What Makes a Technology Privacy Enhancing? Laypersons' and Experts' Descriptions, Uses, and Perceptions of Privacy Enhancing Technologies

Houda Elmimouni[1][0000−0003−0645−9026], Erica Shusas[2][0000−0001−8112−6227], Patrick Skeba[3][0000−0003−3052−3294], Eric P. S. Baumer[3][0000−0001−5338−4421], and Andrea Forte[2][0000−0002−2941−339X]

[1] Luddy School of Informatics, Computing, and Engineering, Bloomington, IN, USA
[2] College of Computing & Informatics, Drexel University, PA, USA
[3] Computer Science & Engineering, Lehigh University, PA, USA

Abstract. What makes a technology privacy-enhancing? In this study, we construct an explanation grounded in the technologies and practices that people report using to enhance their privacy. We conducted an online survey of privacy experts (i.e., privacy researchers and professionals who attend to privacy conferences and communication channels) and laypersons that catalogs the technologies they identify as privacy enhancing and the various privacy strategies they employ. The analysis of 123 survey responses compares not only self-reported tool use but also differences in how privacy experts and laypersons explain their privacy practices and tools use. Differences between the two samples show that privacy experts and laypersons have different styles of reasoning when considering PETs: Experts think of PETs as technologies whose primary function is enhancing privacy, whereas laypersons conceptualize privacy enhancement as a supplemental function incorporated into other technologies. The paper concludes with a discussion about potential explanations for these differences, as well as questions they raise about how technologies can best facilitate communication and collaboration while enhancing privacy.

Keywords: Privacy · Privacy Enhancing Technologies · privacy behaviors · privacy experts · privacy laypersons

1 Introduction

In order to design privacy tools that people can use and benefit from, technologists need to understand what lay people *think* privacy-enhancing technologies (PETs) are, how they *think* they work, and how effective they *think* these technologies are [44, 24, 14]. Characterizations of what constitutes a privacy-enhancing technology (e.g., [27]) are well established in the expert communities that research and develop privacy tools, but past work has shown that experts and laypersons have different conceptions of privacy [41] and of specific tools [23]. Researchers and designers lack an understanding of what people believe makes

a technology good or bad for privacy. How do people, especially laypersons, determine what counts as a privacy–enhancing technology? How do privacy experts and laypersons describe the technologies and strategies they use to protect their privacy? Prior work has established the value of investigating differences between lay and expert approaches to privacy. User experience studies of specific PETs have provided insight about usability barriers to adoption [17, 22], and researchers have used creative methods to understand how laypersons and experts conceptualize privacy [41, 32]. Models have been developed to explain rationales that may guide adoption of PETs [15], and economists have long theorized about the tradeoffs involved in making privacy decisions [43, 1]. Unfurling the privacy paradox—when people's stated privacy concerns and real-world behaviors contradict each other—has occupied scholars in many fields who have applied a variety of theoretical framings [33], including institutional vs. social privacy concerns [55], apathy or lack of control [30], and dual-process theory [42]. To provide further context for understanding people's sometimes puzzling practices and decisions about privacy, it is important to know what they believe a privacy-enhancing technology *is*. In this study we use a sociotechnical perspective to lay the basis for a grounded explanation of privacy-enhancing technology use by cataloging the technologies and related strategies identified as privacy-enhancing by privacy experts and by laypersons.

To construct an inventory of privacy-enhancing technologies used by privacy experts and laypersons and to collect short explanations of their use, we developed and deployed a survey. Adapting methods used by Oates et al. [41] to collect data from experts and laypersons, we recruited privacy experts by soliciting participants from the PETs and HCI privacy research communities, and we recruited laypersons using a demographically-matched panel procured by Qualtrics.

Our contributions include three key findings and a discussion of their implications.

1. One impetus for examining privacy laypersons' practices was to discover whether they reference technologies and strategies for everyday privacy practices that resemble those of experts. In their descriptions of everyday technology use, we found that the *laypersons applied heuristic reasoning* in determining which tools and practices enhanced (or reduced) their privacy while, as expected, the *experts often demonstrated a more technical style of reasoning* when thinking about PETs.
2. Experts and laypersons reported some common technology use and privacy behaviors. However, from the list of technologies reported by each sample, we understand that *ease of use impacts laypersons' use of PETs but does not impact the experts' use as much.* Some laypersons use technologies because they are user friendly or avoid using other technologies because they have usability issues. On the other hand, the *experts reported technologies and behaviors that require dedicated attention* and are often less widely known (e.g., using PETs with difficult user experience, varying their online behaviors, or opening social media in a browser with no other websites concurrently open).

3. Among the technologies popularly mentioned in each sample, *laypersons reported technologies with a primary function other than privacy protection.* In contrast, *technologies cited by experts tend to foreground privacy protection* as a primary function.

We conclude with a discussion that addresses some of the social features of privacy tools use and proposes human-centered design recommendations for privacy-enhancing technologies grounded in the above findings. Specifically, our findings point to the importance of using privacy-enhancing technologies as a substrate for Internet tools with other primary functions.

2 Related Work

Privacy-enhancing technologies (PETs) are tools designed to help people achieve desired experiences of privacy. Privacy-enhancing technology as an area of scholarship has traditionally had a strong emphasis in contributions around the design and effectiveness of technologies themselves. For example, Goldberg et al.'s foundational work on PETs [27] concluded that well-designed technologies—not social interventions and policies subject to "the whims of bureaucrats" (p. 108)—would be the best solutions for individuals to protect their privacy as they ventured online. In later updates to this work, Goldberg rereviewed the state of the art and concluded with a set of general design requirements that reflected a growing interest in human-centered concerns: PETs must be usable, deployable, effective, and robust in order to have broad impact [26]. In the intervening years, interest in social, political, and cultural features of PETs adoption has become a routine feature of PETs scholarship; to understand why people use PETs, researchers need to understand how people make sense of them.

2.1 Conceptualization of privacy and comparison of experts and laypersons

Research has offered frameworks for users' conceptualization of privacy as well as potential factors that might influence online privacy behavior. Baumer and Forte [5] suggest that rather than conceptualizing privacy in terms of literacy, it might be beneficial to analyze people's everyday approaches to protecting their data, which include a person's perceived risks when interacting with technologies, the strategies employed to manage the perceived risks, and the results of those strategies. Kang et al. [32] similarly suggest the experience of privacy violation, rather than an individual's level of literacy or know-how, shapes online privacy practice. In addition, socioeconomic factors may contribute to how people engage with technologies [3, 37, 54]. Being a member of groups that suffer inequality and discrimination puts individuals at higher risk of privacy violations and makes them susceptible to disproportionate harms as a result of such violations [38].

