Expert Strategies to Assist Laypeople in Making Decisions and Adopting Privacy-Enhancing Technologies

Shirin Shams[1][0009−0000−5387−7920], Sebastian Jakob Schillinger[2][0009−0008−4106−2407], and Delphine Reinhardt[3][0000−0001−6802−2108]

[1] University of Göttingen, Institute of Computer Science, Göttingen, Germany
shirin.shams@uni-goettingen.de

[2] University of Göttingen, Institute of Computer Science, Göttingen, Germany
s.schillinger@stud.uni-goettingen.de

[3] University of Göttingen, Institute of Computer Science and Campus Institute Data Science, Göttingen, Germany
reinhardt@cs.uni-goettingen.de

Abstract. Despite the availability and advancement of privacy solutions, including *Privacy Enhancing Technologies* (PETs), a gap remains between individuals motivated to protect their online privacy and their actual adoption of PETs. While research has identified a range of discrete factors influencing PET adoption, these insights lack cohesion, limiting their practical applicability. Instead, we interviewed 16 domain experts from Western democratic countries, synthesising fragmented findings to establish strategies for effectively supporting individuals throughout the entire PET adoption process. Grounded in the *Security and Privacy Acceptance Framework* (SPAF), our study focused on three key areas: motivating action, raising awareness, and aligning adoption pathways with users' needs and abilities. Based on our qualitative analysis, we identified a set of 21 recommendations in five categories to be utilised when assisting individuals in their decision-making and adoption of PETs. Our findings emphasise practical recommendations, such as understanding privacy concerns, leveraging risk awareness, offering personalised recommendations, supporting Uptake and maintaining engagement. By combining expert insights with literature findings, our study informs the design of strategies and software assistants that support individuals in the pre-adoption phase and promote the adoption of PET.

Keywords: Usable Privacy · Privacy Enhancing Technologies · Privacy Tools Adoption · Privacy Preserving Technology Presentation

1 Introduction

A variety of privacy-preserving solutions, including *Privacy-Enhancing Technologies* (PETs), are available to help individuals safeguard personal data and mitigate privacy risks. For example, *Virtual Private Networks* (VPNs) are available across platforms to secure internet traffic. At the same time, tracker-blocking extensions can be integrated into web browsers to limit online tracking. Despite the abundance of these tools, their adoption rate remains strikingly low, even among individuals who express significant concerns about their privacy [7, 44, 45, 56, 60, 72, 90]. For instance, in a study involving 257 participants, more than 80% expressed privacy concerns, yet only 6% had installed privacy-preserving applications on their devices [7]. A more recent study [56] conducted in 2021 confirmed that the complexity of implementation and the vast available tools pose challenges in effective adoption. Further explanation among privacy researchers for the low adoption, including usability challenges, lack of awareness, perceived complexity, or general uncertainty [2, 4, 7, 29, 81].

To address this current state, we argue that for users who already exhibit a baseline level of concern or motivation to enhance privacy, such as in [7], a critical next step lies in understanding how to present PETs to them. This involves supporting individuals in navigating known barriers and facilitating more informed and confident decision-making. While existing studies describe available PETs in various domains [6, 21, 25, 42, 57] and highlight the different factors involved in PETs adoption [2, 10, 12, 29, 78], they offer limited guidance on supporting individuals throughout the journey of understanding risks and mitigation tools specifically in conjunction with individuals' unique needs, concerns, and abilities. As a result, a comprehensive guideline to better present PETs to individuals to enhance the experience and chance of adoption is missing.

To bridge this gap, we focus on the factors and strategies necessary to present PETs in a manner that supports individuals in adopting them. In this study, we hence address the following research question: **RQ:** *What strategies and approaches do experts recommend for presenting PETs to individuals in order to support them throughout the adoption process?* To this end, we leverage the expertise of 16 international domain experts in semi-structured interviews, examining how they engage with people to understand their privacy challenges and subsequently offering PETs to them. This approach enables us to uncover experts' knowledge on themes such as educating individuals about PETs, supporting informed decision-making, and providing tailored recommendations aligned with users' concerns and abilities. Our findings contribute valuable insights for developing a set of recommendations designed to be used for assisting individuals in the process of improving their online privacy practices. Given the scarcity of privacy experts, also acknowledge by themselves (e.g., Expert 5 stated: *"We serve maybe between a dozen and 20 people. There are millions more [...] So, yeah, something that's like an online tool would be really useful"*), we further investigate the potential of a software solution. An online software assistant to support individuals in enhancing their privacy by leveraging expert insights to evaluate its feasibility and inform its design. This work contributes the following:

- We conducted 16 interviews with domain experts, primarily from Western democratic countries, to explore recommendations for supporting individuals in PET adoption. Guided by the Security and Privacy Acceptance Framework (SPAF), the interviews focused on motivation, ability, and awareness. Then, experts discussed a software solution to support users before adoption.

- Our analysis identified five categories with 21 expert-driven recommendations to help individuals enhance their privacy. For instance, the *Understand* category involves learning about users and introducing privacy concepts, while *Streamline options* includes *Personalise* and *Analyse behaviour* (aligning advice with habits). We also outline experts' views on key features, benefits (e.g., reachability), and challenges (e.g., maintenance) of a potential software assistant, acknowledging expert support for all users is unrealistic.
- We contextualised our findings within the literature, especially SPAF, then outlined future directions like user evaluation, potential of a software assistance, and beyond a online assistance.

This paper is structured as: Sec. 2 reviews related work; Sec. 3 details methodology; results appear in Sec. 4; discussion in Sec. 5; and conclusion in Sec. 6.

2 Related Work and Background

This section reviews related work that shaped our study. We cover adoption challenges (Sec. 2.1), user behaviour in privacy adoption (Sec. 2.2), and proposed privacy assistance to support individuals (Sec. 2.3).

2.1 Obstacles in Adopting PETs

Despite the availability of PETs, only a minority leverages them and engages in protecting their privacy, despite their concerns expressed in numerous studies [44, 45, 72, 90]. The prominent explanation for the non-adoption is their lack of usability [2, 7, 29, 48]. Also, a more multi-faceted approach is identified in [2, 29, 78], suggesting additional factors behind the non-adoption. Examples include citizens' personality traits, privacy concerns, or knowledge. These factors have already been investigated in various attempts to predict individuals' intentions of use, adoption or acceptance of specific PETs [9,10,12,14,15,18,38–40,40,46,54,63] or PETs in general [52]. Moreover, context is known to be a salient factor in privacy-related decisions [3, 5, 13, 30, 53, 65–67, 83, 87, 97] and in the adoption of different technologies [20, 74, 98]. A study on VPN apps examined the impact of various attributes (e.g., rating, price, downloads) on citizens' decisions [84].

Users Informing Themselves In contrast, our work focuses on the user experience **before adoption**, specifically, the stage where individuals must first inform themselves and choose among options. Even when users are aware of tools [86], misconceptions about their protection remain [91]. Prior studies also highlight the need for better communication about tool capabilities [24, 86], underscoring that the state-of-the-art falls short in supporting informed privacy decisions. A recent study (2024) [82] evaluated 69 PET-promoting websites and found that they included only about one-third of the influential factors identified in academic literature, revealing a disconnect between providers and best practices on how to support users in making informed privacy decisions. While both their work and ours aim to support PET adoption, they focus on assessing websites, whereas we engage experts to generate actionable recommendations for guiding individuals through the full privacy improvement process. Similarly, Redmiles et al. (2020) [77] found online privacy advice lacked prioritisation and practicality. In contrast, our expert-informed recommendations provide structured support across all stages of privacy decision-making.

2.2 User Behaviour in Privacy Adoption

Due to the mentioned obstacles and shortcomings, motivated users may even be discouraged from protecting their online privacy. Uncertainty about what to do and encountering multiple barriers increase the risk of inaction [71]. Understanding why users fail to adopt privacy solutions, despite valuing privacy, requires examining behavioural models. The *Fogg Behaviour Model* (FBM) [33] explains behaviour as driven by three factors: motivation, ability, and triggers, which interact to enable or hinder actions across various domains.

