Support Personas: A Concept for Tailored Support of Users of Privacy-Enhancing Technologies

Kilian Demuth
PEASEC, TU Darmstadt
Darmstadt, Germany
demuth@peasec.tu-darmstadt.de

Sebastian Linsner
PEASEC, TU Darmstadt
Darmstadt, Germany
linsner@peasec.tu-darmstadt.de

Tom Biselli
PEASEC, TU Darmstadt
Darmstadt, Germany
biselli@peasec.tu-darmstadt.de

Marc-André Kaufhold
PEASEC, TU Darmstadt
Darmstadt, Germany
kaufhold@peasec.tu-darmstadt.de

Christian Reuter
PEASEC, TU Darmstadt
Darmstadt, Germany
reuter@peasec.tu-darmstadt.de

ABSTRACT

In many applications and websites people use in their everyday life, their privacy and data are threatened, e.g., by script tracking during browsing. Although researchers and companies have developed privacy-enhancing technologies (PETs), they are often difficult to use for lay users. In this paper, we conducted a literature review to classify users into different *support personas* based on their privacy competence and privacy concern. With developers of PETs in mind, support personas were envisioned to facilitate the customization of software according to the support needs of different users. In order to demonstrate the usefulness of support personas and based on workshop sessions with 15 participants, we designed a browser extension that supports users with the issue of script tracking by providing different user interfaces for different support personas. The following qualitative evaluation with 31 participants showed that the developed UI elements worked as intended for the different support personas. Therefore, we conclude the concept of support personas is useful in the development process of usable applications that enhance the privacy of the users while also educating them and thus potentially increasing their privacy literacy.

KEYWORDS

support personas, usable privacy, script tracking, privacy

1 INTRODUCTION

With the ongoing digitalization, many people around the world are using their computers and the internet for more and more purposes, ranging from private matters like web browsing to business applications like confidential meetings. Besides the threat of intentional cyberattacks [48], this extensive usage of the internet in everyday life results in people sharing a lot of personal information, intentionally and unintentionally, with different companies. To mitigate this transfer of private information, security researchers have developed several privacy-enhancing technologies (PETs) [20, 21]. These technologies are intended to protect the user's data and prevent eavesdroppers or companies from acquiring information about the user. Often, the problem with these technologies is that their usage is too complicated for a majority of users [17]. This is, for example, one of the reasons why Pretty Good Privacy (PGP) is not widely adopted [18] and can only be used by people who have the required expertise and motivation to act accordingly [7]. Another problem is user reactance, i.e., users that mistrust a tool or security mechanism try not to use it, even though it would be more secure [26].

Research in the area of *usable privacy* - a research field at the intersection of human-computer interaction and privacy research [47] - tries to solve this problem. Existing work aims to identify user categories regarding their respective privacy attitude, e.g., by using users' knowledge and motivation [14], or distinct information cues users find important [40]. Further research has tried to find semantic relationships between users' traits, characteristics, and attitudes and their privacy profiles [49]. Another interesting research topic in the field of usable privacy is to investigate how users can be supported in their privacy decisions. Research has looked at the potential of nudging and soft paternalism [1], or how users can receive recommendations regarding their privacy settings [32, 45, 49]. In this paper, we combine the mentioned research topics and will classify users by their need for support while appropriating new PETs. In this case, support means identifying the users' needs while using a tool and suggesting suitable settings based on these needs. For the classification of users, we use the concept of personas, which are archetypical users with different behaviors, motivations, and goals [44]. Thus, it seems worthwhile to examine whether the identified user groups called "support personas" will differ from the "privacy personas" found by existing research [14].

Since most people use computers for browsing and thus are directly affected by the issue of script tracking, it was easily explainable in our workshop sessions and we used the topic to evaluate our concept of support personas in practice. For this purpose, we developed a browser extension prototype based on user workshops, which makes script tracking more transparent to different user groups by implementing different user interfaces (UIs) tailored to the support personas. We chose this static instead of a dynamic approach to test the feasibility of our idea in a more controlled environment. Finally, we evaluated the extension to verify that it supports users with different backgrounds. In conclusion, this paper

Proceedings on Privacy Enhancing Technologies 2024(4), 797–817

https://doi.org/10.56553/popets-2024-0142

answers the following research question in the context of script tracking: **How can developers of privacy-enhancing technologies provide users with tailored support?**

Based on our reviewed literature (Section 2), the main contribution is the methodological contribution of the novel concept of support personas, which can be used to tailor the support for users trying to appropriate new technology (Section 3). As an empirical contribution, our workshops shed light on the UI requirements of user groups with different privacy concerns and competencies (Section 4). Finally, we provide an artifact contribution by the participatory design of our demonstrator PrivacyAssist, which is a browser extension that makes script tracking more visible to the user (Section 5). Based on the evaluation of its user experience and user support capabilities (Section 6), we discuss the core contributions of our study (Section 7) and conclude the paper (Section 8).

2 RELATED WORK

For the design of support personas, we reviewed literature on the appropriate categorization of users, different modes of user support, and the foundations of our intended application domain (i.e., privacy and script tracking in browsers), which is summarized in the following subsections.

2.1 Categorization of Users

Personas are an important concept to identify users' needs and design applications for distinct user groups specifically [24, 50]. Previous research described different approaches how personas can be developed. One possibility is to use quantitative data and statistical methods in order to identify relevant personas [38, 52]. Another possibility is to use only qualitative data [12].

For privacy applications, previous research developed privacy personas to categorize users regarding their privacy behaviour and attitudes. One of the first categorizations of users is the model of Westin [29], which differentiates users regarding their privacy concern. He identified three groups of users, i.e., the Unconcerned, the Fundamentalists, and the Pragmatic Majority. The Unconcerned are users who trust organizations to collect their personal data. The Fundamentalists are the opposite. They do not trust organizations to handle their personal data. Regarding the privacy paradox, they often prioritize their privacy over benefits they would receive for sharing data. According to Westin, the majority of users are Pragmatists. They weigh their privacy with the benefits they would receive for sharing personal data and are willing to share them if they receive an adequate benefit. To classify users according to those categories, Biselli et al. [5] developed a questionnaire. The questionnaire contains questions regarding the privacy knowledge and the privacy behavior of users and is used to shed light on the general methodological difficulties of accurately classifying users.

Another approach that obtained approval in the research community was developed by Morton and Sasse [40]. They categorized users into five groups with regard to both their privacy knowledge and behavior: Information Controllers, Security Concerned, Benefit Seekers, Crowd Followers, and Organizational Assurance Seekers. This categorization was also used by Dupree et al. [14]. They investigated the privacy motivation and knowledge of users and then examined what clusters developed. Thereby, they confirmed the five clusters found by Morton and Sasse [40]. In conclusion, research has focused on classifying users into different so-called privacy personas. Primarily, this categorization reveals users' attitudes toward privacy and the protection of their data. To the best of our knowledge, there are no works that have classified users regarding the support they need and want when working with PETs.

2.2 Support of Users

In order to elaborate what kind of support users want, we reviewed related work in this research area. For secure systems, Holmström [25] identified a growing need for usable and comprehensible security solutions. Therefore, she developed a security concept to support users with their security decisions and issues. As essential steps when designing a UI, she identified determining the user's security awareness, knowledge, and needs. As Ray et al. [46] found out, people in different age groups have different privacy concerns, highlighting the necessity of addressing individual users differently. This is also important since users with different backgrounds have differing privacy knowledge and behaviors [6, 31]. Especially lay users are often unaware of existing privacy risks [19].

With a focus on the UI, MacDonald and Smith [33] developed design guidelines for interfaces that raise users' awareness of application security. According to them, the design of the interface is crucial for the security of a system, since the computer depends on the information conveyed to the user. Without correct or adequate information, many problems can arise, e.g., confusion or an increased frequency of errors. A good interface design can reduce the risk of these problems and thus increase the system security too. The developed guidelines include the usability, the path of least resistance, the recoverability and revocability of actions, and the explicit user authorization. Other principles [54] imply that the UI should provide elements to inform the user about the current security state of the system in a comprehensible way. Since the user's attention is limited and security is usually not their priority, the UI design should be frugal and simple while providing the information required to make the right decisions.

However, challenges exist even in software designed to support users. Acquisti et al. [1] studied problems in privacy and security decision-making. The identified problems are incomplete and asymmetric information presented to users, heuristics and bounded rationality, as well as different cognitive and behavioral biases. Another problem found by Wu et al. [58] is that texts about security in applications often contain various technical terms that are not understood by many users. In an experiment, they verified the success of using explanations in pop-ups to help users understand such texts. It was also found that there is a big difference between the developers' assumption of user privacy expectations and the actual privacy expectations of users [51].

A concrete application to support users was developed by Barth et al. [3]. They built a privacy rating aimed at helping users to understand how an online service handles their data. The privacy rating was realized by calculating a score that was well accepted by users, including lay users. However, the authors identified problems regarding incomprehensible terms, as users required background knowledge to understand them. Namara et al. [41] tried different concepts to engage users to interact with privacy features on social

networking sites. They found that an automated system comes with the most secure settings for users, but a suggestion system best facilitates interaction between users and the system. In summary, previous research examined which support users need when using PETs and what problems can arise in the context of user's data privacy and security. Nonetheless, there is still a demand for applications that adjust their support to the user's needs in order to support the individual user and not just the main target group of a software, e.g., by helping them to understand security terms.

2.3 Privacy in the Browser

For different browsers, various browser extensions exist that implement different solutions for users to prevent online tracking. Mathur et al. [37] examined the use of such extensions. They present three main findings. First, they found that most internet users only have basic knowledge about online tracking. Second, they observed that every extension has one specific primary use case. Third, they revealed that extensions do not break websites very often, i.e., block too many website elements so that the website does not work anymore. Besides browser extensions, browsers also integrate functions to inform users about the security of a website. One of those functions is the padlock icon, which is displayed in the address bar to signalize an encrypted connection. In a study by von Zezschwitz et al. [56], it was discovered that most users did not know the meaning of this icon. The authors propose that a secondary UI can communicate the meaning of icons or the security of a website or connection more clearly. A similar problem was identified by Mehrnezhad et al. [39], who found that users learned the most about privacy and security by conducting their own research or through friends and family and not by using PETs. Additionally, users often do not know how to effectively control the privacy practices of websites when browsing [53].

Farke et al. [16] examined which impact privacy dashboards, i.e., windows showing the collected private information of the user, have on the end user. They tested this with the Google My Activity dashboard. After using the dashboard, most participants were less concerned about data collection and some stated that they would change a few settings in the dashboard. On the one hand, the researchers highlighted that privacy transparency tools would increase users' trust and improve their privacy perception. On the other hand, they doubted whether these tools encouraged users to view the collected data and change settings. Weinshel et al. [57] developed a browser extension to raise awareness for web tracking. They implemented different interfaces showing different information to the user and evaluated those.

In conclusion, recent literature shows that users of privacy extensions for browsers often have little knowledge about privacy issues and that a secondary UI providing more details about the security of a website or collected data and, thus, educating the users would be beneficial. This secondary UI can be provided as an extension.

2.4 Research Gap

The literature shows that a categorization of users regarding the required support when working with PETs currently does not exist. This paper develops such a categorization by introducing support personas. The concept is then tested in a development process for an application with UI components tailored to the individual user and the assigned support persona. The demonstrator is a browser extension that presents users with more details regarding script tracking and combines approaches from different existing applications. This is relevant since literature shows that existing applications only serve one primary purpose, e.g., a privacy score [37]. During the design of the application, we adhered to the design guidelines established by Spero and Biddle [54]. The use case of script tracking allows us to implement different visualization techniques, which can also be used to visualize other tracking techniques. This is shown by existing applications that use some of the techniques to visualize more tracking techniques like trackers or encryption status. For our use case as a demonstrator, the limitation on scripts is a limitation, but it still demonstrates the use case since the UI elements and their meaning are the same except for the calculation in the background, which uses only scripts in our case. Nevertheless, due to the complexity of tracking, a browser extension for more tracking techniques like cookies or fingerprinting would result in a more complex user interface.

