applied sciences

MDPI

Article

PEDRO: Privacy-Enhancing Decision suppoRt tOol

Paul van Schaik [1,†] and Karen Renaud [2,*,†]

[1] Department of Psychology, School of Social Sciences, Humanities and Law, Teesside University, Middlesbrough TS1 3BA, UK; p.van-schaik@tees.ac.uk
[2] Department of Computer and Information Sciences, University of Strathclude, Glasgow G1 1XQ, UK
* Correspondence: karen.renaud@strath.ac.uk
† These authors contributed equally to this work.

Abstract: Citizens face online privacy threats from social media, online service providers and governments. Privacy-enhancing tools (PETs) can prevent privacy invasion, but the uptake of these is limited. We developed a novel conceptual framework for privacy self-protection, consisting of a classification framework of four distinct privacy threats and our own novel staged model of PET adoption requisites. Through an expert survey (N = 12) and a lay user survey (N = 500), we identified suitable PETs for non-expert users and identified potential barriers to PET adoption. Based on the studies and our theoretical framework, we then developed and implemented a PET decision support tool called PEDRO, and conducted expert evaluations (N = 10) to confirm the validity of its recommendations.

Keywords: privacy-enhancing tool; technology adoption; stage model; PET decision support tool

1. Introduction

Privacy threats from social media and other online service providers are acknowledged, given that they collect personal information and use this to increase their profit margins [1]. Even so, Internet users employ these platforms and accept the privacy risks. The role of government, on the other hand, as a potential threat to digital privacy, is seldom considered. Citizens' privacy can easily be sacrificed by the heavy-handed actions of government agency employees. For example, in 2020, 'kiosks' were introduced by Police Scotland to triage mobile devices during police investigations. The kiosk software was able to extract extensive private information from a smart mobile device. After protests by NGOs and consequent debates in the Scottish Parliament [2], the Information Commissioner condemned the kiosks for potentially violating privacy rights of citizens [3]. The UK government is proposing the use of AI-powered facial recognition across the country [4], as does the Metropolitan Police in London [5] and railway stations across the UK [4]. The Big Brother Watch privacy watchdog is calling out these proposals for their potential to violate privacy (https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/, accessed on 7 October 2024). The UK's Regulation of Investigatory Powers Act 2000 (https://publications.parliament.uk/pa/cm201415/cmselect/cmhaff/711/71103.htm, accessed on 7 October 2024) provides powers to intercept the content of communications, for example, by listening to telephone conversations or voicemail messages, to a wide range of public authorities. As such, UK citizen privacy is under threat from a range of entities, both Big Brother (government) and Middle Brother (organisations).

Privacy-enhancing tools (PETs), such as virtual private networks (VPNs) and anonymous browsers, are available to online users who want to protect themselves from these kinds of privacy threats. Although some of these are widely advertised, the uptake of PETs remains modest, thereby reducing the potential of users to protect their privacy online. A recent (April 2024) survey [6] found that 80% of a UK sample (N = 201) had heard of at least one of the following PETs: VPNs, device encryption, webcam covers, non-tracking search engines, anonymous browsers, and Faraday bags. However, 49% had not used any of these

check for updates

Citation: van Schaik, P.; Renaud, K. PEDRO: Privacy-Enhancing Decision suppoRt tOol. *Appl. Sci.* **2024**, *14*, 9275. https://doi.org/10.3390/app14209275

Academic Editor: Douglas O'Shaughnessy

Received: 7 September 2024
Revised: 30 September 2024
Accepted: 8 October 2024
Published: 11 October 2024

PETs in the last year and 63% were currently not using any. Moreover, even if users were to use one particular PET, this would only partly protect them, as different PETs protect from their own distinct kinds of privacy threats.

Although 100% protection is infeasible, using a range of different PETs that each protect against a specific class of privacy threats will result in a more comprehensive privacy protection regime. This paper outlines how a decision support tool called PEDRO was developed to help online users to encourage the adoption of PETs. The design of this tool builds on an existing classification of privacy threats [7], our novel staged model of PET adoption, and empirical research that is presented in this paper.

The aim of PEDRO was to deconstruct common barriers to adoption based on the staged support of adoption requisites [8], advancing from privacy- and threat awareness towards achieving self-protection via PET adoption. Similar to the Transtheoretical Model [9], our approach challenges existing dominant 'stageless' theories of tool adoption, such as Protection Motivation Theory [10].

To develop the tool, we carried out three studies. The first was an expert survey of PETs, in which cybersecurity experts focused on the effectiveness and feasibility of PET adoption by lay users. The second study was a lay user survey of PETs, in which we asked crowd workers to rate their current adoption of PETs according to our adoption model and to identify PET adoption barriers. The third study developed and evaluated the PET adoption decision support tool (PEDRO), building on the insights gained from studies 1 and 2.

2. Background

2.1. Current State of Research

Existing research on classifying and adopting PETs is reviewed here, as this fed into our creation of the PEDRO adoption decision support tool.

2.1.1. Classification of Privacy-Enhancing Tools

Support for privacy-enhancing tool (PET) adoption decisions needs to build on a solid foundation of privacy threats. Such a classification allows researchers to compare PETs not only in terms of their capabilities [7], but also explicitly links each PET to the privacy threat(s) it mitigates. The Heurix et al.'s [7] taxonomy meets this need by linking privacy threats (called 'aims' in [7], pp. 6–7). The taxonomy builds on four distinct threats:

- Indistinguishability "*which makes it impossible to unambiguously distinguish an entity from another entity*". For example, if a snooper is able to distinguish one particular user from another, they can track the user's activities to violate their privacy; a VPN can prevent this.
- Confidentiality is the requirement to keep personal data "*protected from unintended disclosure*". Encryption keeps users' data and information protected from unintended disclosure, even if leaked.
- Deniability is "*the ability to plausibly deny a fact, possession or transaction*" and "*is the direct opposite of accountability*". For example, when an online user employs a private search engine, no one can link them to their searches, enhancing deniability.
- Unlinkability "*indicates that an entity cannot be linked to another entity where the entities need not necessarily be of the same class*". For example, when an online user makes use of a private browser, they cannot be linked to another piece of data (such as, for instance, personal identity and/or other visited sites).

