What are PETs for Privacy Experts and Non-experts?

Houda El mimouni
Drexel University

Erica Racine
Drexel University

Patrick Skeba
Lehigh University

Eric P. S. Baumer
Lehigh University

Andrea Forte
Drexel University

Abstract

This study lays the basis for a grounded explanation of privacy-enhancing technology (PET) use by reporting on a survey of the technologies identified as privacy enhancing by privacy experts and non-experts. Differences between the two samples suggest that experts identify PETs as technologies whose primary function is enhancing privacy, whereas non-experts view privacy enhancement as a supplemental function incorporated into other technologies. This poster describes how such differences can be used to generate insights about future directions for privacy research and design.

1 Introduction

Privacy-enhancing technologies (PETs) are tools designed to help people achieve desired experiences of privacy. The research literature is teeming with examples of frameworks and definitions of privacy attitudes and behaviors that can inform the usable design of privacy and security technologies, but researchers lack an understanding of how people, especially laypersons, determine what counts as a privacy-enhancing technology. Put differently, when asked what they use to help protect their privacy, what technologies do people mention?

To construct an inventory of privacy-enhancing technologies we developed and deployed a survey. We recruited privacy experts by soliciting participants from the PETs and HCI privacy research communities, and we recruited non-experts using a demographically-matched panel procured by Qualtrics. We found that most of the technologies that are popular among non-experts have a primary function that is not privacy protection, whereas technologies cited by experts tend to have privacy protection as their primary function. We discuss our findings and suggest designing for privacy enhancing technologies as a substrate for Internet tools with other primary functions.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2020.
August 9–11, 2020, Boston, MA, USA.

2 Related Work

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 [8, 10], and researchers have used creative methods to understand how laypeople and experts conceptualize privacy [17, 13]. Models have been developed to explain rationales that may guide adoption of PETs [6], and economists have long theorized about the trade-offs involved in making privacy decisions [19, 1]. Unfurling the privacy paradox [3]—when people's stated privacy concerns and real-world behaviors contradict each other—has occupied scholars in many fields. Such work has yielded practical recommendations [20] and applied a variety of theoretical framings [14], including institutional vs. social privacy concerns [24], apathy or lack of control [12], and dual-process theory [18]. In this study, we lay the basis for a grounded explanation of privacy-enhancing technology use by cataloging the technologies identified as privacy enhancing by privacy experts and by non-experts.

2.1 Conceptualizations of privacy

Researchers have offered frameworks for users' conceptualization of privacy as well as potential factors that might influence online privacy behavior. Kang et al. [13] suggest that the experience of privacy violation rather than expertise shapes online privacy practice. In addition, socioeconomic factors may contribute to perceived risks and how people engage with privacy-related technologies [2, 15]. Being poor and/or being a member of other groups that suffer inequality and discrimination can leave certain individuals at higher

risk of privacy violations and susceptible to disproportionate harms [16].

Some research has been done to investigate the differences between experts and non-experts in their conceptualizations of privacy. Oates et al. [17] used a qualitative analysis of 366 illustrations created by laypeople, privacy experts, children, and adults to reveal that many drawings from non-experts displayed a strong distinction between private and public spaces, while drawings from experts were more likely to illustrate more nuanced data privacy spaces and control over information. In an interview study investigating expert and non-expert understandings of the anonymity system Tor [9], experts showed a deeper understanding of Tor's underlying operation and focused more on the technical details of Tor's operations, while non-experts were more likely to situate Tor within a broader sociotechnical landscape. Chua et al. [7] studied 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). These studies point to differences in how experts and novices think about privacy or use specific applications, but none inventoried and examined what experts and non-experts deem to be privacy-enhancements.

2.2 PETs adoption motivations and barriers

Motivations to adopt PETs, as well as potential barriers to using them [4, 22], are also important background for understanding which PETs experts and non-experts adopt. In exploring how consumers choose between competing PETs, Caulfield et al. [6] considered the context in which a technology is used, the attending privacy requirements, the perception of privacy a technology provides, and the relative value of privacy in relation to competing needs. Others have suggested that factors for limited adoption of PETs on social networking sites include lack of awareness, lack of technical skill, the complexity and diversity of risks involved in privacy management, direct and indirect costs, and privacy not being a cultural value [23]. Researchers found usability issues have hindered the widespread adoption of Tor [8, 10].

While models that explore usability issues and motivations can help scholars understand what factors influence decisions, the question remains: What technologies are people familiar with as PETs? Which of those do they use in their daily lives? Do experts and non-experts differ? We set out to understand what makes a technology a PET—not based on scholarly definitions but grounded in everyday practices and perceptions. To address these questions, we inventoried what technologies people report using in their everyday lives to protect their privacy. We compare self-reported tools use to uncover and cast differences into relief, where they can be analyzed and used to generate insights about future directions for PETs design and research.

