How Website Owners Face Privacy Issues: Thematic Analysis of Responses from a Covert Notification Study Reveals Diverse Circumstances and Challenges

Alina Stöver
TU Darmstadt
Darmstadt, Germany
alina.stoever@tu-darmstadt.de

Nina Gerber
TU Darmstadt
Darmstadt, Germany

Henning Pridöhl
University of Bamberg
Bamberg, Germany

Max Maass
iteratec GmbH
Germany

Sebastian Bretthauer
University of Frankfurt
Frankfurt, Germany

Indra Spiecker gen. Döhmann
University of Frankfurt
Frankfurt, Germany

Matthias Hollick
TU Darmstadt
Darmstadt, Germany

Dominik Herrmann
University of Bamberg
Bamberg, Germany

ABSTRACT

Many websites contain services from third parties. Misconfigurations of these services can lead to missing compliance with legal obligations and privacy risks for website users. Previous research indicates that one cause for such privacy issues is missing awareness. However, reasons for the missing awareness and other reasons for the prevalence of privacy issues are not widely researched; that includes website owners' dealing with those issues. To shed light on the issue, we analyze 1043 responses from website owners to a notification about a privacy issue on their website using thematic analysis, following an exploratory and qualitative approach. Our analysis shows that, next to unawareness of the issue, incorrect technical implementation and ambiguous responsibilities are among the reasons for privacy issues. Also, website owners face different challenges, such as a lack of knowledge or slow organizational coordination and processes. In addition, our results show that the circumstances in which they operate their website influences how they act and what challenges they face. To illustrate these differences in website owners, we derive three personas from our thematic analysis: (1) the Ignorant Hobbyist, (2) the Busy Self-Employed, and (3) the Informed Multi-Stakeholder. These personas cover the majority of the aspects of the analyzed responses and represent the diversity of website owners and their backgrounds. Given the challenges and backgrounds of website owners, we discuss which prerequisites must be fulfilled to remediate privacy issues on websites. Finally, we present measures that support website owners in remediating privacy issues and show how to adapt these measures to the needs of different website owners. We hope that better support for website owners will also lead to better privacy for website visitors.

Proceedings on Privacy Enhancing Technologies 2023(2), 251–264
© 2023 Copyright held by the owner/author(s).
https://doi.org/10.56553/popets-2023-0051

KEYWORDS

Website Owner, Usable Privacy, Compliance, Personas, Thematic Analysis

1 INTRODUCTION

Privacy laws such as the European General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA) are supposed to ensure baseline protection of the privacy of website visitors, who are somewhat ambivalent about online tracking [9, 10, 30]. To be effective, website owners (WOs) must comply with specific requirements when setting up and operating a website. Research has shown that many WOs fail at that task [12, 29, 32, 43]. For example, Maass et al. [26] found that 12.7% of the 1.3 million websites they scanned contained an easy-to-fix privacy issue.

While there is extensive research on why users fail to prevent online tracking [19, 28], little is known about the perspective of WOs on data protection compliance in general and the operation of a privacy-respecting website in particular.

Utz et al. [44] found that WOs often rely on easy-to-use default solutions, whereas website visitor privacy only plays a minor role when deciding to adopt a third-party service. Other studies focused on notifying WOs about privacy or security issues on their website [7, 8, 15, 22, 25, 26, 36, 37, 46, 49]. For example, Maass et al. [26] ran a survey in combination with sending out notifications to inform WOs who used Google Analytics (GA) but had not turned on the IP anonymization (AIP) feature. They found that most of their participants were unaware of the necessity to do so, although this is required according to a ruling [13] of the District Court Dresden (Germany). Many WOs approached Maass et al. [26] needing support to implement this feature – which, in most cases, is as simple as adjusting one line of JavaScript in the site's code.

Prior work, however, falls short in explaining the low awareness of privacy issues among WOs, and what kind of support WOs need to implement mandated privacy protection solutions, such as AIP. A first step might be to understand how the diverse group of WOs is composed in the first place, as WOs can operate websites in very different contexts, e. g., professional or private [44]. Hence, our goal is to (1) explore the circumstances of WOs, (2) identify causes for existing compliance issues, and (3) investigate how WOs try to solve existing issues and what challenges they face in doing so.

We build our analysis on data collected by Maass et al. [26] in 2019. Maass et al. notified more than 4500 German WOs about a privacy compliance violation on their websites. They covertly observed the resulting mitigation attempts to understand the effects of different notification designs. During their study, Maass et al. received 1043 responses from more than 740 senders (41 letter scans, 56 call logs, 946 mails), which they have not analyzed systematically. These responses are an untapped dataset, which may provide insights into WOs' motives, challenges, and solution approaches. We analyzed these responses by conducting a thematic analysis, taking an exploratory approach. Figure 1 gives an overview of our approach and the results.

Besides lack of awareness, we find several other reasons leading to this privacy issue. One often encountered reason is that WOs have implemented AIP incorrectly or incompletely. Another reason is the lack of maintenance of old websites. While some WOs implement AIP on their own, others seek technical or legal support or hand off the task. Many WOs face challenges when trying to implement AIP. While several WOs report that they simply lack the technical understanding to make the code change, others must engage in tedious coordination with various stakeholders involved in their website. Our results also reveal that causes and encountered challenges can heavily depend on the context in which the WOs operate their website.

To better understand the diversity of WOs, we take the results of the thematic analysis as a starting point and derive example WO personas. Personas, as we use them in this paper, are abstract representations of users [35], in this case, the WOs. They are a widely used interaction design technique to help develop products [18, 35]. We derive three personas, which cover most aspects included in the data and reflect the wide range of context and related challenges of WOs: Persona 1, the *ignorant hobbyist*, runs their website to inform about a private interest and often struggles with the technical implementation of AIP. Persona 2, the *busy self-employed*, operates their website to represent a small business. A common challenge for them is the lack of time to deal with privacy issues. Persona 3, the *informed multi-stakeholder*, is involved in website operations as part of their job at a large company. Typical challenges they have to deal with are slow and complex organizational structures.

Finally, we discuss prerequisites for WOs to successfully remediate privacy issues on their websites. These range from the necessary awareness of the privacy issues to the technical ability to solve them. Following, we present measures with details of how these can be adapted for the needs of the three WO personas.

The contribution of this paper is threefold:

- We analyze real-world responses of WOs to a privacy issue on their website following an exploratory approach by using thematic analysis. The results (see Section 4) indicate diverse causes for privacy issues on websites and different approaches to solving these issues, entailing different challenges.
- In Section 5, we elaborate our insights from the thematic analysis for three example personas that cover most of the aspects referred to in our data. The personas represent WOs who operate websites in very different contexts.
- In Section 6, we present prerequisites for successful remediation of privacy issues and give recommendations on how to support WOs in protecting website visitors' privacy, taking into account the needs of different WOs.

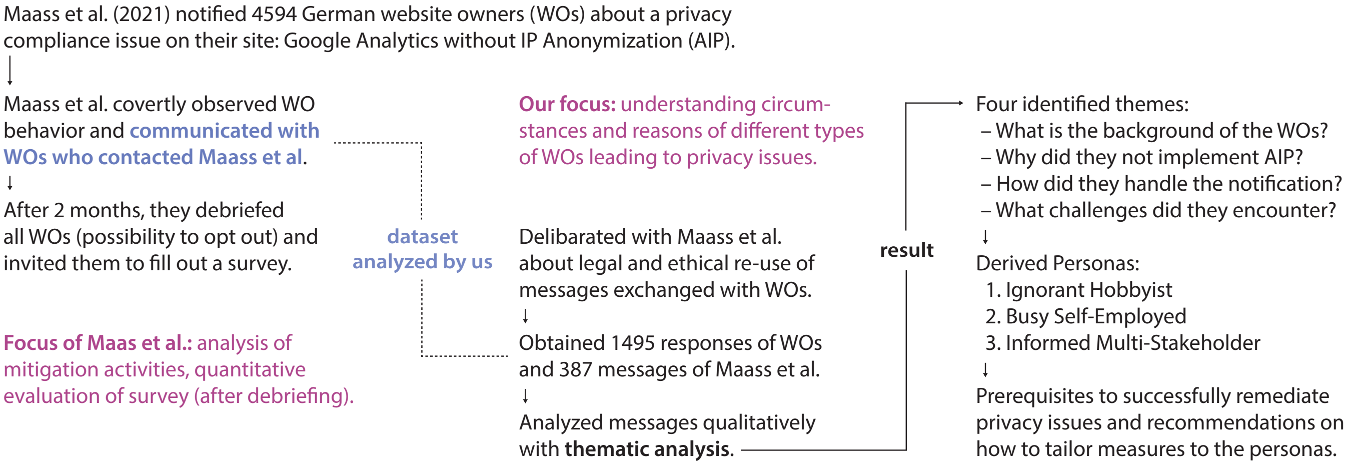
2 RELATED WORK

Our work is related to the recent research efforts that attempt to understand the perspective of *expert users* (see Section 2.1). In Section 2.2, we review relevant work on privacy risks, especially with a focus on website owners (WOs). As WOs we understand those individuals that are responsible for a public website. In contrast to end users, WOs can decide which privacy measures are implemented on their website and thus have a direct impact on the privacy of end users, i. e., their website's visitors. Related work on WOs is reviewed in Section 2.3. We conclude the presentation of related work in Section 2.4 with a description of the study by Maass et al. [26], which provides the basis for this paper.

