S. Shams and D. Reinhardt. Vision: Supporting Citizens in Adopting Privacy Enhancing Technologies. Proceedings of the 3rd European Symposium on Usable Security (EuroUSEC), pp. 253–259. October 2023.

Vision: Supporting Citizens in Adopting Privacy Enhancing Technologies

Shirin Shams
University of Göttingen, Institute of Computer Science
Göttingen, Germany
shirin.shams@uni-goettingen.de

Delphine Reinhardt
University of Göttingen, Institute of Computer Science
and Campus Institute Data Science
Göttingen, Germany
reinhardt@cs.uni-goettingen.de

ABSTRACT

We have witnessed an alarming growth in collecting citizens' information by businesses and organizations. The more citizens' information they collect, the greater their ability to utilize this knowledge for their own interests, often at the expense of society members. Despite the efforts made by privacy ecosystem members (such as researchers and regulatory entities) to protect citizens' privacy against data collectors, the low adoption of *Privacy Enhancing Technologies* (PETs) by citizens remains concerning. To address these concerns, this vision paper proposes a user-centred approach to develop a tool that assists citizens in adopting PETs effectively. To this end, we plan to (1) understand the factors contributing to low PETs adoption via methods such as focus groups and in-depth interviews, (2) design an interactive tool to support citizens in adopting PETs in a user-friendly manner, and (3) evaluate the tool's effectiveness through usability testing. The outcome will serve as an interactive tool which first receives the privacy concerns and needs of each user and then provides personalised PET recommendations accordingly.

CCS CONCEPTS

• **Security and privacy** → **Usability in security and privacy**; • **Human-centered computing** → *Empirical studies in HCI*.

KEYWORDS

Usable Privacy, Privacy Enhancing Technologies, Human Computer Interaction

ACM Reference Format:
Shirin Shams and Delphine Reinhardt. 2023. Vision: Supporting Citizens in Adopting Privacy Enhancing Technologies. In *2023 European Symposium on Usable Security (EuroUSEC 2023), October 16 & 17, 2023, Copenhagen, Denmark*. ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3617072.3617105

1 INTRODUCTION

Based on recent reports, out of the 8 billion world population, 5.18 billion people are now using the Internet [12, 43]. As Internet usage is growing, more citizens' data is collected by businesses, organisations, governments, and other entities. Furthermore, the availability of data analysis tools and methodologies has ushered in a new era for data collectors, enabling them to comprehensively analyze such data with the aim of exerting influence over users' decision-making processes. This exaggerates the power imbalance between citizens and these data collectors.

To address this imbalance, members across the whole privacy ecosystem (i.e., researchers, regulatory entities, privacy organisations, and privacy advocates) have spent tremendous effort to protect citizens' privacy in varied forms such as regulations, standalone technologies, and add-on tools. For example, General Data Protection Regulation (GDPR) in 2018 was a step forward for citizen privacy protection Europe-wide. With GDPR, citizens have the power to give or withdraw their consent regarding data collection. The lack of viable alternatives; however, is alarming and the case of citizens' privacy protection is not resolved yet. With the same aim, *Privacy Enhancing Technologies* (PETs) such as *Virtual Private Networks* (VPNs) have been available for citizens for privacy protection. The rate of PETs adoption; however, stayed low. The complexity of implementation and the wide array of available tools pose challenges in the effective adoption of such tools by citizens [29]. Also, when asking participants to list known PETs, most non-experts indicate technologies with a different primary function than privacy protection [38], which is disquieting.

One solution to tackle this situation is to support citizens in the process of learning and adopting PETs. To provide such support, we need fundamental knowledge about the different steps users take and obstacles they encounter when aiming to adopt PETs. However, we argue that such fundamental knowledge about citizens' experience before being able to use or adopt a PET is missing. The vision of our work, therefore, is to investigate the steps and hindering factors in PETs adoption, with the aim of developing a supporting tool. This tool aims to ease the process of learning about privacy risks and mitigating strategies, and to help users in adopting PETs of interest. Therefore, by adopting a user-centred approach, we will engage in user research, design, implement, and evaluate a supportive tool.

This paper is organized as follows: Sec. 2 explains the related works about citizens' privacy protection. Sec. 3 lays out the research questions, expected contributions, and Methodologies. Sec. 4 and 5 respectively draw a preliminary analysis and a preliminary concept of the potential supporting tool. Sec. 6 concludes this proposal.