The concept of support personas is related to the concept of privacy personas developed by different researchers, e.g., [14, 40]. These personas were largely based on the users' privacy behavior. It was shown [11] that users' reported privacy behavior and real privacy behavior differ. Therefore, we needed to create the support personas to provide users not only with the information they think they need but with the information and support they really need based on their objective competencies.

A research work closely related to our demonstrator is the one by Weinshel et al. [57], who also developed a browser extension for web tracking. Although they tested various interfaces showing different information in a field study, they did not develop different interfaces for specific user groups, in contrast to our work. Another closely related work is the research by Mathur et al. [37], who examined the relationship between the privacy knowledge of users and the usage of browser-based blocking extensions. Our work builds on research by Mathur et al. [37], as they found that users lack knowledge about online tracking and that every extension only serves one purpose, such as a privacy score or detailed information. In addition, we aim to improve user privacy competence and combine different existing extensions in our extension.

3 SUPPORT PERSONA ITEMS

A persona is an archetypical user consisting of attitudes, motivation, behavior, goals, and more [50]. Schneidewind et al. [50] showed that personas can be used to solve different challenges that arise for requirements engineering. They propose that the personas in a given scenario should be developed before determining the requirements for a project. This way, the personas increase the user focus and awareness and can contribute to a better understanding of future users' behavior and needs [24]. In this work, we will adhere to this and develop the support personas before the implementation. The support personas classify users regarding the support they need while appropriating new PETs. Since this paper focuses on privacy-enhancing technologies, we used the two dimensions of *privacy competence* and *privacy concern* to create support personas. Similarly to previous works clustering users [14, 29], we chose to

divide each item into three groups (*low, medium, high*). The dimension *privacy behavior* was not chosen because it was shown that the stated privacy behavior often differs from the actual privacy behavior [28]. The *used privacy practices* are another potential dimension. That was not chosen because, while users may already use PETs, it is possible that they do not know how to use them correctly. This is due to the unavoidable different user groups that use the same application.

3.1 Privacy Competence

Holmström [25] found that it is essential to recognize the user's knowledge of security issues for the development of a user interface for PETs. This way, it can be ensured that only user-understandable information is displayed [58]. Furthermore, more experienced users may not require some explanations, as this could disrupt their work. Additionally, a customized user interface prevents confusion by only displaying information relevant to a specific user. This can enhance the entire system's security [33]. For UIs in general, items like tech literacy could be used to determine the knowledge of users. But since support personas should be used for PETs, we decided to choose a more privacy focused item. Also, Crossler and Bélanger [13] observed that the users' privacy competence determines their use of privacy-protective settings. Thus, we used the user's privacy competence as the first factor to create the support personas.

In order to classify users based on their privacy competence, we need to establish a measure. For this purpose, we chose the questionnaire 'Online Privacy Literacy Scale' (*OPLIS*) by Masur et al. [36]. This questionnaire consists of 20 questions regarding the user's online privacy competence[1] and is shown in Appendix C.1. Although the *OPLIS* scale does not exclusively measure knowledge of tracking technologies, it includes items related to cookies and other similar technologies. Moreover, having a comprehensive understanding of online privacy is crucial for making informed decisions. Therefore, it is suitable for our purpose of identifying the user's privacy competence. Using this questionnaire, we built three user groups according to their privacy competence. A user can achieve a maximum of 20 points by answering all 20 questions correctly. Since the authors [36] attached norm tables to their work, we will use the norm table for the whole population, determining how many people score how many points on average as an indicator for our groups. The first group we built is the one with the least privacy competence. Users in this group achieve ten or fewer points in the *OPLIS* questionnaire and could be users who want to protect their privacy but lack the competence to do so. Therefore, they may need more explanations and easier language in the application. Users who achieve between eleven and 14 points are in the second group, which comprises users with average privacy competence. This user group will probably be the largest one, comprising both people who want to protect their privacy actively by learning more about the topic and people who do not want to learn new things and want the application to just work. The last group with the most privacy competence consists of users achieving 15 points or more. This group includes the expert users who may want the most configurable options and information. We established the boundaries between the groups using the mentioned norm table for the whole population. According to the norm table, each group should represent one-third of the whole population regarding privacy competence.

[1] https://www.oplis.de/index_eng.html

3.2 Privacy Concern

Furthermore, Holmström [25] identified the user's awareness and security needs as important factors when creating a UI. A definition of information privacy concern was developed by Malhotra et al. [34], who defined it as an individual's subjective views of fairness within the context of information privacy. This aspect is of particular interest for our support personas, as users with differing attitudes on privacy need to be addressed differently. For example, a user worried about privacy does not need to be motivated to use PETs but only needs to know what and how to do it [4]. In contrast, users without worries about privacy do not necessarily want privacy warnings to disrupt their workflow and probably have increased risk-taking behavior [10]. Brough and Martin [8] underline that both privacy concern and competence are important for the privacy behavior of the user. Thus, privacy concern is the second factor we looked at when creating the support personas.

As a scale for privacy concern, we chose the "Internet Users' Information Privacy Concerns" (*IUIPC-8*) by Groß [22], which is based on *IUIPC-10* by Malhotra et al. [34]. We chose this scale since it is a well-established instrument to quantify privacy concern [43]. The questionnaire consists of eight items (cf. Appendix C.2). These belong to the dimensions of control, awareness, and collection, which were shown to be relevant dimensions for privacy concerns. The questions are answered by using a Likert 7-point scale ranging from 1="strongly disagree" to 7="strongly agree". A person answering all questions with "7" is considered to have very high privacy concerns. A person answering all questions with "1" is considered to have nearly no privacy concerns. Building on this, we develop three user groups: One consisting of users with low privacy concerns (total score of 19 or less), one with medium privacy concerns (total score between 20 and 38), and one with high privacy concerns (total score of over 39). In the first group, there might be users who are not concerned about their privacy and, therefore, not willing to accept any additional overhead on their main task to protect their privacy. The second group might comprise people who never thought about taking care of their privacy but are willing to learn how to protect it. The last group of users care about their privacy and are also willing to accept additional overhead in order to protect it.

4 PARTICIPATORY DESIGN STUDY

Our implementation aims to provide users with information about script tracking on websites. Although some browser extensions providing information about script tracking already exist, none of these provide different interfaces for different user groups. Thus, we want to build a browser extension that adapts to its user. In contrast to existing "simple" and "advanced" views (i.e., providing only a general overview versus providing more information and configuration options), our different views will be adjusted to the needs of a user, presenting necessary explanations to lay users and more details to sophisticated users. To develop such an extension and the support personas resulting from the developed items (cf. Section 3), we used a participatory design approach. Participatory design has proven to be important in software and product design in

order to consider special characteristics of the future user, either to meet the requirements of a special user group like the elderly [15] or to generally involve different stakeholders in the design process [27]. Specifically, we organized a series of workshops to receive input from different stakeholders, i.e., potential users of the extension. The demographic data of the workshops, surveyed via a form that was filled out by the participants at the beginning of every workshop, can be seen in Table 6. Although most of our participants were young and well-educated, the participants were mixed in terms of knowledge of tracking technologies in browsers. Especially in workshop 2, most of the participants were unfamiliar with the technology behind the examined concept of script tracking, had not used browser extensions to visualize tracking, and needed an introduction. The methodology of the workshops is described in the following section.

4.1 Methodology

We conducted three workshops to develop the concrete support personas and the concept of our implementation. Before conducting the workshops, we obtained IRB approval (EK 16/2022) from the ethics committee at our university. Each workshop was held with five German students from different fields of study, who signed an informed consent form informing them about the workshop and the collected and processed data. The students were recruited through a convenience sampling method from the personal and professional networks of the researchers without special selection criteria and were not financially compensated. Therefore, they were from the same university except for two students who studied at other universities. The workshops were held in person, had an average duration of 79 minutes, were neither video nor audio-recorded, and comprised a (1) motivation of the topic, (2) presentation of known applications, (3) work phase, and (4) conclusion phase.

4.1.1 Motivation of the Topic. At the beginning of each workshop, the topic and our motivation were presented. This was inspired by the introductory section of this paper (cf. Section 1). Additionally, a short introduction to script tracking was presented to explain the concept to the participants. This way, we ensured that every participant knew the basics of the topic and could participate in the workshop. To ensure comparability between the workshops, we followed a script (cf. Appendix A.2). We focused only on script tracking instead of other tracking technologies because otherwise, the cognitive load of the participants would possibly be too high to focus on the support personas and the design of the application. Additionally, this limitation does not influence our implementation since it is only a demonstrator, which shows how support personas can be implemented in a design and implementation process.

4.1.2 Presentation of Known Applications. After the introduction, a few applications offering different UI solutions on how to visualize script tracking and other tracking elements to the user were presented. These applications were Ghostery, Disconnect, DuckDuckGo Privacy Essentials, NoScript, and UMatrix.

Ghostery. Ghostery (Figure 3) shows the number of tracking-related requests as a number in the icon on the extension bar. After clicking on the icon, the user can see the different categories of the identified trackers. Additionally, statistics about the number of blocked trackers, the number of changed requests, and the loading time of the site are presented. In the extended view, the user can see which requests were classified in which category and the status of every request (i.e., blocked or unblocked). Additionally, the user can block or unblock single requests in this view.

Disconnect. Disconnect (Figure 4) also categorizes the found tracking-related requests but, in addition, shows how many trackers were found from Facebook, Google, and Twitter. Additionally, in the normal view, the user is shown how much faster the website loaded and how much bandwidth was saved by using Disconnect. After clicking on the different categories, the user sees the trackers that were blocked in this category. Here, the user can block or unblock individual or all trackers in a category. Finally, Disconnect offers a view where the user can see the trackers visualized as a graph showing the websites the trackers were loaded from. Websites the user has already visited are highlighted.

DuckDuckGo Privacy Essentials. DuckDuckGo Privacy Essentials (Figure 5) assigns a privacy score to every website. This score rates a website's trustworthiness. The score improves when the connection to the website is encrypted, fewer trackers are used by the website, fewer known tracking networks are found on the website, or the privacy policies are known. It also shows how much the score is enhanced by using the extension to block some trackers or enforce the encryption of the connection.

NoScript. NoScript (Figure 6) is an extension that blocks all scripts by default. This can impair the proper functioning of websites the user visits for the first time. The user then has to explore manually which scripts are required for the website to function and unblock scripts accordingly.

uMatrix. uMatrix (Figure 7) analyzes all building blocks of a website and presents them in a matrix. The rows show the different domains from which the building blocks are loaded. The columns tell the user which kind of content is loaded (e.g., a picture, a cookie, or a script). The user is also shown which sources are blocked and which websites, as script sources, are considered not to be relevant for the website to work.

4.1.3 Work Phase. To allow the participants to think freely about concepts of implementation, they were not informed about the results of Section 3, i.e., that we plan to divide the users into three groups per dimension. They were only told that the different user groups will be based on the privacy competence and privacy concern of the users. Thus, all workshop groups considered the first step in the work phase to be to think about possible user groups arising from these two characteristics. After identifying those groups, the participants thought about UI elements suitable for each user group. The results of this phase were noted on a whiteboard and visible to every participant during the entire workshop. This way, the results could be refined and used as a basis for new ideas.