Some research has been done to investigate the differences between experts and laypersons in their conceptualizations of privacy as a concept. Research

by Oates et al.[41] used a qualitative analysis of 366 illustrations created by laypersons, privacy experts, children, and adults to reveal that many drawings from laypersons displayed a strong distinction between private and public spaces, while drawings from experts were more likely to illustrate more nuanced privacy spaces and control over information. In an interview study investigating expert and layperson understandings of the anonymity system, Tor, experts showed a deeper understanding of Tor's underlying operation and focused more on the technical details of Tor's operations, while laypersons were more likely to situate Tor within a broader sociotechnical landscape [23]. Chua et al. [16] looked at novice and expert users of "Social-Local-Mobile services" (SoLoMo) and found that in both groups, "covert" channels (that run in the background) triggered higher privacy concerns than "overt" channels (that respond to explicit requests). However, novice users with different life goals and less experience with mobile applications demonstrated lower privacy concerns than expert users.

2.2 Methods of seeking privacy

Many privacy researchers have used Altman's canonical description of privacy as an ongoing process of boundary regulation to examine privacy strategies online [2, 50, 4, 20]. Lampinen et al. [34] have categorized strategies for boundary regulation as behavioral, such as self-censorship or creating fake accounts, and mental strategies, such as trusting others. Stutzman and Hartzog [50] grouped these strategies into pseudonymity, practical obscurity (obscuring one's profile through modification of privacy settings, pseudonymity, technical separation), and transparent separation, such as maintaining multiple profiles without obscuring identity.

In general, the literature suggests two broad categories into which strategies for maintaining privacy online fall:

1. *Technical Approaches* focus on specific technologies. Anonymous browsers (e.g. Tor browser), Virtual Private Networks (VPNs), non-tracking search engines (e.g. DuckDuckGo), or browsers and plugins/extensions [18]. Anonymous email clients enable individuals to send emails without revealing their origin. Forte et al. [20] refer to the use of Tor and IP-blocking strategies as technical approaches and suggest them among one of two ways that people can counter privacy threats. Proxy servers, Secure Sockets Layer (SSL) technology, and cookie managers [51] are also technical approaches to seeking some degree of privacy and/or anonymity.
2. *Operational Approaches* involve more behavioral strategies. Previous work has described creating multiple accounts [20], or throwaway accounts [4, 35] to dissociate one's self from certain online actions and information sharing. Other examples of operational approaches to seeking privacy include modifying one's behavior or using language meant to obstruct authorship attribution [11].

2.3 PETs adoption motivations and barriers

Motivations to adopt PETs, as well as potential barriers to use [7, 49] are also important factors for understanding expert and layperson PET adoption. In proposing a model to explore how consumers choose between competing PETs, Caulfield et al. [15] consider the context in which a technology is used; the requirement for the level of privacy that a technology must provide in order for an individual to be willing to use it; the belief, or perception, of the level of privacy a technology provides; and the relative value of privacy in relation to how much the individual is willing to trade it for other attributes. Vemou and Karyda [52] suggest lack of awareness of privacy risks and PETs, lack of technical skill, the complexity and diversity of the risks involved in privacy management, direct and indirect costs, and privacy being a cultural value as potential factors for the limited adoption of PETs on social networking sites. Research has found varying amounts of usability issues with the Tor browser and Tor deployment tools that hinder the adoption of Tor as a widespread anonymity system and suggests that usability issues hinder the widespread adoption of Tor [17, 22, 21]. The reputation of Tor as being used for illegal activities and its consequences such as being a target of investigations also hinders Tor use and adoption [29, 56].

Although models that explore usability issues and motivations can help scholars understand what factors influence decisions, questions remain. What PETs are most salient to people and which do they use in their daily lives? Do experts and laypersons differ? What technologies do people seek out and what technologies do people *avoid* in order to enhance their privacy? We set out to understand what makes a technology a PET—not based on scholarly definitions but grounded in a sociotechnical understanding of the technologies and practices that people (both privacy experts and laypersons) report using to enhance their privacy.

3 Study Design

To generate an inventory of privacy-enhancing technology examples as understood by both privacy experts and laypersons, we developed and administered a survey via Qualtrics to two separate samples. This study was approved by the IRBs at Drexel and Lehigh University where all authors were affiliated at the time of data collection.

3.1 Recruitment

We targeted two groups: privacy experts and privacy laypersons. We defined experts as privacy researchers and privacy professionals who contribute to privacy literature as one of their research areas and/or attend to communication channels and conferences centered around privacy. Given the inherent complexities in defining both "expertise" [25] and "privacy" [40], we did not determine an *a priori* skill set to identify privacy experts. Instead we used a similar approach

to Oates et al. [41], who assembled data from experts by collecting data (illustrations in their case) in venues where experts can be found. Similarly Ion et al. [31] and Busse et al. [13] defined their expert samples as people attending privacy conferences.

Thus, to recruit privacy experts, we advertised the study in expert venues. First, we searched for recent privacy-related publications of members of the CHI 2020 subcommittee on privacy and security, and emailed subcommittee members and their co-authors a link to the study. Second, we asked the Privacy-Enhancing Technologies Symposium Twitter account to retweet our recruitment message on Twitter, which they did. This recruitment approach yielded 49 responses in fall (September-October) 2019. No incentives were offered to complete the survey.

To recruit privacy laypersons, we used the demographic profile of our expert sample to acquire a sample from the general population of survey takers on Qualtrics that reflected our expert sample in terms of age, gender, and education level. This departs from Oates et al. [41]'s method of recruiting laypersons by ensuring demographic alignment between our two samples. In this way, we decrease the chance that any differences are due to differences in, say, education but are instead due to differences in privacy expertise. Similary to Oates et al. [41], we also assume that recruiting participants without specifically targeting channels where privacy experts are likely to be found will result in a sample that can be treated as "laypersons." Like Oates et al. [41], we acknowledge it is possible that privacy experts could have responded to the Qualtrics panel, just as laypersons could have been included in the expert sample. During the analysis, we identified one respondent in the laypersons' sample who shared many characteristics with the expert sample. Otherwise, the groups exhibited largely divergent behaviors around and conceptualizations of PETs, which lends confidence to our recruitment-based approach to identifying experts and laypersons.

We recruited 99 participants from Qualtrics in spring (early March) 2020[4]. The minimal eligibility criteria to participate in the survey included being 18 or older and being able to read English.