The applicability of FBM in the context of privacy and security has been questioned by SPAF model [28] (2022), which argues that privacy behaviours differ due to their unique characteristics: (1) **Preventive nature:** privacy actions aim to prevent future risks, which often lack immediate impact, reducing urgency. (2) **Secondary priority**: privacy-related behaviours are often considered secondary tasks, as first noted in 2004 [31] and overshadowed by more immediate tasks. (3) **Abstract mechanisms:** privacy solutions are complex to average users, leading to confusion and mistrust, further reducing the likelihood of adoption. To address these, SPAF redefines factors by replacing FBM's triggers with awareness, emphasising users' understanding of risks and available protections. SPAF suggests awareness triggers action by helping users recognise threats. SPAF emphasises the importance of educating users about potential privacy risks and solutions, thereby helping to bridge the gap between privacy intentions and privacy behaviours.

Building on SPAF's core factors (motivation, awareness, and ability), we structured our interview questions to explore expert perspectives on supporting individuals in these areas. Considering the recency and comprehensiveness of SPAF, we were unable to find any other comparable alternative. Our study extends beyond SPAF by examining the specific strategies experts employ, providing deeper insight into their practical application. To our knowledge, this is the first study to capture expert-driven approaches for bridging the gap between privacy motivation and behaviour.

2.3 Assisting Users in Privacy Adoption

Ultimately, our goal is to propose a solution that informs citizens in a usable way, reducing barriers for individuals seeking to protect their online privacy but who lack confidence in doing so [11]. While [92] introduces a tool aimed at recommending PETs based on expert and user input, it lacks a comprehensive, interactive approach to guide individuals through the full privacy improvement

Table 1. Recommendations for Presenting PETs to Individuals: Literature Insights

Theme	Sub-theme	Description
Technology Presentation	**Description**	Explaining how the PET functions in a clear and user-friendly manner [10, 14, 73, 78].
	Effectiveness	Showing PETs' adoption privacy impact and their accuracy in addressing threats [12, 32, 54].
	Coverage	Clarifying what the PET protects and its limitations to avoid misconceptions [41, 56, 78, 91].
	Simplicity	Highlighting ease of use and straightforward adoption steps (if applicable) [10]
Internet Connection	**Speed**	Addressing potential effects of PETs on internet speed [84]
	Stability	Demonstrating PETs' impact on internet reliability [84]
Social and Emotional	**Emotion**	Motivating by telling stories, presenting fictional future or creating personal relevance [28, 63, 75].
	Interpersonal	Encouraging adoption by peers, and families [12,28,29,79].
	User feedback	Displaying user reviews and ratings for credibility [84].
Trust	**Provider**	Providing clear details on provider [39].
	Product	Showing trustworthiness via evidence or certifications [12].
General	**Language**	Using clear, accessible, and non-technical language [85].
	Price	Facilitating adoption by free versions or trials [84].
	Design and interaction	Offering interactive user-friendly interfaces [64].
	Accessibility	Following guidelines to support users with disabilities [82].

process. Additionally, it does not sufficiently tailor recommendations to individual needs and contexts. This underscores the need for a more holistic solution that supports users at every stage, from understanding options to making privacy decisions aligned with their personal concerns. The development of these strategies or software assistants will extend the existing literature on privacy assistants, though our focus is distinct. Prior work largely centers on helping users with tasks such as (1) selecting appropriate audiences for content shared on social networks [51, 96], (2) managing access to profile attributes [26, 35, 36], (3) setting mobile app permissions [49,50,68,88,89,95], and (4) controlling access to Internet-of-Things resources [1, 23, 27, 62, 80, 99].

Recommendations We reviewed the literature on supporting the adoption of privacy. Although fragmented, it offered useful insights which we grouped into six themes, summarised in Tab. 1 detailed as follows:

Technology Presentation covers how PETs should be described and demonstrated to users. Clear explanations of functionality [10, 14, 73, 78], evidence of effectiveness [12,32,54], and transparency about coverage and limitations [41,56, 78,91] help reduce misconceptions. Emphasising ease of adoption and use further supports user acceptance [10]. **Internet Connection** addresses performance-related concerns, as users often fear that PETs may reduce browsing speed or stability [84]. Providing empirical evidence can help mitigate these concerns and support adoption. **Social and Emotional** highlights the psychological and social factors influencing PET adoption. Emotional strategies, such as storytelling or future scenarios, help users connect personally to privacy concerns [28, 63, 75]. Peer and family discussions support adoption through interpersonal diffusion [12, 28, 29, 79], while user feedback, including reviews and ratings, reinforces PET credibility [84]. **Trust** examines the perceived trustworthiness of the provider and the product. Users value transparency about the provider's affiliations and credibility [39], and trust is further strengthened through security certifications, expert reviews, and third-party endorsements [12]. **General** covers cross-cutting factors that support PET adoption. Using clear, non-technical language improves comprehension and approachability [85]. Pricing models such as free or trial versions can reduce entry barriers [84]. Usability and interaction design should ensure intuitive navigation and minimise cognitive load [64], fostering informed decision-making. Lastly, ensuring accessibility for users with physical or cognitive impairments promotes equitable adoption [82].

3 Methodology

To bridge the gap between individuals motivated to enhance their privacy and the available PETs, we aim to develop a comprehensive understanding of how to present PETs to users and effectively guide them through the adoption process. Our initial literature review, as discussed in 2.3, identified valuable recommendations; however, these findings were fragmented and lacked a cohesive perspective on the entire process. To map out the overall process before engaging with end users, we argue that expert input was essential. Unlike user-centred methods such as user interviews, which may be constrained by participants' limited expertise and lack of a holistic view of the privacy domain, expert perspectives support a broader, well-informed understanding of effective support mechanisms. Hence, we leveraged expert interviews, a widely used method for obtaining in-depth insights [94]. We chose semi-structured interviews, which balance structure and flexibility, allowing discussions to be guided by predefined themes while enabling experts to provide unanticipated insights [16]. Alternative expert-driven methods, such as focus groups, can risk group dynamics influencing individual opinions [47], while surveys may lack the depth needed for qualitative exploration. Therefore, following the approach applied in [29], we decided that expert interviews were the most suitable method for this study. We conducted 16 semi-structured expert interviews, each lasting on average about 50 minutes (ranging from 32 to 74 minutes). All interviews were held online in English via the *BigBlueButton* (BBB) video platform provided by our university, during the last quarter of 2023 and the first quarter of 2024.

In the following, we outline the interview design (Sec. 3.1), recruitment and demographics (Sec. 3.2), analysis process (Sec. 3.3), study limitations (Sec. 3.4), and ethical considerations (Sec. 3.5).

3.1 Interview Design and Procedure

Interview Design As outlined in Sec. 2.2, we drew upon the SPAF [28] to design our interview themes. Our objective was to capture expert perspectives on supporting individuals in the three key factors influencing privacy adoption: motivation, ability, and awareness. We employed a scenario-based interview approach to elicit expert perspectives on supporting individuals (see Appendix 1). Experts were asked to imagine a one-on-one consultation with a user seeking to enhance their online privacy, thereby implying a baseline of concern and motivation of the user. To focus on strategic guidance rather than specific tools, the prompt avoided naming any PETs or privacy solutions, instead using an open-ended scenario: "Imagine you want to support an internet user to improve online privacy [...]." This encouraged high-level reflections on privacy adoption strategies. Experts then shared recommendations for supporting user adoption. Given the limited access to expert advice, we also explored the feasibility of a software assistant, such as a website or app, as an alternative to direct expert guidance to help users enhance their privacy. Experts assessed its potential benefits, challenges, and key features. Each section concluded with an open invitation for additional thoughts to deepen understanding of their perspectives.

Procedure Each interview began with a welcome, followed by an introduction that outlined the interviewer's background, study goals, and procedures for confidentiality and consent. We then collected demographic data (see Appendix 2) and proceeded with the interview scenario and questions, concluding by asking for referrals to other potential experts. A pilot interview was conducted to refine the study, improving (a) question clarity and relevance, (b) structure and flow, and (c) feasibility within the allocated time. Data from the pilot were excluded from the final analysis, as they served solely to enhance the interview procedure.

