“Gimme Cookie!” Exploring Tangible Privacy and Security for Cookie Management In The Wild

Sarah Delgado Rodriguez
sarah.delgado@unibw.de
University of the Bundeswehr Munich
Munich, Germany

Lukas Mecke
lukas.mecke@ifi.lmu.de
LMU Munich
Munich, Germany

Sarah Prange
sarah.prange@ifi.lmu.de
LMU Munich
Munich, Germany

Yen-Ni Sarah O
o.sarah@campus.lmu.de
LMU Munich
Munich, Germany

Christoph Hanschke
hanschke-christoph@outlook.de
LMU Munich
Munich, Germany

Florian Alt
florian.alt@ifi.lmu.de
LMU Munich
Germany



Figure 1: We present the *Cookie Counter*, a tangible privacy and security interface for persistent cookie management (center) to investigate the differences between digital and tangible interfaces in the context of real-world security behaviors and decision-making. Our design was informed by design recommendations from prior work and iterative user input (left shows the initial prototype). We then evaluated its impact on users’ perceptions, usage patterns, and self-reported cookie choices in the wild, comparing it with a purely digital interface (right).

ABSTRACT

Tangible Privacy and Security Interfaces (TaPSIs) transform abstract cybersecurity decisions and behaviors into physical forms to support cognition. However, prior research has rarely evaluated TaPSIs in the wild. Our work addresses this gap by focusing on browser cookies as an example of everyday yet abstract security topics. Cookies can put users’ privacy and security at risk by enabling user profiling and being vulnerable to cyberattacks. We developed the *Cookie Counter*, a tangible cookie management prototype, and compared it to a purely digital browser extension in a two-week field study (N=16). While both versions were rated similarly in usability and user experience, participants in the tangible condition valued immediate visibility and ease of operation, but criticized its portability and the space it occupied. Our work contributes empirical field evidence to TaPSI research and illustrates trade-offs between constant physical peripheral visibility and seamless integration into existing digital workflows.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**.

KEYWORDS

tangible privacy, tangible security, cookies, cookie management

ACM Reference Format:
Sarah Delgado Rodriguez, Lukas Mecke, Sarah Prange, Yen-Ni Sarah O, Christoph Hanschke, and Florian Alt. 2026. “Gimme Cookie!” Exploring Tangible Privacy and Security for Cookie Management In The Wild. In *25th International Conference on Mobile and Ubiquitous Multimedia (MUM ’26), December 01–04, 2026, Glasgow, United Kingdom.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3861188.3861223

Please use nonacm option or ACM Engage class to enable CC licenses
This work is licensed under a Creative Commons Attribution 4.0 International License.
MUM ’26, December 01–04, 2026, Glasgow, United Kingdom
© 2026 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-2791-7/2026/12
https://doi.org/10.1145/3861188.3861223

1 INTRODUCTION

Cybersecurity is often difficult for users to grasp, since security and privacy threats and protection mechanisms operate in abstract digital systems and cannot be directly perceived or assessed through human senses.

The research area of Tangible Privacy and Security Interfaces (TaPSI) addresses this challenge [12]. Its core idea is to make cybersecurity risks and protection mechanisms more understandable by embedding them in users' physical environments. To this end, TaPSI research explores tangible privacy and security control and awareness mechanisms that enable physical manipulation and perception. Hence, TaPSIs can be understood as a step back from digitization, aiming to materialize security-relevant decisions and behaviors through a physical presence that supports cognitive processes such as understanding, reflection, and decision-making [2, 12, 29]. In other words, they aim at leveraging embodied cognition [41] for privacy and security challenges [29].

However, studies of TaPSIs in realistic, everyday use contexts (i.e., in the wild) remain scarce. Therefore, it remains largely unclear to what extent reported benefits and challenges of TaPSIs hold true in realistic usage environments, as privacy and security behaviors measured in laboratory settings might strongly differ from behaviors observed in the wild [13, 35]. In addition, direct comparisons between digital and tangible solutions are rare [12, 42]. Such comparisons are important to disentangle effects stemming from the physicality of an interface from those caused by its underlying functionalities, which can often be similarly implemented in a purely digital manner. Our work addresses these gaps by investigating a TaPSI in an in-the-wild context and comparing it with a functionally equivalent digital alternative.

As a concrete, everyday example of abstract decisions users face, we focus on browser cookies. While browsing online, cookies enable features such as personalized website content and reduced authentication effort. Most websites nowadays display cookie banners: pop-ups that cover parts of the content and inform users about cookie usage. However, increasing knowledge about cookies does not necessarily translate into changes in cookie choices [21, 36]. These choices are particularly consequential for persistent cookies (i.e., cookies that are not automatically deleted once the website is closed), as they enable the creation of extensive user profiles and are vulnerable to several types of attacks [18, 21]. Internet users are thus very frequently confronted with the abstract topic of browser cookies, but often lack adequate means for managing already-granted cookies. This makes cookies a suitable everyday use case for investigating whether TaPSIs can support users' privacy and security behaviors.