3 Study Design

To inventory the privacy-enhancing technologies used by both privacy experts and non-experts, we developed and administered a survey via Qualtrics to both groups. This study was approved by the IRB at *anonymous institution(s)*.

3.1 Recruitment

We targeted two groups: privacy experts and privacy non-experts. We aimed for experts at the intersection of human-centered design and privacy enhancing technologies. First, we posted the survey on Twitter using the last author's account, which was retweeted by the official account of the Privacy-Enhancing Technologies Symposium to its following of privacy researchers. Second, we searched for recent publications of members of the CHI 2020 subcommittee on privacy and security, and emailed subcommittee members and their recent co-authors. This recruitment strategy yielded 77 responses in fall (September-October) 2019.

To recruit privacy non-experts, we used the demographic profile of our expert sample to requisition a sample from the general population of survey takers on Qualtrics that reflected our expert sample in terms of age, gender, and education level. We recruited 100 participants from Qualtrics in spring (early March) 2020 and paid a total of $600. 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 177 survey responses (77 experts and 100 non-experts) were collected during the period the surveys were active. From these, we excluded respondents who did not complete or provided nonsensical responses (such as repeating the same strings of text in open ended responses) to a majority of the survey questions. This procedure yielded 46 responses from privacy experts and 77 from non-experts (see Table 1 for demographics for both samples.

3.3 Survey Protocol and Data Analysis

An identical survey was deployed to the expert and non-expert samples. The survey asked participants to list technologies they are familiar with in multiple categories: up to 5 browsers with special features like ad-blockers, pop-up blockers, or private browsing mode, up to 3 anonymous browsers, up to 3 privacy-enhancing search engines, up to 3 encrypted communications, and up to 3 other privacy technologies. Participants were also asked how frequently and why they used each of the technologies they mentioned. They were then asked what technologies they avoid to protect their privacy and any other ways they protect their privacy. The survey included a short

Privacy experts (n=46)	Gender	Man: 22
		Woman: 20
		Not specified: 2
	Age	Min: 22
		Max: 69
		Avg: 35
	Education	Doctorate: 25
		Master: 13
		Bachelor: 4
		Some college/university: 1
		(blank): 3
Privacy non-experts (n=77)	Gender	Man: 39
		Woman: 38
		Not specified: 0
	Age	Min: 22
		Max: 67
		Avg: 36
	Education	Doctorate: 38
		Master: 25
		Bachelor: 13
		Some secondary/high school: 1

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

demographic questionnaire about gender, age, education level, and countries of residence and citizenship.

The analysis presented here uses descriptive statistics to report on the technologies that participants are familiar with and their frequency of use. The analysis of the open-ended questions is ongoing and not reported here.

4 Findings

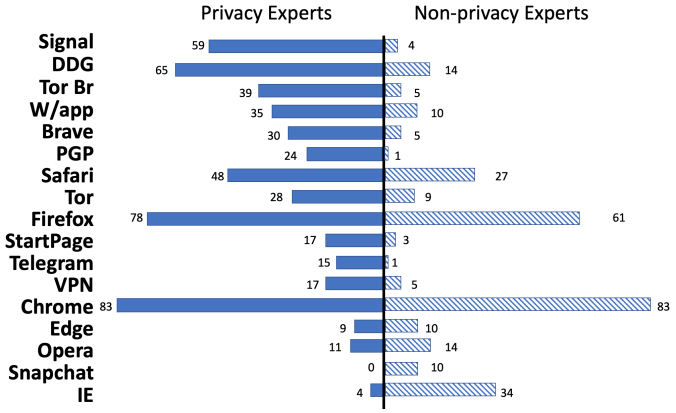
This section reports on PETs identified by expert and non-experts and the frequencies with which participants reported using those PETs. For the purpose of a comparative analysis, we focus only on the technologies that are mentioned by at least 10% of either sample, which yielded 17 different technologies.

Figure 1 shows these 17 technologies, as well as the percentage of each sample that mentioned them. The remainder of this section focuses on differences across the two samples with respect to this set of technologies.

4.1 PETs Familiarity

Most of the technologies that were popular among non-experts advertise main functions other than privacy protection. For example, Snapchat was mentioned by 10% of the non-experts and none of the experts. Snapchat's website emphasizes creativity and self-expression, proclaiming that "Snapchat is a camera" that is connected to your friends[1].

Figure 1: Familiar PETs to privacy experts and non-experts in percent ordered by difference in familiarity



On the other hand, most of the popular technologies cited by experts promote privacy protection as a primary function. For example, Signal was mentioned by 59% of the experts and 4% of the non-experts. Although also a chatting application, Signal promotes itself as a privacy tool; the website proclaims that "Signal is the most scalable encryption tool we have" and includes an endorsement from Edward Snowden[2].