4.1.4 Conclusion Phase. At the end of every workshop, we summarized the results. This gave the participants the chance to clarify misunderstood ideas or add important details.

4.2 Results

4.2.1 First Workshop. The first workshop (90 minutes) was held with five male participants studying computer science or electrical engineering on 07/15/22. After the introduction and motivation of the topic, the participants began to develop user groups based on the users' privacy competence and privacy concern. The first idea was to distinguish between low and high privacy competence and low and high privacy concern, leading to four user groups. After some discussion, two participants mentioned that they do not entirely identify themselves with any of the groups. Thus, a new idea to implement a medium category for both items was developed. Now, all participants found themselves in one category.

After establishing this classification of users, the participants discussed whether some of the categories could be merged in the implementation since users of different categories share the same requirements for the UI. The discussion ended with the result that the participants would implement three different views in the UI depending primarily on the person's privacy competence and less on the privacy concern. This was concluded because the privacy competence would be much more important for determining the level of support given by an application, while the privacy concern would only determine how the user uses the given setting options.

In the last step, the UI elements for the three views were developed. For the first group, i.e., users with low privacy competence, the view should be designed as simple as possible. The participants found a score similar to that from DuckDuckGo Privacy Essentials to be helpful. The extension should also tell the user how many scripts were blocked. Additionally, the pop-up should contain some tips for education and knowledge expansion. In the pop-up, a button to turn off the script blocking on the current website should be implemented. This button should be large enough to be easily noticed by users with less experience. The UI view for users with low privacy competence should serve as a base for the other views. The view for users with medium privacy competence extends this view by introducing different categories of scripts. In the workshop, this classification was not specified but was later implemented by using the categorization of third-party scripts and others developed in the third workshop. Users in this category can decide to block or unblock all scripts of a category. The third and most advanced view for users with high privacy competence lists the individual scripts in all categories and allows the user to block or unblock single scripts. Further, it is shown when scripts from one origin are loaded on many sites visited by the user.

The participants also pointed out the importance of the user's ability to customize the interface. For example, a user with low or medium privacy competence should be able to change the view to the most advanced view if wanted. This setting option must be implemented for all three views.

4.2.2 Second Workshop. The second workshop (79 minutes) was held with five participants, three of them female and two male, on 07/28/22. They were students from different universities studying psychology, computer science, finance, or medicine. After the introduction and motivation, they started to identify four relevant user groups based on users' privacy competence and privacy concern. The first group consists of users with low privacy competence and low privacy concern, the second group of users with low privacy competence but high privacy concern, the third group of users with medium competence and medium concern, and the last one of users with high privacy competence and high privacy concern.

Thereafter, the participants were told to find suitable UI elements for different user groups. During this task, they decided that the requirements for a UI should be linked to the privacy competence of the users. Therefore, users of the first two groups were assigned to the same UI. Thus, three UIs were developed.

The first UI for users with low privacy competence contains a score similar to DuckDuckGo Privacy Essentials. Additionally, the users should be presented with the categories of found scripts similar to the regular view of Ghostery. In this view, it should be possible to turn off the blocking of all scripts if a website does not work. Additionally, the user should get more information and explanations on scripts when clicking on little information buttons ('i'). The second view for users with medium privacy competence should contain a more elaborated score, i.e., with information about its calculation. In addition to the simple view, this extended view should show which script belongs to which category. The most detailed view for users with high privacy competence should contain a matrix similar to the one of uMatrix. The participants found this to be an efficient way to provide the most detail. For users who want even more information, the participants found a graph view like the one in Disconnect helpful. This graph view should be accessible over a button in the detailed view.

The participants pointed out that a user should be able to switch between different views. Further, when the user changes settings in the extended or detailed view, the on/off button in the simple view should adjust and show a custom setting. This way, the user sees that a property was changed when returning to the simple view.

4.2.3 Third Workshop. The third workshop (69 minutes) was held with five participants studying computer science, electrical engineering and information technology, business informatics, and computational engineering on 08/10/22. After the obligatory introduction and motivation of the topic, the participants of the workshop were asked to identify user groups based on users' privacy competence and privacy awareness. Their first thought was to draw a cartesian coordinate system with privacy competence on the x-axis and privacy concern on the y-axis. With this coordinate system on the whiteboard, they started to think about possible user groups inside this system. The first approach mentioned was to divide every axis into two groups, thus having four groups. After a few discussions, the participants concluded that four groups are not enough since 'people in the middle', i.e., with medium privacy competence and concern, would easily fall into one of the extreme groups, e.g., with high privacy competence and concern. Thus, they decided to divide every axis into three groups (low, medium, high), resulting in nine different, more fine-grained user groups.

After identifying the user groups, the participants developed the browser extension UI. Their approach was to use privacy competence as a measure to decide which UI is shown to the user. This strategy results in three different UIs: simple, standard, and expert. The participants mentioned that the user should be able to switch between the interfaces. The privacy concern, on the other hand, should be used to set the default values of the extension, i.e., how

First Workshop	Second Workshop	Third Workshop
• **Three UIs based on privacy competence** • **Possibility to change views** • **Three categories per item** • Privacy concern determines how user uses settings • First UI: **Turn-off button**, **score**, Number of blocked scripts, tips for education and knowledge expansion • Second UI: **Show scripts in categories**, **(un-)block by category**, Extend first UI • Third UI: List all scripts sorted by category, (un-)block single scripts, show often appearing scripts	• **Three UIs based on privacy competence** • **Possibility to change views** • Four user groups: low competence and concern, low competence and high concern, medium competence and concern, high competence and concern • First UI: **Turn-off button**, **information and explanations**, **score**, script categories • Second UI: **Show scripts in categories**, score with calculation information • Third UI: **Matrix view showing building blocks**, graph view of tracking elements	• **Three UIs based on privacy competence** • **Possibility to change views** • **Three categories per item** • Privacy concern as a measure to set default settings • First UI: **Turn-off button**, **information and explanations**, score information to compare security of websites • Second UI: Score, **(un-)block by category**, number of scripts • Third UI: **Matrix view showing building blocks**, as much information as possible

Table 1: Differences and similarities (highlighted in bold) between the workshops

many scripts get blocked. For users with a low concern, the extension should block fewer scripts so that every website works. With increasing concern, more scripts should be blocked. The appearance of the three UIs is described in the following.

The first 'simple' UI should mainly consist of a privacy score like the one by DuckDuckGo. The participants mentioned the idea of extending the privacy score with information on how secure the site is compared to other sites the user visited. This should make the very abstract score more concrete and tangible to the user. Additionally, the simple view should feature a button to disable the extension or block more scripts. The default setting of this slider should be based on the user's privacy concern. Additional information and explanations could be given to the user by using little question marks. The second user interface, called 'standard', should contain the privacy score from the 'simple' interface. In addition, the number of scripts should be shown. The slider from the 'simple' interface should also be extended by providing more information about the blocked scripts, e.g., that all external, i.e., third-party, scripts are blocked or that external and internal, i.e., not third-party, scripts are blocked. The third 'expert' user interface should provide the user with as much detailed information as possible. For this, the participants of the workshop found the matrix representation of the website from uMatrix suitable. An interesting idea mentioned was giving the user the possibility to view the script to be loaded so that an expert could look at it to find out what it does and decide whether it is important. The participants also suggested using buttons included in the 'expert' view to show the user as much information and statistics as possible upon request.

4.3 Summary

In this section, we will summarize the workshops. The differences and similarities between the workshops can be found in Table 1.

4.3.1 Support Personas. A common result of all workshops was to use three gradations on the items of privacy competence and privacy concern. This result hardens the findings of our literature work (Section 3) by confirming the identified support personas in a qualitative setting. The first and third workshops worked with all nine resulting user groups, while the second one only identified four user groups. Still, all workshops proposed three different views based on the privacy competence of the user. The privacy concern was only mentioned by two workshops as a means to set the default settings or describe how the user will use the settings.

For the support personas, this means that the privacy competences of future users are of special importance during the development process. The workshops showed that the interface of PETs should be adjusted to the privacy competence of the user, so that every user gets understandable and relevant information. The privacy concern gets important later in the development process of PETs where the default settings for users are determined. At this stage, users with a higher privacy concern might accept more drawbacks for improved privacy than users with a lower privacy concern.

4.3.2 Browser Extension. According to the workshops, the simplest view should contain a privacy score. Additionally, little question marks should provide explanations when the user clicks on them. This is important for users who want to acquire more knowledge. One workshop concluded that the simplest view should also present the number of blocked scripts and the script categories. Since the other workshops determined that the categories should be mentioned in the second view, we will only show the number of found scripts in the first view. Finally, a button should be implemented to deactivate the extension for a website if it does not work. According to two workshops, the second view should, besides the privacy score, also show the categories of scripts and how many scripts were found in each category. The most extensive view should present the number of found scripts in every category together with the individual scripts and as much information as possible. In the workshops, the matrix representation was found to be most useful for the primary window. After clicking on different buttons, the user should be able to access even more information, e.g., by using a graph view like the one from Disconnect.

5 DESIGN OF PRIVACYASSIST

We built the PrivacyAssist extension for the Firefox web browser[2]. For development, we used the integrated development environment (IDE) WebStorm[3] and tested it by using the Firefox development tools. In the following subsections, we discuss and present the concept, first prototype and final version of the browser extension.

5.1 Concept of the Browser Extension

The concept is based on the studied literature and the workshops (cf. Table 1). It addresses the identified challenges, which are illustrated in Table 2. In Section 3, we highlighted that the user must have the feeling that their actions will be sufficient to improve their own privacy. In our implementation, we take this into account by offering different UIs based on the respective privacy competence that provides users with comprehensible information and explanations. This solution was also suggested in our workshops.

Challenge	Literature/ Workshop Findings	Solution
Give the user confidence in their own capabilities	[14]	Design of different UIs based on the user's privacy competence
Prevention of user frustration	[33], W3	By default, block only external scripts as this should not break websites
Easy to use and understandable UI	[1, 33, 54]	Design different UIs for users with different privacy competence and provide help and additional explanations
Provide more detailed information to experts	W1-W3	Design a view with very detailed information for users with high privacy competence
Freedom of choice	W1-W3	Provide the user the possibility to change views

Table 2: Overview of the identified and addressed challenges

Since we discovered that user frustration can arise from poor interface design, we try to offer users the most suitable interface by default after an evaluation of the respective privacy competence. Moreover, we ensure that a website can function properly and is not impaired by only blocking third-party scripts by default. The user can change this setting for every website. An easy-to-use and comprehensible interface also contributes to more secure decisions by users. We achieve this by providing a very simple interface, especially for users with less privacy competence. The simple interface only shows the privacy score, which is easily recognizable in the menu bar. When the user clicks on the icon, the privacy score and some easily comprehensible information about it is shown, e.g., how it is calculated. Additionally, small buttons with question marks are used to provide additional help and explanations.

[2] https://www.mozilla.org/firefox/
[3] https://www.jetbrains.com/webstorm/

With increasing privacy competence, the user can handle more detailed information. In the second view, the user is shown the different categories of scripts and has the option to block an entire category. The privacy score is also shown in this view. The most extensive view shows all found scripts, sorted by category, and has the option to block individual scripts. In the future, this view can be extended so that the user is provided with more statistics and information, e.g., a graph view like the one from Disconnect.

In the workshops, it was concluded that the user should be able to change views upon request. Hence, we implement this functionality by using different tabs in the browser extension. Additionally, it was mentioned that the title of the different views should not give the user the feeling of having insufficient knowledge to use other views. Thus, the views are labeled "Standard", "Extended", and "Detailed".