3.2 Recruitment and Demographics

We recruited experts via multiple channels: (a) LinkedIn, (b) email invitations through our research network, (c) outreach to recent authors in usable privacy, and (d) promotion at a usable security and privacy conference. We used purposeful sampling [69] to gain in-depth insights. Experts were defined as individuals with at least two years of experience in privacy or security, following [29]. We explicitly included younger experts to capture fresh and diverse perspectives. We did not compensate expert interviewees as they often participate voluntarily, driven by intrinsic motivation to advance knowledge or inform policy [8], e.g. in [29], also as it minimises bias and enhances authenticity [70]. The final sample size for this study was determined based on thematic saturation, defined as the point at which no new themes or insights emerge from the data, as recommended by Morse [61]. Although prior research suggests that qualitative studies often achieve data saturation with approximately 12 interviews [34, 37, 93], we extended our data collection to ensure saturation within the specific context of our study. Ultimately, we conducted 16 expert interviews, a sample size aligned

Table 2. Expert Participants Demographics

ID	Gender	Age	Country of residency	Degree	Job title	Experience in field	User involvement in work
E1	F	◍	Germany	PHD	Research Assistant	◍	○
E2	M	◍	Germany	PHD	Research Associate	◍	◍
E3	F	◍	Germany	PHD	Senior Researcher	●	◍
E4	F	○	Germany	Master	Research Associate	◍	●
E5	M	○	UK	Master	PhD Student	○	●
E6	M	○	Germany	Master	PhD Candidate	◍	●
E7	M	◍	Austria	PHD	Professor	●	○
E8	M	○	Netherlands	PHD	Postdoctoral Researcher	◍	◍
E9	M	○	UK	Master	PhD Candidate	○	●
E10	F	◍	Germany	Master	PhD Candidate	○	●
E11	F	◍	Israel	PHD	Assistant Professor	●	●
E12	F	◍	Canada	PHD	Associate Professor	●	●
E13	F	◍	Sweden	PHD	Associate Senior Lecturer	◍	◍
E14	F	●	Sweden	PHD	Professor	●	●
E15	F	○	Germany	Master	Researcher/ Project Lead	○	○
E16	M	○	USA	PHD	Postdoctoral Assistant	○	◍
Total	Female=9 Male=7	18-34 ○ =7 35-49 ◍ =8 50-64 ● =1	8 countries	Ph.D.=10 Master=6		2-5 years ○ =5 6-10 years ◍ =6 10 plus ● =5	little ○ =3 Medium ◍ =5 A lot ● =8

with the recommendations of [29]. We tracked saturation during interviews and found little new insight in the final three, indicating thematic saturation.

The demographic information of our participants can be found in Tab. 2. Our sample comprised seven males and nine females from eight different countries. While almost balanced, our sample reflects the observed higher proportion of females working in usable privacy. As one expert mentioned, precisely five years of experience, 75% of our sample had five or more years of experience in the field, matching with [17, 43]. Ten had a Ph.D. degree, and six had a Master's degree. Half reported having a high frequency of user interactions as part of their job, five mentioned a medium frequency, and three reported little interaction. Experts are referred to as "E" followed by their ID as follows.

3.3 Qualitative Analysis

We, two researchers (R1 and R2), transcribed all interviews using the automatic transcript software, *Amberscript*. Then, we proofread and corrected the transcribed results. To analyse the transcriptions, we conducted a qualitative analysis of our data using inductive coding with MAXQDA software. We chose this approach as the starting themes are generated based on the interview content, and this approach is more prone to discovering new insights and themes. We followed established guidelines and common practices for coding semi-structured interviews [19,55]. First, we segmented the transcribed audio recordings into thematic sections based on our interview themes. The primary researcher, R1 (the principal investigator [19]), conducted the first phase of detailed coding using open and in vivo coding techniques. During the iterative refinement process, codes addressing similar topics were merged to enhance coherence, while codes containing multiple distinct concepts were subdivided into separate codes to improve granularity. All codes were categorised into relevant thematic groups following this rigorous refinement. Then, both coders independently coded the first five participants to test the codebook. Both coders were allowed to add, delete, combine or separate codes. After several rounds, a codebook (see Appendix 3) consisting of 82 codes was finalised. R1 and R2 then independently coded all transcripts. The coding results were compared using MAXQDA software to identify areas of overlap and discrepancies. To analyse discrepancies, each researcher reviewed codes assigned exclusively by the other coder. First round, each researcher reviewed and validated the other researcher's codes. Unacceptable cases were discussed in a collaborative meeting to reach an agreement.

We achieved an *Inter-Rater Agreement* (IRA) of 95.35% (Kappa = 0.96), which reflects a high level of consistency between the two researchers. The lack of full agreement stemmed from varying interpretations of individual statements. Most of the remaining disagreements involved coding aspects that did not influence the final results. These disagreements typically occurred at the parent code level rather than the final code layer. For example, in one case regarding motivation, one researcher coded the entire response as motivation, while the other identified part of the answer as tailoring down the options. Ultimately, both coded this text segment with different parent codes, as *Personalising.* A smaller subset of disagreements arose from varying interpretations. For instance, the statement *"Hotel websites would change the ordering of things depending on the type of device you went there on. So if you go there on a Mac, they auto sorted. So the more expensive ones are on the top"* (quoted by E12) was coded as *Reveal data collection* by one researcher and as *Raise risk awareness* by another, which in these rare cases we continued with R1, the principal investigator. As noted in prior studies, Kappa values alone can be contentious in complex analyses, as they may not fully capture the depth and context of qualitative coding [19].

3.4 Limitations

This study has several limitations. While centred on expert views, adding user insights would deepen real-world understanding. Future work should validate findings through user studies. The study focused on motivated users, assuming proactive engagement. Yet, society includes a broader range of users, including those with little or no initial motivation to prioritise privacy [11]. We also didn't differentiate between solution types (e.g., simple vs. advanced PETs or device settings), which future work should explore for deeper insights. The study was conducted with experts from Western democracies, and findings should be understood within this context. Privacy in oppressive regimes poses distinct challenges, where tools like VPNs and Tor may be restricted. Research involving diverse cultural and geopolitical contexts [76] is needed for a more inclusive view, especially in high-surveillance or low-literacy environments. Lastly, despite efforts to recruit industry experts, most participants were from academia. While this may limit industry perspectives, academic experts tend to offer structured, context-rich insights that help form recommendations. The sample size (16 participants) should be considered in interpreting the findings.

3.5 Ethical Considerations

Our university *Data Protection Officer* (DPO) expressed a positive opinion on the study. Participants were informed of the study's purpose during recruitment and signed a *General Data Protection Regulation* (GDPR) compliant consent detailing data recording, processing, and storage. At each session, participants were reminded of the study's purpose, withdrawal rights, and confidentiality. Names were later removed, and transcripts were stored in encrypted files.

4 Results

Here, we present key expert recommendations (Sec.4.1), note additional findings beyond core themes (Sec.4.2), and summarise results (Sec. 4.3).

4.1 Recommendations for Supporting Individuals

We structured experts' opinions in themes identified during data analysis, resulting in five categories: (1) Understand, (2) Motivate, (3) Streamline options, (4) Support adoption, and (5) Stay Connected. Each category encompasses multiple recommendations, totalling 21, on how to assist individuals in improving their privacy, summarised in Tab. 3. Then, experts' opinions on a potential software assisting individuals instead of an expert are presented.

Understand Experts identified three key recommendations for effectively developing an initial mutual understanding to help individuals improve their privacy practices. The first recommendation, *Know your audience*, was emphasised by twelve experts. This involves understanding the users' goals, current online behaviours, and background knowledge. For example, E3 stated, *"I think my first move would be to understand what they know about online privacy. [...] So I think the first thing is to ask the users about themselves"*. An almost similar number of experts highlighted *Provide context* as the next recommendation, which is explaining basic privacy knowledge and potential risks to individuals to provide a context for the session. As E2 mentioned, *"At first, I would need to give them a broad understanding of problems in terms of privacy, going on, on the internet"*. This approach also allows the expert to gauge the user's understanding and reactions to the provided information, enabling a more dynamic approach during the session. By observing how users respond, the expert can adapt their guidance to better align with the user's specific needs, knowledge gaps, or concerns, ensuring more effective support. The final recommendation, *Explore practices*, mentioned by five, assesses users' current privacy practices. As E9 noted, it's key to know *"What their current practices are, how can they be improved, and where do they want to go with that?"* Experts expanded on these recommendations later; here, we include only points related to initial understanding and connection-building.