2.1.2. Adoption of Privacy-Enhancing Tools

Existing research on privacy self-protection has focused on awareness or education [11–13]. Specifically, research has been conducted on a possible learning taxonomy for PETs [14,15], as well as privacy awareness and knowledge [16,17], but does not address other factors that contribute to PET adoption such as barriers to adoption and challenges faced by adoptees.

Stageless, multifactor technology acceptance modelling has a long tradition. Researchers have investigated the influence of a variety of factors on technology adoption.

Examples include the technology acceptance model (TAM) [18] and the unified theory of acceptance and use of technology (UTAUT) [19]. Influential factors on adoption include perceived usefulness and perceived ease of use. The technology acceptance model has been applied and extended to help understand users' acceptance of privacy-enhancing tools [20,21], but does not address the PET adoption process stages.

Another line of technology adoption research has used technology diffusion theory [22], which distinguishes a knowledge stage from a persuasion stage. This research has focused on (workers in) organisations rather than on personal adoption. Influential factors include relative advantage, ease of use, compatibility, image, result demonstrability, visibility, voluntariness, and trialability ([23], p. 507). However, this work has not addressed the adoption of privacy protection tools.

According to stageless protection models such as Protection Motivation Theory (PMT) [24], the Health Belief Model (HBM) [25], and the Theory of Planned Behaviour (TPB) [26], intention to protect oneself has a positive effect on self-protection behaviours, and intention itself is influenced by other social–cognitive variables such as threat and coping appraisal (in Protection Motivation Theory). The Theory of Planned Behaviour [27] and Protection Motivation Theory [28] have been applied to understand the determinants of the adoption of privacy-enhancing tools. However, by their nature, stageless models do not address the adoption process.

In staged protection models, such as the Transtheoretical Model of Change (TTM) [9], "*The stage dimension defines behaviour change as a process that unfolds over time and involves progress through a series of stages*" (p. 845). The TTM has mainly been used in health, but also in other domains such as reducing energy consumption [29]. Nevertheless, it has not been applied to PET adoption.

In sum, missing from the existing research is a model that explicitly represents the staged PET adoption process. The current study contributes to support for PET adoption by proposing such a model and uses this as a basis for developing the PEDRO decision support tool to encourage the adoption of PETs by removing barriers to adoption.

2.2. PET Adoption

The aim of PETs and encouraging their adoption is to cultivate citizens' self-protective behaviour. For this, we developed a novel staged PET adoption model (Figure 1). The central idea of the model is the staged development of adoption requisites [8], advancing from privacy and threat awareness towards achieving adoption of a range of PETs. Similar to the Transtheoretical Model [9], our approach challenges existing dominant 'stageless' models of self-protection, such as Protection Motivation Theory [10].

PET adoption is not a one-off simple A-or-B decision; such adoption is a process [30], similar to other kinds of adoption in this domain [31]. Consider that, for a PET to be adopted, the adopter needs to proceed through a number of stages, as shown in Figure 1:

Stage 1. Awareness of privacy threats [32,33].
Stage 2. Wanting to preserve privacy [34].
Stage 3. Knowing about privacy enhancing tools (PETs) [35,36].
Stage 4. Believing that PETs will enhance privacy [37].
Stage 5. Knowing how to use the PET [38,39].
Stage 6. Feeling empowered to use the PET [40].
Stage 7. Not being afraid to use the PET [41].

If all these stages are successfully traversed, adoption becomes possible.

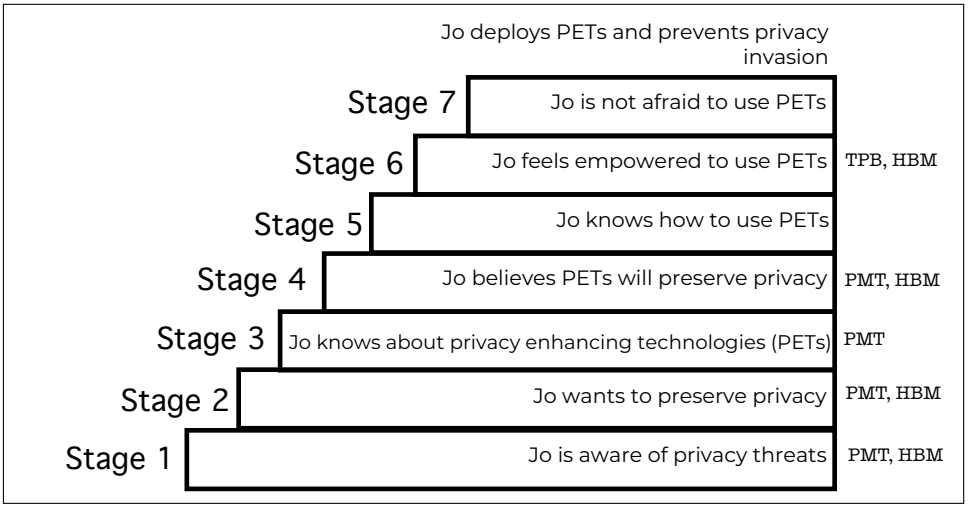

Figure 1. Stage model of PET adoption.

3. Study 1: Experts

We recruited cybersecurity experts using snowball sampling based on personal contacts. They completed a survey to give us insights into the feasibility of PET adoption by lay users. Our expert survey of PETs was guided by the following research question: RQ1: Which PETs do experts believe are feasible for lay users to use? For each of the broad threat categories of: (a) distinguishability, (b) linkability, (c) lack of confidentiality, and (d) lack of deniability (see Section 2.1.1), we identified both software- and hardware-based tools that effectively mitigate each kind of privacy threat (Table 1).

Table 1. Privacy threats (PT*i*) and PETs that counter them.

Privacy Threat [7]	Software PET	Hardware PET
PT1. Distinguishability	Virtual private network (VPN)	Switch off microphone on smart TV
PT2. Lack of confidentiality	Encryption	Webcam cover
PT3. Lack of deniability	Private search engine	Anonymous letter
PT4. Linkability	Anonymous browser	Wrapping smartphone in tin foil

We developed an online survey (https://osf.io/up83r/?view_only=7c89cb6f0d85423cbcf152d141074c11, accessed on 7 October 2024). For each of the chosen PETs, the survey asked about the effectiveness of, feasibility of, challenges of, and ways to encourage the use of PETs that home users could install and deploy.

3.1. Materials and Methods

A list of feasible PETs (for home users) with their features was produced (Table 1).