5.2 First Prototype

The first step of the process was to build a prototype to extract information about the scripts from a loaded website and display it in the extension's pop-up window. Since the source of a script can be used to assess its function, we decided to extract the sources and display them in a list. The extension's pop-up expands and is only active when the extension icon in the browser's menu bar is clicked. To work on the opened websites and inject code into them, a content script is needed, which is loaded into the website like any other script. We use the content script to inspect the Document Object Model (DOM) of the website. The DOM presents the content of a website as a tree-like structure. The root is the document itself with the <html>-tag, which has the <head>-tag and <body>-tag as children. The children of the <body>-tag are the building blocks of the website. We inspect the DOM to extract the scripts embedded into the website. The source attribute of the script tag is important for our implementation to show the user the origin of the scripts.

The content script cannot communicate with the pop-up script directly, as the pop-up script is only active when the pop-up is opened. Therefore, a background script is needed, which runs in the background and can exchange messages with the content script. We use it to extract the origins of the loaded scripts from the content script and store them in a private variable. The pop-up script can access the background script and its variables. This way, the pop-up window can access the origins of the scripts. After accessing the information, we can display it in the pop-up window. The prototype was tested by visiting different websites and evaluating whether all scripts were detected and showed up in the extension's list.

5.3 Final Browser Extension

After a successful implementation of our prototype, we implemented the features developed during the workshops (cf. Section 4): We created three different views for the three user groups with different privacy competences, which are accessible by using a tab-like menu bar. The views are labeled "Standard", "Extended", and "Detailed". According to Workshop 3, the scripts found on a website are classified into two categories, namely internal and external scripts. Internal scripts are scripts that are loaded from the visited website or subdomains thereof. External scripts are scripts from all other sources, so-called third-party scripts. For the application and the following, we use the term external scripts since it is more

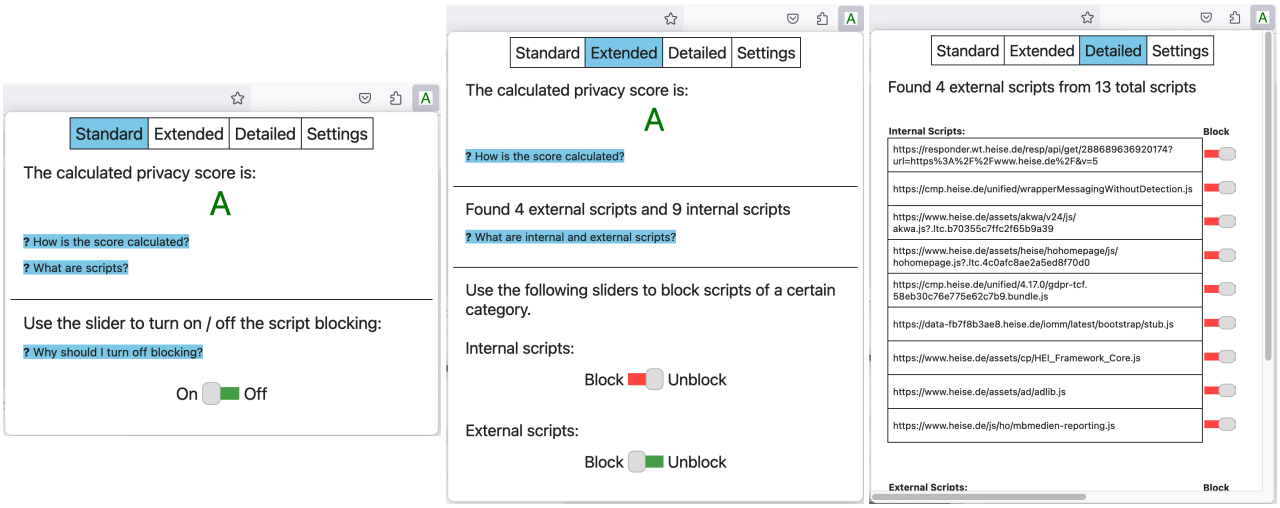

Figure 1: The extension's standard (left), extended (center), and detailed view (right)

comprehensible for lay users. This classification is a simplification of tracking technologies in general and, therefore, a limitation that might lead to a less complex user interface. Nevertheless, our design recommendations (cf. Section 7.3) can still be implemented and evaluated. A more detailed discussion is presented in the limitations (cf. Section 7.4). In our extension, we disregard the specific function of scripts, which may lead to a wrong classification of websites. While other approaches may classify scripts more accurately, this does not influence the UI elements that we want to evaluate to check whether different users like different elements and want different information. Nevertheless, external scripts are a good approximation for finding tracking scripts since many external scripts are used for tracking or advertisement. The functionality is often not influenced by third-party scripts, which the participants also mentioned during the evaluation.

The privacy score is part of the first two views and ranges from "A" for websites with less than or equal to five external scripts, to "B" for websites with a number of external scripts between six and 15, to "C" for websites with over 15 external scripts. The thresholds for the different scores were chosen by evaluating the number of scripts of different websites. Therefore, it was guaranteed that the participants of the evaluation would easily find websites with different privacy scores. This allows for a good demonstration of the functionality of our demonstrator and is not meant to be a real threat analysis. The scores are illustrated by using different colors: green for the score "A", orange for "B", and red for "C". The icon in the menu bar of the browser also changes with the visited website and shows the letter "A", "B", or "C" in the corresponding color. When the user clicks on the icon in the menu bar, the pop-up window opens. The presented view is the view set as default. This is the standard view for users with low privacy competence. Users with medium privacy competence are shown the extended view. The detailed view is shown to users with high privacy competence.

In the standard view (Figure 1, left), the user sees the calculated privacy score. Below, the user is shown help buttons that provide explanations about the privacy score and the concept of scripts. At the bottom, a slider can be used to turn off the extension for the current website. This might be useful if a website was not loading due to blocked scripts. The extended view (Figure 1, center) also shows the privacy score on top. The number of external and internal scripts found is shown below. A help button explains the concept of external and internal scripts. At the bottom of the pop-up, two sliders can be used to block or unblock all external or internal scripts. Finally, the detailed view (Figure 1, right) shows the numbers of found internal and external scripts on top. Below, the user finds a list of all scripts sorted by internal and external scripts. In this view, the user can block and unblock scripts individually. In the settings tab, the user sets the default view.

6 EVALUATION

Since the goal of this work is to develop the concept of support personas and demonstrate their usage in a development process, the main purpose of the evaluation was to examine whether the application provides good support and user experience to all groups. This would mean that the usage of support personas was successful.

6.1 Methodology of the Evaluation

6.1.1 Participants. We conducted the evaluation with 31 participants (cf. Table 3), ten of whom had also participated in the workshop. This allowed us to evaluate whether the developed application met the expectations of the workshop participants. The new users were chosen to ensure that the extension is usable without prior knowledge from the workshops. Some of the interviews were held in person and some remote (cf. Table 3). All interviews were audio recorded to evaluate the Think-Aloud method more precisely. The audio recordings were transcribed and analyzed by two researchers to identify further insights about the user experience. It was inspected how the UI was described, what aspects of the UI were liked or not, and what the reasons were (cf. Section 6.2.2). Before conducting the evaluation, we obtained IRB approval (EK 16/2022)

from the ethics committee at our university. In total, we interviewed 19 men, eleven women, and one diverse person (with an average duration of 35 minutes) from Germany. For the statistical Mann-Whitney-U-Test, this means that we can only determine big effects and thus big differences between the groups with a statistical power of 0.72 for an effect size of 0.9 and an error probability of 0.05. Participants were first recruited from the university context (n=20) and received no financial compensation. These interviews were held between 09/03/2022 and 09/10/2022. To increase the heterogeneity of the sample, we then recruited individuals via the crowdworking platform *Prolific*[4] (n=7) and the personal and professional networks (n=4). The participants from *Prolific* received €8 in financial compensation. Prolific is a platform designed to provide samples for scientific studies. Several studies have confirmed the reliability of Prolific and its ability to collect high-quality and diverse data [2, 42]. The follow-up study was held between 05/15/2023 and 05/24/2023. Since we reached saturation, i.e., no new findings, and the fact that a sample size of 31 is relatively high for qualitative studies in the research area of human-computer-interaction [9], the sample size of 31 participants was seen as sufficient.

6.1.2 Procedure. An important part of the evaluation was the user experience questionnaire (UEQ) [30], which inspects the experience the user had when using the application. All participants were informed about the data collected and processed during the evaluation and signed an informed consent. Before the participants tested the application, we asked for some demographic information (age, gender, study field/job) via a questionnaire form. The participants also answered the OPLIS and the IUIPC questionnaire introduced in Section 3 to determine their respective support personas. The participants were also asked to answer three questions about their previous experience with script tracking.

While using the application, the participant's voice was recorded, and they were asked to think out loud (Think-Aloud method [55]). Thus, we were able to receive an immediate reaction to our UI. This data was evaluated to find out what was unclear, where questions arose, or what was surprising to the user. As an introduction, we explained how the pop-up window of the application can be accessed. After this, the participant was asked to visit a few websites and explore the browser extension. After testing the extension, the participants answered the UEQ questionnaire to rate the user experience and answer a few questions about what they liked or disliked. Of special interest was the question of whether the user learned something by using our extension. This would indicate that we not only developed a usable but also educational application.

Person	Gender	Age	Field of Study / Job	Workshop	Remote
W1	m	20-24	Electrical Engineering B.Sc.	y	n
W2	m	20-24	Business Informatics M.Sc.	y	y
W3	m	25-29	Environmental Engineer	n	n
W4	w	20-24	Finances M.Sc.	y	n
W5	m	25-29	Computer Science M.Sc.	y	n
W6	m	25-29	Int. Business Studies B.Sc.	n	y
W7	m	20-24	Computer Science B.Sc.	y	n
W8	w	20-24	Int. Business Studies M.Sc.	n	n
W9	m	20-24	Comput. Engineering M.Sc.	y	n
W10	w	20-24	Teaching Student (German, Art)	n	y
W11	m	20-24	Media Informatics B.Sc.	n	y
W12	w	20-24	Computer Science M.Sc.	n	y
W13	m	20-24	Project Manager	n	y
W14	m	20-24	Computer Science M.Sc.	y	n
W15	w	20-24	Computer Science M.Sc.	y	n
W16	m	20-24	Computer Science M.Sc.	y	n
W17	m	20-24	Catholic Theology	n	y
W18	w	20-24	Controller	n	y
W19	m	20-24	Psychology B.Sc.	y	n
W20	w	55-59	Secretary	n	n
W21	m	40-44	Self-employed	n	y
W22	d	40-44	Alternative Practitioner	n	y
W23	m	30-34	Team Leader Logistics	n	y
W24	m	40-44	Commercial Employee	n	y
W25	w	30-34	Self-employed	n	y
W26	m	55-59	Banker	n	y
W27	w	55-59	Homemaker	n	y
W28	w	50-54	Commercial Employee	n	y
W29	w	50-54	Judiciary Employee	n	y
W30	m	45-49	Gardener	n	y
W31	m	35-39	IT System Administrator	n	y