EuroUSEC 2023, October 16 & 17, 2023, Copenhagen, Denmark

ACM ISBN 979-8-4007-0814-5/23/10…$15.00
https://doi.org/10.1145/3617072.3617105

2 RELATED WORK

2.1 Low Adoption Despite the Desire

In 2007, Conti and Sobiesk [9] showed that younger participants, in comparison with middle-aged participants, identified themselves as more responsible for protecting their privacy which indicates a growth in digital literacy. Despite this growth, later in 2015, Assal et al. [2] indicated that there is still a noticeable distance between the protecting strategies people choose and the risks they are concerned about. They also showed that 83% of their participants were concerned about their privacy while only 6% of them had installed privacy-preserving applications on their mobile devices. Further studies also show that despite the expressed concern of privacy by citizens, only a small portion of them engage in protecting privacy and using available PETs or other solutions [23, 24, 30, 36, 47]. Understating why users fail to adopt PETs despite their desire is a core inspiration for this vision paper.

2.2 User Behaviour Theory

In order to better understand why citizens do not adopt available solutions despite their desire for privacy, a vital component is to understand user behaviour models, particularly in adopting privacy protections. An important theory for understanding human behaviour is the *Fogg Behvior Model* (FBM), introduced in 2009 [16]. This argues that "behaviour is a product of three factors: motivation, ability, and triggers [at the same time]". However, the *Security and Privacy Acceptance Framework* (SPAF) [11] from 2022 explains that the general human behaviour model does not necessarily apply in the context of privacy. This is firstly because most of privacy behaviours are *preventive*, meaning that they support citizens in staying clear of undesirable future events. These future events might not have tangible applications for people at the moment where an action is required, hence, reducing the chance of engaging in the behaviour. Secondly, privacy behaviours have a *secondary* nature, which was first mentioned by Dourish et al. [14] in 2004. This means that privacy actions are not the main goals of the user. Lastly, the mechanisms of privacy solutions are *abstract* for citizens, which can diminish the likelihood of adoption. Therefore, SPAF proposes motivation, ability and awareness as three non-independent factors for privacy behaviour adoption [11], which need to be available at the same time so a user initiates a behaviour in this context. In SPAF, the awareness factor, which is the primary change in comparison with FBM, focuses on whether people have a correct understanding of both privacy risks and mitigation measures. This means that the awareness of potential risks and how to tackle them can play the role of trigger for citizens to take action in the context of privacy [11].

2.3 Low Adoption Explanation

The prominent explanation among privacy researchers for the low adoption of available privacy solutions by citizens is, in short, a lack of usability [1, 2, 13]. This means that these tools have not been designed with users in mind, are too complex to be understood by non-expert users, and incur too much overhead for them. Another explanation for the current low adoption is given by the authors of SPAF [11], with their evaluation of 100 related works, which showed that the majority of these works missed having the three ingredients of producing a behaviour (ability, motivation, and awareness) [16] simultaneously. Most of these 100 works only focused on removing the barriers regarding ability, some works focused on awareness and motivation, and no prior work focusing on all mentioned factors together has been reported [11]. In addition, two recent studies on the usage of PETs showed that their participants are often not aware of the existence of VPNs and Tor Browser [45], and more advanced PETs [10]. Even if the participants in [45] know about these tools, they have misconceptions about the offered protection, as already shown in [48]. These results indicate that poor usability, low compatibility with users' behaviour models, and limited awareness of options and their capabilities are hindering factors. Investigating further involving factors and addressing preventing factors is, hence, the motivation for this vision paper.

2.4 Practices and Factors

A practice to assist users in better protecting their privacy is proposed by Liu et al. [26], who proposed a *personalised Privacy Assistant* (PPA). PPA assists users with the privacy settings of their mobile device based on the user's profile. An evaluation of PPA showed an effective impact on users, which indicated that users benefit from provided support and personalised recommendations. This work only focused on a restricted area of privacy settings, similarly to [41]. Additionally, Privacy Bird [39] practised to establish a standard for machine-readable privacy policies to be comprehended automatically with the aim of protecting privacy. However, it could not live up as most of the websites did not adopt machine-readable policies. The two mentioned privacy assistants and also numerous others are focusing on a specific area (e.g., privacy settings) or a specific behaviour (e.g., posting on social media). In this work, we aim not to provide users with another tool of the same kind, but with a tool that can provide a personalised overview of already available tools to ease the process of adoption.