We investigated this by first developing a tangible cookie management interface, the *Cookie Counter*. We grounded the design of the *Cookie Counter* in recommendations from related work and applied an iterative development approach guided by end-user input. *Cookie Counter* provides persistent, real-time information to users by showing the current number of browser cookies at a glance. It also enables direct deletion of browser cookies through a simple button press. We then conducted an in-the-wild study with 16 participants who used either the *Cookie Counter* or a purely digital, functionally identical alternative (i.e., a Chrome browser extension) for two weeks. We found that both interfaces were perceived similarly in terms of usability and user experience. Descriptive trends suggest slightly stronger effects of the *Cookie Counter* on participants' cookie behavior, choices, and privacy concerns. Moreover, directly and calmly displaying the cookie count in real time appears to be the most impactful design feature of our TaPSI.

Contribution Statement. We contribute to the understanding of how TaPSIs affect users' security behaviors, concerns, and choices by (1) developing *Cookie Counter*, a TaPSI for persistent cookie management grounded in design recommendations from related work and end-user input, and (2) conducting a user study investigating its effects in the wild in comparison with a digital alternative with the same functionalities.

2 BACKGROUND & RELATED WORK

2.1 Tangible Privacy and Security Interfaces

Delgado Rodriguez et al. [12] define *"Tangible Privacy and Security Interfaces (TaPSI) as 'tangibles' – which means they exist in the physical world and can be manipulated or perceived by touch and potentially other senses – that help users manage, protect, and understand information privacy and/or security"*

Mehta et al. [29] describe *tangible privacy interfaces* as ideally being *direct*, *ready-to-hand*, and *contextual*. The authors argue that such interfaces are *direct*, if they enable timely and intuitive (tangible) interactions through metaphors. They should be *ready-to-hand* by supporting ad hoc interactions through wearable and ambient form factors. This means that well-designed tangible privacy interfaces support periphery-to-center attention transitions, being always ready to use but grabbing the user's attention only when necessary. Finally, TaPSIs should be *contextual* by being adaptable to different usage contexts (e.g., by providing modular hardware or configurable software).

TaPSIs may also apply *"physically-intuitive privacy and security"* [16] features. This term describes the usage of physicalization to provide unambiguous feedback about the state of a potentially privacy-invasive sensor (e.g., a covered camera cannot record the user) [2, 16]. This design approach stems primarily from research on the Internet of Things (IoT). It suggests developing sensors, such as microphones or cameras, that enable physical manipulation and perceptible assurance of the sensors' state (i.e., on or off) [14–16].

Since this strong emphasis on current risks resulting from the proximity of sensing devices does not align well with our focus on persistent browser cookies, we have not made physically-intuitive privacy and security design principles a priority in our work. Instead, we based our design considerations for the *Cookie Counter* mostly but not exclusively on Mehta et al. [29]'s Privacy Care framework in combination with findings from the TaPSI literature survey [12] and additional insights from related works [9, 10, 42].

2.1.1 In-The-Wild Evaluations of TaPSI. Research has shown growing interest in TaPSIs over the last few years, with solutions that address a wide range of privacy and security challenges [12]. However, most research evaluating user perceptions of TaPSIs is limited in ecological validity, as only a few works have evaluated functional TaPSI prototypes in the wild. Examples of existing in-the-wild evaluations of TaPSIs include the trial of *Posit*, an interactive tangible

calendar that enables users to control the disclosure level of schedule dates by changing them based on their placement on a tray [20], a study on the *Peekaboo Cam*, a camera designed to enable observational field research in subjects' homes while maintaining the subjects' comfort and privacy, and the development and evaluation of *PowerCut and Obfuscator*, two tangible approaches to enabling users to control their privacy when using a smart speaker [7]. The work that most closely relates to this paper is "DataCrumb", a physical artifact that uses ambient feedback (i.e., light, sound, and a screen) to encourage reflection about web tracking. The cookie-shaped prototype indicates the number of and the domains of tracking requests that are being detected and blocked [34].

These works describe unique benefits and drawbacks of TaPSI. However, to better understand their impact in practice, it is crucial to compare TaPSIs directly with digital solutions, because many of the proposed benefits of TaPSIs, such as improved awareness, control, and intuitiveness [12], are inherently relative to existing digital solutions.

2.1.2 In-The-Wild Comparison Studies. Only very few works have deployed comparisons of functional TaPSIs against digital alternatives in the wild [12]. In particular, some researchers compared the usability and user perception of commercial tangible and digital two-factor authentication methods in the wild [1, 23, 32, 40].

To the best of our knowledge, only Windl et al.'s work on the SaferHome privacy dashboards for smart homes describes an in-the-wild evaluation of a newly developed TaPSI and a digital alternative [42]. However, the focus of this paper is on floorplan-based privacy dashboards, and therefore, the authors draw few comparative conclusions.