Table 3. Recommendations Set for Supporting Individuals in Improving Their Privacy

Categories	Recommendations	Explanations	Number of Experts
Understand Practices to lay the foundation	**Know your audience**	gaining an understanding of users' needs, online behaviours, and IT & privacy knowledge	12
	Provide context	explaining foundational privacy knowledge and potential risks	11
	Explore practices	Examining users' current privacy practices	5
Motivate Strategies to encourage users to enhance their online privacy in practice	**Raise risk awareness**	Highlighting personal and societal risks through example incidents	16
	Showcase simplicity	Showing easy installation and use (if appl.)	13
	Describe technology	providing user-friendly explanation of how the privacy solution works	8
	Reveal data collection	presenting data being collected from potential channels over time and activities	8
	Avoid frightening	preventing fear of threats and of workload needed for their privacy protection	6
	Highlight benefits	illustrating the tangible changes and benefits	3
Streamline options Key considerations for providing options	**Personalise**	assessing users' needs, concerns, privacy value, preferences, socioeconomic situation, and age concerning IT skills	16
	Analyse behaviour	reviewing hardware (e.g., smart home) and software usage (e.g., visiting websites, social media), and users' current privacy solutions	15
	Acknowledge circumstances	considering users' country, job, disability	6
	Propose usable options	to enable the user to complete the primary task with acceptable quality	5
Support adoption Practices to actively assist users in implementing action	**Offer product options**	such as VPN products, while explaining the features, as opposed to the concept solution, e.g., VPN, Private Browser	13
	Ensure essentials	crosschecking essential solutions and behaviours which are useful for the majority	9
	Cooperate	in adopting the privacy solution	9
	Offer concept solution	explaining the concept solution (e.g., VPN, Private Browser) rather than specific products; provide product options if requested	7
Stay connected Strategies to stay in touch	**Grant resources**	sharing educational or news links, users can learn more and stay connected	12
	Share updates	communicating new solutions and news	7
	Follow up	asking if users' need further support	6
	Share contact	such as email or phone number	5

Motivate In this category, we grouped the experts' suggested approaches into six key recommendations. *Raise risk awareness* is mentioned by all 16 experts, described as demonstrating the potential privacy risk impacts on both personal and societal levels. This involves explaining potential cases of data misuse and their possible impacts on individuals and society. E11 quoted: *"Give them a possible example of what might happen"*. For example, widespread location sharing could serve the interests of data collectors over societal interests. In this regard, E1 mentioned: *" When people get that point of aha moment [...] You could see the difference in the approach [...] So you can see that awareness really makes a difference"*. Next, thirteen experts highlighted *Showcase simplicity*. This involves, where applicable, demonstrating that adopting and using privacy solutions can be straightforward. This would emphasise simplicity, help reduce users' cognitive load, and encourage engagement in privacy-protective behaviours. As E9 mentioned *"I think one of the big barriers to a lot of people using privacy technologies is either real difficulty or the perceived difficulty to it"*. Eight experts emphasised the importance of *Describe technology*, suggesting that explaining how a PET works in a clear, user-friendly way can boost user involvement and motivation to adopt it. This closely aligns with established recommendations in the literature [10, 14, 73, 78]. E14 mentioned, *"Try to motivate and explain the functionality. Yeah. I mean, in the user privacy community, it is also known that the more functional explanations should be fine. And so, not explaining the crypto details. So, it is not a structural explanation but rather a functional explanation on a high level"*. Similarly, *Reveal data collection* was highlighted by eight experts. They noted that showing users how their personal data is collected across different channels over time helps to raise awareness. E12 illustrated this with a practical example of data collection and its personal impact, *"Hotel websites would change the ordering of things depending on the type of device you went there on. So if you go there on a Mac, they auto sorted. So the more expensive ones are on the top"*. This means highlighting the data that can be collected from users when they do not protect their privacy, prompting them to take action. Also, *Avoid frightening* was recommended by six. E6 remarked, *" Generating fear gives the cause stopping through reasoning so they will not think about it [...] What I want is that they start thinking about it"*. A conceptual tension arises here: while enhancing users' awareness of risks is widely advocated, there is simultaneous concern about inducing fear. This raises the question of how these two aims, informing without alarming, can be balanced within user support strategies constructively? *Highlight benefits* were recommended by three experts. Emphasising the benefits of adoption has also been validated by other studies as a key motivator for individuals to enhance their privacy practices. For example, [54] found that perceived effectiveness boosts PET adoption, highlighting the value of showing how a PET addresses privacy concerns.

Streamline Options Experts identified four key recommendations for tailoring privacy options to individuals. All participants emphasised *Personalise* as a key factor for refining PETs to be suggested, indicating that PET options should be crafted based on an individual's needs, goals, and privacy values rather than general criteria. E6 noted, *"Because if it's not tailored to the specific case, to the specific person, to the specific scenario of applications, it will just not work."* Additionally, age was considered a factor in personalising, though most experts agreed it is relevant only when it impacts IT skills, with particular attention recommended for teenagers and the elderly. These groups may need more tailored guidance, as teenagers often require support to develop privacy awareness in their formative years, while elderly individuals may face challenges navigating modern technologies. This means that age-specific interventions should align with the user's familiarity and comfort with digital platforms. Next, *Analyse behaviour*, recommended by 15 experts, involves examining users' online activities, a task that can be complex. Experts suggested several approaches to achieve this, including analysing hardware usage (e.g., smartwatches, smart home devices), assessing software interactions (e.g., frequently visited websites or applications), and exploring current privacy practices. Additionally, *Acknowledge circumstances* refers to accounting for factors such as a user's country of residence, job, or physical and mental disabilities, recommended by six experts to take into account when assisting as it may influence privacy needs. Lastly, *Propose usable options* was recommended by five experts. For instance, E6 highlighted the importance of offering solutions that are effective yet unobtrusive, stating, *"it needs to be an effective solution that does not impact the efficiency of what they want to do."* Similarly, E5 emphasised the need for recommending passive solutions, explaining that privacy tools should work seamlessly without interrupting the user's workflow by mentioning *"[...] something that you kind of use passively"*. These underscore the importance of usability and simplicity in privacy solutions.

Support Adoption To support adopting privacy solutions in practice, 13 experts mentioned *Offer product options.* This means presenting users with a selection of commercial products, such as recommending particular VPN products, rather than merely suggesting the type of solution needed. Experts highlighted that providing concrete product suggestions simplifies decision-making and increases the likelihood of adoption, as users are less likely to face the burden of independently researching and shortlisting suitable products. In 2022, [73] demonstrates that when asked about known PETs, most lay public participants predominantly identified tools with different primary functionalities than privacy protection, indicating a lack of awareness of available solutions, further emphasising the need for providing users with a selection of products. Experts emphasise the value of giving options to users as it is essential to provide flexibility in decisions by offering various product options instead of prescribing a single solution. E5 states, *"I think if I can give more specific solutions [commercial products], that is probably best. [...] to help themselves a bit more and not just use this one tool you give them. You know, it's what's that of saying, give a man a fish head for a day. You teach him to fish; he will be fed for life. It's basically that for privacy"*. E5 further likened this to the proverb about teaching a person to fish, suggesting that privacy support should empower individuals to make informed decisions while offering flexible solutions to suit their needs. *Ensure essentials*, mentioned by nine experts, refers to cross-checking essential protection solutions and behaviours that are helpful for most people. Additionally, the same number of experts recommend to *Cooperate* along with users for adopting the selected solution. E8 quoted: *"I would try to install it on the spot and show how it works"*. E5 also quoted: *"We could just leave them with instructions, but I think they do appreciate just a little bit of hand-holding"*. Lastly, seven experts mentioned *Offer concept solution*, which means suggesting the general type of privacy technology (e.g., VPN or private browser) without endorsing specific products. This stands in contrast to *Offer product options*, which entails presenting concrete tool choices to users. Experts who supported both approaches emphasised that the appropriate strategy should be guided by the individual's context, needs, and preferences. As E16 noted: *"I think we should show both solutions [product options and concept solution] to them. Or I would, depending it on the person"*. This gives rise to an important question: What are the comparative advantages and limitations of offering conceptual solutions versus specific product options in effectively supporting users' privacy-related decisions?