2.1 Expert Users' Perspective on Privacy

Usable privacy research increasingly addresses not only the perspective of individuals who use systems ("end users") but also those who develop and operate systems ("expert users") [23]. According to Kaur et al. [23], among others, expert users include developers and operators. Like WOs, who are the focus of our study, expert users can influence the privacy of end users of their systems with their decisions and actions. So far, however, there is little literature on WOs and privacy. We, therefore, summarize the perspective of expert users on privacy here. When we discuss our results in Section 6, we will deliberate on the similarities and differences between WOs and expert users.

Previous research on expert users and privacy has dealt with the perspective of developers of mobile apps [3, 4, 31] and other software [20, 34], providing a good overview of their privacy attitudes, factors influencing the implementation of privacy measures, and challenges in the implementation. A main *motivation* for expert users to include privacy in their products is to be compliant with regulations such as GDPR [2] and, in the case of mobile apps, to have them accepted by the app stores [3]. Expert users have to balance the benefits of privacy with functionality but also with the need to monetize their product and the additional costs resulting from the implementation of privacy measures [4]. In some cases, they deliberately restrict the privacy of their users to generate income from their data [31] and do not always find all privacy policies useful [4]. When using third-party services, expert users usually fall back on the market standard and use its default settings [31]. In doing so, they hope to meet the legal standards. Expert users who develop apps rely mainly on the feedback received from the stores for determining whether their apps are sufficiently compliant [3]. In general, it appears that they lack awareness of the privacy practices of their products and the practices of the third-party services used in their products [3, 4, 20]. In addition, they often do not feel responsible for protecting end users' privacy but rather see it as the responsibility of the third-party providers or the end users [31, 34, 40].



Maass et al. (2021) notified 4594 German website owners (WOs) about a privacy compliance issue on their site: Google Analytics without IP Anonymization (AIP).

Maass et al. covertly observed WO behavior and communicated with WOs who contacted Maass et al.

After 2 months, they debriefed all WOs (possibility to opt out) and invited them to fill out a survey.

Focus of Maas et al.: analysis of mitigation activities, quantitative evaluation of survey (after debriefing).

Our focus: understanding circumstances and reasons of different types of WOs leading to privacy issues.

Delibarated with Maass et al. about legal and ethical re-use of messages exchanged with WOs.

Obtained 1495 responses of WOs and 387 messages of Maass et al.

Analyzed messages qualitatively with **thematic analysis.**

Four identified themes:
– What is the background of the WOs?
– Why did they not implement AIP?
– How did they handle the notification?
– What challenges did they encounter?

Derived Personas:
1. Ignorant Hobbyist
2. Busy Self-Employed
3. Informed Multi-Stakeholder

Prerequisites to successfully remediate privacy issues and recommendations on how to tailor measures to the personas.

Figure 1: Contrasting our work from Maass et al. [26]; overview of our approach and main results.

There are several factors that influence the implementation of privacy practices and measures, for instance the personal attitude of developers and their privacy knowledge. Organizational factors also play a role: more mature organizations prioritize privacy practices [34], and well-resourced app developers outsource most compliance decisions to auditing services [3]. Smaller companies are less likely to demonstrate positive privacy behaviors [4] and find it more challenging to be compliant [3]. When integrating third-party services, expert users must deal with privacy information being hidden or incomprehensible [40]. Several researchers [3, 4, 34] highlight a high need for usable tools that help expert users to identify and fix privacy issues and check compliance. Preliminary studies have evaluated support approaches for expert users in practice, e. g., sending notifications to raise awareness for privacy and security issues on their website [7, 8, 15, 22, 25, 26, 36, 37, 46, 49] and providing verification tools [26].

2.2 Considered Privacy Risks on Websites

Many WOs rely on third-party services to implement user analytics, advertising, and consent dialogues. These services entail privacy risks for website visitors [44]. For example, consent management providers have been shown to rely on *dark patterns* to increase users' willingness to agree to user analytics [38, 42, 45]. A popular and frequently deployed solution for user analytics is Google Analytics (GA), a service that has been criticized for tracking browsing behavior across the Web [44]. When GA is misconfigured, WOs can additionally harm the privacy of their visitors [44]. To avoid that Google stores the visitor's IP address along with the analytics data, WOs must enable AIP in GA [17]. However, not all WOs have enabled AIP in the past [26], which was required for legal compliance according to a ruling of District Court Dresden (Germany) [13].

The dataset used in our paper is comprised of responses of WOs that were notified about the fact that they had deployed GA without AIP. Analyzing these responses will shed light on the underlying causes that lead to this and other privacy issues, demonstrate how WOs deal with them, and what challenges they face when deploying privacy measures in general.

2.3 Website Owners' Perspective on Privacy

Although already demanded, little attention has been paid to the perspective of WOs on privacy [1, 16, 23]. Utz et al. [44] scraped email addresses from GitHub repositories and invited individuals involved in creating and maintaining websites to a survey (N=395). For ten common website features, Utz et al. investigated whether privacy was a factor considered when integrating a feature, whether survey participants made special efforts to protect end users' privacy, and to what extent participants were aware of third-party data collection. They found that ease of integration drives third-party adoption; visitor privacy is considered when there are legal requirements or related policies. Awareness of data collection and privacy risks is higher when the collection is directly related to the third-party service's purpose. Most of the survey participants studied by Utz et al. have a technical degree, with a third being involved in the website as part of non-paid work (hobbyist). This observation indicates that WOs differ from other expert users [23] who often develop and operate systems full-time [3].

Another related work on privacy aspects and WOs has been published by Hennig et al [21]. They aimed to understand how websites justify the use of cookie disclaimers that do not meet the legal requirements (e. g., by making it more difficult to reject user analytics than to give consent to it). Different from our research, Hennig et al. contacted the data protection officers of the corresponding websites, receiving only a few responses. The responses indicated that one reason for non-compliant cookie banners might be that websites cannot influence the design of the banners because they are provided by third parties (consent management providers).

Both Utz et al. and Hennig et al. invited individuals to participate in a survey. The dataset used in our research is larger and it was not obtained via a survey. It consists of the responses of WOs that were notified about a privacy compliance issue in a covert notification study (see Section 3.3 for ethical considerations on data collection and re-use).

2.4 Privacy Notification Study by Maass et al.

Our work analyses WOs' responses from a notification study of Maass et al. [26]. We, therefore, describe their study in more detail and differentiate it from our work.

Maass et al. examine determinants for effective notifications regarding privacy issues, i. e., notifications that lead to high remediation rates. For that purpose, Maass et al. scanned websites from Germany for a privacy misconfiguration, namely missing AIP of Google Analytics. Missing AIP was ruled to be in violation of data protection laws by the District Court Dresden (Germany) [13] shortly before the notification study of Maass et al. To notify WOs, Maass et al. extracted contact information from the imprint of a website. The notifications were sent in disguise and varied in three conditions: contact channel (email, letter), sender (private individual, computer science researcher, legal research group), and framing (privacy argument, legal compliance issue, legal compliance issue mentioning potential fines). The notification included a reminder after one month and a final debriefing message containing an invitation to a survey. Maass et al. offered support to WOs and provided a postal and email address as well as a phone number for contact purposes. From these contacts of WOs, Maass et al. obtained a dataset of 1882 documents. Of these, 452 were bounces or auto-replies, while 387 were outgoing messages from Maass et al. The remaining 1043 documents in the dataset were actual responses from WOs used for analysis. These responses divide into 41 letters, 946 emails, and 56 phone call logs.

Maass et al. analyzed the influence of the three conditions on the remediation rates using survival analysis, finding remediating rates from 33.9 % (computer science researcher with privacy argument via email) to 76.3 % (legal research group with legal compliance issue mentioning fines via letter). Regarding the survey, they use quantitative methods to report findings on the matter of awareness, reasons for trust in the message, problem understanding and solving, and helpfulness of support tools. Their analysis of the dataset of WOs' responses is limited to quantitatively stating how many responses were requests for help, confirmation of the messages' authenticity, complaints, or thank-you responses.

In this paper, we analyze the dataset of responses *qualitatively* using thematic analysis and derive personas representing typical WOs. While Maass et al. did not distinguish different kinds of WOs, we stress from our analysis that WOs have deviating needs and should be addressed differently to further improve the effectiveness of notifications.

3 METHOD

In this section, we describe our approach to thematic analysis of the dataset of WO responses by Maass et al. [26] and how we derive personas from the thematic analysis. The dataset, made available to us by Maass et al. in confidentiality, has been described in Section 2.4. Ethical considerations of its re-use follow in Section 3.3.