2.2 Browser Cookies

Browser cookies are small text files that websites may store on users' devices to enable functionalities (functional cookies) or to, for example, create user profiles (non-functional cookies) [21]. While some cookies are generally necessary to provide functionality or enhance the user experience, especially persistent cookies (i.e., cookies that persist after a session is closed) can be used to profile users, derive sensitive information, or serve targeted advertisements. Cookies may also grant third parties access to sensitive data or be exploited by malicious attackers, for example, to hijack user sessions and gain unauthorized access to accounts [18, 37]. Our work focuses on browser cookies as a concrete, everyday example of abstract security topics that users repeatedly face.

2.2.1 Legislation & Cookie Banners. Although cookies pose significant privacy and security risks, their storage is generally invisible to users, which is why laws such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) require providers to ensure informed consent or provide opt-out options. Website providers that want to use non-essential cookies (e.g., tracking cookies) must obtain users' informed consent, typically through a cookie banner. Cookie banners are pop-ups that inform users that the website they are visiting uses cookies and usually offer them multiple buttons to confirm their cookie choice.

2.2.2 Users' Cookie Awareness & Choices. Under the GDPR, consent for non-essential cookies must be freely given, which in practice requires that users should be able to refuse cookies as easily as they can accept them. However, many designs fail to provide a clear option to decline cookies or apply deceptive patterns, making such options more difficult to find [19, 21, 22].

However, Strycharz et al. [36] showed that increasing users' knowledge might also not affect their cookie decisions as expected. The authors conducted an online experiment with 294 participants to assess the impact of technical and legal knowledge about online data collection on participants' self-reported privacy-related perceptions of browser cookies. Receiving technical and legal knowledge interventions did not increase participants' motivation to reject tracking cookies. The authors conclude that, from the factors they investigated, only privacy concerns and preferences for personalized ads and recommendations mattered [36]. Consequently, many tracking cookies get accepted. With our work, we make those cookies more visible for users and support deletion.

2.3 Summary and Research Gap

To the best of our knowledge, no direct in-the-wild evaluations of user behavior and its effects on security choices that consider both purpose-designed TaPSIs and functionally equivalent digital alternatives have been conducted yet. Our work addresses this gap by investigating in the wild whether and how a TaPSI designed according to considerations derived from related work affects users' perceptions, behaviors, and choices regarding persistent browser cookies, compared to a purely digital solution. To render this question graspable, we focus on persistent browser cookie management as the use case. Therefore, we designed, implemented, and evaluated a TaPSI for this specific use case. Research on browser cookies and cookie banners shows that users are repeatedly confronted with cookie-related decisions, yet increased knowledge alone does not necessarily translate into changed behavior [21, 36]. We thus assume that users will continue to grant cookies (beyond what may be necessary) and take the approach of supporting them in managing cookies instead. To this end, we propose the *Cookie Counter* as a tangible interface that displays the number of granted cookies and supports quick deletion.

3 RESEARCH APPROACH

With our work, we aim to answer the following research questions:

- **RQ1 - Cookie Awareness & Choices** How does exposure to a TaPSI, compared to a similar digital persistent cookie management tool, impact participants' online privacy concerns and self-reported cookie choices?
- **RQ2 - Usage Behavior** How does participants' behavior in the wild while using a TaPSI compare to their behavior when using a similar purely digital tool?
- **RQ3 - User Experience** How does the user experience and usability of a purposefully designed TaPSI for persistent cookie management compare to a purely digital tool with the same functionalities?

To instantiate a meaningful TaPSI that can answer these questions, our work employs design considerations from prior work (see Section 4.1). In particular, we explore TaPSIs' ability to provide

(1) persistent security-relevant information, (2) direct and intuitive control via physical manipulation, (3) a calm integration into the user's everyday environment, (4) contextual adaptability, as well as (5) a metaphoric physical form.

3.1 Process Overview

Our research process consisted of four steps as shown in Figure 2. We first derived design considerations for a TaPSI for cookie management from design recommendations presented in related work. We then implemented a first version of the corresponding TaPSI and conducted a short formative lab trial with six participants to collect early feedback on the underlying concept and concrete design. Based on these insights, we then implemented the final *Cookie Counter* and a digital alternative. Both prototypes provide the same functionalities to users, but differ in user interaction and directness. We then measured and compared participants' perceptions, security behaviors, and choices in the wild while being exposed to one of the prototypes.

3.2 Ethical Considerations

For our lab trial, we did not seek formal IRB approval, as low-risk lab studies such as this are exempt in our institution. For our in-the-wild study, which could have a larger impact on participants due to the prolonged collection of data related to participants' browsing behavior, we received formal IRB approval. For both studies, we adhered to our institution's ethical guidelines and best practices. Consequently, before consenting to participate, participants received a detailed explanation of the data collection and the study's purpose. They were also informed about the procedures and locations for data storage, in particular that usage data (i.e., categories of visited websites, cookie counts, and timestamps of user interactions) would be stored on a Firebase real-time database. All other information was processed only locally to protect our participants' privacy. In addition, participants were informed about the voluntary nature of participation and the option to withdraw at any time.