We surveyed 12 experts to gauge the feasibility of PET usage by non-expert home users (i.e., choose, install, and deploy) and the effectiveness thereof in mitigating the applicable privacy threat.

Metric. We considered PETs to be infeasible for home usage if a majority of experts did not believe the PET was either feasible for home users (i.e., non-experts) or if its effectiveness in mitigating the threat was questioned.

Recruitment. We used personal contacts and snowball sampling to contact privacy experts in the UK and USA. The UK participants were compensated with shopping vouchers.

Participants. There were 12 participants (10 male; 2 female).

3.2. Results and Discussion

The experts did not consider "switching the microphone off" and "anonymous letters" to be feasible, nor did they consider the former particularly effective (Table 2). There was general agreement that all the others could be adopted and are effective to a certain extent, with a general lack of awareness being considered the major deterrent (Table 2). We also considered the experts' personal usage of each specific PET in deciding whether to retain a PET for our next study.

Table 2. Evaluation of PETs by cybersecurity experts (PT*i* = privacy threat from Table 2).

	Effectiveness; Feasibility	**Challenges**	**Barriers**	**How to Encourage**
Switch Off TV Microphone (PT1)	10 Effective/2 Not; 10 Feasible/2 Not	Complicated; finding setting; TV untrustworthy	Setting not available; apathy; loss of features	Awareness
	2 always do; 1 sometimes do; 2 never do; 7 do not own a smart TV			
Webcam Cover (PT2)	12/12 Effective; 12/12 Feasible	None	Cost; bulky covers	Stories; awareness
	8 use; 2 do not use; 1 used to but does not anymore; 1 did not want to say			
Anonymous Letter (PT3)	12/12 Effective; 12/12 Feasible	Old fashioned; loss of letter; hard to mail; hard to be anonymous; effort	CCTV; cost; cumbersome; time	Hard to see purpose; reduce apathy
	2 have written an anonymous letter; 9 have not; 1 did not want to say			
Wrapping Phone (PT4)	7 Effective/5 Not; 4 Feasible/8 Not	Not easy to use; lack of convenience; additional steps	Prevents phone working; cost; stigma; perception of paranoia	Awareness
	10 never used; 1 prefer not to say			
VPN (PT1)	10 Effective/2 Not; 10 Feasible/2 Not	Installing and understanding; initial setup; use of CAPTCHAs; non-functioning websites	Choosing trustworthy providers; skills and mental models; device compatibility; cost; some devices do not support; language; govt. prohibition	Awareness; secure defaults; reduce cost; improve usability
	12 use a VPN			
Encryption (PT2)	11 Effective/1 Not; 10 Feasible/2 Not	Worries about losing encryption key; complicated	Difficult to install; age-related accessibility issues	Awareness; know-how; make encryption default
	8 use on all devices; 2 do not; 2 prefer not to say			
Non-Tracking Search Engine (PT3)	11 Effective/1 Not; 11 Feasible/2 Not	Finding a suitable one; knowing how to change default search engine; change resistance; lock into Google in software apps	Not knowing which one to use; poor quality of search results; some results not being shown; inaccessibility	Awareness
	6 use a non-tracking search engine; 5 do not; 1 prefer not to say			
Anonymous Browser (PT4)	10 Effective/2 Not; 9 Feasible/3 Not	Usability issues; difficulty installing; speed issues; hard to configure; change resistance	Too complex; worried that it is only for bad people; speed; TOR blocking; govt. monitoring; language	Awareness; do not encourage; distribute by default; instructions; feedback
	7 sometimes use; 4 do not; 1 prefer not to say			

3.3. Conclusions

From study 1, the answer to **RQ1:** (*Which PETs do experts believe are feasible for lay users to use?*) is that the PETs that should be considered for inclusion in our decision support tool are VPN, encryption, non-tracking search engine, anonymous browser, wrapping phones, and webcam covers.

4. Study 2: Lay Users

We surveyed 500 crowd workers to identify PET adoption barriers to address the following research questions: **RQ2a:** *What is the level of PET adoption by lay Internet users*; and **RQ2b:** *What barriers prevent people from using PETs?*

4.1. Materials and Methods

4.1.1. Research Design and Procedure

We used a 1-factor survey design with two survey conditions (one for software PETs and another for hardware PETs). The factor was PET (Table 1) and most of the PETs were as used in study 1 (see Section 3), with face mask substituted for switching off microphone on smart TV. For each PET, we (a) explained the privacy threat, (b) introduced the mitigating PET, (c) took them step-by-step through the stages shown in Table 1 and asked for their position regarding the adoption barrier in each of the stages.

4.1.2. Instrumentation and Participants

We constructed an online survey (https://osf.io/up83r/?view_only=7c89cb6f0d85423cbcf152d141074c11, accessed on 7 October 2024) that was implemented in two versions: one for hardware PETs and another for software PETs. For each of the PETs, the survey posed a set of questions according to the stage model (Table 3 and Figure 1). Five hundred crowd workers were recruited from an online survey panel to take part in the survey. In the hardware PET condition, 255 took part and in the software PET condition 245. There were 100 participants in each of the age bands 18–30, 31–40, 41–50, 51–60, and over 60. There were 252 female and 248 male participants.

Table 3. Survey questions to analyse PET adoption barriers. Stages refer to Figure 1.

Stage 1	Have you heard of this privacy threat?
Stage 2	How important is it to you to prevent this kind of privacy threat?
Stage 3	Have you heard of this PET?
Stage 4	To what extent do you think this PET will prevent this kind of privacy threat?
Stage 5	Do you know how to use this PET?
Stage 6	Do you feel empowered (encouraged and supported) to use this PET?
Stage 7	Are you afraid to use this PET?
	Do you use this PET?
	(If used to but not anymore) Why have you stopped using this PET? (If no) Why do you not use this PET? (If yes) Why do you think other people might not use this PET?

4.2. Results

4.2.1. Adoption Model Stages

Model stage 1. A majority of participants were familiar with the privacy principle of confidentiality (hardware condition: 67%; software condition: 76%), but only a minority were familiar with the principles of deniability, indistinguishability, and unlinkability (18–35%).

Model stage 2. A majority (hardware: 79%; software: 75%) considered confidentiality very or extremely important, but, in comparison, for the other principles the figure varied around 50% (38–57%).