Some other works focused on investigating factors involved in the adoption of privacy solutions by users [1, 5, 6, 13, 42]. For example, understanding the privacy technology is a factor which correlated with the perceived usefulness of the technology. Moreover, the perceived ease of use is a factor which correlated with the intention to use the technology [5]. This means that explaining the technology and clarifying how to use it have positive effects on adoption. Another investigation revealed fundamental factors in the non-adoption of privacy solutions, such as incomplete threat models, misaligned incentives, and a general absence of understanding of the technology [42]. There are additional factors involved in citizens' intention of use, adoption or acceptance of privacy solutions, such as citizens' personality traits, privacy concerns, and knowledge [4–8, 18–20, 25, 28, 31]. These works suggested that there are additional factors behind the non-adoption of PETs, which need to be investigated.

Despite the mentioned practises and detected factors, there is, to the best of our knowledge, no tool that can take each individual into account, based on the mentioned factors, and that accordingly proposes personalised PETs recommendations to the user. Producing such a tool is, hence, the ultimate goal of our work: a tool

that supports users to step behind uncertainty, and take action in protecting privacy in a usable manner with low cognitive load.

3 RESEARCH QUESTIONS, CONTRIBUTION, AND METHODOLOGIES

The target of our work is to provide citizens with a tool which can support them, even when they have little knowledge of privacy, to the stage where they can confidently take action and adopt a solution. To achieve this, we outlined our research questions, expected contributions, and potential methodologies in Fig. 1.

The starting phase will be understating what users are experiencing when aiming to choose PETs, hence, **RQ 1.1** and **RQ 1.2** are formulated. **RQ 1.1:** *What behaviour models do users have when informing themselves to select a tool, specifically a PET for protecting privacy? What are the obstacles and concerns they encounter in this process?* This considers multiple aspects, including behaviour models of adopting privacy tools, concerns about personal privacy, concerns about privacy tools and adopting processes, and obstacles experienced or predict to experience. We expect to find explanations about what users currently experience, what mental model they have, and why adoption is low. **RQ 1.2:** *What are the online information resources available to assist citizens in choosing desirable PETs, What advantages and disadvantages do these resources have?* This uncovers what types of information are available and how they are presented to users, what parts are serving well, and what parts have been designed with poor usability. With a triangulation strategy, four user-based methods and one expert-based method are planned for this phase to ensure the quality of the gathered data, develop a comprehensive understanding of the citizens' current user experience, and behaviour models. The planned user-based methods (mainly to answer **RQ 1.1**) are Focus Groups, User-based Evaluations, In-depth Interviews, and Online Surveys. The planned expert-based method (mainly to answer **RQ 1.2**) is Information Source Analysis.

The results of **RQ 1.1** and **RQ 1.2** will lay the groundwork for **RQ 2:** *What characteristic should an interactive tool have to support citizens in adopting desired PETs in a usable and efficient fashion?* An interactive tool capable of receiving relevant user data and providing personalised PETs recommendations will be produced in this phase. The tool will also make decision consequences transparent to the user. The production of **RQ 2** will be evaluated by **RQ 3:** *How and to what extent does the proposed tool for adopting PETs support citizens in practice?* As such, the results of the user testing phase are expected to cast a light on the advantages and disadvantages of the proposed tool, followed by potential improvements. Designing, implementing, and evaluating this tool shall be a cycle to continuously include user feedback, and further ensure usability and effectiveness. With such a user-centred tool, we aim to draw a bridge between the privacy research ecosystem and citizens to optimise the usage of research ecosystem results by users. Such a final product serves in the direction of empowering citizens in protecting privacy.

4 PRELIMINARY ANALYSIS

To have an insight into what citizens are going through to adopt privacy solutions online, we had a brief look into the results of searching related terminologies on the most used online search engine, Google [17] and a controversial artificial intelligent chat bot called ChatGPT [34]. The goal was not to evaluate the products that appear in search results but to analyse the information sources proposing these with respect to their information presentation styles and decision-support functions. For users motivated in protecting privacy by searching online, there is a diverse range of starting points. There are systematic rigorous approaches for Information source Analysis like [40]. Here, we only look at two main points, which we call broad solution search and product solution search. The first observations of these two points can be seen in the following.