3.3 Limitations

We collected self-reported data in both studies, which may be prone to social desirability bias. Moreover, we recruited participants through university channels. We recruited those living in Munich, Germany and its suburbs for one of the conditions of our in-the-wild study, due to logistical constraints. Due to issues with the survey tool, we were unable to record participants' reported gender correctly in our final study. In addition, our sample sizes were rather small, as is common in exploratory HCI studies [6], particularly in in-the-wild studies, where recruiting participants willing to reliably incorporate a research prototype into their daily routines can be challenging. For example, Windl et al. used a similar sample size of 16 participants in their in-the-wild study [42]. Nevertheless, our sample size limits the generalizability of our findings, and some between-group effects may have gone undetected. Participants from the in-the-wild study also started with high cookie awareness and internet user privacy concerns, which may have resulted in ceiling effects. Finally, the study took two weeks and can, thus, not capture longer-term exposure effects.

4 DEVELOPING THE *COOKIE COUNTER*

4.1 Design Considerations

We derived the following design considerations for our persistent cookie management TaPSI on the Privacy Care Framework by Mehta et al. [29] and supplemented it with additional insights from the TaPSI design space [12] and further design frameworks for TaPSIs by Delgado Rodriguez et al. [9] and Windl et al. [42]:

Realtime Information: To foster directness [29], the TaPSI should provide realtime information that users can grasp at a glance at all times without having to first interact with it [12]. We implemented this by continuously visualizing the current number of stored cookies. Showing the number of stored cookies at all times is an easy-to-grasp reminder that cookies persist.

Direct and Intuitive Control: The TaPSI should enable quick and intuitive user responses to the provided information [12, 29]. We implement this by deleting persistent cookies with a single button press. This process ignores cookies from currently open websites to avoid data loss or the need for re-authentication.

Ambient TaPSI in Meaningful Environment: To ensure that the TaPSI is always ready-to-hand to perform ad hoc interactions [29], it should be placed in a meaningful environment (i.e., where it will be needed most) [10, 42], which is near the device that runs the web browser. Moreover, it should support periphery-to-center attention transitions to reduce users' mental load. We implemented this by applying two levels of information granularity, with the tangible calmly and steadily providing only the most important information at a glance. Users can access more fine-grained control and information features through a browser extension.

Contextual Adaptability: Contextual adaptability in TaPSIs can be achieved through modularization of hardware and customizable software features [29]. We implemented software-based customization, enabling users to set a custom cookie limit and create an allowlist of websites exempt from cookie deletion. In the initial version, we provided the delete button as an additional device that could be disconnect. In contrast, the second version of our *Cookie Counter* instead enabled hardware modularization through an additional decorative bust that could be removed.

Metaphoric Appearance: Metaphors can increase the intuitiveness of interactions and interest in or engagement with a TaPSI [11, 12, 28, 29]. We therefore opted for a playful design that integrates a character, as suggested by [30] and [9], with a well-known connection to "cookies", the Cookie Monster muppet from Sesame Street[1] – a metaphor used in prior works [8, 38, 39].

Usage Data Logging: In order to answer our research question on usage behaviors, we incorporated data logging.

[1] https://sesameworkshop.org/our-work/shows/sesame-street/, last accessed April 20, 2026

[2] In the spirit of diversity, equity, and inclusion, we have replaced a charged term used in our original user interface with an alternative in these screenshots.

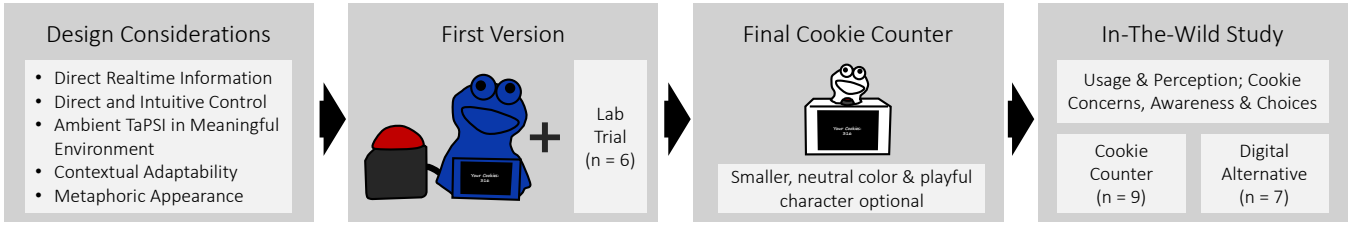
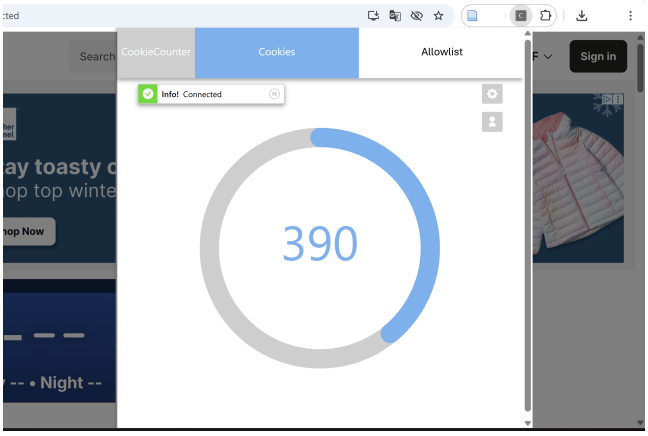
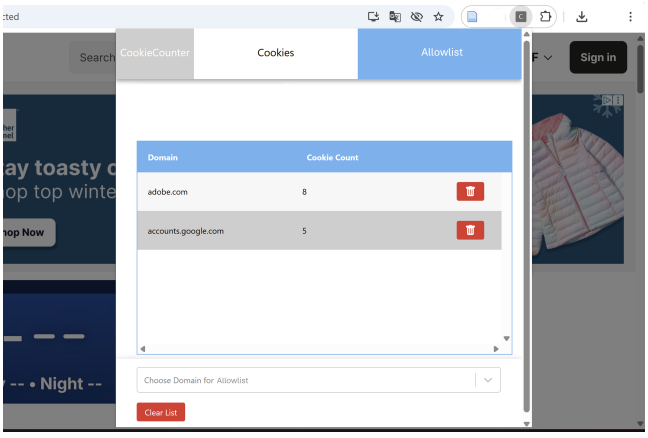