Model stage 3. The majority were familiar with the following PETs: encryption (85%), VPN (82%), and webcam cover (67%), but the majority were unfamiliar with wrapping phone (83%), face mask (78%), and anonymous letter (62%). Roughly equal numbers were familiar or unfamiliar with non-tracking search engines (45–47%) or anonymous browsing (46–47%).

Model stage 4. A majority (58%) found encryption either quite or very effective. Most of the other PETs were found to be either effective or quite or very effective by a majority. However, this was a minority for face masks (32%) and wrapping phones (34%).

Model stage 5. For all the PETs, only a minority knew how to use them. Compared to other PETs, the number of those with knowledge of how to use a VPN was relatively high (49%), but for encryption the number without this knowledge was relatively high (56%).

Model stage 6. A majority felt empowered to use a webcam cover (64%) or a VPN (60%). The feeling of empowerment was equally split for encryption and non-tracking search engine. A majority did not feel empowered to use anonymous browsing (57%), anonymous letter (75%), face mask (82%), or tin foil (83%).

Model stage 7. Fear to use was relatively low for each PET (1–18%).

PET use. Current users were the minority for each PET. These were relatively large minorities for webcam cover (28%) and VPN (25%). Next, were encryption (16%), anonymous browsing (14%), and non-tracking search engine (11%). Anonymous letter, face mask, and tin foil were used by 5% or less.

4.2.2. Extent of Privacy Self-Protection

By definition, users will more fully self-protect their privacy the more PETs they use. Therefore, we undertook an analysis of the extent of self-protection ('defence in breadth') in terms of the number of PETs in relation to the adoption model stages, including PET use (Figure 2).

Hardware PETs. There was limited evidence for defence in breadth for the different model stages, and even less so for PET use. For each of the model stages, the percentage of users declined with the number of PETs.

Software PETs. There was limited evidence for defence in breadth for familiarity with privacy threat and knowledge how to use PET, and even less so for PET use. For the model stages familiarity with privacy threat, knowing how to use a particular PET, and PET use, the percentage of users declined with the number of PETs. However, this trend did not occur, and the distribution was more even, for familiarity with PETs and feeling empowered to use PETs.

Overall, the majority of users did not employ any of the PETs. Therefore, only a minority of users employed one PET. Even fewer users employed more than one PET. In conclusion, the respondents did not protect themselves against a range of threats to their online privacy by adopting PETs.

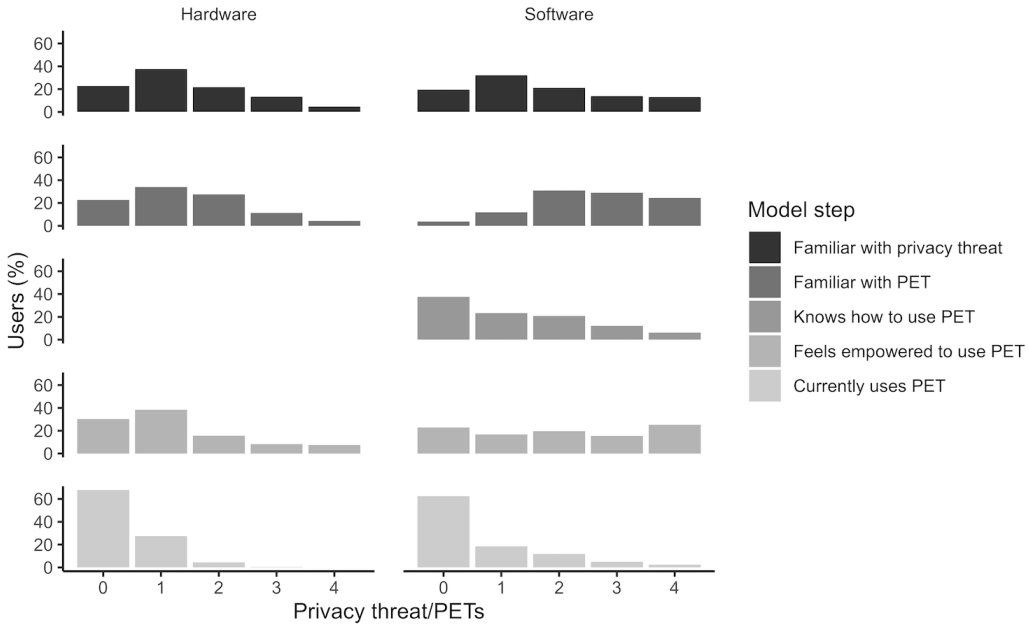

Figure 2. Frequency distribution of PETs per model stage ('defence in breadth') (study 2).

4.2.3. Barriers to PET Adoption

A thematic content analysis was conducted of the open-ended questions asking about reasons for not using a PET, reasons for stopping PET use, reasons why others may not use a PET, and reasons for fear of using a PET (Table 4). The sub-themes (with more than one

response providing evidence for a theme) from the analysis are barriers to PET use. These were organised in main themes and are presented in Table 4. The largest main themes (in terms of the number of sub-themes) are a lack of awareness or perceived benefit and incompatibility with ways of working or other technology. Other main themes are a lack of knowledge, a lack of empowerment, a lack of social acceptance, and a lack of trust. The main themes provide further support for our stage model of PET adoption. In particular, a lack of PET awareness represents the model stages awareness of privacy threat and awareness of PET. The theme of a lack of perceived benefit represents the model stage effectiveness. Incompatibility is not explicitly represented in the stage model, but could cause a lack of empowerment. A lack of knowledge represents the model stage knowing how to use a particular PET and a lack of empowerment represents the stage empowerment to use the PET. A lack of social acceptance could be a cause for a lack of empowerment and a lack of trust could be a cause for not using the PET, although neither of these lacks are explicitly represented in the stage model.

Table 4. Barriers to PET adoption (study 2)—stages *i* from Figure 1.