4.1 Broad Solution Search

By broad solution search, we refer to the stage where users are interested to take action but are not sure about the steps to take. Therefore, they start with broader search strings such as "How should I improve my online security and privacy?". To have an insight into what users may experience in such a situation, we used the above-mentioned string in the Google search engine [17] (in private browsing mode) and briefly analysed the first five web page results (excluding sponsored results). The mentioned research string is provisional and will be revised based on the user research phase. As seen in Tab. 1, all five web pages provide a generic list of solutions to users without any personalising over user needs and concerns. This increases the cognitive load users have to put in to read these generic lists to understand which parts are suitable for them, which drops the chance of adoption. In addition, users are confronted with seven to ten different solution areas including VPNs, authentication, antivirus, and privacy settings on each web page. Looking more in-depth at these areas, three web pages had partially communicated action points for each area, and two web pages lacked such support. This makes it hard for users to take the next action toward adopting solutions, which can be considered as a hindering factor. Lastly, none of these web pages provide explanations about what a solution/tool cannot cover. Therefore, users cannot be clear on the coverage of each tool, which is misleading.

The same string in ChatGPT [34] (with a fresh logging credential), resulted in a list of 17 items. Each item is a brief solution explanation without an action point, and an explanation of what cannot be covered by the respective privacy solution. The first three items are given in the following:

1. Use strong, unique passwords for each online account, and consider using a password manager to securely store them. 2. Enable two-factor authentication (2FA) whenever possible for an additional layer of security. 3. Keep your devices, operating systems, and applications up to date with the latest security patches.

4.2 Product Solution Search

By product solution search, we refer to the stage where users are convinced about adopting a specific privacy solution (e.g., VPN) and are in the stage of searching and comparing different available products of that solution. In order to have an insight into what users might experience in such a situation, we used the word "VPN" in the Google search engine (in private browsing mode) and briefly analysed the first five results (excluding sponsored results). As

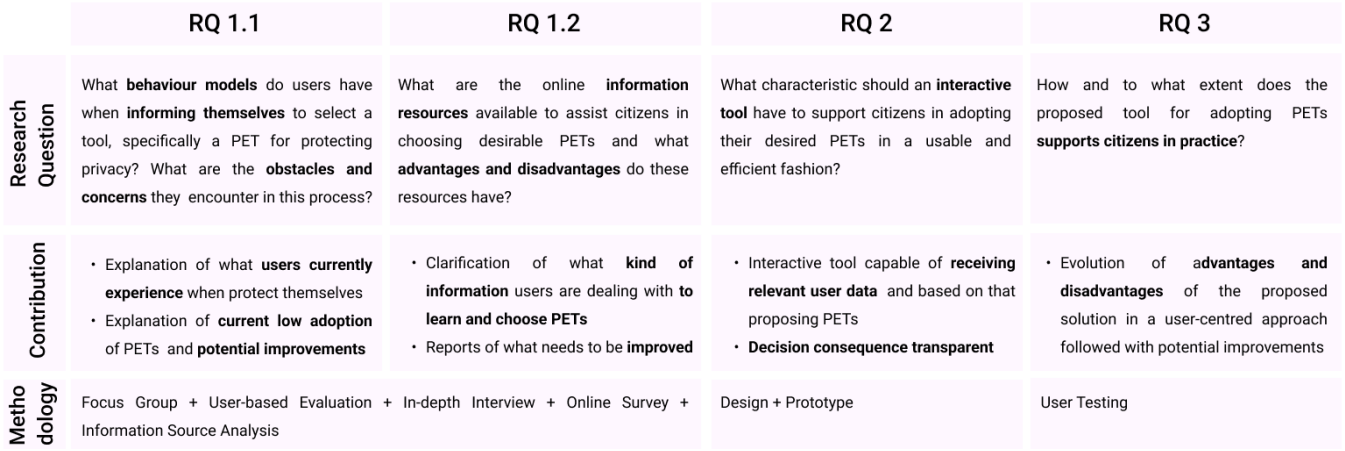


Figure 1: Research Questions and Contributions and Methodology.