Figure 2: Our research process consisted of four subsequently conducted steps. We first derived design considerations from related work and used them to design the first version of our *Cookie Counter*. We then collected user input through a short formative lab trial that informed the final design of the *Cookie Counter*. We finally conducted an exploratory user study in the wild with 16 participants who used either the *Cookie Counter* or a purely digital alternative.



(a) Overview Tab



(b) Allowlist Tab[2]

Figure 3: We developed a Chrome extension to enable cookie management functionalities and provide an interface for customization. Its graphical user interface pops up when a user clicks on the extension's icon in the browser's menu bar. Note that this Figure shows the browser extension of the *Cookie Counter*. The *digital alternative* looks slightly different (see Figure 1).

4.2 Initial Version

The *Cookie Counter* accesses cookie management functionalities through a browser extension. We used Node.js as a runtime environment, and TypeScript and React for the graphical user interface. A service worker handles all communication between the browser extension and the tangible interface.

Figure 3 shows the graphical interface of the browser extension, which consists of two tabs: the *overview* tab and the *allowlist* tab. The overview tab shows the number of cookies, the icon for modifying the cookie limit, and a notification about the status of the connection with the tangible interface. When the cookie limit is reached, the extension will automatically delete all persistent cookies. In the allowlist tab, users can view and configure their allowlist of domains from which cookies should not be deleted. This enables them to add domains they trust or frequently use, and for which they do not want to re-authenticate every time they open them. To enable quantitative behavior analysis, we logged the following user interaction data in a Firebase Realtime Database:

Setup Events: Extension installed/ restarted; connection to the tangible interface established/ interrupted (usually when Chrome starts/ closes).
Browsing Behavior: New website opened and its URL.
***Cookie Counter* Usage:** Allowlist entry added/ deleted and number of entries; cookie limit changed and new value; cookie deletion event and number of cookies before deletion.

The initial tangible interface contained an ESP32 microcontroller and a 4-inch TFT-LCD display with a 480 x 320 pixel resolution (see left side of Figure 1). The built-in Wi-Fi enabled wireless communication with the extension. The casing of *Cookie Counter* consisted of a free 3D model[3] of the Cookie Monster, which we modified to accommodate all components. A large red button, housed in an external enclosure, triggers cookie deletion.

4.3 Formative Lab Trial

To refine our initial design, we conducted a formative lab trial with six subjects that we recruited directly from our personal networks. They were not compensated for their participation in this short trial (15-20 minutes).

[3]Cookie Monster Model by Cerberus333,https://www.thingiverse.com/thing:455544, last accessed on January 15, 2026

Procedure. For our trial, we used a desk setup with a PC running Google Chrome and the browser extension installed, a screen, keyboard, mouse, and the initial version of the *Cookie Counter*. For each participant, the browser was reset, all cookies were deleted, and the automatic cookie limit was set to 1000.

Participants first provided their demographics, browsing behavior, and cookie deletion behavior in an online survey. They subsequently received a short introduction about browser cookies, the *Cookie Counter* and its functionalities. Participants then had ten minutes to use the Google Chrome browser as they usually would and interact with the *Cookie Counter*. Finally, a second survey inquired about their opinions regarding our underlying concept, the ease of use of the prototype, its design, as well as wishes and thoughts for improvements through free-text answers.

Findings. We had four female and two male participants who were 27-28 years old. All used Google Chrome regularly and reported using web browsers 2.5 to 12 hours daily and never ($N = 3$) or rarely ($N = 2$) deleted cookies before. Details in Appendix A.