3.2 Participants

A total of 148 survey responses were collected during the period the surveys were active, of which 123 were included in the final dataset—46 from the privacy expert sample and 77 from the laypersons' sample (See Table 1 for details about participants). The participants who were excluded did not answer the questions about technologies or practices and/or provided nonsensical text like entering random words. Whereas the majority of our participants reported residing in the USA, 16 of our privacy experts sample reported other countries (Canada, France, India, Italy, Switzerland, UK, Germany). Table 1 shows demographics for both

[4] A total of 106 Qualtrics participants were solicited: 6 as a preliminary test and 100 additional participants. However, only 99 entered any data in the survey. Qualtrics data collection was limited to U.S. respondents and ended before widespread emergence of the COVID-19 pandemic in the United States.

samples. Because of the relative uncertainty involved in recruiting experts via social networks and work-of-mouth vs laypersons via a survey panel commissioned from Qualtrics, the number of participants in each sample is uneven.

Table 1. Cross tabulation of participant demographics from the two samples.

Demographics		Privacy experts ($n = 46$)	Privacy laypersons ($n = 77$)
Gender	Man	22(48%)	39(51%)
	Woman	20(43%)	38(49%)
	Not specified	2 (4%)	0 (0%)
Age	Min	22	22
	Max	69	67
	Avg	35	36
Education	Doctorate	25(54%)	38(49%)
	Master	13(28%)	25(32%)
	Bachelor	4 (9%)	13(17%)
	Some college/university	1 (2%)	0 (0%)
	Some secondary/high school	0 (0%)	1 (1%)
	Blank	3 (7%)	0 (0%)

3.3 Survey Protocol

An identical survey was deployed to the privacy expert sample and to the laypersons' sample. The survey included both closed- and open-ended questions to allow both for systematic numeric reports of things like technology use frequency and for respondents to express details about their privacy technology use, privacy behaviors, and motivations.

The survey began with an explanation that we were interested in technology use related to privacy: *the purpose of this survey is to understand what technologies you and other people use to protect your privacy while using computers, phones, and other electronic devices.* We intentionally did not define privacy for participants or introduce the term "privacy enhancing technology" in order to allow participants to articulate their understandings through their responses and examples of technologies. The survey included an initial semi-open portion that asked participants to freely list technologies they are familiar with in multiple categories: browsers with special features like ad-blockers, pop-up blockers, or private browsing mode, anonymous browsers, privacy-enhancing search engines, encrypted communications, and other privacy technologies. These categories were derived from both scholarly and popular articles that listed types of privacy-enhancing technologies to establish a baseline with which to compare expert and layperson responses. In the first question we asked "Which of the following types of technologies are you familiar with? please provide as many examples that you can think of (leave blank if don't know of any)." For each category mentioned above, we asked them to provide up to three examples of technologies they are familiar with. The participants' answers were then piped

and used in follow-up questions about the frequency of and motivations for using the technologies they cited. Respondents were also asked about the technologies they avoid to protect their privacy and any other ways they protect their privacy online. The survey concluded with a short demographic section about gender, age, and education level. With the exception of the two questions verifying eligibility, answering any question was not obligatory.

3.4 Data Analysis

The expert and layperson data were first analyzed separately in the same manner. We designed the study not to enable making statistical inferences about differences between the practices of the two participant groups, but rather to offer descriptions of the practices employed by each sample. Thus, data from close-ended questions were analyzed using descriptive statistics as a way of providing insights about the practices described. The answers to open-ended questions, on the other hand, were analyzed using thematic analysis [10] to examine differences in the ways participants wrote about privacy and their practices. We identified themes by coding the data line-by-line [9]. Thematic analysis goes beyond identifying and counting occurrences of words or phrases to identifying implicit ideas [28]. The first and second authors used Dedoose to collaboratively code the data. Each of the coders independently coded the data and then discussed discrepancies to converge on a shared understanding and codebook. Multiple coders were used, not to verify their correctness, but to facilitate a critical process and strengthen the conceptual integrity of the codes [39]. All the authors repeatedly discussed themes identified in the data and connections among them. The first and second authors then worked together on collapsing themes into affinity groups [6]. For instance, privacy-related motivations for using privacy technologies were grouped together separately from non-privacy-related motivations. After coding and affinity grouping data from the expert and layperson data sets separately, the findings from each were compared and further analyzed to identify differences and commonalities. We report our findings about both samples' privacy-enhancing technologies use and privacy behaviors in the next section.

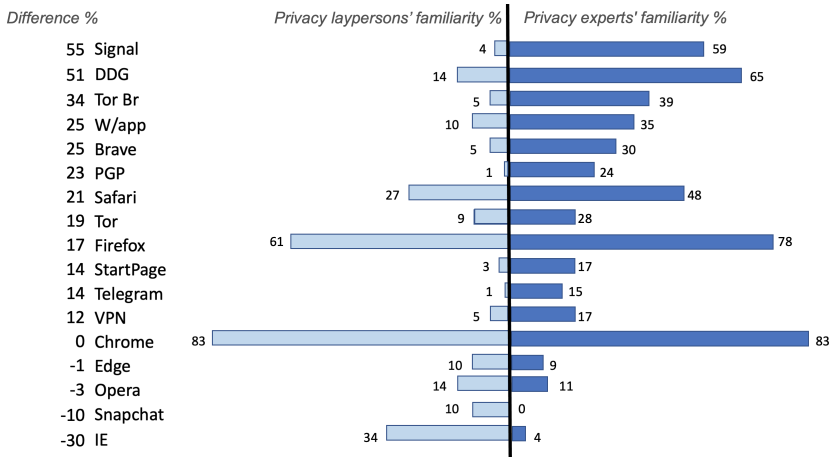
4 Findings

The themes that emerged from analysis of survey data describe reported use of privacy-enhancing technologies and behaviors among privacy experts and laypersons in our sample. First, to aid comparisons, we identify a list of PETs mentioned by both samples.

The lists of technologies identified by privacy experts and laypersons included 29 common technologies. The expert sample further identified 40 technologies that were not mentioned by the laypersons, and the laypersons cited 51 technologies that were not mentioned by the experts. Most of these technologies were only cited once or twice.

To make a comparative analysis more tractable and to address unevenness of sample size, we focus only on the technologies that are mentioned by at least 10% of either sample. The list includes 16 technologies, 15 of which were mentioned at least once by both groups of respondents (See Figure 1). In the sections below we examine qualitative differences between the technologies reported by each group.

Fig. 1. Percent of privacy experts and laypersons who mentioned each PET, ordered by difference in percent between the two samples.



The remainder of this section uses these lists of technologies to analyze: PETs named by each sample; frequency of use; various classes of PETs; classifications of PETs; technologies respondents seek out, as well as technologies they avoid; respondents' motivations for using PETs; and other reported privacy strategies.