Table 3: Overview of the participants of the evaluation

6.2 Results of the Evaluation

6.2.1 Classification and Preferences of Users. According to the OPLIS questionnaire and our ranking based on the norm table of the entire population, 17 participants were classified as having high, 10 participants as having medium, and four participants as having low privacy competence (Table 5). Thus, we evaluated the application with users corresponding to every identified support persona. We found that 16 of the 31 participants preferred the view recommended to them, while most (22) of the users preferred the "Extended" view due to the combination of simplicity and information. The eleven participants with high competence who preferred the "Extended" view indicated that the "Detailed" view did not provide the score and the possibility to block whole categories of scripts. This shows that the score and, therefore, the classification of websites is a feature many users want. It was also the feature that was mainly used while trying the application. Nevertheless, six participants preferred the "Detailed" view because they liked the display of the addresses and the possibility of blocking individual scripts. With one exception, the "Detailed" view was preferred only by people with a high level of privacy competence, which supports our workshops' result that this user group prefers to receive more information. They also acknowledged the "Detailed" view as a possibility to get further information or more adjustment options. This corresponds with the preference of the developed support persona that people with a high privacy competence like to have the possibility to adjust settings and like to have as many information as possible. In contrast to the workshop results, the evaluation shows

[4] https://prolific.co/

that even though users with a high privacy competence like the settings of the “Detailed” view, in everyday life, they (twelve out of 17) prefer a simpler view like the “Extended” view. One participant even prefers the “Simple” view in everyday life. Half of the four participants with a low privacy competence preferred the "Standard" view, while the other half preferred the "Extended" view after reading the explanations in the "Standard" view and familiarizing themselves with the extension. Regarding the educational aspect of our browser extension, all 21 participants without prior knowledge about scripts and script tracking stated that they learned what scripts are. Additionally, they stated that they understood the difference between external and internal scripts. This mirrors the considerations from the workshops, and our literature findings that lay users with a low privacy competence need easy-to-understand explanations. In addition, the fact that users who did not know about script tracking read the explanations in the “Standard” view shows the functioning of our UI design. The explanations allowed the users to understand and use the “Extended” view. In addition, the extended view provided the settings that nine of the ten participants with medium privacy competence wanted.

6.2.2 User Experience. Since the objective of our work was to develop an application that supports the user best and is thus easy to use, the results of the UEQ questionnaire were of particular interest. It measures six different aspects: attractiveness, perspicuity, novelty, stimulation, dependability, and efficiency.

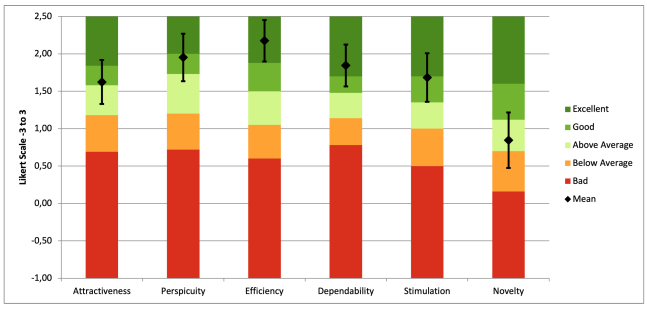

Figure 2: Results of the UEQ-questionnaire

The results (cf. Figure 2) show that our browser extension has good to excellent scores in all aspects except for the novelty rating. The lower score for the novelty is not surprising since our application combines features from existing browser extensions to present the appropriate information to the user. The perspicuity score shows that our application is easy to use, to learn, and comprehensible. This is supported by the statements of the participants who found the extension "very intuitive" (W5, W7, W10, W15, W16, W21, W24), "easy to handle" (W29) and the explanations "easy to understand" (W2, W3, W6, W8, W10, W15). Many participants also liked the given privacy score in the menu bar, which gives good information to see if a website is more privacy-protecting or not (W2, W4, W9, W11, W18, W20, W26, W31). A point of criticism was the missing score range for the privacy score (W7, W9, W31). Considering the feedback we received, attractiveness and stimulation could be improved with the implementation of a more modern design and the use of toggle switches instead of slide switches.

We performed a Mann-Whitney-U-Test [35] to evaluate whether the user experience varies between workshop participants and others. The results can be seen in Table 4. In Section D, the detailed results can be seen. We found that for the two-sided significance level of 0.05, there is only a difference between both groups regarding dependability. The participants who also took part in the workshops assessed the dependability higher, which shows that they felt more comfortable when working with the application.

Item	Test Statistics U	z-Value	p-Value
Attractiveness	97	-0.338	0.735
Perspicuity	69	-1.521	0.128
Novelty	80.5	-1.035	0.301
Stimulation	87.5	-0.74	0.459
Dependability	49	-2.367	0.018
Efficiency	110	0.211	0.833

Table 4: Mann-Whitney-U-Test results on the UEQ answers

In conclusion, 26 out of the 31 participants stated they would use the browser extension in their everyday life. Most of them concluded that the tool would be easy to use and convey a good impression of the potential tracking that is performed on a website. Although most of them would not use it to actively block scripts, the first impression of the given privacy of a website shown by the privacy score would be a reason to use the browser extension. One participant (W1) said that he already has a similar application installed, which has more functions and, thus, would not use the application. Another participant (W16) stated that he would consider changing to our extension due to the simplicity and clarity. W21 and W31 stated that they would use it if they saw an advantage to other applications or the built-in tracking protection of the browser.

7 DISCUSSION

The core contribution of our work lies in the development of the concept of support personas that are used to classify users in different categories to provide them with the support they need and want when using PETs. We verified the concept by applying it to a browser extension that informs the user about scripts and script tracking during web browsing. The evaluation results show that the extension is not only easy to use but also educates the user.

7.1 Methodological Contribution

In our research question, we asked how users of PETs with different backgrounds can be supported through UI components. The related work shows that there is a demand for applications that support the individual user in making more informed decisions [25]. Additionally, it was shown that in applications providing explanations for less experienced users, they often struggle to understand the terms used in the explanations [3, 58]. This underlines that more research is required to provide support for different types of users. We concluded that in order to provide customized support to each user, we would need to divide users into distinct groups. Since the concept of personas has proven to be helpful in requirements engineering [50], we developed support personas that represent user groups based on the support a user wants and needs from

Person	Privacy Competence	Privacy Concern	Knew About Scripts & Script Tracking Before	Preferred View
W1	high	high	yes	Detailed
W2	high	high	yes	Detailed
W3	medium	high	no	Extended
W4	high	high	no	Extended
W5	high	high	yes	Extended
W6	high	high	no	Detailed
W7	medium	high	yes	Extended
W8	high	high	no	Extended
W9	high	high	yes	Detailed
W10	medium	high	no	Extended
W11	medium	high	no	Extended
W12	high	high	yes	Extended
W13	medium	high	no	Detailed
W14	high	high	no	Extended
W15	high	high	yes	Extended
W16	high	high	yes	Extended
W17	high	high	no	Extended
W18	high	high	no	Detailed
W19	medium	high	yes	Extended
W20	medium	high	no	Extended
W21	medium	high	no	Extended
W22	high	high	no	Standard
W23	medium	high	no	Extended
W24	high	high	no	Extended
W25	low	high	no	Standard
W26	high	high	no	Extended
W27	low	high	no	Standard
W28	medium	high	no	Extended
W29	low	high	no	Extended
W30	low	high	no	Extended
W31	high	high	yes	Extended

Table 5: Overview of the results of the questionnaires

an application. These are the main contribution of the paper. We based the support personas on the user's privacy competence and concern. The needs of the different personas were then developed and refined in workshops for participatory design.

Support personas have some common aspects with privacy personas developed in previous works. The privacy personas were either based on users' privacy concern or privacy competence, together with users' privacy behavior [29, 40]. The difference between privacy personas and support personas lies in the purpose for which they were developed. While privacy personas were developed to classify users with regard to their attitude toward privacy, the protection of their data, and their behavior when using technology, support personas aim to elaborate on how different user groups can be supported by providing them with the best user experience when using PETs. Additionally, support personas allow for UI customizations that are adjusted to the users' needs and not only their current privacy behavior. The definition of a persona includes not only the items on which they are based but also the motivation, attitude, and goals of a user. The motivation and goals of support personas are differing from those of privacy personas because of the different focus. The demonstrator PrivacyAssist shows that we could address the different user groups by using support personas in the development process. Other developers of PETs can also use the developed support personas and the UI guidelines (cf. Table 2) to develop PETs that are more usable for all different users. Especially by considering the support personas, the developers will have the needs of all the different users in mind. This will help to develop applications not only for a specific target group but for all users. That will lead to PETs, which are not only usable by security experts but also by lay users. Thus, the support personas are an important contribution to the development of a UI that best supports the user while appropriating new PETs and the key contribution of our paper.

7.2 Support Personas During Development

To evaluate the concept of support personas in a development process, we designed a browser extension, PrivacyAssist, that provides users with information about script tracking. It identifies third-party scripts that are often used for script tracking and informs users about their usage on visited websites (cf. Section 5.3). It was found that internet users often only have basic knowledge about online tracking [37] and that a UI providing the user with more information about the security of a website is needed [56]. It was also shown that a privacy dashboard presenting details about potential privacy threats improves users' privacy perception [16].

To involve different stakeholders in the design process [27], the design of the extension's UI was conceptualized during three workshop sessions with a total of 15 participants. The contributions of the workshops were guidelines that should be adhered to when developing a usable application. Thus, we complement the design guidelines developed by existing works [1, 14, 33, 54]. Additionally, we found that the UI should be primarily based on the user's privacy competence to provide the best support possible. In comparison to existing approaches, PrivacyAssist combines their functionality and provides different user interfaces for different support personas. During the evaluation, we verified that our application is easy to use and educational for the different support personas. We showed that different users prefer different UIs that present the information they want and need. Users with less knowledge about scripts considered the explanations we provided in the application as very helpful. More advanced users liked the detailed information and configuration options provided in the "Detailed" view. This shows that support personas are a valuable contribution to the development process of PETs.

7.3 Recommendations

The related literature [1, 25, 33] suggests that users' understanding of security issues and awareness of their security needs are critical when designing user interfaces. Therefore, we designed our support personas according to these two factors, namely privacy concern and privacy competence. Future work can use the support personas to examine user groups in different privacy scenarios. Every support persona requires different features of a privacy enhancing user interface. These should be addressed by developers of PETs. Regarding privacy concerns, users with low values may become

frustrated if the user interface hinders their workflow, such as by blocking suspicious scripts that remove essential parts of a website. Conversely, users who highly value privacy would likely tolerate a certain degree of performance drawbacks as long as their privacy is not compromised. Therefore, the default values in PETs should be set according to the users' level of privacy concern. When it comes to the privacy competence of users, there should be different UIs for each user group, e.g., providing easy-to-understand explanations for novices, which ideally increases their privacy competence, and extensive information and settings for experts. However, users should not be restricted to a single UI and have the option to switch views if they desire. For instance, while an expert user may occasionally desire detailed information, it may be advantageous to provide a simpler view for the majority of the time. To account for individual preferences, we suggest involving users early in the development process, allowing them to provide feedback and contribute to design decisions to avoid misinterpretations early on and increase the UI's usability. Easy-to-understand explanations also increase the privacy literacy of the users, which helps users secure their privacy. For users, we recommend that they should inform themselves about privacy topics to be more aware and knowledgeable and make more secure decisions. For browser tracking, users should be aware that data about them or about their browsing behavior is often distributed to third parties. Our developed application can help assess whether a website runs scripts that can possibly track users. Based on this information, users should decide which information they provide to the website or whether they want to visit another website. Especially personalized information can help users to get the information they need to make more secure decisions.