Stay Connected As illustrated by E13, privacy protection often requires ongoing support beyond a single session. The experts proposed different recommendations for staying connected. E13 quoted: *"Obviously privacy is not something set in stone. It's dynamic. We change our privacy preferences over time. When I'm 20, I'm probably thinking about this construct differently when I'm using Facebook than when I'm using Facebook when I'm 35. I'm already a different person. So we would still need to have a way to convince the user that it's worth spending time on making those adjustments from time to time"*. As a result, we identified four recommendations supporting this aspect. The first recommendation is *Grant resources*, mentioned by 12 experts, which involves sharing educational materials that enable users to stay informed independently. This means that providing these resources makes individuals more likely to remain engaged with privacy support over time and engage in further privacy-enhancing behaviours. Additionally, *Share updates*, noted by seven experts, involves sending users periodic updates as a direct way to maintain a connection. Six experts recommended *Follow up*, checking in to reinforce engagement, for example, E2 noted: *"I could also ask them to report on how things [previous solutions] have worked out for them"*. Experts also suggested sharing contact info to ensure users can seek help when needed. Finally, *Share contact* information, such as email address, was suggested to ensure users can seek help when needed. E2 quoted: *"I would offer them to just contact me if any further questions arise"*, and E5 said: *"making yourself quite approachable and available [for staying in contact]"*.

Software Assistant We categorised expert views on the potential of a software assistant into key elements, benefits, and challenges.

Elements Experts emphasised personalisation, recommendation, and awareness as key elements. Ten experts mentioned a personalisation element for the software that gathers users' needs, preferences, online behaviour, and privacy goals. E3 explained, *"So just ask what the most important things people do online and what they don't do. So like online shopping, online banking, reading, new social networking, and so this would be, I guess, also the first step in this tool"*. An equal number of experts mentioned a recommendation element for the software that provides tailored suggestions based on the information gathered through personalisation. Nine experts highlighted the importance of an awareness element to educate users on privacy risks and mitigation strategies. Additionally, four experts recommended incorporating interactive elements such as gamification and multimedia to enhance engagement. E15 expressed, *"I would always go for gamification"* while E7 suggested, *"[utilising] video because people don't read* *web pages anymore"*. Three experts suggested solution checklists; two stressed prioritising them for effective user action. E6 noted, *" Prioritisation needs to depend on what is the most dangerous thing that can happen to them right now"*.

Advantages Experts identified the scalability and technological strengths as key advantages. Half of the experts emphasised the software's ability to reach a broad audience simultaneously, provide immediate support, and operate independently of geographical constraints as critical features. As E5 stated, *"We [experts] serve maybe between a dozen and 20 people. There are millions more. It is not a local area. And probably a lot of them would appreciate this kind of information. So, yeah, something that's like an online tool would be really useful"*. E11 further noted, *"[N]ot everyone knows the experts [...] so people can just reach out to that platform"*. Additionally, six experts highlighted the technical strengths of the software. They mentioned it could streamline privacy improvement by linking users directly to relevant resources and solutions. E9 pointed out, *"[Users] be able to go at their own pace and learn what they want"*. Moreover, the tool fosters a judgment-free environment, encouraging users to seek assistance without fear of criticism. E10 remarked, *"[M]aybe I need to find a way to visit porn websites without everyone knowing it. And I would probably shy away from talking about that with my friends, but I can talk about that with the software"*. These features position the software assistance as an inclusive and reachable alternative to expert consultations.

Challenges Experts identified several challenges. Seven experts noted that some individuals might not use it due to a preference for human interaction or a lack of awareness of its existence. E8 remarked, *"There are people who would probably just not enjoy talking to the robot [assistant tool]"*. Seven experts emphasised the need for continuous maintenance to address evolving privacy threats and mitigation strategies and incorporate user feedback, acknowledging the associated costs. E3 stated, *"[T]he landscape of privacy-enhancing tools changes quite a lot. And the question is, who is going to maintain the software to be up to date?"* Trust emerged as a concern, with six experts noting users may doubt recommendations or fear privacy risks. Usability and technical barriers were also raised, stressing the need for a user-friendly, stable, unbiased, and accessible platform. These challenges highlight areas requiring attention.

4.2 Additional Findings

Although many privacy-preserving technologies are available [24] and the scenario was intentionally open-ended, experts mainly mentioned widely available PETs like VPNs, ad blockers, private search engines, privacy-focused browsers, Tor, and encrypted communication tools. This implies their focus was on broad strategies rather than specific tools. Additionally, although reported by one or two experts, the following offers practical guidance on specific aspects.

Start with Simple Solutions: E3 stressed beginning with straightforward and implementable solutions to boost confidence and reduce perceived difficulty.

Provide Manageable Options: E1 and E8 advised presenting users with a limited, manageable set of solutions during each session. This prevents overwhelming users and fosters a more focused adoption process. **Leverage Peer Support Networks:** E11 emphasized the effectiveness of peer-to-peer support. A 2022 study [58] demonstrated this through an app aiding older adults with help from friends, family, or community volunteers. **Consider Caregiver Responsibilities:** E3 and E11 stressed that any privacy improvement strategies must account for individuals' responsibilities toward children or the elderly. **Integrate Gamification:** E10 and E15 suggested incorporating gamification into the adoption process. This approach could make the experience more engaging by introducing elements of fun and achievement. **Multi-Tool Approach:** E14 underlined the necessity of informing users that maintaining privacy requires a combination of tools and behaviour rather than relying on a single solution.

4.3 Summary

The analysis of the gathered information resulted in five categories of recommendations. Among these recommendations, *Raise risk awareness* and *Personalise* were highlighted by all experts, underscoring the critical importance of tailoring privacy solutions to individual needs and effectively communicating potential risks to drive engagement to encourage widespread adoption. Experts also suggested that a software solution could effectively empower more individuals in diverse locations at any time to enhance their privacy. However, they noted that not being used, maintenance, and trust are challenges that must be addressed.

5 Discussion

This section compares findings (Sec.5.1) and outline future directions (Sec.5.2).

5.1 Comparing with Existing Works

By addressing our research question (*What strategies and approaches do experts recommend for presenting PETs to individuals throughout the adoption process?*), our study offers actionable recommendations aligned with the three SPAF factors [28], which guided our work (see Sec. 2). For awareness and motivation, experts highlighted *Raise risk awareness* and *Showcase simplicity* as central strategies. Regarding ability, *Personalise* and *Analyse behaviour* emerged as key, underscoring the need to tailor solutions to individuals. These findings demonstrate how SPAF principles can be operationalised through experts' practical guidance. They also address gaps found in recent studies; for instance, the analysis of 69 PET-promoting websites [82] showed most provided static, non-personalised, one-way information. In contrast, our experts stressed the importance of tailored support based on user behaviour. As E9 noted, *"It can't just be, here's a bunch of tools [...] Obviously a lot of PETs aren't one size fits all."* Similarly, [77] identified a crisis in advice prioritisation, with users struggling to make informed privacy choices. Our findings address this through expert-backed strategies for streamlining options and supporting user decision-making. In sum, our work builds on SPAF [28] and complements prior research [77,82] by offering expert-driven measures to support individuals throughout the privacy adoption.

Comparing with Literature Recommendations The comparison between expert insights and literature recommendations (outlined in 2.3) revealed shared priorities and notable differences. Both emphasise simplicity, trust, and clear explanations. However, experts offered a more comprehensive, process-oriented approach beyond the initial presentation to include long-term engagement. They stressed a structured progression: starting with understanding users' privacy knowledge and habits, and continuing with sustained support. Notably, the *Understand* category, which encompasses warming up interactions and assessing current practices, is largely absent from the literature. Experts also introduced *Avoid frightening* as a key to reducing user hesitation, another overlooked aspect. While personalisation and behavioural analysis were seen as essential by all experts, these were underrepresented in prior research. Experts further noted that privacy adoption is an ongoing process, which the literature seldom addresses. Literature-based insights remain valuable for PET presentations, offering guidance on elements such as provider details and user feedback, although less emphasised by experts. Together, expert and literature insights complement each other, supporting more effective, user-centred PET adoption strategies.