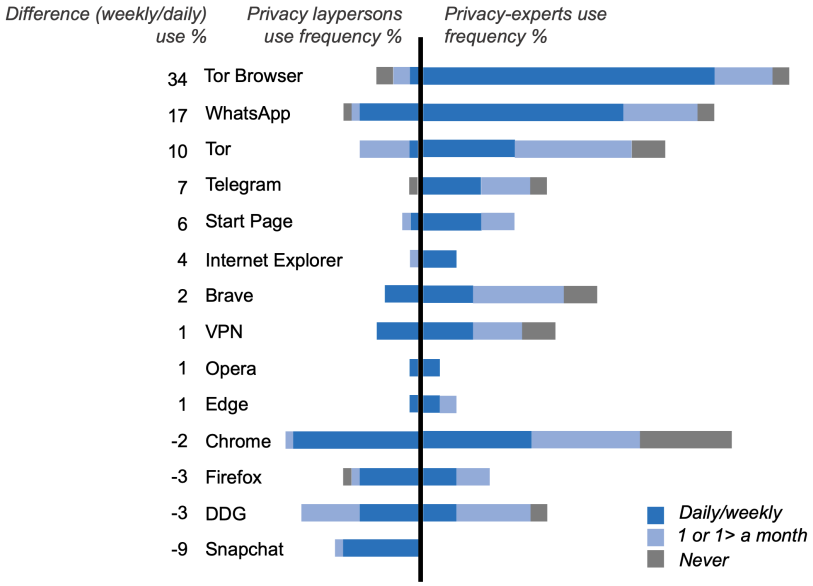
4.1 Reported PETs and Frequency of Use

As a first point of comparison, the technologies that laypersons reported using tend to advertise main functions other than privacy protection—for example, Snapchat. Snapchat's website emphasizes creativity, social connection, and self-expression, proclaiming that "Snapchat is a camera... that is connected to your friends."[5] On the other hand, experts' reported technology use emphasized technologies that promote privacy protection as a primary function such as Tor or Signal. In comparison to Snapchat, Signal is a chat app that promotes itself first as a privacy tool; the website proclaims that "Signal is the most scalable encryption tool we have" and includes an endorsement from Edward Snowden[6].

[5] https://whatis.snapchat.com accessed 9/15/2022
[6] https://www.signal.org/ accessed 9/15/2022

Use frequency data reinforces this finding about privacy as a primary or secondary feature of the technologies cited by both samples (see Figure 2). For example, the biggest discrepancies in daily/weekly reported use by experts vs laypersons were Tor Browser, Whatsapp, and Telegram, all of which advertise privacy as a central feature. Snapchat was not cited by any expert.

Fig. 2. Frequency of PET use reported by experts and laypersons.



Survey respondents were prompted to list examples of PETS in different categories, such as web browsers, encrypted communications tools, or anonymous browsers. Categories are powerful indicators of meaning [8] and the ways respondents categorized PETs reflect the ways they conceptualize the tools. We noted that the way experts categorized technologies reflected their expert understanding of the common traits of different technologies.

Recall that 29 technologies were listed by both the expert and laypersons' sample; however, the two samples frequently diverged in their categorization of technologies on this shared list. In some cases there was agreement, for instance, most experts and laypersons agreed that WhatsApp is an encrypted communication technology and DuckDuckGo is a privacy-enhancing search engine. On the other hand, some technologies were categorized differently. For example, Chrome is categorized by experts as a web browser while the laypersons' categorization of Chrome included anonymous browser, encrypted communication, and privacy-enhancing search engine in addition to web browser. Brave was categorized by experts as either an anonymous browser or web browser, but laypersons additionally categorized it as a privacy-enhancing search engine.

4.2 Technologies Sought Out and Technologies Avoided

The divergence of expert and layperson perceptions of PETs also manifests in the technologies they reported avoiding or seeking to protect their privacy. We extracted lists of technologies sought out and avoided from open-ended responses (see Table 2 and Table 3).

Table 2. Technologies avoided.

Expert		Common	Layperson
Google Chrome	Cloud storage	Amazon Echo	Bitly
Tinder	Credit cards	Facebook	Capital One
Twitter	Epic Games Launcher	Siri	Instagram
Venmo	File sharing websites	Social networks	Internet Explorer
Voice Assistant	Fitness trackers		URL shortener
Wifi; public/shared	Game/casino websites		Link manager
Windows OS	Google Home		Public computers
Smart devices/IoT	Google search		Ring doorbell
Laptop/cell phone cameras	Amazon.com		USAA
Apps which collect data	LinkedIn		
Centralized messaging apps	Personal assistants		
Closed-source software/hardware			

Table 3. Technologies sought out.

Expert	Common	Layperson
DuckDuckGo	Ad blockers	Laptop encryption
Instagram stories	Two-factor authentication	Security apps for mobile
Open source software	Virtual private networks	Norton
Password generator		PayPal
Protonmail		
Telegram		
Tor browser		
Tor		
Ublock		

We also coded answers related to what technologies people reported avoiding and/or seeking out. For instance, in the case where a participant mentions that they use technology ‘x’ or they try to avoid technology ‘y’.

Affinity diagramming for the technologies avoided show that both groups avoid some IoT technologies such as Echo and Alexa, social media platforms such as Facebook, banking technologies such as credit cards and “capitalone”, shared public platforms such as WiFi or computers, certain browsers and certain websites. However, experts report a greater number of technologies they avoid.

The smaller sample of 46 privacy experts group generated 33 responses describing 51 unique technologies avoided. The larger sample of 77 laypersons yielded only 30 responses and 19 unique technologies avoided. Note that when multiple services were listed (Google home, Google search) or both concrete examples (Amazon Echo) and the concomitant abstract categories (Voice assistant), these were counted separately.

Abstract categories were unique to the expert list. A number of privacy experts listed Internet of Things (IoT), voice assistants, and personal assistants as entire categories of things to be avoided. In contrast, the layperson list included concrete examples of IoT technologies like "Ring Doorbell" or "Amazon Echo" but did not identify classes of things to be avoided, with the exception of "social media". Similarly, avoiding credit cards appears on the expert list, whereas laypersons listed specific banks but not credit cards in general. The presence of abstractions suggests that experts understand of privacy threats underlying their avoidance of specific technologies, whereas laypersons did not signal this same understanding.

Participants were asked to describe strategies they use to protect their privacy in an open-ended question. Responses to all open-ended questions were coded to identify technologies participants reported seeking out to protect their privacy. The list of technologies above is not expected to be exhaustive but informative and can prompt insights about some of the technologies both groups want to use, try to use, or actually use.

4.3 PETs use motivation

For each technology they reported using, survey respondents were asked why they used it. The reported motivations for PETs use show that experts' main reasons for using PETs are privacy centered whereas laypersons' motivations are often not privacy related.