7.4 Limitations

While the participants in the workshops had different study backgrounds, they were students from the researchers' personal and professional networks, which could result in different biases. Although the presentation of existing applications helped the participants to get an idea of the application to be developed, all participants only used existing modules, while completely new ideas were not developed. This limited the novelty of the extension. Another limitation lies in the privacy score we calculated for the visited websites. Currently, the score's calculation is based on the number of found third-party scripts. Although those scripts are often used for tracking the user, they can also be used to load content, e.g., new fonts, which is not relevant for security. Another problem is that websites like *www.youtube.com* do not use third-party scripts but track the user using their own scripts. For both cases, it would be beneficial to know the exact purpose of a loaded script. This feature was also requested during the evaluation, as it provides knowledge crucial for deciding whether to block a script or not.

The distinction between first- and third-party scripts represents a simplification of a complex tracking ecosystem (e.g., including browser fingerprinting, cookies, or tracking requests) to a certain degree. However, it enabled the development of a proof of concept of how support personas can be used in the development process of PETs. With a more fine-grained distinction, e.g., in essential, functional, and marketing scripts, more visualizations and settings would be necessary. Additionally, further explanations would be needed, which could make the extension more complicated. All this must be evaluated in practice, although we think that with our given recommendations, like the usage of easy language, the development of an extension for all users is still possible. Additionally, PrivacyAssist can be extended by implementing more features, like the visualization of additional tracking elements.

Finally, another limitation is that all participants were ranked as having high privacy concern. One reason could be the used questionnaire. While a good construct validity and reliability was shown [23], the questionnaire could show weaknesses in practice. Eventually, a more specific questionnaire on the topic of script tracking could have solved the problem, but this would have restricted the generalizability of the support personas. Another reason could be that users, when asked, rate their privacy concern higher than it actually is. This can be in relation to the privacy paradox.

7.5 Future Work

Future work could explore the concept of support personas further and draw on it to build more secure applications that can be utilized by users with different knowledge and backgrounds. To further refine the concept of support personas, another evaluation classifying users not only by their support persona but also by their privacy persona, e.g., using the questionnaire by Biselli et al. [5], may be conducted to compare both concepts. Additionally, PrivacyAssist could be extended to support more security and privacy-related concepts of web browsing, e.g., cookies. A modular and dynamic application could also help to make the application more personalized. During our evaluation, some users mentioned that it would be helpful to see the purpose of an individual script in the detailed view. Future research could try to analyze scripts and explain their function to the common user. This could enhance the accuracy of the privacy score by building it on the purpose of the identified scripts. For further feedback, a feedback option for end users can be implemented. An implementation of a domain-to-entity mapping could improve the helpfulness of the source information of scripts.

8 CONCLUSION

More secure critical use cases of computers in peoples' everyday lives require secure applications. A problem with such applications is that they are not easy for lay users to use. One reason is that the applications are often developed with advanced users as the primary target group. Thus, users with limited knowledge receive less support and, e.g., do not understand the explanations provided. So, we developed a strategy to support every user of secure applications. The core of this strategy is the concept of support personas that classify users by the support they need. To demonstrate how this concept can be implemented in a development process, we developed PrivacyAssist, a browser extension that supports the user in the context of found scripts in a participatory design approach. In three workshops, tailored UIs for three different user groups were created. During the evaluation, we found that offering different UIs for different user groups is very helpful and provides every user with the level of support needed. We also verified that our application is easy to use and educational. Thus, we conclude that support personas are a suitable strategy to support users with different backgrounds when using PETs.

ACKNOWLEDGMENTS

This research work has been funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – SFB 1119 (CROSSING) – 236615297 and by the German Federal Ministry of Education and Research and the Hessian Ministry of Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE.

REFERENCES

[1] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, et al. 2017. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)* 50, 3 (2017), 1–41.

[2] Troy L Adams, Yuanxia Li, and Hao Liu. 2020. A Replication of Beyond the Turk: Alternative Platforms for Crowdsourcing Behavioral Research – Sometimes Preferable to Student Groups. *AIS Transactions on Replication Research* 6 (10 2020), 15. Issue 1. https://doi.org/10.17705/1atrr.00058

[3] Susanne Barth, Dan Ionita, Menno DT De Jong, Pieter H Hartel, and Marianne Junger. 2021. Privacy rating: a user-centered approach for visualizing data handling practices of online services. *IEEE transactions on professional communication* 64, 4 (2021), 354–373.

[4] Lemi Baruh, Ekin Secinti, and Zeynep Cemalcilar. 2017. Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication* 67, 1 (2017), 26–53.

[5] Tom Biselli, Enno Steinbrink, Franziska Herbert, Gina Maria Schmidbauer-Wolf, and Christian Reuter. 2022. On the Challenges of Developing a Concise Questionnaire to Identify Privacy Personas. *Proceedings on Privacy Enhancing Technologies (PoPETs)* 4 (2022), 645–669. https://petsymposium.org/2022/files/papers/issue4/popets-2022-0126.pdf

[6] Tom Biselli, Laura Utz, and Christian Reuter. 2024. Supporting Informed Choices about Browser Cookies: The Impact of Personalised Cookie Banners. *Proceedings on Privacy Enhancing Technologies (PoPETs)* 2024 (2024), 171–191. Issue 1. https://doi.org/10.56553/popets-2024-0011

[7] Glencora Borradaile, Kelsy Kretschmer, Michele Gretes, and Alexandria LeClerc. 2021. The motivated can encrypt (even with PGP). *Proceedings on Privacy Enhancing Technologies* 2021, 3 (2021), 49–69.

[8] Aaron R Brough and Kelly D Martin. 2020. Critical roles of knowledge and motivation in privacy research. *Current Opinion in Psychology* 31 (2020), 11–15. https://doi.org/10.1016/j.copsyc.2019.06.021 Privacy and Disclosure, Online and in Social Interactions.

[9] Kelly Caine. 2016. Local Standards for Sample Size at CHI. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 981–992. https://doi.org/10.1145/2858036.2858498

[10] Hsuan-Ting Chen and Wenhong Chen. 2015. Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. *Cyberpsychology, Behavior, and Social Networking* 18, 1 (2015), 13–19.

[11] Kay Connelly, Ashraf Khalil, and Yong Liu. 2007. Do I do what I say?: Observed versus stated privacy preferences. *Lecture Notes in Computer Science* 4662 (2007), 620.

[12] Alan Cooper. 1999. *The Inmates are Running the Asylum*. Vieweg+Teubner Verlag, Wiesbaden, 17–17. https://doi.org/10.1007/978-3-322-99786-9_1

[13] Robert E. Crossler and France Bélanger. 2019. Why Would I Use Location-Protective Settings on My Smartphone? Motivating Protective Behaviors and the Existence of the Privacy Knowledge–Belief Gap. *Information Systems Research* 30, 3 (2019), 995–1006. https://doi.org/10.1287/isre.2019.0846 arXiv:https://doi.org/10.1287/isre.2019.0846

[14] Janna Lynn Dupree, Richard Devries, Daniel M. Berry, and Edward Lank. 2016. Privacy Personas: Clustering Users via Attitudes and Behaviors toward Security Practices. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 5228–5239. https://doi.org/10.1145/2858036.2858214

[15] Ezequiel Duque, Guilherme Fonseca, Heitor Vieira, Gustavo Gontijo, and Lucila Ishitani. 2019. A Systematic Literature Review on User Centered Design and Participatory Design with Older People. In *Proceedings of the 18th Brazilian Symposium on Human Factors in Computing Systems* (Vitória, Espírito Santo, Brazil) *(IHC '19)*. Association for Computing Machinery, New York, NY, USA, Article 9, 11 pages. https://doi.org/10.1145/3357155.3358471

[16] Florian M Farke, David G Balash, Maximilian Golla, Markus Dürmuth, and Adam J Aviv. 2021. Are Privacy Dashboards Good for End Users? Evaluating User Perceptions and Reactions to Google's My Activity. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, virtual event, 483–500.

[17] Simson Garfinkel and Heather Richter Lipford. 2014. Usable security: History, themes, and challenges. *Synthesis Lectures on Information Security, Privacy, and Trust* 5, 2 (2014), 1–124.

[18] Shirley Gaw, Edward W. Felten, and Patricia Fernandez-Kelly. 2006. Secrecy, Flagging, and Paranoia: Adoption Criteria in Encrypted Email. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Montréal, Québec, Canada) *(CHI '06)*. Association for Computing Machinery, New York, NY, USA, 591–600. https://doi.org/10.1145/1124772.1124862

[19] Nina Gerber, Benjamin Reinheimer, and Melanie Volkamer. 2019. Investigating People's Privacy Risk Perception. *Proc. Priv. Enhancing Technol.* 2019, 3 (2019), 267–288.

[20] Ian Goldberg. 2003. Privacy-Enhancing Technologies for the Internet, II: Five Years Later. In *Privacy Enhancing Technologies*, Roger Dingledine and Paul Syverson (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 1–12.

[21] I. Goldberg, D. Wagner, and E. Brewer. 1997. Privacy-enhancing technologies for the Internet. In *Proceedings IEEE COMPCON 97. Digest of Papers*. IEEE, San Jose, CA, USA, 103–109. https://doi.org/10.1109/CMPCON.1997.584680

[22] Thomas Groß. 2020. Validity and Reliability of the Scale Internet Users' Information Privacy Concern (IUIPC)[Extended Version]. *arXiv preprint arXiv:2011.11749* abs/2011.11749 (2020), 59 pages.

[23] Thomas Groß. 2023. *Toward Valid and Reliable Privacy Concern Scales: The Example of IUIPC-8*. Springer International Publishing, Cham, 55–81. https://doi.org/10.1007/978-3-031-28643-8_4

[24] Jonathan Grudin and John Pruitt. 2002. Personas, participatory design and product development: An infrastructure for engagement. In *Proc. PDC*, Vol. 2. CPSR, 2202 N. 41st Street, Seattle, WA 98103, 144–152.

[25] Ursula Holmström. 1999. User-centered design of secure software. In *Proceedings of Human Factors in Telecommunications*. Citeseer, USA, 8 pages.

[26] Anat Hovav and Frida Ferdani Putri. 2016. This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. *Pervasive and Mobile Computing* 32 (2016), 35–49. https://doi.org/10.1016/j.pmcj.2016.06.007 Mobile Security, Privacy and Forensics.

[27] Karlheinz Kautz. 2011. Investigating the design process: participatory design in agile software development. *Information Technology & People* 24, 3 (2011), 217–235.

[28] Spyros Kokolakis. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security* 64 (2017), 122–134.

[29] Ponnurangam Kumaraguru and Lorrie Faith Cranor. 2005. *Privacy indexes: a survey of Westin's studies*. Carnegie Mellon University, School of Computer Science, Institute for Software Research, Pennsylvania, USA.

[30] Bettina Laugwitz, Theo Held, and Martin Schrepp. 2008. Construction and Evaluation of a User Experience Questionnaire, In HCI and Usability for Education and Work: 4th Symposium of the Workgroup Human-Computer Interaction and Usability Engineering of the Austrian Computer Society, USAB 2008, Graz, Austria, November 20-21, 2008. Proceedings 4. *USAB 2008* 5298, 63–76. https://doi.org/10.1007/978-3-540-89350-9_6

[31] Jooyoung Lee, Sarah Rajtmajer, Eesha Srivatsavaya, and Shomir Wilson. 2021. Digital Inequality Through the Lens of Self-Disclosure. *Proceedings on Privacy Enhancing Technologies* 2021, 3 (2021), 373–393.

[32] Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, Shikun Aerin Zhang, Norman Sadeh, Yuvraj Agarwal, and Alessandro Acquisti. 2016. Follow my recommendations: A personalized privacy assistant for mobile app permissions. In *Twelfth symposium on usable privacy and security (SOUPS 2016)*. USENIX Association, Santa Clara, CA, 27–41.