5.2 Future Directions

User Evaluation. The next step is to test these recommendations in the lab with diverse users differing in motivation, literacy, and privacy concerns. **Privacy Software Assistance.** Based on the scarcity of experts and insights from this study, we see potential for a privacy software assistance, such as a website or app, to provide support to a broad segment of society at any time and location. By incorporating expert recommendations, the tool should be designed to capture users' requirements and concerns, subsequently suggesting PETs, promoting engagement and adoption. We advocate a user-centred design approach, starting with understanding user behaviour, integrating expert insights, and refining the tool through iterative development and usability testing. **Beyond Software Assistance.** Beyond software assistants, expert recommendations can be implemented through various channels and actors, such as privacy champions [59], peer educators [22], social supporters [58], and partnerships with NGOs and advocacy groups. They can be integrated into existing programs, supported by open-access toolkits, and scaled through train-the-trainer models.

6 Conclusion

Our research contributes to addressing the ongoing challenge of bridging the gap between individuals' motivation to protect their privacy and the actual adoption of PETs. Through interviews with 16 experts, we gained 21 actionable recommendations on how individuals can be supported. The proposed recommendations highlight strategies, such as streamlining privacy options through tailored suggestions and behavioural analysis, to facilitate PET adoption. This work provides a practical foundation for designing strategies and software to support users, ultimately promoting greater adoption of PETs and enhanced privacy outcomes.

Acknowledgments. We thank our participants for sharing their expertise. This work is funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation), referenced as 505982147. OpenAI was used partially for text editing.

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

Appendix

Appendix 1 Interview Scenarios and Questions

Scenario: Imagine you want to support an internet user in improving their online privacy in a one-on-one (online or in-person) session, like a consulting session, or helping friends and family members who are not experts in this area. These individuals come to you because of their interests, meaning they probably have minimal motivation and IT skills. Take a moment to think of this imaginary session. Think of how you would, in general, organise such a session; we are not focused on a specific product to be recommended, but on the process you take. **Overall Approach:** - 1. What would be your main agenda for such a session? - 2. How would you structure the session? **Motivation, Awareness and Ability** - 1. To motivate users to take privacy solutions in practice, would you have any specific strategy? (- Do you think showing what data is possibly collected from users can play a motivational role for them? - Do you believe telling the potential risk they are running by not protecting their privacy can play a motivational role? - Would you explain these risks in personal impact, societal impact, or both to increase motivation? - Do you think mentioning the ease of usage for privacy solutions can be motivational?) - 2. How do you determine the most suitable privacy solutions to suggest to an individual from all potential options? - 3. Would you think knowing about users can be beneficial for you to provide better solutions? Why? (If yes, what would you like to know about a user?) - 4. Would you rather try to give direct solutions (exact tool) or explain the solutions on a general level? Why? - 5. Would you see benefits in asking participants to install the solution immediately in the session? Why? - 6. What would you do to motivate the user to stay connected to you to receive further privacy advice even after the session? - 7. Would you suggest any information resources to individuals where they can learn more about online privacy by themselves (e.g., websites, videos)? **Software Assistant Tool Scenario. Scenario:** Instead of a one-to-one person session, imagine an online assistance tool that aims to support individuals in improving privacy. Something like a webpage or an application that people use to get out of the maze of massive online information and have assistance in improving their online privacy. - 1. Do you see any specific advantages in having such a tool available for individuals? Why? - 2. Do you see any specific disadvantages or risks in having such a tool? Why? - 3. To enhance such an assistance tool's efficacy in supporting individuals, what, in your opinion, should be the ideal user interaction flow?

Appendix 2 Demographic Questions

What is the highest university degree you have achieved? - Which country are you based in? - What is your current job or study title? - To what level does your work or study involve citizens' interaction with privacy or security? - How long have you been in the privacy or security sector (work and study)? - How do you describe your gender identity? - Which age group do you belong to?

Appendix 3 Codebook

Tab.4 and Tab. 5 present the codebooks used for qualitative analysis.

Table 4. Codebook used for qualitative data analysis - software assistance

Them	**Code**
Modules and Features	Information Resources – General checklist – Recommendation – Prioritising – Education and awareness – Should be personalised – Redirect to a human – Chatbot, gamification, video and audio – Motivation – Example (current solutions) – Trust in the tool itself
Advantages	Yes, such a tool helps – People access (scalable) – Time (scalable) – Location (scalable) – Link to resources – Link to adoption – Broader recommendations – Judgment-free – Automatic audit
Disadvantages	Usability, accessibility, technical – Quality of recommendations – People do not use it and are not aware of it – Experts are more comfortable – Maintenance and reliability – Improvement potentials

Table 5. Codebook used for qualitative data analysis - main

Them	Code
Overall Approach	Emotion Consideration – Users' current privacy strategies, tools – Receiving user concerns, needs and goals – Users' current understanding of privacy – Teaching the privacy basics to users – Learning about users' online behaviour and devices – Giving risk awareness to the user – Explaining the technology (privacy solution) and its advantages to the user – Providing recommendation to user – General advice for everybody –Answering users' specific questions – Users' argument for not taking action (adopting privacy solution)
Motivation	Show users tangible changes and benefits (of adoption) – Prevent fear and frightening users – Easiness and complication of use – Impact level (personal, society) – Show users tangible changes
Awareness	User awareness (general) – Risk awareness – Showing users the data being collected from them (ways and possibilities) – Explain the technology solution to users – Give users examples
Recommendation Refining	Job of the user – Disability of user – Manageable portion of solution for users – Physical location – Quality and usability of privacy solution – User's current privacy practices – Personalising – Responsibility for children or the elderly – Age of user – Offering a general list of solutions – User concerns, questions and goals – User online behaviour – Start with an easy recommendation – IT knowledge of user – The software users use – The hardware users use
Solutions Type	Give users both concept and concrete solutions – Give users concrete options to choose – Depends on the user or situation (to give a direct solution or just a concept) – Act (adopt the solution) with users right away (in the session) – Give the available options and features
Education	Giving education resources to the user – Do not give education resources to the user – Depending on the user and if users want education resources – Depending on education resources (types and characteristics)
Maintain Engagement	Open questions at the end – Sharing the expert contact (expert must be approachable) – Necessity of regular update – Enjoyable events and community base – Sharing privacy news – Expert follow up on user – Feedback session for this session privacy tasks – Fix a time for the next meeting – Give the user the reliability feeling

References

1. Abdi, N., Ramokapane, K.M., Such, J.M.: More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In: Proc. of the USENIX Conf. on Usable Privacy and Security (2019)
2. Abu-Salma, R., Sasse, M.A., Bonneau, J., Danilova, A., Naiakshina, A., Smith, M.: Obstacles to the Adoption of Secure Communication Tools. In: Proc. IEEE Symposium on Security and Privacy (2017)
3. Acquisti, A., Brandimarte, L., Loewenstein, G.: Privacy and Human Behavior in the Age of Information. Science (2015)