Affinity diagramming for the coded motivation responses revealed four main themes of motivations. Some categories overlap. For instance "privately doing things" overlaps with "avoiding tracking" since one might avoid tracking in order to do something privately, however, we used participants' explanations to differentiate A. purposeful efforts to maintain privacy during specific activities in order to conceal those activities from B. avoiding tracking as a general practice for all activities as a defensive measure against surveillance. Below we explain them with more details and quotes from the data. Here we refer to an expert participant as 'E' and a layperson participant as 'L'.

- **Avoiding things: such as not be tracked, malware, cookies, surveillance, history data.** For example, E46 reported using private browsing mode to avoid creating a digital profile based on previous searches. She wrote: *"searching for things i would not like to have in my digital profile (for example buying pregnancy clothes for my sister in law. i don't want my entire amazon recommendations to be around pregnancy)."* Similarly, L66 reported using private browsing mode to avoid leaving a history that could be tracked.

He reported: *"Private browsing protects you from people with access to your computer snooping at your browsing history – your browser won't leave any tracks on your computer. It also prevents websites from using cookies stored on your computer to track your visits."*

- **Protecting things: such as password, email, financial information, anonymity.** In some cases, although privacy experts and laypersons may share the same motivation, the technology they use to achieve privacy differs. E6 reported using StartPage to protect personal information. He stated: *"Routine protection from sharing too many personally-attributed interests with major search engine companies."* Similarly, E39 uses OpenPGP to protect his email: *"to keep my mails confidential. mostly through autocrypt. I try to encrypt everything from trivial mails to confidential ones."* On the other hand, L29 mentions using Chrome to protect their information: *"It is very secure for me to search the internet without worrying leak of information."*
- **Privately doing things: such as private communication, illegally downloading movies, accessing suspicious websites, and searching about people.** As noted, while "privately doing things" seems to be similar to "avoiding being tracked," the coding of these instances reflects the expressions of the participants, which emphasize keeping specific actions out of sight rather than potential aggregate tracking threats. For example, E23 mentions using Tor to download illegal movies so that his identity cannot be connected with that specific action but does not describe using it as a general practice to avoid tracking.
- **Other non-privacy motivations: better experience, required, fun, curiosity and default.** Both groups mentioned a better browsing experience, fun, convenience, popularity, curiosity and the fact that the technology is either default or required to interact with some of their social connections. The latter motivation appears frequently in the data and reflects the impact of the social aspects of PETs adoption and use. For example E46 uses Signal because it was required by a friend. She reported: *"some of my friends are quite serious about their privacy so they only use signal for chatting and i downloaded it particularly for them. i also once had a friend who shared very serious and private info about themselves and used a fake account on signal in case i decided to somehow take screenshots or show anyone this content then they could claim it is not theirs."* L46 used DuckDuckGo just to try it out. She mentions: *"I tried it out when I first heard about it a couple of years ago but prefer Google Chrome."*. L60 uses Brave and says: "It pays you."

As demonstrated in the excerpts above, privacy experts and laypersons reported some common motivations for using PETs. Some of these motivations are privacy related and some others are not. Both groups reported using PETs to **avoid** malware, being tracked, accepting cookies, and personal data collection, to **protect** passwords, email, and other personal information and to privately **do things** such as communicating with others.

While experts mentioned some non-privacy-related motivations such as fun and curiosity, their list of privacy-related motivations was more detailed and

extensive and included technical features of online interaction, such as hiding their network address, accessing multiple accounts, avoiding having metadata known about them, blocking scripts, accessing prohibited content, and searching sensitive topics. Laypersons often used generic terms to describe motivations such as keeping activities private, communicating, protecting privacy and personal reasons like "it is good," "it pays you," or "I like it."

4.4 Other Privacy Strategies

Affinity diagramming of the data showed privacy behavior similarities at the level of general overarching themes but we noted differences between the two samples in some specific behaviors. The overarching themes include:

- Being aware and checking behaviors: such as being aware of data shared with others and checking links before clicking.
- Limiting/avoiding certain behaviors: limiting personal data shared, social media logins/use. data retention.
- Deleting/disabling behaviors:turning off/not using location-based services, deleting/managing cookies
- Using fake/disposable/different identifiers: such as emails, personal information, user names
- Managing passwords: not reusing important passwords, using password managers or generators
- Using physical privacy devices: device camera covers and privacy screens

Privacy behaviors reported by laypersons are practices that we interpret to be general practices that are well-known and widely advocated such as limiting social media use, device use, and data sharing. The experts' behaviors on the other hand included more idiosyncratic and resource-intensive practices that required more time and attention. Some experts reported going beyond limiting social media use, device use, and data sharing to limiting internet and technology use in general. In addition, some privacy experts mentioned more complicated and detailed strategies such as: opening Facebook and Linkedin incognito with no other websites open at the same time, intentionally engaging in inconsistent use behavior, and using their own server for services.

Although the sample of experts is smaller than the layperson sample (46 privacy experts vs 77 laypersons), the data generated by privacy experts sample includes more privacy behaviors (34) compared to the number of privacy behaviors generated by the layperson sample (24).

5 Discussion and Implications

The above analysis suggests that privacy experts and laypersons have different styles of reasoning and approach privacy issues differently; experts conceive of PETs as technologies whose primary function is protecting or enhancing privacy

or that are promoted as such. Laypersons, in contrast, think of privacy enhancement as an add-on functionality to tools like browsers, chat applications, and websites. This discussion compares our main finding with results from the related literature and then considers the finding's implication for future work.

5.1 Comparison with Prior Work

Technical vs. Heuristic Understanding of PETs In many of the differences described above, the expert sample often demonstrated a more technical understanding of PETs and attended to specific implementation details thereof. In contrast, the laypersons tended to apply heuristic reasoning in determining which tools and practices enhanced (or reduced) their privacy. For example, as described above (Section 4.2), laypersons described avoiding individual products or companies (e.g., Capital One, Internet Explorer), while experts described avoiding more broad categories of technologies defined by some common technical detail (e.g., public or shared Wifi, "smart" IoT devices, fitness trackers). Similarly, in the motivations described above (Section 4.3), respondents from the expert sample described strategies that reveal an understanding of how data are aggregated and analyzed, e.g., not "sharing too many personally attributed interests with major search engine companies." In contrast, respondents from the layperson sample made higher level statements, such as describing Chrome as being "very secure [...] without worrying leak of information."

Such differences align somewhat with work by Gallagher et al. [23] on the Tor anonymity system. They found that experts have a deeper understanding of Tor's underlying architecture and focused on the technical details of Tor's operations– similar to our findings about experts' engagement with more technical details–, while laypersons were more likely to situate Tor within a broader sociotechnical landscape. Also the work by [41] on laypersons and privacy experts suggests that experts were more likely to illustrate more nuanced data privacy spaces and control over information than laypersons. While the work by [23] focused only on comparing the use of Tor by laypersons and experts, our study considers all the salient technologies to the experts and laypersons as well as reported privacy behaviors. In addition, contrary to the [41] study that focused on how privacy is defined, our focus is to learn about what PETs are for each sample.