3.1 Thematic Analysis of Responses

For our data analysis, we chose a qualitative and exploratory approach that allows us to reflect the broad range of themes in our data. We use thematic analysis, the state-of-the-art method for identifying, analyzing, and reporting patterns and themes in qualitative data [6]. We followed the steps suggested by Braun and Clarke [6] using MAXQDA as software [47]. For this, one author familiarized themselves with the data by reading the documents multiple times. That same author then developed a codebook by coding the documents on the sentence level, going back and forth several times. The author then met with a second author to discuss and refine the codebook. Both authors used this codebook to code all documents independently. Following Clarke and Braun's [11] understanding of thematic analysis, we did not calculate inter-rater reliability. To ensure a high quality of the analysis, the authors in the next step came together to discuss ambiguities and agree on a final coding. After this, the authors grouped the data into four themes: (1) Circumstances of WOs, (2) Reasons for lack of AIP, (3) WOs approach to missing AIP, and (4) Challenges in the implementation of AIP (for results on these themes, see Sections 4.1–4.4). The codebook with its themes and categories is presented in Appendix A.

3.2 Derivation of Personas

The thematic analysis revealed that WOs operate websites in different contexts under different circumstances, which can result in specific challenges and needs. To better reflect this diversity, we derived personas from the results of the thematic analysis. To develop our personas, we followed Pruitt and Grudin's approach [35]. In a workshop, the themes and categories of the thematic analysis were noted down on post-its and then clustered by two authors. The clustering aimed to find personas that represent the diversity in the circumstances of WOs and their specific challenges. On the one hand, the personas should be as distinct as possible, and on the other hand, they should cover the range of cases represented in the data as well as possible. Pruitt and Grudin recommend developing three to six personas to keep the number of characters manageable. In our clustering process, we conclude that three personas best reflect the WO represented in our data. These three example personas (see Figure 2) precisely match some of the WOs in our dataset; some WOs in our dataset have only individual aspects of one of the personas. While developing the personas, it was important for us to keep in mind that our database does not represent a complete picture of reality since presumably only specific WOs provide details in their responses. For example, it is reasonable to assume that WOs who work in large companies tend to disclose less information. However, this does not mean that these cases do not exist. To avoid creating a distorted picture through apparent objectivity, we deliberately refrain from quantifying cluster properties in this section.

3.3 Ethical Considerations

As analyzing WO responses involves human subjects, we have followed best practices to assess the ethical acceptability of our research and to minimize the risk for all subjects contributing to the dataset. Our dataset has been collected by Maass et al. [26], who have carefully weighed the harms (effort and stress of contacted persons) and benefits (mitigation of potentially costly compliance violations) of notification. They also elaborated on the legality of the collection of contact addresses from the imprint of the websites. Maass et al. sent the notifications in disguise, without mentioning their study, to avoid observer effects. To address the respect for persons principle of ethical research, Maass et al. sent out an extensive debriefing to all WOs, informing them about the study in writing after its completion. Most importantly, the debriefing explicitly mentioned that the communication may be analyzed for research purposes and that WO responses may be quoted in publications without disclosing the identity of the WO or the person. The authors respected the request of WOs to be removed from the study. Maass et al. received approval from two ethics committees of the three institutions involved. The third institution did not offer a process for ethics approval, but they received approval from the department's dean. In preparation of our research, Maass et al. provided us with their ethics applications and the accompanying documents. In return, we shared our research design and goals with Maass et al. The approved ethics applications mention, among other details relevant to the study of Maass et al., that all WO responses obtained during the study are stored and analyzed. Furthermore, the ethics applications state that the dataset may only be accessed by specific researchers but not released publicly. Together, we concluded that the existing ethics applications cover our planned research. In further discussions, we deliberated the balance of expected benefits (further insights on the reasons for privacy issues on websites and how to address them adequately) and potential harms resulting from us getting access to responses of WOs and messages sent by Maass et al. To minimize the risk of unintended identity disclosure, we refrain from providing background information about individual WOs. Moreover, all responses are carefully quoted only in excerpts so that no conclusions can be drawn about the sender or organization. Finally, we verified that we could access the relevant part of the dataset by Maass et al. without violating any privacy laws.

4 ANALYSIS OF RESPONSES

Thematic analysis of the responses revealed four themes, namely, the circumstances of the WOs, the reasons for the lack of AIP, WOs' approaches to solving the problem, and the challenges encountered by WOs. When analyzing the responses, we assume that Google Analytics can be used legally on German websites when AIP is enabled since this legal opinion was widely believed at the time of the notification study by Maass et al. and confirmed by a German court ruling [13]. We note that today's understanding of the legal situation might be different [33]. In the following we also quote from the responses (R). Note that the numbering here goes up to 1882, because we have adopted the sequential numbering from the original dataset. We deliberately refrain from reporting exact numbers to avoid the impression of generalizability. We only coded the information provided in the responses. Hence, we often lack background information, like in which context a website was created. The information from the responses probably paints a distorted picture of the circumstances of the WOs, since it can be assumed that, e. g., primarily WOs with lower technical skills approached Maass et al. asking for advice. Consequently, our data likely does not reflect the general population of WOs. Instead, our findings represent a first step to gaining insight into the largely unexplored perspective of WOs and need to be validated and extended through further research.

4.1 What Are the Circumstances of the Responding WOs?

First, we want to understand the circumstances of the WOs in the dataset. This information provides the basis for understanding what challenges they face in protecting the privacy of website visitors and what resources they have at their disposal to address them.

Context of Website Owning. Most WOs own their website professionally, either as employees in a larger company or as self-employed individuals. Nevertheless, a considerable number of people write that they own the website in a private context. Reasons for owning a website in a private context include involvement in associations (e. g., in the cultural or sports sector) and informing the general public about a specific concern (e. g., a particular animal). Private WOs are often very motivated to set up and maintain the website but do not necessarily have the necessary technical knowledge. While employees in large companies can usually rely on the support of professionals such as web developers, system administrators, and lawyers, the websites of employees in smaller companies are often managed by third parties, usually due to a lack of time and knowledge. However, better support in larger companies comes with a potential lack of flexibility, as WOs here have to coordinate more frequently with a larger number of people.

WOs who own a website as part of a self-employed activity encounter various difficulties. While they rely on running the website to promote and sell their services or products, they do not necessarily have the technical knowledge. In addition, they have to fit website maintenance into their usually already tight time budgets, where it sometimes takes a back seat to supposedly more pressing tasks.

Involvement of WOs in Development and Maintenance of the Website. Although they have legal responsibility for the website, most participants report not being actively involved in developing and maintaining their website. While private WOs often develop and maintain their website themselves, participants often outsource this for websites they own in a professional context: In the case of employees, usually, the organization has entrusted an external agency with this task. Self-employed WOs, who usually have fewer financial resources, tend to use the free services of IT-savvy people from their private environment, e. g., their grandchildren, for this purpose. However, most WOs who are not involved in the development and maintenance of the website are neither aware of potential privacy issues nor feel responsible for resolving them. Even willing WOs often fail just because they do not know how to make changes to the website. In cases where only the website development has been outsourced or the website has been taken over from a predecessor but WOs now run the website themselves, some of the participants still report not being able to respond adequately to privacy issues because they lack an overview of the website code or are not even able to read the code at all. Several participants also admit that they no longer maintain websites they developed some time ago.

Privacy Motivation of WOs. The importance attached to the privacy protection of their website visitors varies between different WOs. Many WOs respond that privacy is important to them. It is not always apparent whether this is a mere empty phrase, primarily about compliance or the actual protection of visitor privacy. A minority admits to having no interest whatsoever in protecting the privacy of their website visitors, as R1258 states: *"Just leave me alone! It sucks"*. Nevertheless, several WOs are explicitly interested in making their website as privacy-preserving as possible. WOs in the latter group emphasize their intention by reporting that they immediately deleted GA without replacement or replaced it with a more privacy-friendly alternative in response to the notification. These WOs usually report that they have no interest in the user data, e. g., because they own a non-commercial website. For example, R1347 states: *"I never look at who, when, how often was on which page. For my 'business' there is no need at all"*.

4.2 Why Did WOs not Implement AIP Previously?

Next, we focus on why privacy issues arise on websites, as this forms the basis for developing solutions to address these issues.

Incorrect Technical Implementation. Most frequently, participants reported that they had tried to implement AIP but failed in the technical implementation. Individual manual checks of the website code confirm that sometimes incorrect code was indeed imported, e. g., by ignoring upper and lower case or as Response (R) R215 reported *"we discovered that ga (send) was set before ga (anonymizeIp, true)"*. Nevertheless, it remains unclear to what extent some participants cite technical hurdles as excuses for lacking AIP. In some cases, the primary problem was that AIP was not implemented exhaustively, for example, when a website was developed by another person or service provider, and the WO had no overview of the website code.

Lack of Privacy Awareness. Not only WOs who have outsourced the development or maintenance of their website to others are sometimes not aware that there is a privacy violation on their website due to the lack of AIP in GA. Still, especially in cases where the website development was taken over by another entity or was done some time ago, the WOs are not even aware that GA was integrated on their website, and some WOs don't even know what GA is. For example, R245 (phone call) had created the website with their son and did not know Google Analytics at all. However, some participants also unknowingly incorporated GA into their website themselves by using an existing template for website development that included GA. While many participants knew they had included GA on their website, they were unaware that enabling AIP is legally required. Especially WOs who run the website on the side and are not very tech-savvy reported that it was difficult for them to always be up to date on issues concerning the website. On the other hand, some participants were convinced that their website was legally compliant, falsely assuming that they had already set up AIP. Here it usually turns out that the implementation was incomplete or incorrect.