4. Adams, A., Sasse, M.A.: Users Are Not the Enemy. Communications of the ACM (1999)
5. Altman, I.: The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding. ERIC (1975)
6. Argyrakis, J., Gritzalis, S., Kioulafas, C.: Privacy enhancing technologies: A review. In: Proc. Electronic Government: Second International Conference (2003)
7. Assal, H., Hurtado, S., Imran, A., Chiasson, S.: What's the Deal With Privacy Apps? A Comprehensive Exploration of User Perception and Usability. In: Proc. 14th International Conference on Mobile and Ubiquitous Multimedia (2015)
8. Beauchamp, T.L., Childress, J.F.: Principles of biomedical ethics. Edicoes Loyola (1994)
9. Benenson, Z., Girard, A., Krontiris, I.: User Acceptance Factors for Anonymous Credentials: An Empirical Investigation. In: Proc. Workshop on the Economics of Information Security (WEIS) (2015)
10. Benenson, Z., Girard, A., Krontiris, I., Liagkou, V., Rannenberg, K., Stamatiou, Y.: User Acceptance of Privacy-Abcs: An Exploratory Study. In: Proc. 2nd Human Aspects of Information Security, Privacy, and Trust (2014)
11. Boerman, S.C., Kruikemeier, S., Zuiderveen Borgesius, F.J.: Exploring motivations for online privacy protection behavior: Insights from panel data. Communication Research (2021)
12. Bracamonte, V., Pape, S., Kiyomoto, S.: Investigating User Intention to Use a Privacy Sensitive Information Detection Tool. In: Symposium on Cryptography and Information Security (SCIS) (2021)
13. Brandimarte, L., Acquisti, A., Loewenstein, G.: Misplaced Confidences: Privacy and the Control Paradox. Social Psychological and Personality Science (2013)
14. Brecht, F., Fabian, B., Kunz, S., Mueller, S.: Are You Willing to Wait Longer for Internet Privacy? Proc. European Conference on Information Systems (ECIS) (2011)
15. Brecht, F., Fabian, B., Kunz, S., Mueller, S.: Communication Anonymizers: Personality, Internet Privacy Literacy and their influence on Technology Acceptance. In: Proc. of ECIS (2012)
16. Brinkmann, S.: Unstructured and semi-structured interviewing. The Oxford handbook of qualitative research (2014)
17. 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)
18. Cabinakova, J., Zimmermann, C., Mueller, G.: An Empirical Analysis of Privacy Dashboard Acceptance: The Google Case. In: Proc. European Conference on Information Systems (ECIS) (2016)
19. Campbell, J.L., Quincy, C., Osserman, J., Pedersen, O.K.: Coding in-depth semistructured interviews: Problems of unitisation and intercoder reliability and agreement. Sociological methods & research (2013)
20. Caulfield, Tristan and Ioannidis, Christos and Pym, David: On the Adoption of Privacy-Enhancing Technologies. In: Proc. 7th Decision and Game Theory for Security (GameSec). Springer (2016)
21. Cha, S.C., Hsu, T.Y., Xiang, Y., Yeh, K.H.: Privacy enhancing technologies in the Internet of Things: Perspectives and challenges. IEEE Internet of Things Journal (2018)
22. Chang, H.H., Wong, K.H., Lee, H.C.: Peer privacy protection motivation and action on social networking sites: Privacy self-efficacy and information security as moderators. Electronic Commerce Research and Applications (2022)

23. Colnago, J., Feng, Y., Palanivel, T., Pearman, S., Ung, M., Acquisti, A., Cranor, L.F., Sadeh, N.: Informing the Design of a Personalized Privacy Assistant for the Internet of Things. In: Proc. of the Conf. on Human Factors in Computing Systems (CHI) (2020)
24. Coopamootoo, K.P.: Usage patterns of privacy-enhancing technologies. In: Proc. of ACM CCS (2020)
25. Curzon, J., Almehmadi, A., El-Khatib, K.: A survey of privacy enhancing technologies for smart cities. Pervasive and Mobile Computing (2019)
26. Darwish, R., Ghazinour, K.: A Novel Approach for Studying Privacy Behavior in Social Media. In: IEEE Inter. Conf. on Computational Science and Computational Intelligence (2017)
27. Das, A., Degeling, M., Smullen, D., Sadeh, N.: Personalized Privacy Assistants for the Internet of Things: Providing Users With Notice and Choice. IEEE Pervasive Computing (2018)
28. Das, S., Faklaris, C., Hong, J.I., Dabbish, L.A., et al.: The Security & Privacy Acceptance Framework (SPAF). Foundations and Trends in Privacy and Security (2022)
29. De Luca, A., Das, S., Ortlieb, M., Ion, I., Laurie, B.: Expert and {Non-Expert} Attitudes Towards (Secure) Instant Messaging. In: Proc. 12th Usable Privacy and Security (SOUPS) (2016)
30. Derlega, V.J., Chaikin, A.L.: Privacy and Self-disclosure in Social Relationships. Journal of Social Issues (1977)
31. Dourish, P., Grinter, R.E., Delgado De La Flor, J., Joseph, M.: Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem. Personal and Ubiquitous Computing (2004)
32. Fishbein, M.: A Theory of Reasoned Action: Some Applications and Implications. (1979)
33. Fogg, B.J.: A Behavior Model for Persuasive Design. In: Proc. 4th International Conference on Persuasive Technology (2009)
34. Fugard, A.J., Potts, H.W.: Supporting thinking on sample sizes for thematic analyses: a quantitative tool. International journal of social research methodology (2015)
35. Ghazinour, K., Matwin, S., Sokolova, M.: Monitoring and Recommending Privacy Settings in Social Networks. In: Proc. of the Joint EDBT/ICDT Workshops (2013)
36. Ghazinour, K., Matwin, S., Sokolova, M.: Yourprivacyprotector, a Recommender System for Privacy Settings in Social Networks. International Journal of Security, Privacy and Trust Management (2013)
37. Guest, G., Bunce, A., Johnson, L.: How many interviews are enough? An experiment with data saturation and variability. Field methods (2006)
38. Harborth, D., Pape, S.: Examining Technology Use Factors of Privacy-Enhancing Technologies: the Role of Perceived Anonymity and Trust. In: Proc. of AMCIS (2018)
39. Harborth, D., Pape, S.: How Privacy Concerns and Trust and Risk Beliefs Influence Users' Intentions to Use Privacy-Enhancing Technologies-the Case of Tor. 52nd Hawaii International Conference on System Sciences (2019)
40. Harborth, D., Pape, S., Rannenberg, K.: Explaining the Technology Use Behavior of Privacy-Enhancing Technologies: The Case of Tor and Jondonym. Privacy Enhancing Technologies (2020)
41. Herbert, F., Becker, S., Schaewitz, L., Hielscher, J., Kowalewski, M., Sasse, A., Acar, Y., Dürmuth, M.: A World Full of Privacy and Security (Mis) Conceptions? Findings of a Representative Survey in 12 Countries. In: Proc. ACM Conference on Human Factors in Computing Systems (CHI) (2023)

42. Heurix, J., Zimmermann, P., Neubauer, T., Fenz, S.: A taxonomy for privacy enhancing technologies. Computers & Security (2015)
43. 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)
44. Klasnja, P., Consolvo, S., Choudhury, T., Beckwith, R., Hightower, J.: Exploring Privacy Concerns About Personal Sensing. In: Proc. 7th Pervasive Computing (2009)
45. Kokolakis, S.: Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon. Computers & security (2017)
46. Krontiris, I., Benenson, Z., Girard, A., Sabouri, A., Rannenberg, K., Schoo, P.: Privacy-abcs as a case for studying the adoption of pets by users and service providers. In: Proc. of APF (2015)
47. Krueger, R.A.: Focus groups: A practical guide for applied research. Sage publications (2014)
48. Lee, L., Fifield, D., Malkin, N., Iyer, G., Egelman, S., Wagner, D.: A Usability Evaluation of Tor Launcher. PoPETs (2017)
49. Liu, B., Andersen, M.S., Schaub, F., Almuhimedi, H., Sadeh, N., Agarwal, Y., Acquisti, A.: To Deny, or Not to Deny: A Personalized Privacy Assistant for Mobile App Permissions. FTC PrivacyCon (2016)
50. Liu, B., Schaarup Andersen, M., Schaub, F., Almuhimedi, H., Zhang, S., Sadeh, N., Acquisti, A., Agarwal, Y.: Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions. In: Proc. 12th Symposium on Usable Privacy and Security (SOUPS) (2016)
51. Liu, C., Zhu, T., Zhang, J., Zhou, W.: Privacy Intelligence: A Survey on Image Privacy in Online Social Networks. ACM Comp. Surv. (2022)
52. Mangiò, F., Andreini, D., Pedeliento, G.: Hands off My Data: Users' Security Concerns and Intention to Adopt Privacy Enhancing Technologies. Italian Journal of Marketing (2020)
53. Marx, G.T.: Murky Conceptual Waters: The Public and the Private. Ethics and Information Technology (2001)
54. Matt, C., Peckelsen, P.: Sweet Idleness, but Why? How Cognitive Factors and Personality Traits Affect Privacy-Protective Behavior. In: 2016 49th Hawaii International Conference on System Sciences (HICSS). IEEE (2016)
55. Mayring, P., et al.: Combination and integration of qualitative and quantitative analysis. In: Forum Qualitative Sozialforschung/Forum: Qualitative Social Research (2001)
56. Mehrnezhad, M., Coopamootoo, K., Toreini, E.: How Can and Would People Protect From Online Tracking? Proc. Privacy Enhancing Technologies (2021)
57. Melzi, P., Rathgeb, C., Tolosana, R., Vera-Rodriguez, R., Busch, C.: An overview of privacy-enhancing technologies in biometric recognition. ACM Computing Surveys (2024)
58. Mendel, T., Toch, E.: Meerkat: A Social Community Support Application for Older Adults. In: CHI Conference on Human Factors in Computing Systems Extended Abstracts (2022)
59. Menges, U., Hielscher, J., Kocksch, L., Kluge, A., Sasse, M.A.: Caring not scaring-an evaluation of a workshop to train apprentices as security champions. In: Proc. of the 2023 European Symposium on Usable Security (2023)
60. Miltgen, C.L., Peyrat-Guillard, D.: Cultural and Generational Influences on Privacy Concerns: A Qualitative Study in Seven European Countries. European journal of information systems (2014)