Similar comparisons could be made for many of the technologies that were mentioned more often by one sample than the other (e.g., Internet Explorer vs. Tor Browser).

4.2 PETs frequency of use

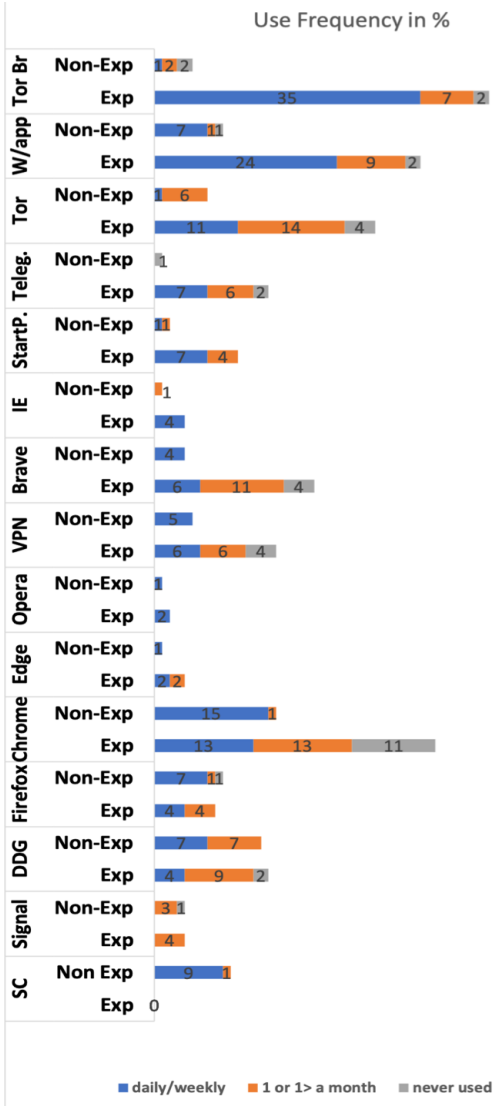
The use frequency data reinforces the above-mentioned finding about primary and secondary functions of the technologies cited by both samples (see Figure 2). For example, the biggest discrepancies in daily/weekly reported use by experts vs non-experts were Tor Browser (35% vs 1%), Whatsapp (24% vs 7%), and Telegram (7% vs 0%), all of which advertise privacy as a central feature. Snapchat was not cited by any expert.

5 Discussion and Implications

The above analysis suggests that experts conceive of PETs as things where the primary function is protecting or enhancing privacy. Non-experts, in contrast, think of PETs as things that have some other primary function but include some sort of privacy-oriented features. This discussion compares our main finding with results from the related literature and then considers the finding's implication for future work.

[1] https://whatis.snapchat.com accessed 5/30/2020
[2] https://www.signal.org/ accessed 5/30/2020

Figure 2: PETs use frequencies ordered by difference of frequency of daily/weekly use



5.1 Privacy as primary function vs. secondary function

Our findings suggest fundamental differences in how experts and non-experts define the term "privacy-enhancing technology." The research literature defines PETs as technologies for "protecting personal identity" [5], "protecting or enhancing an individual's privacy," and "minimizing the collection and use of personal data" [21]. This definition aligns more closely with technologies mentioned more often by the expert sample (e.g., Tor, Duck Duck Go, PGP) than those mentioned more often by the non-expert sample (e.g., Snapchat, Edge). This alignment is perhaps unsurprising, since the recruitment for our expert sample targeted populations likely to be familiar with the PETs literature. Nonetheless, this difference suggests an important locus for future work.

5.2 Privacy protection as an embedded feature in everyday life technologies

Goldberg [11] posited:

> in order for a [privacy-enhancing] 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.

The results presented here provide empirical support for this strategy. Dedicated privacy tools, such as Tor, provide significant utility to a set of expert users. To ensure that PETs are adopted more broadly, designers of Internet tools should also consider embedding robust, sophisticated privacy features in technologies that have some primary function besides privacy enhancement. More broadly applied, these findings suggest a need for privacy-enhancing infrastructures that subsume privacy features at the application layer.

6 Conclusion

Our findings revealed that both experts and non-experts share some familiarity and use of PETs to protect their privacy. However, what each sample defines as a "privacy-enhancing technology" differs. Our data reveal that privacy experts use technologies that have a primary function of privacy protection. For the non-experts, privacy is sought through technologies that have privacy as a secondary or tertiary function. In this way, privacy experts and non-experts construe different technologies as enhancing privacy. We conclude by suggesting that technology designers should embed privacy features in the design of everyday technologies.