Table 1: Broad Solution Search in Google

Web Page Name	Information personalising	Number of Areas	Action Point	Lack of Coverage
Aura [3]	No, generic list	10	Partially	Not mentioned
The New York Times [46]	No, generic list	7	Partially	Not mentioned
Help Desk Geek [21]	No, generic list	7	Partially	Not mentioned
NPR [33]	No, generic list	8	Not mentioned	Not mentioned
HP [22]	No, generic list	10	Not mentioned	Not mentioned

illustrated in Tab. 2, three web pages belong to product providers, presenting their VPNs. The other two are a browser store presenting six VPN extensions and a web page comparing five VPNs. A total of 14 VPN options are available only via five first search result links. Users may experience poor usability and high cognitive load while going through these 14 options, comparing them, and trying to adopt one. In addition, each of these web pages includes different types of information about products in different styles. For example, some provide a textual explanation at the beginning, some do it later on their page, and some do not provide it at all. This situation demands more time and attention from the user to develop an understanding of available options and make a decision.

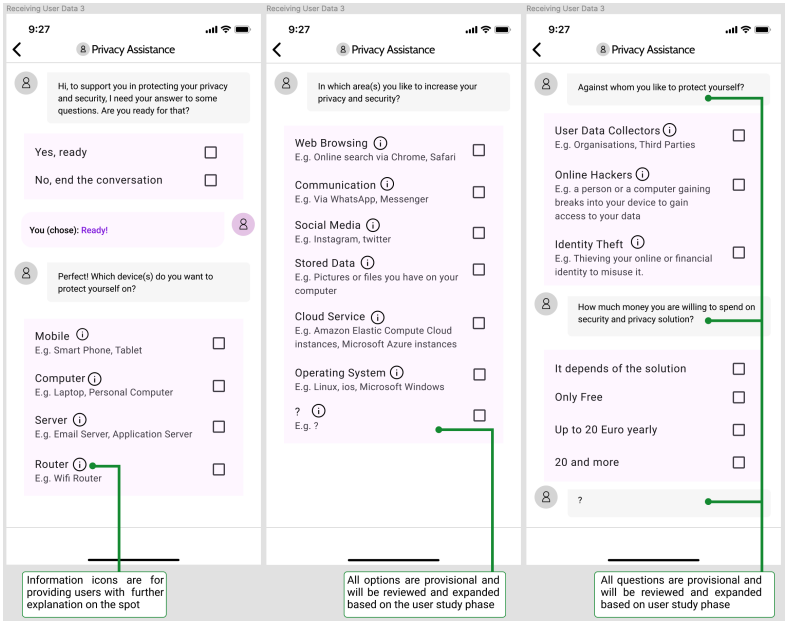
The above-mentioned insights indicate the uneasy situation users encounter in protecting privacy by searching online. Users are confronted by multiple information sources and various recommendations in diverse privacy areas. In addition, the majority of positive factors (e.g., explaining to users how a solution works) for supporting users reported by academic works (we referred to some of these factors in Sec. 2) in adopting PETs were not observed in above-mentioned information sources. This situation motivates this vision paper toward seeking solutions for serving citizens a supporting tool, providing tailored and digestible privacy recommendations with the aim of adoption growth.

5 PRELIMINARY CONCEPT

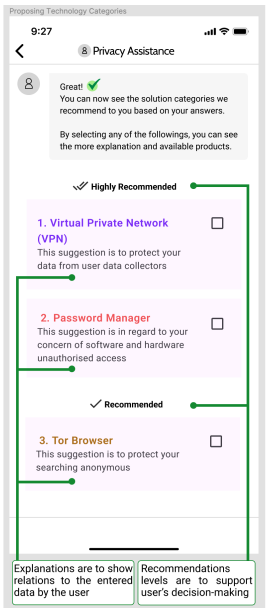
To further show the vision of this paper, we present a preliminary concept (Fig. 2a, 2b, and 2c.) of our supporting tool here. All of the design components (derived from Material Design [27]) and user flows are subject to change based on further context and user research. The user interface style used here is conversational to ease the interaction for users, the effectiveness of which will be tested. Further modality will also be studied. The primary audience of this tool will be the users who have the initial motivation to start searching online and need support to make decisions. We will first only focus on stand-alone PETs as privacy solutions recommendations, which may further be extended in our future work by including different privacy solutions. During this interaction, unavoidable vocabulary, which can potentially be complicated or unknown to the user, will be accompanied by further explanations and daily life examples. In this preliminary concept, the first phase, shown in Fig. 2a, is receiving factors which are playing a primary role in user decision-making. To this end, the tool will be able to ask about factors such as devices to be protected, areas (e.g., Web Browsing and Communication) to be secured, individuals/entities to be protected against, and budget to be allocated. More in-depth factors are to be defined based on the user research phase and influential factors reported in academic works. Nevertheless, we predict factor types such as situational factors (e.g., device(s), location(s), used solutions, areas/platforms willing to be protected in) and specific privacy factors (e.g., against whom to be protected).