61. Morse, J.M.: The significance of saturation (1995)
62. Nah, F., Tan, C.H.: HCI in Business: A Collaboration with Academia in IoT Privacy (2015)
63. Namara, M., Wilkinson, D., Caine, K., Knijnenburg, B.P.: Emotional and Practical Considerations Towards the Adoption and Abandonment of VPNs as a Privacy-Enhancing Technology. Proc. Privacy Enhancing Technologies (2020)
64. Nielsen, J.: Enhancing the Explanatory Power of Usability Heuristics. In: Proc. Human Factors in Computing Systems (SIGCHI) (1994)
65. Nissenbaum, H.: Privacy as Contextual Integrity. Wash. L. Rev. (2004)
66. Nissenbaum, H.: Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press (2009)
67. Nissenbaum, H.: Respecting Context to Protect Privacy: Why Meaning Matters. Science and engineering ethics (2018)
68. Olejnik, K., Dacosta, I., Soares Machado, J., Huguenin, K., Khan, M.E., Hubaux, J.P.: SmarPer: Context-Aware and Automatic Runtime-Permissions for Mobile Devices. In: IEEE S&P (2017)
69. Palinkas, L.A., Horwitz, S.M., Green, C.A., Wisdom, J.P., Duan, N., Hoagwood, K.: Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. Administration and policy in mental health and mental health services research (2015)
70. Patton, M.Q.: Qualitative research & evaluation methods: Integrating theory and practice. Sage publications (2014)
71. Pfleeger, S.L., Sasse, M.A., Furnham, A.: From Weakest Link to Security Hero: Transforming Staff Security Behavior. Journal of Homeland Security and Emergency Management (2014)
72. Phelps, J., Nowak, G., Ferrell, E.: Privacy Concerns and Consumer Willingness to Provide Personal Information. Journal of public policy & marketing (2000)
73. Racine, E., Skeba, P., Baumer, E.P., Forte, A.: What are PETs for Privacy Experts and Non-experts. In: Proc. Symposium on Usable Privacy and Security (2020)
74. Rad, M.S., Nilashi, M., Dahlan, H.M.: Information Technology Adoption: A Review of the Literature and Classification. Universal Access in the Information Society (2018)
75. Rader, E., Wash, R., Brooks, B.: Stories as Informal Lessons About Security. In: Proc. 18th Symposium on Usable Privacy and Security (2012)
76. Raman, R., ABDALLA MIKHAEIL, C., James, T., Venkatesh, V.: Cultural differences in the adoption of privacy-enhancing technologies. AMCIS TREOs (2024)
77. Redmiles, E.M., Warford, N., Jayanti, A., Koneru, A., Kross, S., Morales, M., Stevens, R., Mazurek, M.L.: A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web. In: Proc. 29th USENIX Security Symposium (2020)
78. Renaud, K., Volkamer, M., Renkema-Padmos, A.: Why Doesn't Jane Protect Her Privacy? In: Proc. 14th International Symposium om Privacy Enhancing Technologies (2014)
79. Rogers, E.M.: Diffusion of Innovations the Free Press of Glencoe. NY (1962)
80. Seymour, W., Kraemer, M.J., Binns, R., Van Kleek, M.: Informing the Design of Privacy-Empowering Tools for the Connected Home. In: Proc. of the CHI Conf. on Human Factors in Computing Systems (2020)
81. Shams, S., Reinhardt, D.: Vision: Supporting Citizens in Adopting Privacy Enhancing Technologies. In: Proc. European Symposium on Usable Security (2023)
82. Shams, S., Reinke, S., Reinhardt, D.: Left Alone Facing a Difficult Choice: An Expert Analysis of Websites Promoting Selected Privacy-Enhancing Technologies. In: Proc. of the 29th Nordic Conference on Secure IT Systems (NordSec) (2024)

83. Solove, D.J.: Introduction: Privacy Self-management and the Consent Dilemma. Harv. L. Rev. (2012)
84. Sombatruang, N., Omiya, T., Miyamoto, D., Sasse, M.A., Kadobayashi, Y., Baddeley, M.: Attributes Affecting User Decision to Adopt a Virtual Private Network (VPN) App. In: Proc. 22nd Information and Communications Security (ICICS). Springer (2020)
85. Stokes, J., August, T., Marver, R.A., Czeskis, A., Roesner, F., Kohno, T., Reinecke, K.: How Language Formality in Security and Privacy Interfaces Impacts Intended Compliance. In: Proc. Human Factors in Computing Systems (CHI) (2023)
86. Story, P., Smullen, D., Yao, Y., Acquisti, A., Cranor, L.F., Sadeh, N., Schaub, F.: Awareness, Adoption, and Misconceptions of Web Privacy Tools. Proc. Privacy Enhancing Technologies (2021)
87. Stutzman, F.D., Gross, R., Acquisti, A.: Silent Listeners: The Evolution of Privacy and Disclosure on Facebook. Journal of Privacy and Confidentiality (2013)
88. Tan, H.Z., Zhao, W., Shen, H.H.: A Context-Perceptual Privacy Protection Approach on Android Devices. In: IEEE International Conf. on Communications (ICC) (2018)
89. Tsai, L., Wijesekera, P., Reardon, J., Reyes, I., Egelman, S., Wagner, D., Good, N., Chen, J.W.: Turtle Guard: Helping Android Users Apply Contextual Privacy Preferences. In: SOUPS (2017)
90. Udo, G.J.: Privacy and Security Concerns as Major Barriers for E-commerce: A Survey Study. Information management & computer security (2001)
91. Ur, B., Leon, P.G., Cranor, L.F., Shay, R., Wang, Y.: Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising. In: Proc. 8th Symposium on Usable Privacy and Security (SOUPS) (2012)
92. Van Schaik, P., Renaud, K.V.: PEDRO: Privacy-Enhancing Decision suppoRt tOol. Preprints (2024)
93. Vasileiou, K., Barnett, J., Thorpe, S., Young, T.: Characterising and justifying sample size sufficiency in interview-based studies: systematic analysis of qualitative health research over a 15-year period. BMC medical research methodology (2018)
94. Volkamer, M., Renaud, K.: Mental models-general introduction and review of their application to human-centred security. In: Number theory and cryptography: Papers in honour of Johannes Buchmann on the occasion of his 60th birthday (2013)
95. Wijesekera, P., Reardon, J., Reyes, I., Tsai, L., Chen, J.W., Good, N., Wagner, D., Beznosov, K., Egelman, S.: Contextualizing Privacy Decisions for Better Prediction (and Protection). In: Proc. of the CHI Conf. on Human Factors in Computing Systems. (2018)
96. Xu, A., Zhou, Z., Miyazaki, K., Yoshikawa, R., Hosio, S., Yatani, K.: DIPA2: An Image Dataset with Cross-cultural Privacy Perception Annotations. Proc. ACM IMWUT (2024)
97. Xu, H., Teo, H.H., Tan, B.C., Agarwal, R.: The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-based Services. Journal of Management Information Systems (2009)
98. Yang, S., Lu, Y., Gupta, S., Cao, Y.: Does Context Matter? The Impact of Use Context on Mobile Internet Adoption. International Journal of HCI (2012)
99. Zibuschka, J., Horsch, M., Kubach, M.: The ENTOURAGE Privacy and Security Reference Architecture for Internet of Things Ecosystems. Open Identity Summit (2019)