thomas, Madiha Tabassum, Bill Chu, and Heather Lipford. 2018. Security During Application Development: An Application Security Expert Perspective. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, Article 262, 12 pages. https://doi.org/10.1145/3173574.3173836

[71] Kerry-Lynn Thomson, Rossouw Von Solms, and Lynette Louw. 2006. Cultivating an organizational information security culture. *Computer fraud & security* 2006, 10 (2006), 7–11. https://doi.org/10.1016/S1361-3723(06)70430-4

[72] Inger Anne Tøndel, Martin Jaatun, and Daniela Cruzes. 2020. IT Security Is From Mars, Software Security Is From Venus. *IEEE Security & Privacy* 18, 04 (July 2020), 48–54. https://doi.org/10.1109/MSEC.2020.2969064

[73] Ismini Vasileiou and Steven Furnell. 2019. Personalising Security Education: Factors Influencing Individual Awareness and Compliance. In *Information Systems Security and Privacy*, Paolo Mori, Steven Furnell, and Olivier Camp (Eds.). Springer International Publishing, Cham, 189–200. https://doi.org/10.1007/978-3-030-25109-3_10

[74] Daniel Votipka, Rock Stevens, Elissa M. Redmiles, Jeremy Hu, and Michelle L. Mazurek. 2018. Hackers vs. Testers: A Comparison of Software Vulnerability Discovery Processes. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 374–391. https://doi.org/10.1109/SP.2018.00003

[75] Isabel Wagner and David Eckhoff. 2018. Technical Privacy Metrics: A Systematic Survey. *Comput. Surveys* 51, 3, Article 57 (June 2018), 38 pages. https://doi.org/10.1145/3168389

[76] Ari Ezra Waldman. 2018. Designing without privacy. *Houston Law Review* 55 (2018), 659. https://ssrn.com/abstract=2944185

[77] Charles Weir, Ingolf Becker, James Noble, Lynne Blair, Angela Sasse, and Awais Rashid. 2019. Interventions for Software Security: Creating a Lightweight Program of Assurance Techniques for Developers. In *2019 IEEE/ACM 41st International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP)*. IEEE, 41–50. https://doi.org/10.1109/ICSE-SEIP.2019.00013

[78] Charles Weir, Ingolf Becker, James Noble, Lynne Blair, M. Angela Sasse, and Awais Rashid. 2020. Interventions for long-term software security: Creating a lightweight program of assurance techniques for developers. *Software: Practice and Experience* 50, 3 (2020), 275–298. https://doi.org/10.1002/spe.2774

[79] Charles Weir, Ben Hermann, and Sascha Fahl. 2020. From Needs to Actions to Secure Apps? The Effect of Requirements and Developer Practices on App Security. In *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, Boston, MA, 17 pages. https://www.usenix.org/conference/usenixsecurity20/presentation/weir

[80] Sara J Weston, M Teresa Cardador, Patrick L Hill, Ted Schwaba, Jennifer Lodi-Smith, and Susan K Whitbourne. 2020. The Relationship Between Career Success and Sense of Purpose: Examining Linkages and Changes. *The Journals of Gerontology: Series B* PP (09 2020), 10 pages. https://doi.org/10.1093/geronb/gbaa162

A SCREENING SURVEY

[After the participant read the participant information sheet and consent form, and agreed to participant in the study.]