Ambiguous Responsibility. Some WOs were aware that using AIP is required for legal compliance, but not that they as WOs are legally responsible for implementing it. Even after receiving the notification, some participants remained convinced they did not have to act. For example, R198 (phone call) insisted that Google would automatically anonymize the IP addresses of website visitors within the EU. Others referred to the de facto technically responsible persons (e. g., R77: *"The association member who maintains the website is not aware of any fault."*), which is especially problematic in those cases where the person in question is no longer available at all, e. g., R833: *"Unfortunately, I lost my webmaster"*. Still, particularly in larger organizations, it is often unclear who is responsible for technically implementing AIP, e. g., R1368: *"I am in the process of finding out who is responsible for this"*. Some WOs are no longer responsible, e. g., because they are no longer active as association board members but are still listed as such on the website.

Reliance on Other's Judgments. As already pointed out in Section 4.1, many WOs outsource the development or maintenance of their website to others, such as agencies, or rely on templates when setting up their website. In many cases, the WOs expect service providers to be aware of potential privacy issues, even if they were not contracted to maintain the website but only to develop it. When templates have been used for website creation, many WOs tend to assume that they are on the safe side if they simply adopt the default settings. Many WOs seem to lack awareness that they, as owners, are legally responsible for regular website maintenance. Others, however, have had their website explicitly checked for GDPR compliance by a specialist (e. g., the data protection officer), but without the missing AIP being noticed. It remains unclear, however, whether this inspection included a technical examination of the website code by a technically versed person or whether, for example, only the privacy policy was checked for legal correctness.

Deliberate Lack of Maintenance. Even participants who are theoretically aware that they are responsible for the maintenance of the website often justified the lack of AIP to us by saying that the website was not up to date because it was currently being revised, that they were currently working on a new website and therefore no longer maintained the old one, or that website maintenance had been abandoned a long time ago and the website remained only as an artifact on the internet, e. g., R160: *"[The website] is up to date as of 2012"*.

4.3 After Being Notified, How Did WOs Handle the Issue?

Many WOs reported how they addressed the lack of AIP. We identified the following four common approaches.

WOs Implement AIP Themselves. Most participants reported that they implemented AIP themselves after receiving the notification. This fact suggests that the notification provided the awareness or knowledge previously lacking to address the problem. Still, especially participants who do not operate the website within their employment in a larger organization may also (inevitably) refrain from getting professional support for cost reasons, e. g., R1123: *"[...] as relatively small associations [...] we can not afford the appropriate experts for such issues"*. However, this finding should be taken with a grain of salt since we cannot be sure that the participants did not seek help anyway without mentioning this in their response.

WOs Implement AIP With Support. Some participants indicate that they implemented AIP themselves but sought legal or technical support in the process, e. g., to find the appropriate place in the code or to identify bugs in the code. Legal support was usually asked to review whether action is necessary, e. g., R1562: *"We talked to our lawyer and you are right"*. While most participants asked the senders of the notification for technical or legal support, only a few participants indicated that they had asked Google directly for support in implementing AIP, e. g., R863: *"I [. . .] asked Google how to delete an analytics account completely, since there is no information on the internet about this"*.

WOs Delegate Implementation of AIP. Many WOs reported delegating the implementation of AIP. This approach was taken, for example, when the WOs did not feel able or responsible to solve the problem themselves, e. g., because they did not operate the website themselves or because they worked in a larger organization with distributed responsibilities. In a professional context, an internal or external IT expert or the service provider responsible for developing or maintaining the website is often assigned to implement AIP. Likewise, the data protection officer is often called in, and sometimes even a lawyer is commissioned with the implementation, who, *"is responsible for data protection in our organization"*. Participants who own the website in a private context or as part of a self-employed activity are, however, often more likely to pass the task on to technically skilled people from their private environment.

WOs Do Not Implement AIP. Only a few WOs stated that they could not solve the issue due to lack of time or insufficient knowledge, e. g., R1015: *"Unfortunately, it is very complicated to change this and costs me time and money, which is why I did not pursue the matter further"*. However, some of these participants also pointed out directly that they did not see any need to implement the lacking IT anonymization. Probably there are more who don't solve the problem on their current site anymore because they plan, as described in subsection 4.2, to rebuild the site.

4.4 What Challenges Did WOs Encounter?

After receiving the notification, several challenges arose for the WOs who attempted to implement AIP.

Lack of Resources. Especially private and self-employed WOs often do not have the financial and time resources to take care of technical aspects of their website. On the one hand, website maintenance often has to take a back seat to other business tasks in the day-to-day business, especially when private problems come up, such as one WO who reported that her husband had recently passed away. On the other hand, these WOs, in particular, may lack the necessary money to hire a specialist for website maintenance or data protection.

Lack of Technical Knowledge. Many participants report that they lack the basic technical understanding to implement AIP. Overall, many participants even describe themselves as technically unskilled, e. g., R168: *"I am 68 years old, retired and have installed wordpress through a provider [. . .]. I do not understand the javascript and do not know how to embed this"*. In this context, some participants also complained that without technical expertise, it was challenging to stay abreast of and implement new data protection requirements, e. g., R267: *"I am not a professional in websites and the ongoing changes in data protection can only be realized if you deal with it on a daily basis"*.

Problems With the Code. But even WOs who, in principle, have the technical understanding to implement AIP often encounter problems when working with the code. For example, some participants have trouble finding the appropriate code location, while others unsuccessfully try to delete GA completely from their code. Others report getting error messages without being able to identify the specific error, e. g., R71: *"I immediately tried to fix the error, but I could not find it"*.

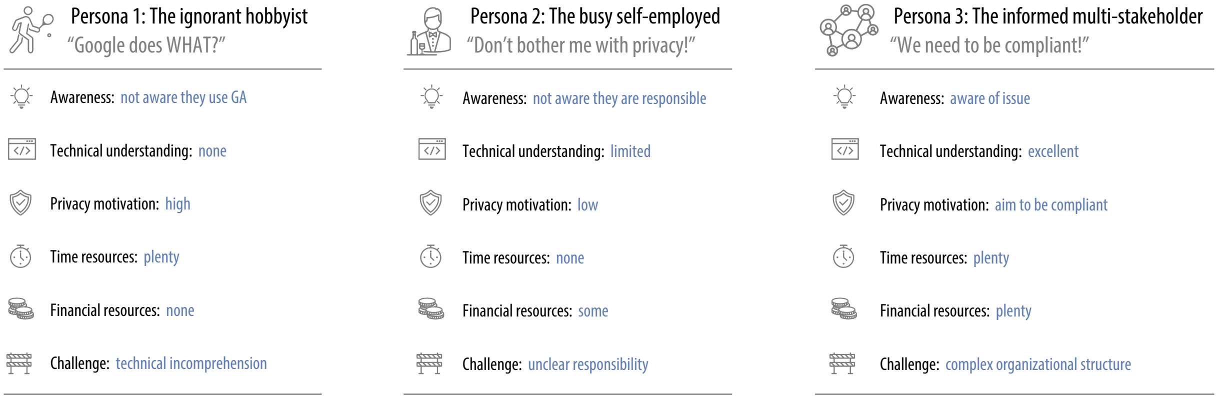
Dependencies and Slow Processes in Organizations. Employees in larger organizations often have both time and financial resources as well as access to internal or external subject matter experts to support them in implementing AIP. However, being part of a larger organizational structure brings other challenges, such as reliance on other employees who may be unavailable due to vacation or parental leave, or even have yet to be found if the position whose responsibilities include website maintenance is currently vacant. Complex organizational structures, in which responsible parties must approve every change at various management levels, can also significantly delay basic adjustments such as abandoning GA or implementing AIP. In this regard, for example, R531 reports: *"When I started my job and took stock of the situation, I actually already identified the problem and passed it on to my management. The matter has also been discussed internally since last week and alternatives are currently being sought in order to develop an appropriate basis for decision-making for the person responsible"*.

5 DERIVED PERSONAS

In Section 4 we presented reasons for privacy issues on websites and revealed challenges WOs face while fixing these issues. The thematic analysis revealed that WOs operate websites in different contexts under different circumstances, which can result in specific challenges and needs. In this section, we elaborate on our insights from Section 4 for three example personas representing different WO types from our data. As we use them in this paper, personas are abstract representations of users [35]. They are a widely used interaction design technique to help develop products [18, 35]. We developed the personas in a workshop – for details, see Section 3 – so that they (1) cover the majority of cases in our data and (2) reflect the wide range of circumstances of WOs and related challenges. The personas can help to understand the challenges of the different WOs. Moreover, they provide a basis for developing support options for WOs that consider their specific needs.