This finding raises questions about the role of expertise in informing everyday privacy practices. We have discussed literature that frames privacy practices as outcomes of experiences of violation [32] or need [3, 37, 54] as opposed to reflecting a particular level of "literacy" [23]; yet, our findings in this survey suggest that privacy experts' practices differ from those of laypersons. Specifically, experts more often attended to the technical details of such systems, while laypersons applied higher level heuristic reasoning. While perhaps unsurprising, given the respective backgrounds of these two samples, this difference also highlights a key point. Experts do not simply have *more knowledge* or a *better understanding* of PETs than laypersons; rather, the two samples in this study demonstrated fundamentally *different styles* of reasoning about their privacy. This is not to say that expertise is irrelevant. Expertise matters, but perhaps

not in the ways that we might expect. For instance, experts and laypersons may differ in the ways that their PETs use is influenced by the PETs used in their social network. Indeed, such differences represent an important area for future work.

Difficult User Experience vs. Good User Experience Based on the findings about use motivations that show some laypersons use technologies because they are user friendly or avoid using other technologies because they have usability issues, we understand that the UX of PETs impact their use. The PETs that our expert respondents reported more use of appear to require more dedicated attention and technology skills. Concerns about the relationship between privacy and usability are a perennial topic; indeed an entire conference, the *Symposium on Usable Privacy and Security*, is dedicated to addressing the problem of unusable privacy and security tools. In our sample, experts were far more likely to use Tor browser, an open source project that has long-documented usability weaknesses [17, 36, 21] than, for example, Internet Explorer, which (despite ubiquitous grumblings about all browsers' failings) is designed to be a general-use consumer product. In the same vein, privacy behaviors reported by laypersons seem to be popular and widely-advocated (e.g., strong password, consideration of audience). On the other hand, the privacy behaviors that are reported by the experts are complex in that they require multiple steps and prerequisite knowledge.

What might entice people to overcome the barriers associated with a more difficult user experience? We found that experts and laypersons alike reported social interaction as a motivation for adopting privacy enhancing technologies. Some participants adopted PETS because a heightened level of privacy protection was required by a more concerned or more vulnerable social contact. This suggests that privacy may have a transitive property and that communication and collaboration technologies in particular occupy an important design space for privacy-enhancing technologies.

Privacy: Primary Concern vs. Afterthought The survey data show that experts are more likely to approach privacy as a primary concern, while laypersons tend to think about other aspects first and then later consider privacy. This is evidenced by the salient technologies for each sample, their reported frequency of using them, as well as each sample's reported motivations for that usage. The experts reported they are mostly familiar with Signal, Tor browser, Brave, Tor, VPN, and StartPage, all of which include privacy enhancement as a primary function. In contrast, the laypersons reported that they are mostly familiar with Internet Explorer, Snapchat, and Edge, which do not place as much emphasis on privacy. The use frequency reveals similar findings as the laypersons use Chrome, Snapchat, and Firefox more frequently while the experts report use of Tor browser/Tor more often.

This distinction is only partly a question of the technology itself and how it is presented to users. For instance, a technology such as PGP is first and

foremost a privacy technology, whereas a technology such as Chrome is first and foremost a web browser. However, examples such as the Tor browser, which foregrounds privacy while having the primary function of browsing the web, end up in a blurry middle. Similar points could be raised about Signal (a messaging app that foregrounds privacy) or DuckDuckGo (a search engine that foregrounds privacy).

Instead, the distinction to be made here revolves around how users *conceive of* these technologies. The qualitative analysis of open-ended responses makes it clear that the privacy experts in our sample conceive of certain technologies being first and foremost about protecting their privacy. In contrast, the laypersons in our sample are more likely to conceive of privacy as an added feature included in another technology they are already using.

These findings highlight how the definition of PETs in the literature does not align with privacy laypersons' use and perceptions of PETs, but with the experts'. PETs are for "protecting personal identity" [12], "protecting or enhancing an individual's privacy," and "minimizing the collection and use of personal data" [47]. Privacy experts perceive PETs as technologies where privacy protection/enhancement is the primary function. The laypersons' sample, in contrast, often describes other kinds of technologies as PETs, particularly those where privacy protection/enhancement is a secondary or tertiary function.

5.2 Implication: Privacy protection as an embedded feature in everyday life technologies.

Our grounded data examines which technologies are salient to privacy experts and laypersons and shows which technologies and practices for enhancing privacy are used. It reveals that privacy experts and laypersons conceive of PETs somewhat differently. In the expert sample, PETs are reported to be technologies that are designed for privacy purposes primarily, whereas laypersons define PETs as technologies that help them achieve their tasks but have privacy as a secondary or tertiary function. Furthermore, our findings about use motivations show that some laypersons use technologies because they are user friendly while avoiding other technologies because they have usability issues.

At least two possible interpretations could account for this finding, each with slightly different implications. First, this finding aligns with other studies showing that a difficult UX is one justification for why laypersons do not use PETs [53, 48, 17, 45, 22]. This finding also builds on that prior work by suggesting that usability issues are more of a deterrent for laypersons than they are for experts. This interpretation suggests that designers prioritize the usability and UX of technologies whose primary function is privacy protection. Second, another possible interpretation is that laypersons simply do not know about the privacy dedicated technologies, either because they do not know other people using them or because such technologies were never advertised to them. This interpretation suggests that energy be put into information dissemination efforts.

An alternative strategy could address either of these interpretations. Whether laypersons do not know about privacy dedicated technologies or have difficulty

using them, laypersons could be served by designing privacy in the technologies they use in their everyday life. Goldberg posits that:

> In order for a technology to be useful, it must be possible for everyday users doing everyday things to obtain it and benefit from it. This means it needs to be compatible with their preferred operating system, their preferred web browser, their preferred instant messaging client, and so on. Ideally, the technology would be built right in so that the user doesn't even need to find and install separate software packages. [26, p. 15]

Our findings add emphasis to Goldberg's assertion. Not only would such an arrangement be *ideal* for the uptake of technologies with strong privacy protections. Rather, these findings suggest having PETs "built right in" may be *necessary* for them to be adopted by a diverse user base whose expertise lies outside the field of privacy.

Thus, we suggest that designers of Internet tools should be aware of the privacy needs and desires of users and embed privacy features that would help them protect their privacy. By using that approach, users do not need to take extra steps to explore, to understand, and to learn about privacy and privacy tools.