Participants thoroughly tested the device and sometimes pressed the button several times because the count did not drop to 0. This led to an average of 7.17 deletions during the trial.

All participants liked the idea of the *Cookie Counter*. Two participants highlighted that they felt that our prototype increased their awareness of browser cookies: *"The display is great, especially the fact that you can see in real time how many cookies there are (there are an astonishing number)"* (T6).

All participants found the usage very easy, and three specifically noted the ease of pressing a button to delete the cookies. Two participants also highlighted that they liked the Cookie Monster design. Nevertheless, three participants criticized the initial version as much too large, and one disliked its blue color. One participant also mentioned that the Cookie Monster design is too childish, and another one would prefer a design without the monster.

Summary. Participants were able to successfully use the initial version of our *Cookie Counter* and appreciated the underlying idea of having a tangible device that shows the number of cookies and allows them to be deleted with a simple button press. However, they disliked the size and color of the initial version. The playful Cookie Monster design was specifically mentioned as a positive feature by some participants and as a negative feature by one participant.

4.4 Final *Cookie Counter*

Based on the lab trial, we adapted the tangible interface design and the browser extension's data logging to minimize the risk of collecting sensitive data during the subsequent field study.

Figure 1 shows both versions of the tangible interface side-by-side to enable size comparisons and the final version in more detail in the middle. The final *Cookie Counter* is a white cuboid with a display to monitor the number of cookies and a button to delete the cookies. Optionally, the user can place a small bust of the Cookie Monster from Sesame Street on top of the box for decoration. A much smaller red push button is now directly integrated into the case. To enable the smaller design, we also replaced the ESP32 board we used with a smaller ESP8266-based microcontroller.

To protect our field study participants' privacy, we modified the data logging to log only the types of visited websites, rather than their URLs. To implement this, we locally mapped visited domains to the categories listed in Appendix B. We developed the mapping based on the first 1000 domains of the research-oriented top websites ranking list Tranco [25][4], as well as frequently visited domains from a previous 10- 14-day-long field study conducted at our university in 2024 with 10 participants. A test with the websites visited by participants during our lab trial achieved a coverage of 60.82% using this mapping. All remaining visited domains would be assigned to "Other".

5 IN-THE-WILD STUDY

We conducted a between-groups field study. Participants who registered were randomly assigned to either the *Cookie Counter* condition or the *digital alternative* condition.

5.1 Study Apparatus

5.1.1 Digital Alternative. The Chrome extension developed for the *Cookie Counter* builds the foundation of the purely digital comparison baseline. To enable all user interactions the *Cookie Counter* integrates, we added a button to delete cookies to the extension and removed the connection notification (see Figure 1, right).

5.1.2 Online Surveys. We developed two SoSci Surveys and hosted them on university servers:

Start Survey The start survey contained questions about participants' demographics and affinity for technology (Affinity for Technology Interaction (ATI) [17] scale). In addition, we inquired about their browsing (i.e., most used browser, frequency and duration of internet use, browser extensions, and private browsing functionalities) and cookie deletion habits (i.e., how often and how they delete their cookies).

Final Survey The final survey focused on participants' experiences with the *Cookie Counter*. For this, we applied the System Usability Scale (SUS) [5], the short version of the User Experience Questionnaire (UEQ-S) [24], some Likert items regarding their opinions and thoughts on using the *Cookie Counter* and the effects it had on them after using it (e.g., whether it motivated them to learn more about cookies or whether the number of cookies was as they expected), as well as some open-ended questions for comments or suggestions regarding functionality or design.

In addition, we repeated items in both the start and final survey to identify changes in participants' self-reported behaviors and perceptions due to their exposure to the *Cookie Counter* or the digital alternative. We used 5-point Likert scales asking whether they had heard of browser cookies before, whether they believed that a browser cookie captures data about them, and whether they believed that a browser cookie could be used by the website provider or a third party to collect data about them. We also asked which options they usually choose on cookie banners (i.e., accept all cookies, configure selection, or reject all cookies) and applied the Internet Users' Information Privacy Concerns scale (IUIPC-10) [26].

[4]The Tranco list is available at https://tranco-list.eu/list/ZW95G. It was generated on June 7, 2025, to include domains seen in Germany, where the study was conducted.

5.2 Procedure

We recruited our participants using institutional social media channels and mailing lists. To participate in the study, participants were required to confirm that they use Google Chrome regularly and in a stable environment (i.e., the same WiFi network). They also had to confirm that they would do so throughout the study.

After signing up for the user study, participants in the *digital alternative* group received instructions on installing the browser extension. Participants in the *Cookie Counter* condition were asked to schedule on-site appointments to collect the device before taking it home for the duration of the study. They subsequently received a brief explanation of how the *Cookie Counter* works and installation instructions they were asked to perform immediately.