5.1 Persona 1: The Ignorant Hobbyist

Persona 1, the ignorant hobbyists, own their website either out of private interest, e. g., to inform about a particular concern or in the context of their activity in a (smaller) association. They are not technically experienced and have already reached the limits of their technical understanding with the creation of the website, for which they have relied on a template or support from their private environment. Therefore, they usually do not even know that they use GA on their website. Since they do not need the data generated by GA and tend to attach great importance to the privacy protection



Persona 1: The ignorant hobbyist “Google does WHAT?”	Persona 2: The busy self-employed “Don’t bother me with privacy!”	Persona 3: The informed multi-stakeholder “We need to be compliant!”
Awareness: not aware they use GA	Awareness: not aware they are responsible	Awareness: aware of issue
Technical understanding: none	Technical understanding: limited	Technical understanding: excellent
Privacy motivation: high	Privacy motivation: low	Privacy motivation: aim to be compliant
Time resources: plenty	Time resources: none	Time resources: plenty
Financial resources: none	Financial resources: some	Financial resources: plenty
Challenge: technical incomprehension	Challenge: unclear responsibility	Challenge: complex organizational structure

Figure 2: Example personas that represent different types of WOs we identified in our data.

of their website visitors, they are annoyed by the realization that they have (illegally) shared the IP addresses of their website visitors with GA so far and see this as another example of the need to defend themselves against the overpowering data collector Google. They are, therefore, motivated to solve the problem of the lack of AIP immediately, e. g., by completely removing GA from their website.

Although they usually have enough free time to spend on solving the problem, they still usually reach the limits of their technical understanding. They quickly feel overwhelmed with the problem solution since they lack a basic understanding of the code. They usually do not have the financial resources to get professional support; hence, they often fail to implement AIP. While some resort to shutting down their website, usually when it is no longer maintained anyway, others choose to ignore the problem out of helplessness. However, some ignorant hobbyists turned to the senders of the notification for technical support, as they were overwhelmed with the instructions received as part of the notification – and with help, managed to implement AIP or remove GA from their website.

5.2 Persona 2: The Busy Self-Employed

Persona 2, the busy self-employed, are mostly self-employed individuals or persons who own a small local business. They have a limited interest in user metrics and therefore rely on the use of a tracking tool. Yet, they often do not know that they, as the WO, are responsible for implementing AIP and assume that the web design agency with whose help they created the website or even Google itself will already properly implement any legal requirements. The website is usually only a means to an end for them and should take up as little of their already limited time as possible, so they are usually annoyed by having to deal with data protection issues.

They usually have limited financial resources, so they rely to some extent on the help of an agency or a lawyer. However, one initial challenge is deciding who they should contact, as the parties involved do not have a mutual exchange of information, and the lawyer can, for example, provide information on what is required under data protection law, but not on how this can be implemented technically. Some Persona 2 also fail at implementing AIP because they do not even have the access data to edit their website since another person (who is, however, in some cases no longer available) has taken over the website creation for them, without providing them with the access data afterwards. Accordingly, such websites are often not maintained at all. However, many Persona 2 mitigate the issue by (a) implementing AIP, (b) exchanging GA for a more privacy-friendly alternative such as Matomo, (c) delegating the implementation to an agency or a technically-savvy person from their private environment, or (d) relying on the guidance provided as part of the notification, as well as the tool for checking the implementation.

5.3 Persona 3: The Informed Multi-Stakeholder

Persona 3, the informed multi-stakeholders, own the website because of their job in a larger company. GA is deliberately used on the website to track and analyze behavior. Persona 3 are mostly aware that the GDPR requires AIP, which is why most Persona 3, in contrast to Persona 1 and 2, have already implemented this to some extent, but often not comprehensively. In this respect, Persona 3 are less interested in the privacy protection of their website visitors than in complying with the legal requirements to avoid penalties. Persona 3 have extensive financial and human resources, which is why the implementation of AIP is mostly delegated to internal or external service providers. One difficulty in implementation, however, can be that those involved lack an overview of the usually complex website structures and, therefore, forget to implement them in some places.

Furthermore, Persona 3’s organization is usually in a conflict of goals, as it would like to collect extensive user data, which is why it does not want to, e. g., delete GA entirely or replace it with a less sensitive tracking tool. Therefore, the decision on how to solve the problem usually involves various stakeholders within the company, some of whom have very different technical and legal background knowledge, making communication even more difficult. Depending on the organizational structure, the decision passes through several management levels and decision-making bodies, which slows down the process considerably.

A portion of the notifications sent out by Maass et al. [27] included a statement that IP addresses must be pseudonymised or anonymized when collecting the analytics data to conform with data protection laws. These notifications were mostly perceived by

Persona 3 as particularly helpful, as they could cite this statement as an additional argument in internal communications. Although Persona 3 were already aware that AIP was required by law, the externally received notice lent additional weight to this argument. Therefore, most Persona 3 implemented AIP after receiving the notification with the help of internal service providers (e. g., the IT department).

6 DISCUSSION

Following an exploratory approach, we analyzed 1043 real-world responses from WOs who reacted to a notification about missing AIP, a privacy issue on their website. The thematic analysis of the responses revealed four themes, namely, the circumstances of the WOs, the reasons for the lack of AIP, WOs' approaches to solving the problem, and the challenges encountered by WOs. These themes are important because they reveal that WO have a high need for support in order to become compliant. However, the circumstances and needs of WO are so diverse that genuinely effective support must also take them into account. The themes and derived personas show that different needs of different target groups are first and foremost a problem. At the same time, they offer various starting points on how support can be designed and how WOs can be approached to improve compliance rates. In this section, we summarize our findings with reference to related work and show what prerequisites must be met for WOs to fix privacy issues successfully. We also present measures, considering the needs of different personas. Finally, we discuss the possible effects of our dataset choice, the limitations of our work, and ideas for future work.

6.1 Comparison to Related Work

We found that WOs run websites for different interests and under different circumstances. Different circumstances result in specific challenges and support needs for different WOs. To make this diversity tangible, we presented three example personas that cover the majority of cases and reflect the wide range of circumstances of WOs in our data: Persona 1, the ignorant hobbyists, own their website out of private interest, often with high motivation to protect end users' privacy but with little technical skills to implement respective measures. Persona 2, the busy self-employed, often own the website to represent their small business online, have very little time to devote to the website, and often have limited interest in user data. Persona 3, the informed multi-stakeholders, own the website as part of a job at a larger company where they rely on user data and often need to involve many other stakeholders in decisions concerning the website.

Usable privacy research already includes privacy persona approaches [5, 14, 24, 48]. However, these differ from our approach in two respects. On the one hand, existing concepts are not concerned with the abstract representation of users but rather with the classification of users, e. g., according to their privacy concerns, as by Westin [24, 48]. Furthermore, existing approaches focus on end users and their privacy motivation, knowledge, or concerns [5, 14, 24, 48]. However, end users differ from WOs, who are responsible for privacy measures deployed on a website. WOs also influence the design of systems. Issues such as compliance and lack of website maintenance are of interest to them. While our three WO personas are challenging to compare to end-user personas, we do find some overlap with aspects identified in previous research on expert users and WOs. For instance, Utz et al. [44] showed that around a third of individuals involved in running websites do so as non-paid work as "hobbyists", like our Persona 1. Similar to our Persona 2, previous studies [3, 4] found that app developers in smaller companies struggle particularly with implementing privacy measures.

Overall, we find that a common reason for the lack of AIP is that WOs lack awareness of privacy issues. This finding is in line with related work that showed that developers are often unaware of the data practices of third-party services that they integrate into their products [3, 4, 20]. Our data reveal that for WOs the problem is even more profound: especially Persona 1 and 2 are not only unaware of the lack of AIP but sometimes do not even know what GA is or that they have implemented GA on their website. AIP is also often implemented incorrectly, which can often be fixed with minimal changes to the code. This finding indicates that WOs, in contrast to other expert users, sometimes lack the technical understanding of website code. Unlike other expert users, many WOs (especially Persona 1 and 2) are neither interested in nor need user data. Many WOs do not pursue economic interests with their website but use it for private interests or to present their small businesses, unlike developers who often aim for immediate monetization of their apps directly [31]. Another reason for the lack of AIP is that websites are no longer actively maintained. This aspect has not yet been mentioned in other contexts but may become more relevant in the future, especially with the constantly increasing number of mobile apps. Similar to results obtained for expert users, we observe that lacking AIP also occurs because WOs are unaware of their responsibility – or they see it with third-party providers or end users [31, 34, 40]. Similar to results obtained for developers, many WOs rely on other entities, such as web design agencies or privacy officers, when it comes to privacy issues [31].

Our analysis also reveals that some WOs resolve privacy issues themselves, while others seek technical and legal support. This observation indicates a strong need for WO support on privacy issues. This support, similar to what has already been called for in previous publications [3, 4, 34], should primarily address Personas 1 and 2, who have little money and time for privacy measures. When support options are designed, the different needs of WOs should be considered.

A major challenge, especially for Persona 1 and 2, is the lack of resources, which is in line with the findings of Balebako et al. [4] who show that the presence of resources greatly influences whether privacy measures are implemented and that resources are especially lacking in small companies. In addition, Personas 1 and 2 have to deal with a general lack of technical knowledge. This situation is an important difference between our study and the study by Utz et al. [44], where most respondents had a technical background.

Regardless of specific challenges, several basic prerequisites must be met for WOs to address the privacy issue eventually. We present these in the following section.

6.2 Prerequisites to Remedy Privacy Issues

Our results indicate that six prerequisites must be met for all WOs to implement AIP. Figure 3 provides an overview.