[33] Rodney MacDonald and Ross Smith. 2004. Towards interface specification and design guidelines to raise user awareness of application security. *computer* 16 (2004), 24.

[34] Naresh K Malhotra, Sung S Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research* 15, 4 (2004), 336–355.

[35] Henry B Mann and Donald R Whitney. 1947. On a test of whether one of two random variables is stochastically larger than the other. *The annals of mathematical statistics* 18, 1 (1947), 50–60.

[36] Philipp K Masur, Doris Teutsch, and Sabine Trepte. 2017. Entwicklung und Validierung der Online-Privatheitskompetenzskala (OPLIS). *Diagnostica* 63, 4 (2017), 256–268.

[37] Arunesh Mathur, Jessica Vitak, Arvind Narayanan, and Marshini Chetty. 2018. Characterizing the Use of {Browser-Based} Blocking Extensions To Prevent Online Tracking. In *Fourteenth symposium on usable privacy and security (SOUPS 2018)*. USENIX Association, Santa Clara, CA, 103–116.

[38] Jennifer (Jen) McGinn and Nalini Kotamraju. 2008. Data-Driven Persona Development. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Florence, Italy) *(CHI '08)*. Association for Computing Machinery, New York, NY, USA, 1521–1524. https://doi.org/10.1145/1357054.1357292

[39] Maryam Mehrnezhad, Kovila Coopamootoo, and Ehsan Toreini. 2022. How Can and Would People Protect From Online Tracking? *Proceedings on Privacy Enhancing Technologies* 1 (2022), 105–125.

[40] Anthony Morton and M Angela Sasse. 2014. Desperately seeking assurances: Segmenting users by their information-seeking preferences. In *2014 Twelfth Annual International Conference on Privacy, Security and Trust*. IEEE, IEEE, Toronto, ON, Canada, 102–111. https://doi.org/10.1109/PST.2014.6890929

[41] Moses Namara, Henry Sloan, and Bart P Knijnenburg. 2022. The Effectiveness of Adaptation Methods in Improving User Engagement and Privacy Protection on Social Network Sites. *Proceedings on Privacy Enhancing Technologies* 2022, 1 (2022), 629–648.

[42] Eyal Peer, Laura Brandimarte, Sonam Samat, and Alessandro Acquisti. 2017. Beyond the Turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology* 70 (2017), 153–163. https://doi.org/10.1016/j.jesp.2017.01.006

[43] Sören Preibusch. 2013. Guide to measuring privacy concern: Review of survey and observational instruments. *International journal of human-computer studies* 71, 12 (2013), 1133–1143.

[44] John Pruitt and Jonathan Grudin. 2003. Personas: Practice and Theory. In *Proceedings of the 2003 Conference on Designing for User Experiences* (San Francisco, California) *(DUX '03)*. Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/997078.997089

[45] Bahman Rashidi, Carol Fung, and Tam Vu. 2015. Dude, ask the experts!: Android resource access permission recommendation with RecDroid. In *2015 IFIP/IEEE international symposium on integrated network management (IM)*. IEEE, Ottawa, ON, Canada, 296–304.

[46] Hirak Ray, Ravi Kuber Flynn Wolf, and Adam J Aviv. 2021. "Warn Them" or "Just Block Them"?: Investigating Privacy Concerns Among Older and Working Age Adults. *Proceedings on Privacy Enhancing Technologies* 2 (2021), 27–47.

[47] Christian Reuter, Luigi Lo Iacono, and Alexander Benlian. 2022. A quarter century of usable security and privacy research: transparency, tailorability, and the road ahead. , 2035–2048 pages.

[48] Thea Riebe, Marc-André Kaufhold, and Christian Reuter. 2021. The impact of organizational structure and technology use on collaborative practices in computer emergency response teams: An empirical study. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (2021), 1–30.

[49] Odnan Ref Sanchez, Ilaria Torre, Yangyang He, and Bart P Knijnenburg. 2020. A recommendation approach for user privacy preferences in the fitness domain. *User Modeling and User-Adapted Interaction* 30, 3 (2020), 513–565.

[50] Lydia Schneidewind, Stephan Hörold, Cindy Mayas, Heidi Krömker, Sascha Falke, and Tony Pucklitsch. 2012. How personas support requirements engineering. In *2012 First International Workshop on Usability and Accessibility Focused Requirements Engineering (UsARE)*. IEEE, Zurich, Switzerland, 1–5.

[51] Awanthika R Senarath and Nalin Asanka Gamagedara Arachchilage. 2018. Understanding user privacy expectations: A software developer's perspective. *Telematics and Informatics* 35, 7 (2018), 1845–1862.

[52] Rashmi Sinha. 2003. Persona Development for Information-Rich Domains. In *CHI '03 Extended Abstracts on Human Factors in Computing Systems* (Ft. Lauderdale, Florida, USA) *(CHI EA '03)*. Association for Computing Machinery, New York, NY, USA, 830–831. https://doi.org/10.1145/765891.766017

[53] Daniel Smullen, Yaxing Yao, Yuanyuan Feng, Norman Sadeh, Arthur Edelstein, and Rebecca Weiss. 2021. Managing potentially intrusive practices in the browser: A user-centered perspective. *Proceedings on Privacy Enhancing Technologies* 2021, 4 (2021), 500–527.

[54] Eric Spero and Robert Biddle. 2020. Out of sight, out of mind: UI design and the inhibition of mental models of security. In *New security paradigms workshop 2020*. Association for Computing Machinery, New York, NY, USA, 127–143.

[55] Maarten Van Someren, Yvonne F Barnard, and J Sandberg. 1994. The think aloud method: a practical approach to modelling cognitive. *London: AcademicPress* 11 (1994), 29–41.

[56] Emanuel von Zezschwitz, Serena Chen, and Emily Stark. 2022. " It builds trust with the customers"-Exploring User Perceptions of the Padlock Icon in Browser UI. In *2022 IEEE Security and Privacy Workshops (SPW)*. IEEE, San Francisco, CA, USA, 44–50.

[57] Ben Weinshel, Miranda Wei, Mainack Mondal, Euirim Choi, Shawn Shan, Claire Dolin, Michelle L Mazurek, and Blase Ur. 2019. Oh, the places you've been! User reactions to longitudinal transparency about third-party web tracking and inferencing. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. Association for Computing Machinery, New York, NY, USA, 149–166.

[58] Tingmin Wu, Rongjunchen Zhang, Wanlun Ma, Sheng Wen, Xin Xia, Cecile Paris, Surya Nepal, and Yang Xiang. 2020. What risk? I don't understand. An Empirical Study on Users' Understanding of the Terms Used in Security Texts. In *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*. Association for Computing Machinery, New York, NY, USA, 248–262.

A WORKSHOPS

A.1 Workshop Participants

Information on the date, Gender, Age and Background of the 15 workshop participants.

Date	Gender	Age	Field of Study
	m	20-24	Computer Science M.Sc.
15.07.2022	m	25-29	Computer Science M.Sc.
10:30 -	m	20-24	Electrical Engineering M.Sc.
12:00	m	20-24	Computer Science B.Sc.
	m	20-24	Computer Science M.Sc.
	w	20-24	Medicine
28.07.2022	w	20-24	Finance M.Sc.
18:00 -	w	20-24	Psychology B.Sc.
19:19	m	20-24	Psychology B.Sc.
	m	20-24	Computer Science M.Sc.
	w	20-24	Computer Science M.Sc.
10.08.2022	m	20-24	Computer Science M.Sc.
10:30 -	m	20-24	Electrical Engineering B.Sc.
11:39	m	20-24	Business Informatics M.Sc.
	m	20-24	Computational Engineering M.Sc.

Table 6: Overview of the workshop participants

A.2 Workshop Instructions

Introduction. In this workshop, elements of a graphical user interface for script tracking will be developed. Script tracking is the tracking of the user across multiple websites using scripts. The elements of the interface should look different for different user groups in order to adapt to their needs and wishes. The user groups should be developed based on the privacy competence and privacy concern. *The topics privacy competence and privacy concern were defined by showing the questionnaires used to evaluate those (cf. Appendix C).*

Work Phase. During the work phase, the participants work out the advantages and disadvantages of the existing applications for individual user groups and can also develop new UI elements. The results are structured according to the user groups found and recorded on a white board for all to see, so that the results can be refined in an ongoing process and used as a basis for further element ideas.

B ANTI-TRACKING APPLICATIONS

This section provides an overview of common UI solutions for visualizing script tracking and other tracking elements in a web browser.

B.1 Ghostery

Ghostery displays the number of tracking-related requests in its extension bar icon. Clicking on the icon reveals various categories of identified trackers, along with statistics such as the number of blocked trackers, changed requests, and site loading time. In the extended view, users can see categorized requests and their status (blocked or unblocked), and have the option to individually block or unblock requests.

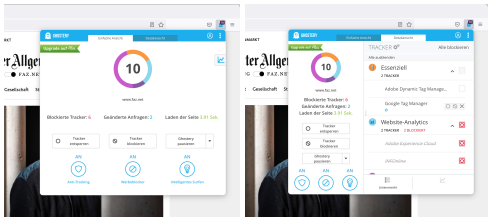

Figure 3: Ghostery Simple View (left), Extended View (right)

B.2 Disconnect

Disconnect categorizes and displays tracking-related requests, specifying the number of trackers from Facebook, Google, and Twitter. The normal view highlights faster website loading and saved bandwidth. Users can block or unblock individual or all trackers in each category. Disconnect also provides a visual graph of trackers and their sources, with highlighted visited websites.

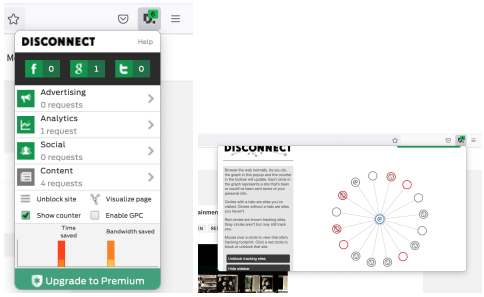

Figure 4: Disconnect Normal View (left), Graph View (right)

B.3 DuckDuckGo Privacy Essentials

DuckDuckGo Privacy Essentials provides a privacy score for each website, indicating its trustworthiness. The score increases with encrypted connections, fewer trackers, minimal tracking networks, and known privacy policies. The extension also showcases the score improvement achieved by blocking specific trackers or enforcing encryption.

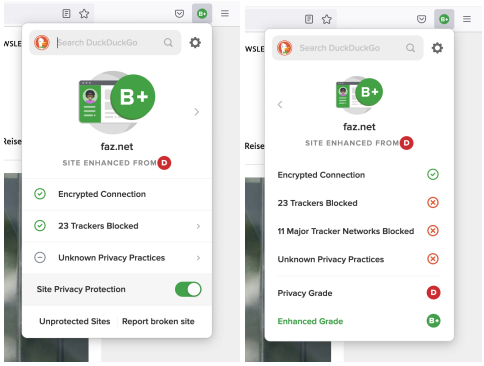

Figure 5: DuckDuckGo Privacy Essentials

B.4 NoScript

NoScript is a default script-blocking extension. While it may impact the initial functionality of visited websites, users can manually identify and unblock necessary scripts for proper operation.

Figure 6: NoScript

B.5 uMatrix

uMatrix assesses a website's elements and organizes them in a matrix. Rows display the domains from which building blocks are loaded, while columns specify the type of content (e.g., picture, cookie, or script). The user can observe blocked sources and identify websites deemed irrelevant as script sources for the website's functionality.