We instructed all participants to complete the start questionnaire before using the prototype or digital alternative in any way they wished for two weeks. After this period, they received an email containing a link to the final questionnaire and instructions on how to uninstall the extension. Participants were compensated with 12€ for their efforts. We piloted our user study with two volunteers to review the whole process and identify possible problems. Based on the pilot testers' feedback, we slightly adjusted our surveys to make instructions clearer.

5.3 Collected Data & Analysis

We gathered both quantitative and qualitative data. In particular, we measured participants' use of both prototypes using data logs and self-reported data (i.e., Likert scales and free-text responses). We collected participants' perceptions of the prototypes' usability and user experience using standard scales and author-generated items (again: Likert scales and free-text responses). To explore the effects of both prototypes on participants' cookie-related behaviors, we administered pre- and post-study tests as described above.

We analyzed all quantitative measures descriptively and report on these findings in the following. A sensitivity analysis approximating the between-group comparison with an independent-samples t-test indicated that, assuming $\alpha = .05$ and $power = .80$, our sample would allow us to detect only very large between-group differences (Cohen's $d \geq 1.52$). We therefore performed inferential tests to identify such differences where possible, but refrain from discussing non-significant findings in the text, as their absence of statistical significance should not be interpreted as evidence of no effect. In particular, we used Mann–Whitney U tests [27] with exact p-values, given our sample sizes and irregular (i.e., non-normal) distributions of answers [31], which we assessed through Q–Q plots.

The qualitative data we collected consisted solely of participants' short free-text responses, most of which were less than one sentence. Hence, we did not apply a full thematic analysis, since we primarily captured qualitative insights to supplement our quantitative findings with contextual details in order to facilitate a better interpretation. Instead, we iteratively refined our mutual observations loosely inspired by Braun and Clark [4]. For this, one researcher organized participants' answers by similarity and derived underlying trends. A second researcher subsequently reviewed the resulting observations for completeness relative to the original dataset.

6 RESULTS

6.1 Participants

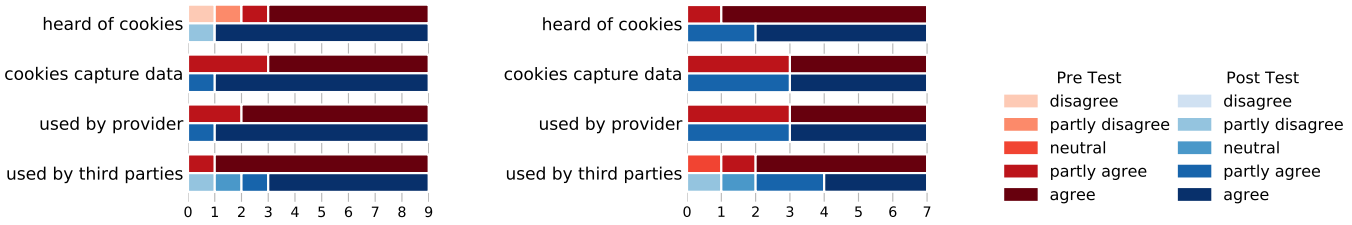
We recruited 18 participants for our user study – 9 for each group. However, two participants from the *digital alternative* group uninstalled the extension after one day, reporting slowed-down homepage loading times, and their data were thus excluded from our analysis. The remaining 16 participants were on average 35.75 years old (range: 21 -66). Both groups had similar mean ages, 34.78 years for the *Cookie Counter* group ($n = 9$) and 37.00 years for the digital alternative group ($n = 7$, see Appendix C for more details). Most participants in both groups were highly educated, with university degrees ($n_{CookieCounter} = 5$, $n_{Digital} = 3$) or A-level-equivalent qualifications ($n_{CookieCounter} = 3$, $n_{Digital} = 3$). Their mean ATI score was 2.58 (SD = 0.56) for the *Cookie Counter* group and 3.62 (SD = 0.83) for the digital alternative group.

Browsing & Cookie Deletion Habits. Participants in both groups indicated a comparable overall internet usage with 6.33 hours (*Cookie Counter* group, $SD = 5.12$) and 6.00 hours daily (digital alternative group, $SD = 3.60$). Both groups also used the internet mostly for private activities – 4.94 hours on average in the *Cookie Counter* group and 3.57 hours/day in the digital group. Overall, Google Chrome was the most commonly used browser ($n = 8$). In the *Cookie Counter* group, Mozilla Firefox was most common ($n = 4$), followed by Google Chrome ($n = 3$). In the digital alternative group, most participants used Google Chrome ($n = 5$). Overall, participants from the *Cookie Counter* group reported more frequent cookie deletion than those from the digital alternative group. Seven participants of the *Cookie Counter* group stated that they do not delete cookies at all, and the remaining two participants delete their cookies rarely. In the digital alternative group, only one participant did not delete their cookies, three participants indicated deleting their cookies rarely, and the remaining participants deleted their cookies monthly ($n = 1$) and several times a day ($n = 2$).