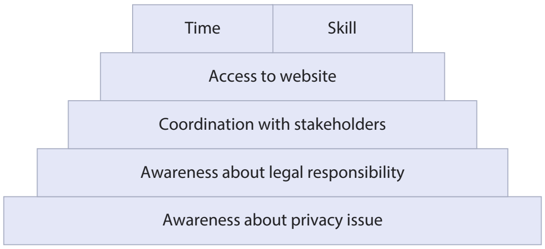

Time
Skill
Access to website
Coordination with stakeholders
Awareness about legal responsibility
Awareness about privacy issue

Figure 3: Prerequisites for WOs to remedy privacy issues on their websites.

Awareness of Privacy Issue. First, WOs must be aware that their website bears a privacy risk for their visitors. Therefore, WOs need to know which third-party services are included on their site, which data they collect, and which privacy risks are associated with them. For our use case, this means that WOs must be aware that GA is integrated on their website and that AIP is necessary.

Awareness of Legal Responsibility. WOs need to be aware that, as website owners, they are legally responsible for implementing data protection measures on their websites – even if they are not responsible for the technical implementation because, e. g., an IT person or web design agency is in charge. In our case, all websites fall under the GDPR, which requires WOs to implement data protection measures.

Coordination with Stakeholders. In larger organizations, many stakeholders are often directly or indirectly involved in decisions relating to the organization's website. Accordingly, they must also agree that there is indeed a privacy issue and that or how it must be resolved. In our use case, the necessity for action follows from data protection laws and was confirmed by the LG Dresden ruling [13]. Nevertheless, all stakeholders must understand this legal situation and prioritize the issue. Previous research has shown that the general privacy culture in companies influences the implementation of privacy measures [34]. A privacy-respecting culture could also help prioritize the issue among decision-makers. One approach here can be the employment of so-called privacy champions – people who strongly care about promoting privacy [39].

Access to Website. To make changes to their website's code, WOs need access to that. This prerequisite becomes an issue if a website was set up long ago and access has been lost, or the individuals who maintained the website are not available (e. g., webmaster is on vacation). In our use case, some WOs found that they also need credentials for their GA account to fix the privacy issue. Another issue arises if AIP was incorrectly implemented in third-party service that the WO had included on their website (e. g., a contact form). In this case, WOs are still legally responsible but cannot act because they lack the necessary access to the third-party systems.

Time. WOs need time to deal with the privacy issue and solve it or look for alternatives. In our use case, most of the time, the effort for the necessary code changes to enable AIP is small and should take little time. However, this adjustment can be time-consuming for WOs with little technical knowledge (Persona 1) or who must communicate with different stakeholders (Persona 2). It is, therefore, essential to unburden WOs with little time. Following a privacy-by-design approach, agencies or template providers could, for instance, implement privacy-friendly alternatives (e. g., Matomo) by default.

Technical Skills. WOs need technical skills to address privacy issues, or they must be able to purchase them. This prerequisite is a notable difference compared to other expert users like developers, who often have the technical know-how. Many WOs, however, lack technical skills, especially if the website is only a means to an end, e. g., to represent a small company on the internet but not the core business of WOs. For our use case, this means that WOs need to know where exactly in the code to implement AIP or how to remove GA from their website altogether. Especially if WOs have not built their website themselves, it can be challenging to identify the correct positions in the code.

6.3 Measures for Different WO Personas

According to our dataset, WOs operate in different circumstances and face diverse challenges when solving privacy issues. We have captured these in the form of three example personas (see Section 5). The prerequisites to be able to solve privacy issues are not equally met by all WOs. To help WOs become compliant, we propose several measures. We build on measures already proposed in the literature for expert users, such as developers. For example, Maass et al. [27] present an automated website scanning portal that allows to benchmark security and privacy features of websites. Tahaei et al. [41] propose the creation of multimedia materials for privacy that supports app developers. A number of studies have already looked at how to notify developers, admins and WOs about privacy and security issues [7, 8, 15, 25, 26, 36, 37, 46, 49]. However, with our findings in mind, it is essential to adapt these measures to the circumstances of different WO personas. Tailoring the measures to the different circumstances and challenges increases the likelihood that the measure will be effective and not, at worst, counterproductive. For example, notifications informing WOs about a privacy issue on their website may have different content. While mentioning a potential penalty in a notification can serve as a good argument for action in larger companies, it may trigger fear and possibly reactance in a hobbyist. In Table 1, we present several potential measures and show how they can be adapted for different WO personas, taking our findings into account.

6.4 Possible Effects of Dataset Choice

Our dataset consists of real-world responses from WOs related to a specific problem (missing AIP). The choice of the dataset allows for completely new insight, at the same time it might have impacted the themes uncovered in the thematic analysis. We will discuss this possible influence in the following subsection.

Our dataset refers to a certain use case, hence, at least some of our themes are likely to have a specific focus. Because of that, the set of themes might not be exhaustive: E. g., for other use cases,

Table 1: Measures to support WOs to address privacy issues on websites.

			Considerations for tailoring measures to needs of different Personas		
Prerequisites addressed	**Measure**	**Description**	**Persona 1: Ignorant Hobbyist**	**Persona 2: Busy Self Employed**	**Persona 3: Informed Multi-Stakeholder**
Awareness about privacy issue	Information campaigns	Inform WOs about current privacy issues on websites that are revelant for them.	Raise awareness that website privacy risks may exist; remind that websites that are no longer needed or that are not maintained should be taken offline; find suitable channels, e.g., print media, online media, NGOs, national data protection authorities.	Create awareness of responsibility, e.g., in the form of newsletters that inform when WOs need to act. Create a central point of contact (e.g., website) that contains all relevant information on the topic of privacy for websites.	Create awareness among decision makers in a company, e.g., through dedicated business media.
Awareness about legal responsibility	Notifications	Notify WOs about privacy issue on their website.	Should create awareness that there is a website that has privacy issues – which is a risk. Refrain from mentioning penalties to avoid stress.	Should make WO's responsibility clear, but refrain from naming penalties if necessary to avoid reactance.	Can refer to legal consequences including possible penalties of the issue to increase prioritization among decision makers.
Awareness about privacy issue	Self-check tools	Allow WOs to check their site for specific privacy issues.	Should concretely show the privacy issue and explain its consequences.	Should particularly focus on aspects relevant to the WO, e.g., risks of non-compliance.	Could be offered as paid service that offers comprehensive compliance checks of sites.
Skill	Training	Convey knowledge on legal and technical privacy aspects.	Must be inexpensive, e.g., in the form of videos or podcasts available online; easily understandable for technical laypersons.	Should be as little extra work as possible and could therefore be included in other trainings for self-employed or small businesses.	Can address different stakeholders, e.g., training privacy champions to strengthen the privacy culture in the company.
Awareness about privacy issue, Skill, Time	Checklists/ Guidelines	Provide checklists (what has to be considered) and guidelines (how to address it).	Should be rich in detail and easy to understand for people with little technical knowledge.	Should be concise and easy to read for people with little time.	Can use technical terms and should address special cases relevant for larger and more complex websites.

additional challenges could arise, such as lacking technical solutions, e. g., there might be no privacy-preserving templates for cookie banners [42] or additional costs of anonymization, e. g., if the data captured by the privacy-infringing solution is more valuable for the WO than in our use case.

It is possible that participants only responded and explained themselves at all because they did not initially know what the actual intention of the notification from Maass et al. [26] was, i.e., data collection for a scientific study, and possibly hoped to avoid legal consequences by explaining themselves or shifting responsibility to others, e. g., an external service provider. Thus, because of the legal or official framing of the notifications, it might be that more WOs delegated the implementation of IP anonymization than in a setting in which more informal notifications would have been sent. In this case, perhaps more WOs would have ignored or delayed a response to the issue.

Our dataset includes somewhat more responses from WOs who were notified by letter than by email in Maass et al.s' study. The number of responses also varies across the different arguments that Maass et al. had made. WO, who were informed that the issue on their website meant a compliance violation that may result in a penalty charge, reported back most frequently. Hence, in the dataset that served as the basis for our thematic analysis, responses from WOs that had received a potentially scary notification with special weighting (by the letter medium) are overrepresented. Because of the legal component, WOs might have turned more frequently to their legal department or lawyer for support, while with a different, e. g., more technical, focus, perhaps more WOs would have asked their IT department or admin to solve the issue. Thus, the different notifications in the study of Maass et al. may indeed trigger different responses from the WOs.

However, they also opened up a much wider possibility space for responses than focusing on a single type of notification, e. g., email without legal arguments. The data set thus provides a good basis for a qualitative exploratory analysis such as the one we undertook. We further assume that the different notifications could also reach such WOs that were not involved in previous studies. For example, the Busy-Self-employed WO would not have taken the time to participate in a survey or responded to a rather non-officially looking notification.

Last but not least, there could have been other or more personas that we did not discover because the corresponding WOs did not contact us, e. g., professionals who did not have the issue on their website or were able to solve it quickly themselves.