Lack of Awareness or Perceived Benefit (Stage 1/2/4)
The user is not aware of the privacy threat and/or a particular PET to protect themselves against the privacy threat (stage 1).
The user does not feel a need to use a PET to protect this privacy aspect/does not want to protect this privacy aspect (stage 2).
The user sees no need for using the PET because of their misunderstanding of the technical aspect of the privacy threat.
The user feels the PET (e.g., a letter) will not be effective at preserving their privacy (stage 4).
The user feels that the benefits of the PET are less than the effort required ('privacy calculus' (stage 4).
The user has the habit of using convenient technology without the PET (stage 4).
The protection mechanism that the PET provides is not appropriate for the activity/work the user does (stage 4).
The user does not use the technology/activity that would require using the PET.
The user employs another solution instead of using the PET or the PET is already installed.
The PET is prohibitively expensive or a cheaper alternative is available.
Lack of Knowledge (Stage 2/5)
The user feels they have insufficient knowledge about the PET (Stage 2).
The user sees no need for using the PET because of their misunderstanding of the technical aspect of the privacy threat.
Lack of Trust (Stage 4)
The user does not trust the PET to protect their privacy.
Lack of Empowerment (Stage 6)
The user does not feel empowered to use the PET.
Lack of social acceptance.
Incompatibility with ways of working or other technology.
The PET (e.g., webcam cover) can damage hardware (webcam) or is incompatible with other technology.
The PET has known unfavourable consequences/side effects.
Afraid to Use (Stage 7)
The PET poses a threat to security.
The PET (e.g., webcam cover) can reduce performance or functionality of hardware (webcam) and software.

Note: Main themes in italic. Sub-themes as plain text.

4.3. Conclusions

We can now answer **RQ2a** (*What is the level of PET adoption by lay Internet users*). The level of PET adoption varied considerably between model stages. In particular, in stage 1 (awareness of privacy principle) and stage 2 (importance of privacy principle) the level was either high or low; in stage 3 (awareness of PET), high or middling; in stage 4 (effectiveness of PET), predominantly high, but also middling or low; in stage 5 (knowing how to use PET) and stage 6 (empowerment), middling or low, in stage 7 (fear), low. In addition, the extent to which PETs were used varied, but a majority did not use each of the PETs. The stage model results provide a PET adoption baseline. The introduction of the PET decision support tool may increase adoption.

With respect to **RQ2b**, (*What barriers prevent people from using PETs?*), we found a number of barriers that impact PET adoption, which aligned with our staged model. These will be used to organise the guidance for non-specialist users within the tool (study 3). Based on the barriers that were identified, anonymous letter and face mask were not included in the design of the PET decision support tool (study 3). This is because our sample did not consider these to be socially acceptable or effective. In the remaining set

of PETs, there is considerable variation in the level of adoption at the different adoption model stages and between PETs.

The conclusion from studies 1 and 2 is that the PETs that should be considered for inclusion in our decision support tool are VPN, encryption, non-tracking search engine, anonymous browser, Faraday bag (Note that we moved from "wrapping phone" to the more effective 'Faraday bag' for this decision support tool, the latter being more effective than the former), and webcam cover.

5. Study 3: PEDRO: Design, Implementation, and Evaluation

5.1. Design and Implementation

The design of the PEDRO (PET Decision Support Tool) website was implemented using HTML to preserve the privacy of users, and uses JavaScript version 3.7.1 to support interactivity (see Figures 3–5).

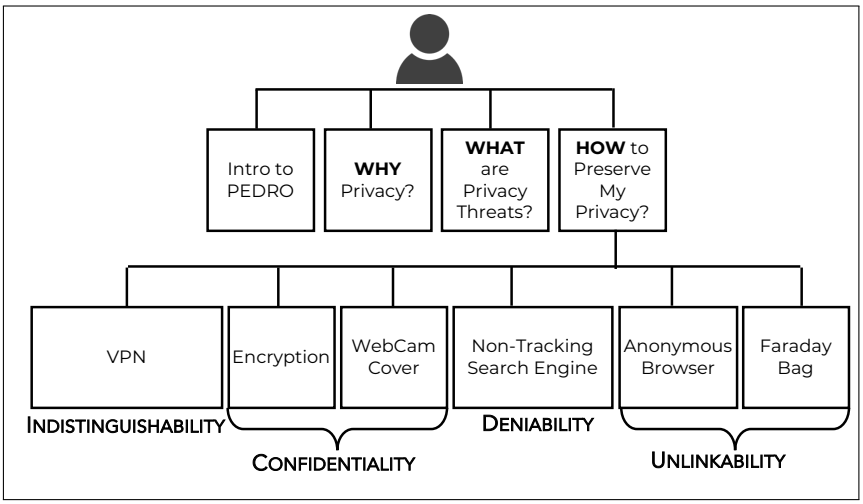

Figure 3. PEDRO architecture.

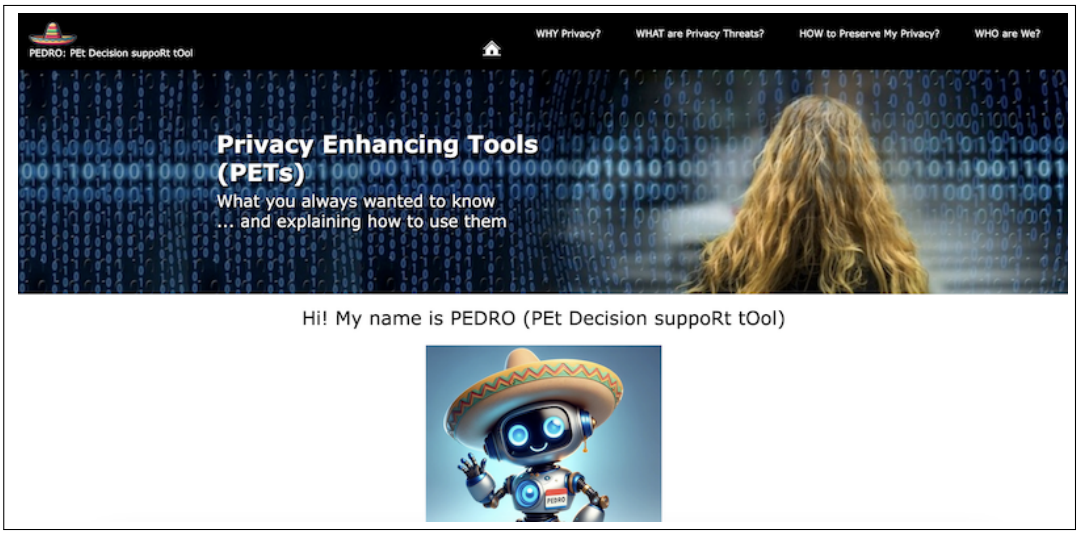

Figure 4. PEDRO home page.