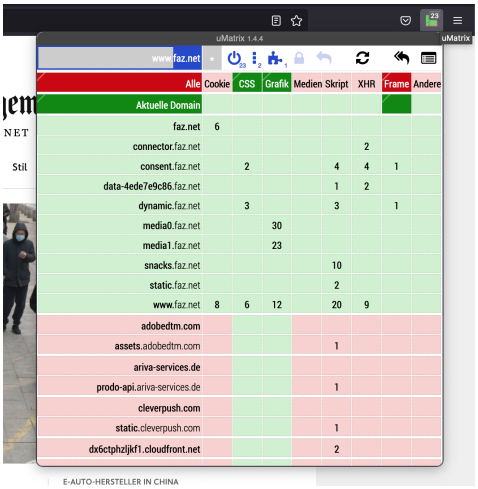

Figure 7: uMatrix

C QUESTIONNAIRES

C.1 OPLIS Questionnaire

In the following, the questions and answers of the OPLIS questionnaire by Masur et al. [36] are presented. The correct answers are written in bold.

(1) The National Security Agency (NSA) accesses only public user data, which are visible for anyone. (true / **false** / do not know)
(2) Social network site operators (e.g. Facebook) also collect and process information about non-users of the social network site. (**true** / false / do not know)
(3) User data that are collected by social network site operators (e.g. Facebook) are deleted after five years. (true / **false** / do not know)

(4) Companies combine users' data traces collected from different websites to create user profiles (**true** / false / do not know)
(5) E-mails are commonly passed over several computers before they reach the actual receiver. (**true** / false / do not know)
(6) What does the term 'browsing history' stand for? In the browsing history ...
  (a) **... the URLs of visited websites are stored.**
  (b) ... cookies from visited websites are stored.
  (c) ... potentially infected websites are stored separately.
  (d) ... different information about the user are stored, depending on the browser type.
(7) What is a 'cookie'?
  (a) **A text file that enables websites to recognize a user when revisiting.**
  (b) A program to disable data collection from online operators.
  (c) A computer virus that can be transferred after connecting to a website.
  (d) A browser plugin that ensures safe online surfing.
(8) What does the term 'cache' mean?
  (a) **A buffer memory that accelerates surfing on the Internet.**
  (b) A program that specifically collects information about an Internet user and passes them on to third parties.
  (c) A program, that copies data on an external hard drive to protect against data theft.
  (d) A browser plugin that encrypts data transfer when surfing online.
(9) What is a 'Trojan'? A Trojan is a computer program, that ...
  (a) **... is disguised as a useful application, but fulfills another function in the background**
  (b) ... protects a computer from viruses and other malware
  (c) ... was developed for fun an d has no specific function.
  (d) ... caused damage as computer virus in the 90ies but doesn't exist anymore.
(10) What is a 'firewall'?
  (a) **A fallback system that will protect the computer from unwanted web attacks.**
  (b) An outdated protection program against computer viruses.
  (c) A browser plugin that ensures safe online surfing.
  (d) A new technical development that prevents data loss in case of a short circuit.
(11) Forwarding anonymous user data for the purpose of market research is legal in the European Union. (**true** / false / do not know)
(12) The EU-Directive on data protection ...
  (a) **... has to be implemented into national data protection acts by every member state.**
  (b) ... does not exist yet.
  (c) ... functions as a transnational EU-data protection act.
  (d) ... solely serves as a non-committal guideline for the data protection acts of the member states.
(13) In Germany the same standard general terms & conditions (GTC) applies for all social networking sites (SNS). Any deviations have to be indicated. (true / **false** / do not know)
(14) According to German law, users of online applications that collect and process personal data have the right to inspect which information about them is stored. (**true** / false / do not know)
(15) Informational self-determination is ...
  (a) **... a fundamental right of German citizens.**
  (b) ... a philosophical term.
  (c) ... the central claim of data processors.
  (d) ... the central task of the German Federal Data Protection Commissioner.
(16) Tracking of one's own internet is made more difficult if one deletes browser information (e.g. cookies, cache, browser history) regularly. (**true** / false / do not know)
(17) Surfing in the private browsing mode can prevent the reconstruction of your surfing behavior, because no browser information is stored. (**true** / false / do not know)
(18) Using false names or pseudonyms can make it difficult to identify someone on the Internet. (**true** / false / do not know)
(19) Even though It-experts can crack difficult passwords, it is more sensible to use a combination of letters, numbers and signs as passwords than words, names or simple combinations of numbers. (**true** / false / do not know)
(20) In order to prevent the access to personal data, one should use various passwords and user names for different online applications and change them frequently. (**true** / false / do not know)

C.2 IUIPC-8 Questionnaire

In the following, the questions of the IUIPC-8 questionnaire are presented. The questionnaire is taken from Groß [22]. The questions are answered using a 7-point Likert scale, anchored on 1='Strongly Disagree' to 7='Strongly Agree'.

(1) Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.
(2) Consumer control of personal information lies at the heart of consumer privacy.
(3) Companies seeking information online should disclose the way the data are collected, processed, and used.
(4) A good consumer online privacy policy should have a clear and conspicuous disclosure.
(5) It usually bothers me when online companies ask me for personal information.
(6) When online companies ask me for personal information, I sometimes think twice before providing it.
(7) It bothers me to give personal information to so many online companies.
(8) I'm concerned that online companies are collecting too much personal information about me.

C.3 User Experience Questionnaire

In the User Experience Questionnaire from Laugwitz et al. [30], the user has to decide between two adjectives on a 7-point scale, which adjective correlates best with the own user experience. The adjectives are:

- Unlikable - Pleasing
- Unattractive - Attractive
- Unpleasant - Pleasant

- Unfriendly - Friendly
- Annoying - Enjoyable
- Bad - Good
- Confusing - Clear
- Difficult to learn - Easy to learn
- Complicated - Easy
- Not understandable - Understandable
- Usual - Leading edge
- Dull - Creative
- Conservative - Innovative
- Conventional - Inventive
- Demotivating - Motivating
- Boring - Exiting
- Inferior - Valuable
- Not interesting - Interesting
- Obstructive - Supportive
- Does not meet expectations - Meets expectations
- Unpredictable - Predictable
- Not secure - Secure
- Inefficient - Efficient
- Slow - Fast
- Cluttered - Organized
- Impractical - Practical

D UEQ RESULTS AND MANN-WHITNEY-U-TEST

In the following, you will find the results of each UEQ item (Attractiveness, Perspicuity, Novelty, Stimulation, Dependability and Efficiency).

ID	Group	Attractiveness	Ranks Group 1	Ranks Group 2
5	1	42	1.5	
20	2	42		1.5
18	2	41		3.5
28	2	41		3.5
7	1	40	5	
11	2	39		6.5
23	2	39		6.5
17	2	36		8
24	2	35		9
8	2	34		12.5
13	2	34		12.5
14	1	34	12.5	
15	1	34	12.5	
27	2	34		12.5
29	2	34		12.5
3	2	33		17.5
4	1	33	17.5	
16	1	33	17.5	
26	2	33		17.5
1	1	32	21.5	
6	2	32		21.5
10	2	32		21.5
12	2	32		21.5
2	1	30	25.5	
19	1	30	25.5	
22	2	30		25.5
31	2	30		25.5
21	2	29		28
9	1	28	29	
25	2	24		30
30	2	21		31
Rank sum			168	328

Table 7: Results from the UEQ-Attractiveness item

ID	Group	Perspicuity	Ranks Group 1	Ranks Group 2
7	1	28	3	
18	2	28		3
20	2	28		3
22	2	28		3
28	2	28		3
8	2	27		7
16	1	27	7	
19	1	27	7	
5	1	26	9.5	
12	2	26		9.5
1	1	25	12.5	
13	2	25		12.5
14	1	25	12.5	
15	1	25	12.5	
3	2	24		17
6	2	24		17
9	1	24	17	
26	2	24		17
29	2	24		17
2	1	23	21.5	
4	1	23	21.5	
11	2	23		21.5
21	2	23		21.5
17	2	22		25
23	2	22		25
24	2	22		25
27	2	21		27
31	2	19		28
10	2	18		29
25	2	16		30
30	2	13		31
Rank sum			124	372

Table 8: Results from the UEQ-Perspicuity item

ID	Group	Novelty	Ranks Group 1	Ranks Group 2
20	2	28		1
23	2	25		2.5
28	2	25		2.5
4	1	24	4.5	
8	2	24		4.5
5	1	23	7	
6	2	23		7
16	1	23	7	
7	1	22	10.5	
14	1	22	10.5	
18	2	22		10.5
22	2	22		10.5
10	2	21		13.5
19	1	21	13.5	
1	1	20	16	
9	1	20	16	
31	2	20		16
13	2	19		18.5
27	2	19		18.5
11	2	17		20.5
21	2	17		20.5
2	1	16	23.5	
25	2	16		23.5
26	2	16		23.5
29	2	16		23.5
3	2	14		27
15	1	14	27	
30	2	14		27
17	2	13		29.5
24	2	13		29.5
12	2	12		31
Rank sum			135.5	360.5

Table 9: Results from the UEQ-Novelty item

ID	Group	Stimulation	Ranks Group 1	Ranks Group 2
11	2	28		2.5
14	1	28	2.5	
18	2	28		2.5
20	2	28		2.5
7	1	27	5.5	
28	2	27		5.5
6	2	26		7
5	1	25	8.5	
27	2	25		8.5
16	1	24	10	
2	1	23	13.5	
4	1	23	13.5	
13	2	23		13.5
17	2	23		13.5
22	2	23		13.5
31	2	23		13.5
1	1	22	19.5	
3	2	22		19.5
8	2	22		19.5
15	1	22	19.5	
23	2	22		19.5
24	2	22		19.5
10	2	21		24
19	1	21	24	
29	2	21		24
9	1	20	26	
21	2	18		27
25	2	16		28.5
26	2	16		28.5
30	2	15		30
12	2	14		31
Rank sum			142.5	353.5

Table 10: Results from the UEQ-Stimulation item

ID	Group	Dependability	Ranks Group 1	Ranks Group 2
2	1	27	3.5	
5	1	27	3.5	
7	1	27	3.5	
15	1	27	3.5	
18	2	27		3.5
28	2	27		3.5
6	2	26		7.5
11	2	26		7.5
1	1	25	10.5	
16	1	25	10.5	
22	2	25		10.5
31	2	25		10.5
3	2	24		15
4	1	24	15	
14	1	24	15	
23	2	24		15
24	2	24		15
9	1	23	19.5	
10	2	23		19.5
12	2	23		19.5
19	1	23	19.5	
8	2	22		23
13	2	22		23
20	2	22		23
17	2	21		25
26	2	20		26
21	2	19		27.5
29	2	19		27.5
27	2	18		29
25	2	16		30
30	2	15		31
Rank sum			104	392

Table 11: Results from the UEQ-Dependability item

ID	Group	Efficiency	Ranks Group 1	Ranks Group 2
11	2	28		3
15	1	28	3	
18	2	28		3
20	2	28		3
22	2	28		3
5	1	27	8	
6	2	27		8
7	1	27	8	
16	1	27	8	
28	2	27		8
1	1	26	12	
3	2	26		12
14	1	26	12	
4	1	25	16	
17	2	25		16
23	2	25		16
24	2	25		16
26	2	25		16
8	2	24		20.5
9	1	24	20.5	
12	2	24		20.5
31	2	24		20.5
2	1	23	23.5	
10	2	23		23.5
13	2	22		25
19	1	21	27	
21	2	21		27
29	2	21		27
30	2	17		29
25	2	16		30.5
27	2	16		30.5
Rank sum			138	331

Table 12: Results from the UEQ-Efficiency item