(1) What is your current employment status? (Check all that apply).
   • Full time employee (or contractor equivalent) • Part-time employee (or contractor equivalent) • Freelance/consultant • Furloughed (temporarily laid off) or on leave • Unemployed • Student • Retired
(2) Please select the statement that best describes your primary role at your current or most recent job.
   • Jobs NOT related to computer science, informatics, computer engineering, or related fields • Designing products (e.g. UI designer, interaction designer) • Developing software (e.g. programmer, developer, web developer, software engineer) • Testing software (e.g. tester, quality analyst, automation engineer) • Managing software development (e.g. project manager, IT manager, scrum master) • Privacy and/or security engineering (e.g. security engineer, privacy engineer, penetration tester, ethical hacker, cryptographer) • Other
(3) What is your job title? (Free text)
(4) How many members are there in your team that you work with directly? (Free text)
(5) How many employees work in your organisation?
   • 1-9 employees • 10-99 employees • 100-999 employees • 1,000-9,999 employees • 10,000 or more employees
(6) Overall, how many years have you worked in roles related to software development or IT? (Free text)
(7) Where did you mainly learn to program and develop software? (Choose all that apply.)
   • Self-taught • High school courses • College or university courses • Online courses • Industry or on-the-job training • Other
(8) Which of the following sectors most closely matches the one in which you are employed?
   • Business • Academia/education • Government • Non-profit • Other
(9) Which one best describes your English proficiency level?
   • Basic Knowledge • Conversational/Functional • Proficient • Fluent/Native speaker
(10) In which country do you currently reside? (List of countries)
(11) What is your gender?
   • Male • Female • Non-binary • Prefer not to say • Prefer to self describe
(12) How old are you? (Free text)
(13) If you'd like to participate in the study, what email address should we use to contact you? (Free text)
(14) What software would you prefer to use for the interview? (You can keep the video camera turned off).
   • Zoom • Google Hangouts Meet • Teams • Skype • Other
(15) Do you have any comments or questions about the study? (Optional)

If you are selected for the interview, you will be notified over email within 2 weeks from today. Please keep an eye on the email inbox for the address that you provided in this survey.

B INTERVIEW SCRIPT

[After the interviewer has introduced themselves, and obtained verbal consent.]

(1) Can you tell me just briefly about what you do in your job?

(2) Before the interview, we asked other people in your organisation to tell us who they think promotes user privacy, and among other people, they nominated you. Why do you think they consider you to be playing this role?
(3) Could you define the term "privacy" as you normally use it in your work context?
    - In your opinion, what is the difference between security and privacy?
(4) What motivates you to promote user privacy in your work, formally or informally?
(5) What do you find most rewarding about promoting user privacy?
(6) What do you find most challenging or frustrating about promoting user privacy?
(7) Think about formal or informal strategies that you use to promote or support users' privacy in product design and development:
    - Which ones do you find most effective? Why? How do you know it's effective?
    - Which ones do you find least effective? Why? How do you know it's ineffective?
(8) In addition to your role, what other strategies in your organisation have you found most effective in promoting users' privacy?
    - Which strategies have you found to be least effective?
(9) What communication channels for promoting privacy specifically do you think are the most effective and least effective? Why?
(10) How are your efforts for promoting user privacy valued by other people within your team? Within the organisation?
    - What kind of feedback do you get?
    - Can you talk about any times when you felt that what you said or did wasn't appreciated?
(11) How do you keep up with the latest in privacy?
(12) Is there anything else you'd like to add with respect to what we've talked about today?

C CODEBOOK

(1) Conceptualisations of privacy
    • Data management / control • Transparency / trust • Human right / ethical value as definition • Protect access to personal information • Legal compliance • Relationship between privacy and security • Complex / contextual term • Approaches to privacy (e.g. privacy-by-design and differential privacy)
(2) Motivations
    • Organisational • Personal • Sense of responsibility
(3) Rewards and positive feedback
    • Challenging task • Seeing shift / change in the company culture • Official promotion / incentives • Impact on end-user / society
(4) Challenges and negative feedback
    • Attitudes • Communications issues • Dominant conceptualisation • Tension between priorities • Technical complexity
(5) Strategies
    • External influence • Improving company culture values • Relying on instinct / being careful • Tools, APIs, and libraries • Training • Punishment • Documentation • Reviews / review meetings
(6) Communication channels
    • Special events • Communication / productivity platforms • Verbal / messaging channels • Written communications
(7) Criteria for (in)effectiveness of a strategy or a communication channel
    • Experience / intuition • Practical usefulness of processes / procedures • Impact on end products and decisions • Auditability / transparency / accountability • Fewer arguments / disagreements • Measurability • Relevance / targetedness • Difficulty to find / browse
(8) Information resources
    • In-person networking • Online resources • Experiences of other companies • Academic research • Internal organisational channels