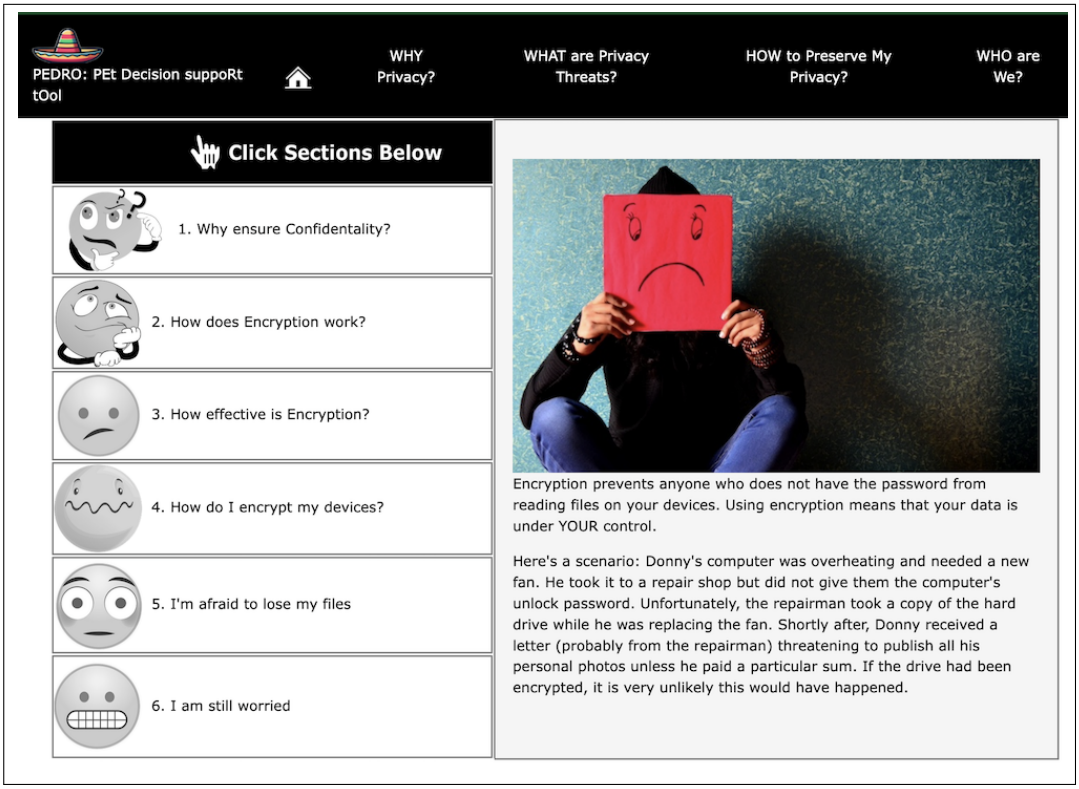

Figure 5. Confidentiality 'how' page.

PEDRO addresses each of the privacy threats introduced in the background section, and also explains why privacy is important (Section 2), what privacy threats exist (Section 1), and how privacy can be assured in the face of these threats (Section 3). In some cases, advice is directly provided, and, in others, helpful YouTube videos are embedded. URLs for advice sources are provided.

The core page for each of the six PETs is interactive, addressing each of the adoption requisites shown in Figure 1 and providing information that can remove those barriers. Each of the pages opens with a story—originally generated by ChatGPT version 4oand tweaked as feedback was provided by experts. All images on the site are either non-copyrighted or generated by ChatGPT to match the context. Each emoticon in the left panel can be clicked on, with the information on the right changing to provide specific information (see Figure 5).

5.2. Expert Evaluation

We carried out two studies to validate the website: the first with five cybersecurity experts and the second with five usability experts. All experts were recruited via convenience sampling and given shopping vouchers to thank them. An online form was created with screenshots of every PEDRO page. Under the screenshot was a text area where they could provide comments on that page, whether related to the veracity of the advice or comments on usability issues. All feedback was used to iteratively improve the website as each evaluator reported issues. For a final check, one cybersecurity expert and one usability expert evaluated the revised version of the tool, and, based on their feedback, the tool was improved one last time. The production version is hosted at https://pedro.infinityfreeapp.com/index.html, accessed on 7 October 2024., see Supplementary Materials.

6. General Discussion

The aim of this study was to cultivate citizens' self-protective behaviour by developing, refining, and using a novel staged PET adoption model. Three studies were conducted.

First, in our expert survey of PETs, cybersecurity experts analysed the feasibility of PET adoption by lay users.

Second, in our lay user survey of PETs, crowd workers rated their level of adoption according to the stage model and identified PET adoption barriers. The conclusion from these two studies regarding the selection of PETs for use in the tool that was to be developed was the same: VPN, encryption, non-tracking search engine, anonymous browser, Faraday bag, and webcam cover.

Third, we then developed a PET decision support tool called PEDRO based on the results of study 1 and study 2. Specifically, the tool explicitly represents and addresses the adoption model stages. Specific barriers that were identified in study 2 were explicitly addressed in the content of the tool to promote PET adoption.

Previous research has studied people's use of existing PETs and grouping PETs without an underlying theoretical model [42]. Other research has proposed a user-centred approach to develop an interactive tool that assists citizens in the process of learning and adopting PETs without a theoretical framework for classifying privacy threats and PETs, without an underlying adoption model [43]. Previous research has also developed new PETs and studied their acceptance (for example, Lucier), but not provided decision support for PET use. Existing research has also studied people's interest in PET use [44] rather than PET decision support. In sum, previous research has not systematically designed and implemented decision support for PET use based on responses from experts and lay users. Our work is unique in addressing this design and implementation.

The decision support tool that has been developed opens opportunities for future work in several areas. Our conceptual framework, consisting of the stage adoption model together with the classification of privacy threats, allows for potential new PETs to be added.

Empirical evaluation of the tool will be important to establish to what extent using the tool leads to the adoption of PETs. In addition, when the tool has been publicised, responses by online users to the tool will be useful to further improve the tool design. In the first instance, non-specialist UK citizens and, more generally, citizens from English-speaking countries are the target user population. A potential further development is a foreign language version in collaboration with international partners. The potential impact of the tool will include increased PET use by online users and, as a result, better privacy self-protection against a range of privacy threats (defence in breadth).