6 Limitations and Conclusion

This study's findings are grounded in the data collected via two identical surveys, one addressed to privacy experts and one to laypersons.

Most of this study's limitations revolve around data collection. For example, our data rely on participants self-reporting their behaviors. Some participants might experience "social desirability bias and thus may over report their behavior," [19] while other participants may forget or misrepresent their behavior. Other limitations pertain to our sampling procedures. For example, we do not know if our laypersons' sample includes some privacy experts. Additionally, demographically matching the laypersons' sample and the expert sample resulted in participants with PhDs being dramatically over-represented among laypersons. Although higher education levels have been correlated with higher levels of privacy concern [46], the effect of oversampling high academic achievement among the laypersons' sample on practices and strategies is not known. Furthermore, our expert sample includes a few international respondents, but the laypersons all reside in the U.S. We do not know what cultural differences might be at play; for example, some experts from Europe may have reported using technologies that are popular in Europe but relatively unknown in the U.S and vice versa. We believe the international character of the privacy research community mitigates some of this concern since the privacy experts were recruited based on their participation in conferences that annually publish and meet together. Importantly, in the survey instruments, we provided an example of categories of technology we wanted to prompt people to name and describe, including Tor

for "anonymous browser," Snapchat for "encrypted communication," and DuckDuckGo for "privacy-enhancing search engine." It is notable that, although the presence of these illustrative examples could have triggered additional mentions of them in the data, there is no obvious indication that the example technologies are over represented. For instance, despite being used as an example, Snapchat was mentioned by no experts as an example of encrypted communication. While this might suggest a limitation in the sense that the examples primed the participants, the variety of responses that we got back suggests that respondents were not constrained by the examples that we provided. The same survey questions were administered to both samples and each sample came up with different technologies.

Our findings revealed that both experts and laypersons share some technical approaches (technology use) and operational approaches (privacy behaviors) to protect their privacy. However, they have different reasoning styles. The way each sample conceives of privacy-enhancing technologies differs according to which technologies they use and for what motivations. Our data reveal that privacy experts leverage their technical understanding of technologies to inform use of technologies and strategies that are complex, have a difficult UX, and have a primary function of privacy protection. For the laypersons, privacy is sought through technologies that have privacy as a secondary or tertiary function. Finally, experts were more likely to report technologies they avoid and avoidance strategies and to link them to abstract categories which suggests they understand threats underlying their avoidance of specific technologies. We conclude by underscoring opportunities for technology designers to embed privacy features in the design of everyday life technologies to serve a wider cross-section of people.

Acknowledgements This material is based on work supported in part by the NSF under Grants No. CNS-1814533 and CNS-1816264.

Bibliography

[1] Acquisti, A., Taylor, C., Wagman, L.: The economics of privacy. Journal of economic Literature **54**(2), 442–92 (2016)

[2] Ahern, S., Eckles, D., Good, N.S., King, S., Naaman, M., Nair, R.: Over-exposed? privacy patterns and considerations in online and mobile photo sharing. In: Proceedings of the SIGCHI conference on Human factors in computing systems. pp. 357–366 (2007)

[3] Ames, M.G., Go, J., Kaye, J., Spasojevic, M.: Understanding technology choices and values through social class. In: Proceedings of the ACM 2011 conference on Computer supported cooperative work. pp. 55–64 (2011)

[4] Andalibi, N., Haimson, O.L., De Choudhury, M., Forte, A.: Understanding social media disclosures of sexual abuse through the lenses of support seeking and anonymity. In: Proceedings of the 2016 CHI conference on human factors in computing systems. pp. 3906–3918 (2016)

[5] Baumer, E.P., Forte, A.: Undoing the privacy paradox with data styles (2017)

[6] Beyer, H., Holtzblatt, K.: Contextual design. interactions **6**(1), 32–42 (1999)

[7] Borking, J.J.: Why adopting privacy enhancing technologies (pets) takes so much time. In: Computers, privacy and data protection: an element of choice, pp. 309–341. Springer (2011)

[8] Bowker, G.C., Star, S.L.: Sorting things out: Classification and its consequences. MIT press (2000)

[9] Boyatzis, R.E.: Transforming qualitative information: Thematic analysis and code development. sage (1998)

[10] Braun, V., Clarke, V.: Using thematic analysis in psychology. Qualitative research in psychology **3**(2), 77–101 (2006)

[11] Brennan, M., Afroz, S., Greenstadt, R.: Adversarial stylometry: Circumventing authorship recognition to preserve privacy and anonymity. ACM Transactions on Information and System Security (TISSEC) **15**(3), 1–22 (2012)

[12] Burkert, H., et al.: Privacy-enhancing technologies: Typology, critique, vision. Technology and privacy: The new landscape pp. 125–142 (1997)

[13] Busse, K., Schäfer, J., Smith, M.: Replication: No one can hack my mind revisiting a study on expert and non-expert security practices and advice. In: Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019). pp. 117–136 (2019)

[14] Caulfield, T., Ioannidis, C., Pym, D.: On the adoption of privacy-enhancing technologies. In: International Conference on Decision and Game Theory for Security. pp. 175–194. Springer (2016)

[15] Caulfield, T., Ioannidis, C., Pym, D.: On the adoption of privacy-enhancing technologies. In: Zhu, Q., Alpcan, T., Panaousis, E., Tambe, M., Casey, W. (eds.) Decision and Game Theory for Security, vol. 9996, pp. 175–194.

Springer International Publishing (2016). https://doi.org/10.1007/978-3-319-47413-7_11, http://link.springer.com/10.1007/978-3-319-47413-7$_1$1, $seriesTitle$: $LectureNotesinComputerScience$

[16] Chua, W.Y., Chang, K.T.T., Wan, M.P.H.: Information privacy concerns among novice and expert users of solomo. In: PACIS (2014)

[17] Clark, J., Van Oorschot, P.C., Adams, C.: Usability of anonymous web browsing: an examination of tor interfaces and deployability. In: Proceedings of the 3rd symposium on Usable privacy and security. pp. 41–51 (2007)

[18] Evangelho, J.: Why you should ditch google search and use duckduckgo. Forbes (2018)

[19] Fisher, R.J.: Social desirability bias and the validity of indirect questioning. Journal of consumer research **20**(2), 303–315 (1993)

[20] Forte, A., Andalibi, N., Greenstadt, R.: Privacy, anonymity, and perceived risk in open collaboration: A study of tor users and wikipedians. In: Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing. pp. 1800–1811 (2017)

[21] Gallagher, K.: Measurement and Improvement of the Tor User Experience. Ph.D. thesis, New York University Tandon School of Engineering (2020)