6.5 Limitations

Our work has several limitations related to the chosen use case, data collection, and the resulting dataset. *Use case:* The use case that served as a basis for this paper clearly required action by WOs to be compliant at the time of the Maass et al. notification. Not all privacy-issues on websites have such a clear legal basis, as this can change due to changes in the law or new court rulings. Thus, challenges that WOs face in other cases may vary, as may their motivations to design privacy-preserving websites. *Data collection:* The data basis of our study are responses sent by WOs in a notification study. It is important to keep in mind that Maass et al. varied the notification content and medium. These different conditions may have triggered different response behavior in the WOs. We discussed this issue in more detail in the previous subsection. *Sample:* Our dataset only includes responses from WOs in Germany that have implemented GA without AIP on their website. Thus, the results are not representative for all WOs but should be seen as an exploratory possibility space. Our sample may be biased by self-selection, because only WOs with a concern have contacted Maass et al. This can lead to WOs who have a problem being overrepresented in the sample. At the same time, however, this focus fits our research question and gives a realistic view of the actual problems of WOs. It is quite possible that WOs, whose websites are not covered by GDPR, have a different motivation to become privacy compliant. It is also possible that their awareness, knowledge and support options, e. g., through data protection officers, differ from our sample. Nevertheless, we believe our results can serve as a starting point for further systematic research, e. g., surveys with a representative sample of WOs. *Data analysis:* Our qualitative analysis allows to understand the different themes uncovered in depth. However, quantification, e. g., how many people belong to one persona, or statistical analysis about, e. g., correlations, are not possible.

6.6 Future Work

Our work has a strong exploratory character. From the findings, several questions arise for further exciting investigations. *Verification of WO characteristics:* Our results indicate that WOs are a very diverse group, which we exemplify in three personas. Further studies, e. g., surveys or interviews, need to verify these initial findings. *Investigation of underlying psychological constructs:* In our data, we have found evidence that psychological constructs, such as different expressed motivations of WOs, are also a factor influencing privacy implementation. Investigating these and other underlying constructs, e. g., WOs' self-efficacy expectations, may help to better understand and support WOs. *Development and evaluation of support solutions:* We provide recommendations for a range of measures that address the needs of different WO personas. While the effectiveness of some measures, such as notifications, has already been proven by studies [26], the adaptation of the measures for the needs of different WO personas and a corresponding evaluation of the effectiveness is still missing. *Investigation of further use cases:* This paper focused on a particular use case (missing AIP) where WOs had to take action for legal compliance. It would be interesting to learn the outcomes for use cases where user privacy is compromised, but the legal situation is less clear-cut.

7 CONCLUSION

Following an exploratory and qualitative approach, we analyzed responses from WOs that were notified about a privacy issue on their website. We identify reasons for privacy issues, such as lack of awareness and faulty implementations. WOs must overcome distinctive challenges when addressing a privacy issue, such as a lack of technical knowledge or slow organizational structures. However, what challenges WOs face and how they deal with those depend heavily on the context in which they operate the site. When developing measures to support WOs in privacy matters, their different contexts and resulting needs must be considered. Our analyses reveal that WOs may differ from other people who operate and develop systems. Therefore, we conclude that usable privacy research should specifically address the perspective of this underexplored group.

ACKNOWLEDGMENTS

This work has been co-funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation, grant number 251805230/GRK 2050) and by the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE. It has also been co-funded by Stiftung Innovation in der Hochschullehre within the Project DiKuLe at University of Bamberg. This work was also supported by funding from the topic Engineering Secure Systems of the Helmholtz Association (HGF) and by KASTEL Security Research Labs.

REFERENCES

[1] Yasemin Acar, Sascha Fahl, and Michelle L. Mazurek. 2016. You are Not Your Developer, Either: A Research Agenda for Usable Security and Privacy Research Beyond End Users. In *2016 IEEE Cybersecurity Development (SecDev)*. IEEE, New York, NY, USA, 3–8.

[2] Nitin Agrawal, Reuben Binns, Max Van Kleek, Kim Laine, and Nigel Shadbolt. 2021. Exploring design and governance challenges in the development of privacy-preserving computation. In *CHI Conference on Human Factors in Computing Systems (CHI '21), May 8–13, 2021, Yokohama, Japan*. ACM, New York, NY, USA, 1–13.

[3] Noura Alomar and Serge Egelman. 2022. Developers Say the Darnedest Things: Privacy Compliance Processes Followed by Developers of Child-Directed Apps. *Proceedings on Privacy Enhancing Technologies* 4 (2022), 250–273.

[4] Rebecca Balebako, Abigail Marsh, Jialiu Lin, Jason I Hong, and Lorrie Faith Cranor. 2014. The Privacy and Security Behaviors of Smartphone App Developers. In *Workshop on Usable Security (USEC'14)*. Internet Society, San Diego, CA, USA.

[5] Tom Biselli, Enno Steinbrink, Franziska Herbert, Gina M Schmidbauer-Wolf, and Christian Reuter. 2022. On the Challenges of Developing a Concise Questionnaire to Identify Privacy Personas. *Proceedings on Privacy Enhancing Technologies* 2022, 4 (2022), 645–669.

[6] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.

[7] Davide Canali, Davide Balzarotti, and Aurélien Francillon. 2013. The Role of Web Hosting Providers in Detecting Compromised Websites. In *Proceedings of the 22nd International Conference on World Wide Web (WWW '13)*. ACM, New York, NY, USA, 177–188. https://doi.org/10.1145/2488388.2488405

[8] Orçun Çetin, Mohammad Hanif Jhaveri, Carlos Gañán, Michel van Eeten, and Tyler Moore. 2016. Understanding the role of sender reputation in abuse reporting and cleanup. *Journal of Cybersecurity* 2, 1 (2016), 83–98.

[9] Farah Chanchary and Sonia Chiasson. 2015. User Perceptions of Sharing, Advertising, and Tracking. In *Proceedings of the Eleventh Symposium on Usable Privacy and Security*. USENIX Association, Ottawa, 53–67.

[10] Sonia Chiasson, Yomna Abdelaziz, and Farah Chanchary. 2018. Privacy Concerns Amidst OBA and the Need for Alternative Models. *IEEE Internet Computing* 22, 2 (2018), 52–61. https://doi.org/10.1109/MIC.2017.3301625

[11] Victoria Clarke and Virginia Braun. 2013. *Successful qualitative research: A practical guide for beginners.* Sage Publications Ltd, Los Angeles. 1–400 pages.

[12] Martin Degeling, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. 2019. We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. In *Network and Distributed System Security Symposium (NDSS 2019)*. Internet Society, Reston, VA, USA. https://doi.org/10.14722/ndss.2019.23378

[13] Landgericht Dresden. 2019. *Urteil vom 11.1.2019 – 1a O 1582/18 = CR 2019, 604.* Spirit Legal. https://www.spiritlegal.com/files/userdata_spiritlegal-com/downloads/19-06-20-LG-Dresden-Google-Analytics-Urteil.pdf

[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 (CHI '16)*. ACM, New York, NY, USA, 5228–5239. https://doi.org/10.1145/2858036.2858214

[15] Zakir Durumeric, Frank Li, James Kasten, Johanna Amann, Jethro Beekman, Mathias Payer, Nicolas Weaver, David Adrian, Vern Paxson, Michael Bailey, and J. Alex Halderman. 2014. The Matter of Heartbleed. In *Proceedings of the 2014 Conference on Internet Measurement Conference (IMC '14)*. ACM, New York, NY, USA, 475–488. https://doi.org/10.1145/2663716.2663755

[16] Avshalom Ginosar and Yaron Ariel. 2017. An analytical framework for online privacy research: What is missing? *Information & Management* 54, 7 (2017), 948–957.

[17] Google Inc. 2020. *IP Anonymization (or IP masking) in Analytics*. https://support.google.com/analytics/answer/2763052?hl=en

[18] Frank Y Guo, Sanjay Shamdasani, and Bruce Randall. 2011. Creating effective personas for product design: insights from a case study. In *International Conference on Internationalization, Design and Global Development*. Springer, Springer-Verlag, Berlin Heidelberg Germany, 37–46. https://doi.org/10.1007/978-3-642-21660-2_5

[19] Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2020. "It's a Scavenger Hunt": Usability of Websites' Opt-Out and Data Deletion Choices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. ACM, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376511

[20] Irit Hadar, Tomer Hasson, Oshrat Ayalon, Eran Toch, Michael Birnhack, Sofia Sherman, and Arod Balissa. 2018. Privacy by designers: software developers' privacy mindset. *Empir. Softw. Eng.* 23, 1 (2018), 259–289. https://doi.org/10.1007/s10664-017-9517-1

[21] Anne Hennig, Heike Dietmann, Franz Lehr, Miriam Mutter, Melanie Volkamer, and Peter Mayer. 2022. Your Cookie Disclaimer is Not in Line with the Ideas of the GDPR. Why?. In *International Symposium on Human Aspects of Information Security and Assurance*. Springer, Cham, Switzerland, 218–227.

[22] Anne Hennig, Fabian Neusser, Aleksandra Alicja Pawelek, Dominik Herrmann, and Peter Mayer. 2022. Standing out among the daily spam: How to catch website owners' attention by means of vulnerability notifications. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA, 1–8.

[23] Mannat Kaur, Michel van Eeten, Marijn Janssen, Kevin Borgolte, and Tobias Fiebig. 2021. Human Factors in Security Research: Lessons Learned from 2008-2018. *CoRR* abs/2103.13287 (2021). arXiv:2103.13287 https://arxiv.org/abs/2103.13287

[24] Ponnurangam Kumaraguru and Lorrie Faith Cranor. 2005. *Privacy Indexes: A Survey of Westin's Studies*. Technical Report CMU-ISRI-5-138. Carnegie Mellon University.