Acknowledgments

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

References

[1] Alessandro Acquisti, Curtis Taylor, and Liad Wagman. The economics of privacy. *Journal of economic Literature*, 54(2):442–92, 2016.

[2] Morgan G Ames, Janet Go, Joseph'Jofish' Kaye, and Mirjana Spasojevic. Understanding technology choices

and values through social class. In *Proceedings of the ACM 2011 conference on Computer supported cooperative work*, pages 55–64, 2011.

[3] Susan B. Barnes. A Privacy Paradox: Social Networking in the United States. *First Monday*, 11(9), 2006.

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

[5] Herbert Burkert et al. Privacy-enhancing technologies: Typology, critique, vision. *Technology and privacy: The new landscape*, pages 125–142, 1997.

[6] Tristan Caulfield, Christos Ioannidis, and David Pym. On the adoption of privacy-enhancing technologies. In Quanyan Zhu, Tansu Alpcan, Emmanouil Panaousis, Milind Tambe, and William Casey, editors, *Decision and Game Theory for Security*, volume 9996, pages 175–194. Springer International Publishing, 2016. ISBN 978-3-319-47412-0 978-3-319-47413-7. doi: 10.1007/978-3-319-47413-7_11. URL http://link.springer.com/10.1007/978-3-319-47413-7_11. Series Title: Lecture Notes in Computer Science.

[7] Wen Yong Chua, Klarissa Ting-Ting Chang, and Maffee Peng-Hui Wan. Information privacy concerns among novice and expert users of solomo. In *PACIS*, 2014.

[8] Jeremy Clark, Paul C Van Oorschot, and Carlisle Adams. Usability of anonymous web browsing: an examination of tor interfaces and deployability. In *Proceedings of the 3rd symposium on Usable privacy and security*, pages 41–51, 2007.

[9] Kevin Gallagher, Sameer Patil, and Nasir Memon. 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)*, pages 385–398, 2017.

[10] Kevin Gallagher, Sameer Patil, Brendan Dolan-Gavitt, Damon McCoy, and Nasir Memon. 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*, pages 1290–1305, 2018.

[11] Ian Goldberg. Privacy-enhancing technologies for the internet, ii: Five years later. In *International Workshop on Privacy Enhancing Technologies*, pages 1–12. Springer, 2002.

[12] Eszter Hargittai and Alice Marwick. "what can i really do?" explaining the privacy paradox with online apathy. *International Journal of Communication*, 10:21, 2016.

[13] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. "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)*, pages 39–52, 2015.

[14] Spyros Kokolakis. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. 64:122–134, 2017. ISSN 01674048. doi: 10.1016/j.cose.2015.07.002. URL https://linkinghub.elsevier.com/retrieve/pii/S0167404815001017.

[15] Alice Marwick, Claire Fontaine, and Danah Boyd. "nobody sees it, nobody gets mad": Social media, privacy, and personal responsibility among low-ses youth. *Social Media+ Society*, 3(2):2056305117710455, 2017.

[16] Nora McDonald and Andrea Forte. The politics of privacy theories: Moving from norms to vulnerabilities. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2020.

[17] Maggie Oates, Yama Ahmadullah, Abigail Marsh, Chelse Swoopes, Shikun Zhang, Rebecca Balebako, and Lorrie Faith Cranor. Turtles, locks, and bathrooms: Understanding mental models of privacy through illustration. 2018(4), 2018. URL https://content.sciendo.com/view/journals/popets/2018/4/article-p5.xml. Place: Berlin Publisher: Sciendo.

[18] Chanda Phelan, Cliff Lampe, and Paul Resnick. It's creepy, but it doesn't bother me. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 5240–5251, 2016.

[19] Richard A Posner. The economics of privacy. *The American economic review*, 71(2):405–409, 1981.

[20] Ashwini Rao, Florian Schaub, Norman Sadeh, Alessandro Acquisti, and Ruogu Kang. Expecting the unexpected: Understanding mismatched privacy expectations online. In *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*, pages 77–96, 2016.

[21] Yun Shen and Siani Pearson. Privacy enhancing technologies: A review. *HP Laboratories*, 2739:1–30, 2011.

[22] Sarah Spiekermann. The challenges of privacy by design. *Communications of the ACM*, 55(7):38–40, 2012.

[23] Konstantina Vemou and Maria Karyda. A classification of factors influencing low adoption of pets among sns users. In *International Conference on Trust, Privacy and Security in Digital Business*, pages 74–84. Springer, 2013.

[24] Alyson Leigh Young and Anabel Quan-Haase. Privacy protection strategies on facebook: The internet privacy paradox revisited. *Information, Communication & Society*, 16(4):479–500, 2013.