7. Conclusions

Many PET adoption models rely on effective communication of the risks of not using a PET and the benefits of adopting one. This paper proposes a staged model, each stage of which represents a particular barrier to adoption which, if removed, could open the way to adoption of the tool. We have published the PEDRO website to address each of these barriers in turn to encourage PET adoption.

Supplementary Materials: The following supporting information can be accessed at https://pedro.infinityfreeapp.com/index.html, accessed on 7 October 2024.

Author Contributions: Conceptualization, P.v.S. and K.R.; Methodology, P.v.S. and K.R.; Software, K.R.; Investigation, P.v.S. and K.R.; Writing—original draft, P.v.S. and K.R.; Project administration, P.v.S.; Funding acquisition, P.v.S. and K.R. All authors have read and agreed to the published version of the manuscript.

Funding: The authors are grateful to REPHRAIN (EPSRC: EP/W032473/1) for financial support.

Institutional Review Board Statement: The study was conducted according to the guidelines of the Declaration of Helsinki, and approved by the Ethics Committee of the school of Computer and Information Science, University of Strathclyde (# 2592), 14 May 2024.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Data are available on request from the authors.

Acknowledgments: We thank Craig van Slyke for his advice and inputs into the design of PEDRO.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Debatin, B.; Lovejoy, J.P.; Horn, A.K.; Hughes, B.N. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *J. Comput.-Mediat. Commun.* **2009**, *15*, 83–108. https://doi.org/10.1111/j.1083-6101.2009.01494.x.
2. BBC. Police Scotland Cyber Kiosks 'Could Be Unlawful'. 2018. Available online: https://www.bbc.com/news/uk-scotland-46225771 (accessed on 7 October 2024).
3. Tibbitt, A. Privacy Watchdog Orders Police Scotland to up Standards at Mobile Phone Labs. 2021. Available online: https://theferret.scot/privacy-watchdog-orders-police-scotland-to-up-standards-at-mobile-phone-labs/ (accessed on 7 October 2024).
4. nna Gross.; Murgia, M. UK Government Seeks Expanded Use of AI-Based Facial Recognition by Police. 2023. Available online: https://www.ft.com/content/858981e5-41e1-47f1-9187-009ad660bbbd (accessed on 7 October 2024).
5. BBC. Met Police to Deploy Facial Recognition Cameras. 2020. Available online: https://www.bbc.com/news/uk-51237665# (accessed on 7 October 2024).
6. PureProfile. (Pureprofile). Prevalence of the use of privacy-enhancing technology. Personal communication, 2024.
7. Heurix, J.; Zimmermann, P.; Neubauer, T.; Fenz, S. A taxonomy for privacy enhancing technologies. *Comput. Secur.* **2015**, *53*, 1–17. https://doi.org/10.1016/j.cose.2015.05.002.
8. Rosenberg, A. *Philosophy of Social Science*; Westview Press: Boulder, CO, USA, 2008.
9. Prochaska, J.O. Decision making in the transtheoretical model of behavior change. *Med Decis. Mak.* **2008**, *28*, 845–849. https://doi.org/10.1177/0272989X08327068.
10. Prentice-Dunn, S.; Rogers, R.W. Protection motivation theory and preventive health: Beyond the health belief model. *Health Educ. Res.* **1986**, *1*, 153–161. https://doi.org/10.1093/her/1.3.153.
11. Alshehri, A.; Clarke, N.; Li, F. Privacy enhancing technology awareness for mobile devices. In Proceedings of the International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019), Nicosia, Cyprus, 15–17 July 2019; University of Plymouth: Plymouth, UK, 2019; pp. 73–88.
12. O'Hagan, J.; Saeghe, P.; Gugenheimer, J.; Medeiros, D.; Marky, K.; Khamis, M.; McGill, M. Privacy-enhancing technology and everyday augmented reality: Understanding bystanders' varying needs for awareness and consent. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* **2023**, *6*, 1–35. https://doi.org/10.1145/3569501.
13. Basyoni, L.; Tabassum, A.; Shaban, K.; Elmahjub, E.; Halabi, O.; Qadir, J. Navigating Privacy Challenges in the Metaverse: A Comprehensive Examination of Current Technologies and Platforms. *IEEE Internet Things Mag.* **2024**, *7*, 144–152. https://doi.org/10.1109/IOTM.001.2300197.
14. Paul, S.K.; Knox, D. A taxonomy and gap-analysis in digital privacy education. In *Proceedings of the International Symposium on Foundations and Practice of Security*; Springer: Cham, Switzerland, 2022; pp. 221–235. https://doi.org/10.1007/978-3-031-30122-3_14.
15. Klymenko, A.; Meisenbacher, S.; Messmer, F.; Matthes, F. Privacy-Enhancing Technologies in the Process of Data Privacy Compliance: An Educational Perspective. In Proceedings of the CIISR@ Wirtschaftsinformatik, Paderborn, Germany, 18 September 2023; pp. 62–69.
16. Gerber, N.; Gerber, P.; Drews, H.; Kirchner, E.; Schlegel, N.; Schmidt, T.; Scholz, L. FoxIT: Enhancing mobile users' privacy behavior by increasing knowledge and awareness. In Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust, Orlando, FL, USA, 5 December 2017; pp. 53–63.
17. Ghazinour, K.; Messner, K.; Scarnecchia, S.; Selinger, D. Digital-PASS: A simulation-based approach to privacy education. In Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society, London, UK, 11 November 2019; pp. 162–174. https://doi.org/10.1145/3338498.3358647.
18. Davis, F.D.; Venkatesh, V. Toward preprototype user acceptance testing of new information systems: Implications for software project management. *IEEE Trans. Eng. Manag.* **2004**, *51*, 31–46. https://doi.org/10.1109/TEM.2003.822468.
19. Blut, M.; Chong, A.; Tsiga, Z.; Venkatesh, V. Meta-analysis of the unified theory of acceptance and use of technology (UTAUT): Challenging its validity and charting a research agenda in the red ocean. *J. Assoc. Inf. Syst.* **2022**, *23*, 13–95.
20. Harborth, D.; Pape, S. Examining technology use factors of privacy-enhancing technologies: The role of perceived anonymity and trust. In Proceedings of the AMCIS 2018, New Orleans, LA, USA, 16–18 August 2018; p. 15.
21. Lucier, D.M.; Howell, R.T.; Okabe-Miyamoto, K.; Durnell, E.; Zizi, M. We make a nice pair: Pairing the mID with a NeuroTechnology privacy enhancing technology improves mID download intentions. *Comput. Hum. Behav. Rep.* **2023**, *11*, 100321. https://doi.org/10.1016/j.chbr.2023.100321.
22. Eaton, J.; Kortum, S. International technology diffusion: Theory and measurement. *Int. Econ. Rev.* **1999**, *40*, 537–570. https://doi.org/10.1111/1468-2354.00028.
23. Yuen, K.F.; Cai, L.; Qi, G.; Wang, X. Factors influencing autonomous vehicle adoption: An application of the technology acceptance model and innovation diffusion theory. *Technol. Anal. Strateg. Manag.* **2021**, *33*, 505–519. https://doi.org/10.1080/09537325.2020.1826423.