Table 2: Product Solution Search in Google

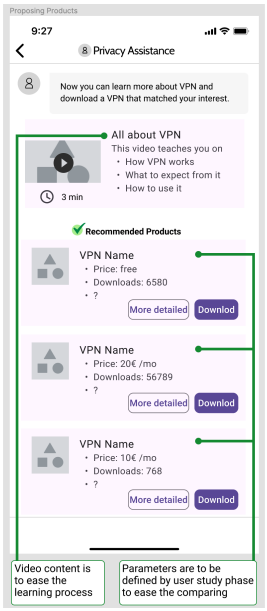
Web Page Name	Presents	Includes Information Such As
NordVPN [32]	Single product	Textual explanation, device availability, subscription link
ExpressVPN [15]	Single product	Subscription link, textual explanation, device availability
Chrome Web Store [44]	Browser extensions	6 products + rating, download No, extension link
PCMag UK [35]	Comparing products	5 products + rating, product link, pros and cons
ProtonVPN [37]	Single product	Subscription link, textual explanation, device availability



(a) Receiving User Data.



(b) Proposing Technology Categories.



(c) Proposing Products.

Figure 2: Preliminary Concept, © 2016 Google Inc. Used under the Apache License 2.0

In the next step, based on each user's answers to the questions, the tool provides personalised solutions recommendations, which are specifically matching to the respective user's answers (e.g., recommendations covering her/his mentioned concerns and being compatible with her/his communicated devices). The tool will propose privacy solutions in the form of technology categories (e.g., VPN, Tor Browser) in two levels, i.e., highly recommended and recommended, as seen in Fig. 2b. We plan to present solutions on at least two levels to make them more comprehensible by users. Then, when the user selects any of the categories, products (including commercial and open source) available in that category (e.g., different VPN products) will be presented to the user, as shown in Fig. 2c. Also, explanations about the technology such a how it works, what to expect from it, and how to use it, will be available in an easy-to-digest way, like a short video and/or in different complexity levels to support users with different topic background knowledge. The criteria which affect users' decision on choosing the final product, will be visible and comparable between products. Defining and presenting this solution's procedure, user flows, and criteria in a usable manner is a goal for our work.

6 CONCLUSION

The rise in collecting user data by businesses and organisations, coupled with the low adoption of privacy solutions by citizens, emphasises the importance of new ways to support citizens in privacy protection. In the majority of cases, privacy defaults are in the favour of businesses' goals, and the options available for citizens to protect their data against these defaults are not intuitive. To this end, we aim to propose a supportive tool which is more compatible with users' behaviour models and has better usability to support citizens in privacy protection. In this regard, we planned a user-centred process which will start with investigating users' behaviour and concerns in the context of privacy. Then, we will design and implement an interactive tool which proposes PETs based on individual data. We will evaluate our tool with users to ensure its practicality and usability. The novelty of our approach lies in putting users' needs and concerns as the core of our process to propose a tool which eases privacy protection for citizens, instead of expecting users to tailor privacy solutions for themselves.

REFERENCES

[1] Ruba Abu-Salma, M Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. 2017. Obstacles to the Adoption of Secure Communication Tools. In *Proc. IEEE Symposium on Security and Privacy*.

[2] Hala Assal, Stephanie Hurtado, Ahsan Imran, and Sonia Chiasson. 2015. 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*.

[3] Aura.Com. 2023. How to Protect Your Privacy Online. Retrieved May 20, 2023 from https://www.aura.com/learn/how-to-protect-your-privacy-online

[4] Zinaida Benenson, Anna Girard, and Ioannis Krontiris. 2015. User Acceptance Factors for Anonymous Credentials: An Empirical Investigation. In *Proc. Workshop on the Economics of Information Security (WEIS)*.

[5] Zinaida Benenson, Anna Girard, Ioannis Krontiris, Vassia Liagkou, Kai Rannenberg, and Yannis Stamatiou. 2014. User Acceptance of Privacy-Abcs: An Exploratory Study. In *Proc. 2nd Human Aspects of Information Security, Privacy, and Trust*.