[25] Frank Li, Grant Ho, Eric Kuan, Yuan Niu, Lucas Ballard, Kurt Thomas, Elie Bursztein, and Vern Paxson. 2016. Remedying Web Hijacking: Notification Effectiveness and Webmaster Comprehension. In *Proceedings of the 25th International Conference on World Wide Web*. ACM Press, New York, New York, USA, 1009–1019. https://doi.org/10.1145/2872427.2883039

[26] Max Maass, Alina Stöver, Henning Pridöhl, Sebastian Bretthauer, Dominik Herrmann, Matthias Hollick, and Indra Spiecker. 2021. Effective notification campaigns on the web: A matter of trust, framing, and support. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, 2489–2506.

[27] Max Maass, Pascal Wichmann, Henning Pridöhl, and Dominik Herrmann. 2017. PrivacyScore: Improving privacy and security via crowd-sourced benchmarks of websites. In *Annual Privacy Forum*. Springer, Cham, Switzerland, 178–191. https://doi.org/10.1007/978-3-319-67280-9_10

[28] Arunesh Mathur, Jessica Vitak, Arvind Narayanan, and Marshini Chetty. 2018. Characterizing the Use of Browser-Based Blocking Extensions To Prevent Online Tracking. In *Proceedings of the Fourteenth Symposium on Usable Privacy and Security*, Mary Ellen Zurko and Heather Richter Lipford (Eds.). USENIX Association, 103–116.

[29] Célestin Matte, Nataliia Bielova, and Cristiana Santos. 2020. Do Cookie Banners Respect my Choice? : Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework. In *2020 IEEE Symposium on Security and Privacy*. IEEE, New York, NY, USA, 791–809. https://doi.org/10.1109/SP40000.2020.00076

[30] William Melicher, Mahmood Sharif, Joshua Tan, Lujo Bauer, Mihai Christodorescu, and Pedro Giovanni Leon. 2015. (Do Not) Track Me Sometimes: Users' Contextual Preferences for Web Tracking. *Proceedings on Privacy Enhancing Technologies* 2016, 2 (2015), 135–154. https://doi.org/10.1515/popets-2016-0009

[31] Abraham H Mhaidli, Yixin Zou, and Florian Schaub. 2019. "We Can't Live Without Them!" App Developers' Adoption of Ad Networks and Their Considerations of Consumer Risks. In *Proceedings of the Fifteenth Symposium on Usable Privacy and Security*. USENIX Association, 225–244.

[32] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 2020. Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. ACM, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376321

[33] NOYB. 2022. UPDATE on 101 complaints: Austrian DPA rejects "risk based approach" for data transfers to third countries. Retrieved on August, 31, 2022 from https://noyb.eu/en/update-noybs-101-complaints-austrian-dpa-rejects-risk-based-approach-data-transfers-third-countries.

[34] Leysan Nurgalieva, Alisa Frik, and Gavin Doherty. 2021. WiP: Factors Affecting the Implementation of Privacy and Security Practices in Software Development: a Narrative Review. In *Proceedings of the 8th Annual Symposium on Hot Topics in the Science of Security, HotSoS 2021*. ACM, New York, NY, USA.

[35] John Pruitt and Jonathan Grudin. 2003. Personas: practice and theory. In *Proceedings of the 2003 conference on Designing for user experiences*. ACM, New York, NY, 1–15.

[36] Ben Stock, Giancarlo Pellegrino, Frank Li, Michael Backes, and Christian Rossow. 2018. Didn't You Hear Me? Towards More Successful Web Vulnerability Notifications. In *Proceedings of the 2018 Network and Distributed System Security Symposium*.

[37] Ben Stock, Giancarlo Pellegrino, Christian Rossow, Martin Johns, and Michael Backes. 2016. Hey, You Have a Problem: On the Feasibility of Large-Scale Web Vulnerability Notification. In *USENIX Security*. 1015–1032.

[38] Alina Stöver, Nina Gerber, Christin Cornel, Mona Henz, Karola Marky, Verena Zimmermann, and Joachim Vogt. 2022. Website operators are not the enemy either - Analyzing options for creating cookie consent notices without dark patterns. In *Mensch und Computer 2022 - Workshopband*, Karola Marky, Uwe Grünefeld, and Thomas Kosch (Eds.). Gesellschaft für Informatik e.V., Bonn. https://doi.org/10.18420/muc2022-mci-ws01-458

[39] Mohammad Tahaei, Alisa Frik, and Kami Vaniea. 2021. Privacy champions in software teams: understanding their motivations, strategies, and challenges. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA, 1–15.

[40] Mohammad Tahaei, Tianshi Li, and Kami Vaniea. 2022. Understanding Privacy-Related Advice on Stack Overflow. *Proceedings on Privacy Enhancing Technologies* 2022, 2 (2022), 114–131.

[41] Mohammad Tahaei, Kopo M Ramokapane, Tianshi Li, Jason I Hong, and Awais Rashid. 2022. Charting App Developers' Journey Through Privacy Regulation Features in Ad Networks. *Proceedings on Privacy Enhancing Technologies* 1 (2022), 24.

[42] Michael Toth, Nataliia Bielova, and Vincent Roca. 2022. On dark patterns and manipulation of website publishers by CMPs. *Proceedings on Privacy Enhancing Technologies* 2022, 2 (2022), 478–497.

[43] Martino Trevisan, Stefano Traverso, Eleonora Bassi, and Marco Mellia. 2019. 4 Years of EU Cookie Law: Results and Lessons Learned. *Proceedings on Privacy Enhancing Technologies* 2019, 2 (2019), 126–145. https://doi.org/10.2478/popets-2019-0023

[44] Christine Utz, Sabrina Amft, Martin Degeling, Thorsten Holz, Sascha Fahl, and Florian Schaub. 2022. Privacy Rarely Considered: Exploring Considerations in the Adoption of Third-Party Services by Websites. *arXiv preprint arXiv:2203.11387* (2022).

[45] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. (Un)Informed Consent: Studying GDPR Consent Notices in the Field. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 973–990. https://doi.org/10.1145/3319535.3354212

[46] Marie Vasek and Tyler Moore. 2012. Do Malware Reports Expedite Cleanup? An Experimental Study. In *Proceedings of the 5th Workshop on Cyber Security Experimentation and Test*. 1–8. https://doi.org/10.1016/j.egypro.2011.02.120

[47] VERBI Software, Berlin, Germany. 2020. *MAXQDA 2020 [computer software]*. VERBI Software. maxqda.com

[48] Alan F Westin. 1968. Privacy and freedom. *Washington and Lee Law Review* 25, 1 (1968), 166.

[49] Eric Zeng, Frank Li, Emily Stark, and Adrienne Porter Felt. 2019. Fixing HTTPS Misconfigurations at Scale: An Experiment with Security Notifications. In *Workshop on the Economics of Information Security (WEIS 2019)*. 1–19.

A CODEBOOK OF THE THEMATIC ANALYSIS

Table 2: Code book with themes, categories, and subcategories that resulted from the thematic analysis.

Category	Subcategories	Frequencies
Theme 1: Backgrounds on WOs		
Context of website owning	professional context (employed, self-employed); private (personal interest, association)	928
Involvement of WOs in development of website	WO did not build website; WO built website with support; WO built website without support	37
Involvement of WOs in maintenance of website	WO has website operated; WO operates website with support; WO runs website without support	45
Privacy Motivation	WO does not want to care about privacy; WO has no time for maintenance/privacy; privacy/compliance is important; WO looks for GA alternatives; WO did not know their had GA on website; WO does not use CA data at all; WO deletes GA	142
Theme 2: Reasons for lack of AIP		
Incorrect technical implementation	incorrect implementation of AIP; incomplete implementation of AIP; wrong code applied by mistake	97
Lack of privacy awareness	WO thinks there is no privacy issue; WO thinks they have no GA on website	77
Ambiguous responsibility	WO is not aware of responsibility; responsible person/contact person is gone	34
Reliance on others judgments	problem lies with third-party provider/outside WO's influence; WO had relied on certification of website by others; default setting taken from provider	61
Deliberate lack of maintenance	website has not been maintained for a long time; website was set up a long time ago; website is currently being revised/new website is being created	72
Theme 3: WOs' approach to missing AIP		
WOs implement AIP themselves	–	314
WOs implement AIP with support	–	64
WOs delegate implementation of AIP	–	188
WOs do not implement AIP	–	4
Kind of support	legal support; technical support	25
Supporting instances	Google support; study organizers; lawyer; IT person; service provider who maintains website; person from private environment; website provider; data protection officer	276
Theme 4: Challenges in the implementation of AIP		
Lack of resources	personal reasons; website is not WO's daily business; WO has no money for professionals	23
Lack of technical knowledge	difficult to keep up to date; lack of technical knowledge	78
Problems with code	trouble deleting GA; WO cannot find error	66
Dependencies and slow process in organizations	responsible person currently not available; website is not maintained; complex coordination with other stakeholders	72