24. Rogers, R.W. A protection motivation theory of fear appeals and attitude change. *J. Psychol.* **1975**, *91*, 93–114. https://doi.org/10.1080/00223980.1975.9915803.
25. Maiman, L.A.; Becker, M.H. The health belief model: Origins and correlates in psychological theory. *Health Educ. Monogr.* **1974**, *2*, 336–353. https://doi.org/10.1177/109019817400200404.
26. Ajzen, I. The theory of planned behavior. *Organ. Behav. Hum. Decis. Process.* **1991**, *50*, 179–211. https://doi.org/10.1016/0749-5978(91)90020-T.
27. Yao, M.Z.; Linz, D.G. Predicting self-protections of online privacy. *CyberPsychology Behav.* **2008**, *11*, 615–617. https://doi.org/10.1089/cpb.2007.0208.
28. Matt, C.; Peckelsen, P. Sweet idleness, but why? How cognitive factors and personality traits affect privacy-protective behavior. In Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA, 5–8 January 2016; pp. 4832–4841.
29. AlSkaif, T.; Lampropoulos, I.; Van Den Broek, M.; Van Sark, W. Gamification-based framework for engagement of residential customers in energy applications. *Energy Res. Soc. Sci.* **2018**, *44*, 187–195. https://doi.org/10.1016/j.erss.2018.04.043.
30. Morton, A.; Sasse, M.A. Privacy is a process, not a PET: A theory for effective privacy practice. In Proceedings of the 2012 New Security Paradigms Workshop, Bertinoro, Italy, 18–21 September 2012; pp. 87–104. https://doi.org/10.1145/2413296.2413305.
31. Alkaldi, N.; Renaud, K. MIGRANT: Modeling smartphone password manager adoption using migration theory. *ACM SIGMIS Database DATABASE Adv. Inf. Syst.* **2022**, *53*, 63–95. https://doi.org/10.1145/3533692.3533698.
32. Caviglione, L.; Lalande, J.F.; Mazurczyk, W.; Wendzel, S. Analysis of human awareness of security and privacy threats in smart environments. In Proceedings of the Human Aspects of Information Security, Privacy, and Trust: Third International Conference, HAS 2015, Held as Part of HCI International 2015, Los Angeles, CA, USA, 2–7 August 2015. Proceedings 3; Springer: Cham, Switzerland, 2015; pp. 165–177.
33. Alkhalifah, A.; Al Amro, S. Understanding the Effect of Privacy Concerns on User Adoption of Identity Management Systems. *J. Comput.* **2017**, *12*, 174–182.
34. Deuker, A. Addressing the privacy paradox by expanded privacy awareness–the example of context-aware services. In Proceedings of the Privacy and Identity Management for Life: 5th IFIP WG 9.2, 9.6/11.4, 11.6, 11.7/PrimeLife International Summer School, Nice, France, 7–11 September 2009; Revised Selected Papers 5; Springer: Berlin/Heidelberg, Germany, 2010; pp. 275–283.
35. Story, P.; Smullen, D.; Yao, Y.; Acquisti, A.; Cranor, L.F.; Sadeh, N.; Schaub, F. Awareness, adoption, and misconceptions of web privacy tools. *Proc. Priv. Enhancing Technol.* **2021**, *2021*, 308–333.
36. Alsaleh, M.; Alomar, N.; Alarifi, A. Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. *PLoS ONE* **2017**, *12*, e0173284. https://doi.org/10.1371/journal.pone.0173284.
37. Gürses, S. PETs and their users: A critical review of the potentials and limitations of the privacy as confidentiality paradigm. *Identity Inf. Soc.* **2010**, *3*, 539–563. https://doi.org/10.1007/s12394-010-0073-8.
38. 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 Proceedings of the Privacy Technologies and Policy: Third Annual Privacy Forum, APF 2015, Luxembourg, Luxembourg, 7–8 October 2015; Revised Selected Papers 3; Springer: Cham, Switzerland, 2016; pp. 104–123.
39. Vemou, K.; Karyda, M. A classification of factors influencing low adoption of pets among sns users. In Proceedings of the Trust, Privacy, and Security in Digital Business: Proceedings 10th International Conference, TrustBus 2013, Prague, Czech Republic, 28–29 August 2013; Springer: Berlin/Heidelberg, Germany, 2013; pp. 74–84.
40. Poireault, K. Russia Blocks VPN Services in Information Crackdown. 2024. Available online: https://www.infosecurity-magazine.com/news/russia-blocks-vpn-services-2024/ (accessed on 7 October 2024).
41. HIDE.me. Using a VPN in Restrictive Countries—How To Bypass Censorship. 2024. Available online: https://hide.me/en/blog/using-a-vpn-in-restrictive-countries/ (accessed on 7 October 2024).
42. Coopamootoo, K.P. Usage patterns of privacy-enhancing technologies. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, 9–13 November 2020; pp. 1371–1390. https://doi.org/10.1145/3372297.342334.
43. Shams, S.; Reinhardt, D. Vision: Supporting Citizens in Adopting Privacy Enhancing Technologies. In Proceedings of the 2023 European Symposium on Usable Security, Copenhagen, Denmark, 16–17 October 2023; pp. 253–259. https://doi.org/10.1145/3617072.3617105.
44. Makin, D.A.; Ireland, L. The secret life of PETs: A cross-sectional analysis of interest in privacy enhancing technologies. *Policing: Int. J.* **2020**, *43*, 121–136. https://doi.org/10.1108/PIJPSM-07-2019-0124.