[6] Vanessa Bracamonte, Sebastian Pape, and Shinsaku Kiyomoto. 2021. Investigating User Intention to Use a Privacy Sensitive Information Detection Tool. *Proc. Symposium on Cryptography and Information Security*.

[7] Franziska Brecht, Benjamin Fabian, Steffen Kunz, and Sebastian Mueller. 2011. Are You Willing to Wait Longer for Internet Privacy? *Proc. European Conference on Information Systems(ECIS)*.

[8] Johana Cabinakova, Christian Zimmermann, and Guenter Mueller. 2016. An Empirical Analysis of Privacy Dashboard Acceptance: The Google Case. *Proc. European Conference on Information Systems(ECIS)*.

[9] Gregory Conti and Edward Sobiesk. 2007. An Honest Man Has Nothing to Fear: User Perceptions on Web-Based Information Disclosure. In *Proc. 3rd Symposium on Usable Privacy and Security*.

[10] Kovila PL Coopamootoo. 2020. Usage Patterns of Privacy-Enhancing Technologies. In *Proc. ACM SIGSAC Conference on Computer and Communications Security*.

[11] Sauvik Das, Cori Faklaris, Jason I Hong, Laura A Dabbish, et al. 2022. The Security & Privacy Acceptance Framework (SPAF). *Proc. Foundations and Trends in Privacy and Security*.

[12] DataReportal.Com. 2023. Digital Around the World. Retrieved May 25, 2023 from https://datareportal.com/global-digital-overview#:~:text=There%20are%205.18%20billion%20internet,higher%20in%20many%20developing%20economies.

[13] Alexander De Luca, Sauvik Das, Martin Ortlieb, Iulia Ion, and Ben Laurie. 2016. Expert and Non-expert Attitudes Towards (Secure) Instant Messaging.

[14] Paul Dourish, Rebecca E Grinter, Jessica Delgado De La Flor, and Melissa Joseph. 2004. Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem. *Proc. Personal and Ubiquitous Computing*.

[15] ExpressVPN.Com. 2023. Express Virtual Private Network Product. Retrieved May 20, 2023 from https://www.expressvpn.com/

[16] Brian J Fogg. 2009. A Behavior Model for Persuasive Design. In *Proc. 4th International Conference on Persuasive Technology*.

[17] Google.Com. 2023. Google Search Engine. Retrieved May 20, 2023 from https://www.google.com/

[18] David Harborth and Sebastian Pape. 2018. Examining Technology Use Factors of Privacy-Enhancing Technologies: The Role of Perceived Anonymity and Trust. *Proc. 24th Americas Conference on Information Systems*.

[19] David Harborth and Sebastian Pape. 2019. How Privacy Concerns and Trust and Risk Beliefs Influence Users' Intentions to Use Privacy-Enhancing Technologies-the Case of Tor. *Proc. 52nd Hawaii International Conference on System Sciences*.

[20] David Harborth, Sebastian Pape, and Kai Rannenberg. 2020. Explaining the Technology Use Behavior of Privacy-Enhancing Technologies: The Case of Tor and Jondonym. *Proc. Privacy Enhancing Technologies*.

[21] HelpDeskGeek.Com. 2020. How to Improve Your Online Privacy and Security. Retrieved May 20, 2023 from https://helpdeskgeek.com/how-to/how-to-improve-your-online-privacy-and-security/

[22] HP.Com. 2021. 10 Simple Steps to Take Right Now to Protect Your Privacy Online. Retrieved May 20, 2023 from https://www.hp.com/us-en/shop/tech-takes/how-to-protect-your-privacy-online

[23] Predrag Klasnja, Sunny Consolvo, Tanzeem Choudhury, Richard Beckwith, and Jeffrey Hightower. 2009. Exploring Privacy Concerns About Personal Sensing. In *Proc. 7th Pervasive Computing*.

[24] Spyros Kokolakis. 2017. Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon. *Proc. Computers & Security*.

[25] Ioannis Krontiris, Zinaida Benenson, Anna Girard, Ahmad Sabouri, Kai Rannenberg, and Peter Schoo. 2016. Privacy-Abcs as a Case for Studying the Adoption of Pets by Users and Service Providers. In *Proc. 3rd Privacy Technologies and Policy*.

[26] Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, Shikun Zhang, Norman Sadeh, Alessandro Acquisti, and Yuvraj Agarwal. 2016. Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions. In *Proc. 12th Symposium on Usable Privacy and Security (SOUPS)*.