[22] Gallagher, K., Patil, S., Dolan-Gavitt, B., McCoy, D., Memon, N.: Peeling the onion's user experience layer: Examining naturalistic use of the tor browser. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. pp. 1290–1305 (2018)

[23] Gallagher, K., Patil, S., Memon, N.: New me: Understanding expert and non-expert perceptions and usage of the tor anonymity network. In: Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017). pp. 385–398 (2017)

[24] Garg, V., Camp, J.: Heuristics and biases: implications for security design. IEEE Technology and Society Magazine **32**(1), 73–79 (2013)

[25] Gobet, F., Ereku, M.H.: What Is Expertise? Psychology Today (Feb 2016)

[26] Goldberg, I.: Privacy-enhancing technologies for the internet, ii: Five years later. In: International Workshop on Privacy Enhancing Technologies. pp. 1–12. Springer (2002)

[27] Goldberg, I., Wagner, D., Brewer, E.: Privacy-enhancing technologies for the internet. In: Proceedings IEEE COMPCON 97. Digest of Papers. pp. 103–109. IEEE (1997)

[28] Guest, G., MacQueen, K.M., Namey, E.E.: Applied thematic analysis. Sage Publications (2011)

[29] Harborth, D., Pape, S., Rannenberg, K.: Explaining the technology use behavior of privacy-enhancing technologies: The case of tor and jondonym. Proceedings on Privacy Enhancing Technologies **2020**(2), 111–128 (2020)

[30] Hargittai, E., Marwick, A.: "what can i really do?" explaining the privacy paradox with online apathy. International Journal of Communication **10**, 21 (2016)

[31] Ion, I., Reeder, R., Consolvo, S.: "... no one can hack my mind": Comparing expert and non-expert security practices. In: Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015). pp. 327–346 (2015)

[32] Kang, R., Dabbish, L., Fruchter, N., Kiesler, S.: "my data just goes everywhere:" user mental models of the internet and implications for privacy and security.

In: Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015). pp. 39–52 (2015)
[33] Kokolakis, S.: Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon **64**, 122–134 (2017). https://doi.org/10.1016/j.cose.2015.07.002, https://linkinghub.elsevier.com/retrieve/pii/S0167404815001017
[34] Lampinen, A., Tamminen, S., Oulasvirta, A.: All my people right here, right now: Management of group co-presence on a social networking site. In: Proceedings of the ACM 2009 international conference on Supporting group work. pp. 281–290 (2009)
[35] Leavitt, A.: " this is a throwaway account" temporary technical identities and perceptions of anonymity in a massive online community. In: Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing. pp. 317–327 (2015)
[36] Lee, L., Fifield, D., Malkin, N., Iyer, G., Egelman, S., Wagner, D.: A usability evaluation of tor launcher. Proceedings on Privacy Enhancing Technologies **2017**(3), 90–109 (2017)
[37] Marwick, A., Fontaine, C., Boyd, D.: "nobody sees it, nobody gets mad": Social media, privacy, and personal responsibility among low-ses youth. Social Media+ Society **3**(2), 2056305117710455 (2017)
[38] McDonald, N., Forte, A.: The politics of privacy theories: Moving from norms to vulnerabilities. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. pp. 1–14 (2020)
[39] McDonald, N., Schoenebeck, S., Forte, A.: Reliability and inter-rater reliability in qualitative research: Norms and guidelines for cscw and hci practice. Proc. ACM Hum.-Comput. Interact. **3**(CSCW) (Nov 2019). https://doi.org/10.1145/3359174, https://doi.org/10.1145/3359174
[40] Mulligan, D.K., Koopman, C., Doty, N.: Privacy is an essentially contested concept: A multi-dimensional analytic for mapping privacy. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences **374**(2083), 20160118 (Dec 2016). https://doi.org/10.1098/rsta.2016.0118
[41] Oates, M., Ahmadullah, Y., Marsh, A., Swoopes, C., Zhang, S., Balebako, R., Cranor, L.F.: Turtles, locks, and bathrooms: Understanding mental models of privacy through illustration **2018**(4) (2018), https://content.sciendo.com/view/journals/popets/2018/4/article-p5.xml, place: Berlin Publisher: Sciendo
[42] Phelan, C., Lampe, C., Resnick, P.: It's creepy, but it doesn't bother me. In: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems. pp. 5240–5251 (2016)
[43] Posner, R.A.: The economics of privacy. The American economic review **71**(2), 405–409 (1981)
[44] Renaud, K., Volkamer, M., Renkema-Padmos, A.: Why doesn't jane protect her privacy? In: International Symposium on Privacy Enhancing Technologies Symposium. pp. 244–262. Springer (2014)
[45] Ruoti, S., Andersen, J., Zappala, D., Seamons, K.: Why johnny still, still can't encrypt: Evaluating the usability of a modern pgp client. arXiv preprint arXiv:1510.08555 (2015)

[46] Sheehan, K.B.: Toward a typology of internet users and online privacy concerns. The information society **18**(1), 21–32 (2002)
[47] Shen, Y., Pearson, S.: Privacy enhancing technologies: A review. HP Laboratories **2739**, 1–30 (2011)
[48] Sheng, S., Broderick, L., Koranda, C.A., Hyland, J.J.: Why johnny still can't encrypt: evaluating the usability of email encryption software. In: Symposium On Usable Privacy and Security. pp. 3–4. ACM (2006)
[49] Spiekermann, S.: The challenges of privacy by design. Communications of the ACM **55**(7), 38–40 (2012)
[50] Stutzman, F., Hartzog, W.: Boundary regulation in social media. In: Proceedings of the ACM 2012 conference on computer supported cooperative work. pp. 769–778 (2012)
[51] Turner, E.C., Dasgupta, S.: Privacy on the web: An examination of user concerns, technology, and implications for business organizations and individuals. Information Systems Management (2006)
[52] Vemou, K., Karyda, M.: A classification of factors influencing low adoption of pets among sns users. In: International Conference on Trust, Privacy and Security in Digital Business. pp. 74–84. Springer (2013)
[53] Whitten, A., Tygar, J.D.: Why johnny can't encrypt: A usability evaluation of pgp 5.0. In: USENIX Security Symposium. vol. 348, pp. 169–184 (1999)
[54] Yardi, S., Bruckman, A.: Income, race, and class: exploring socioeconomic differences in family technology use. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. pp. 3041–3050 (2012)
[55] Young, A.L., Quan-Haase, A.: Privacy protection strategies on facebook: The internet privacy paradox revisited. Information, Communication & Society **16**(4), 479–500 (2013)
[56] Zabihimayvan, M., Sadeghi, R., Doran, D., Allahyari, M.: A broad evaluation of the tor english content ecosystem. In: Proceedings of the 10th ACM Conference on Web Science. pp. 333–342 (2019)