[27] M2.Material.Io. 2022. Material Design. Retrieved May 20, 2023 from https://m2.material.io/components

[28] Christian Matt and Philipp Peckelsen. 2016. Sweet Idleness, but Why? How Cognitive Factors and Personality Traits Affect Privacy-Protective Behavior. In *Proc. 49th Hawaii International Conference on System Sciences (HICSS)*.

[29] Maryam Mehrnezhad, Kovila Coopamootoo, and Ehsan Toreini. 2022. How Can and Would People Protect From Online Tracking? *Proc. Privacy Enhancing Technologies*.

[30] Caroline Lancelot Miltgen and Dominique Peyrat-Guillard. 2014. Cultural and Generational Influences on Privacy Concerns: A Qualitative Study in Seven

European Countries. *Proc. European Journal of Information Systems.*

[31] Moses Namara, Daricia Wilkinson, Kelly Caine, and Bart P Knijnenburg. 2020. Emotional and Practical Considerations Towards the Adoption and Abandonment of VPNs as a Privacy-Enhancing Technology. *Proc. Privacy Enhancing Technologies.*

[32] NordVPN.Com. 2023. Nord Virtual Private Network Product. Retrieved May 20, 2023 from https://nordvpn.com/

[33] NPR.Org. 2020. Your Technology Is Tracking You. Take These Steps for Better Online Privacy. Retrieved May 20, 2023 from https://www.npr.org/2020/10/09/922262686/your-technology-is-tracking-you-take-these-steps-for-better-online-privacy

[34] OpenAI.Com. 2023. GhatGPT Chat Bot. Retrieved May 20, 2023 from https://openai.com/blog/chatgpt

[35] PCMag.Com. 2023. the Best VPN Services for 2023. Retrieved May 20, 2023 from https://uk.pcmag.com/vpn/138/the-best-vpn-services

[36] Joseph Phelps, Glen Nowak, and Elizabeth Ferrell. 2000. Privacy Concerns and Consumer Willingness to Provide Personal Information. *Proc. Public Policy & Marketing.*

[37] ProtonVPN.Com. 2023. Proton Virtual Private Network Product. Retrieved May 20, 2023 from https://protonvpn.com/

[38] Erica Racine, Patrick Skeba, Eric PS Baumer, and Andrea Forte. 2020. What Are Pets for Privacy Experts and Non-experts. In *Proc. Symposium on Usable Privacy and Security.*

[39] Joseph Reagle and Lorrie Faith Cranor. 1999. The Platform for Privacy Preferences. *Proc. ACM Communications.*

[40] Elissa M Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L Mazurek. 2020. A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web. *Proc. 29th USENIX Security Symposium.*

[41] Delphine Reinhardt, Franziska Engelmann, and Matthias Hollick. 2015. Can I Help You Setting Your Privacy? A Survey-Based Exploration of Users' Attitudes Towards Privacy Suggestions. In *Proc. 13th International Conference on Advances in Mobile Computing and Multimedia.*

[42] Karen Renaud, Melanie Volkamer, and Arne Renkema-Padmos. 2014. Why Doesn't Jane Protect Her Privacy?. In *Proc. 14th International Symposium om Privacy Enhancing Technologies.*

[43] Statista.Com. 2023. Number of Internet and Social Media Users Worldwide as of April 2023. Retrieved May 24, 2023 from https://www.statista.com/statistics/617136/digital-population-worldwide/

[44] Chrome Web Store. 2023. Extensions. Retrieved May 20, 2023 from https://chrome.google.com/webstore/search/vpn

[45] Peter Story, Daniel Smullen, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2021. Awareness, Adoption, and Misconceptions of Web Privacy Tools. *Proc. Privacy Enhancing Technologies.*

[46] Thorin Klosowski The New York Times. 2023. How to Protect Your Digital Privacy. Retrieved May 20, 2023 from https://www.nytimes.com/guides/privacy-project/how-to-protect-your-digital-privacy

[47] Godwin J Udo. 2001. Privacy and Security Concerns as Major Barriers for E-commerce: A Survey Study. *Proc. Information Management & Computer Security.*

[48] Blase Ur, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. 2012. Privacy-Abcs as a Case for Studying the Adoption of Pets by Users and Service Providers. In *Proc. 8th Symposium on Usable Privacy and Security (SOUPS).*