6.2 Pre- & Post-Tests: Awareness, Concerns & Choices

6.2.1 Cookie Awareness Items. Participants in both groups were already aware of browser cookies before our user study. For instance, participants in both groups agreed that they had heard of browser cookies before, believed that cookies capture data about them, and believed that cookies can be used by the website provider or third parties for this purpose ($medians = 5$, see Figure 4). This high starting point makes it difficult to assess the potential increase in participants' awareness. Correspondingly, most median values remained at "agree" in the post-tests. The only observable difference was a slight decrease in agreement among participants in the digital alternative group when asked whether cookies can be used by third parties to capture data about users ($median_{digital,pre} = 5$, $median_{digital,post} = 4$).

6.2.2 Cookie Banner Choices. Table 1a provides an overview of our participants' self-reported cookie banner-related behavior. Most participants in the *Cookie Counter* group reported usually choosing the "Accept all cookies" ($n = 5$) option on cookie banners, with fewer selecting "Reject all cookies" ($n = 4$) before using the *Cookie Counter*. After using the *Cookie Counter*, the number of participants



(a) *Cookie Counter* Group **(b) Digital Alternative Group**

Figure 4: Participants' answers to whether they have heard of browser cookies, whether they believe cookies capture data about them, and whether cookies can be used by the website provider or third parties to collect information about them.

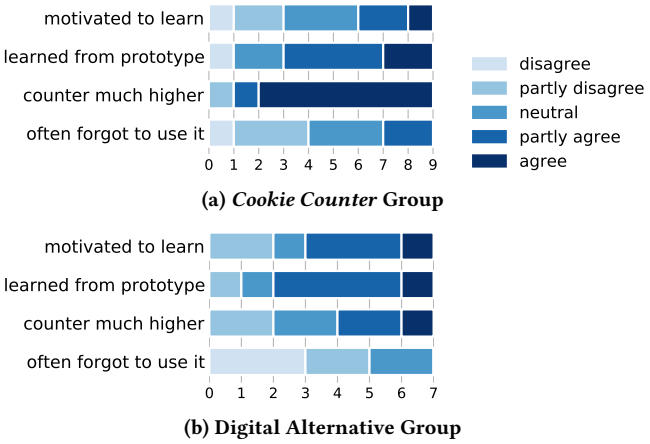
Table 1: Comparison of pre- and post-study cookie banner choices and IUIPC scores.

	Cookie Counter			Digital Alternative		
	Pre	Post	Change	Pre	Post	Change
Accept all cookies	5	3	-2	1	1	0
Select cookies	0	1	+1	2	1	-1
Reject all cookies	4	5	+1	4	5	+1

(a) Counts of self-reported cookie banner choices

	Cookie Counter			Digital Alternative		
	Pre	Post	Change	Pre	Post	Change
control	6.07	6.26	+0.2	6.43	6.238	-0.19
awareness	6.15	6.15	0.00	6.38	6.24	-0.14
collection	4.81	4.61	-0.19	6.43	5.93	-0.50
overall IUIPC	5.68	5.67	+0.01	6.41	6.13	-0.28

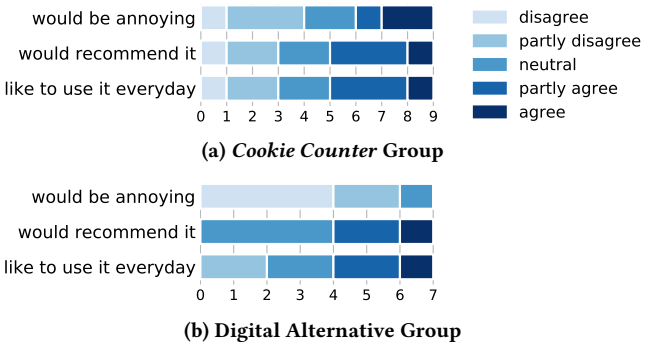
(b) Participants' IUIPC score.



(a) *Cookie Counter* Group

(b) Digital Alternative Group

Figure 5: We asked participants to rate the impact both prototypes had on their knowledge and awareness of browser cookies, and if they forgot to use them.



(a) *Cookie Counter* Group

(b) Digital Alternative Group

Figure 6: We asked participants to rate how they felt about potentially using the prototypes in their daily lives.

choosing "Reject all cookies" increased by one ($n = 5$). Similarly, before the study began, the most frequent choice in the digital alternative group was "Reject all cookies" ($n = 4$), followed by "Select cookies" ($n = 2$) and "Accept all cookies" ($n = 1$). After using the extension, the number of participants choosing "Reject all cookies" increased by one ($n = 5$).

6.2.3 Internet Users' Information Privacy Concerns (IUIPC-10). Participants in the digital alternative group showed higher IUIPC scores compared to participants in the *Cookie Counter* group before starting the user study. The pre- and post-study IUIPC scores of the *Cookie Counter* groups remained almost stable. In particular, we observed only slight increases and decreases of $|change| <= 0.20$ in the control and collection scores. The pre- and post-study scores of the digital alternative group, however, all showed a decrease in privacy concerns. In particular, the control and awareness scores showed small changes ($|change| <= 0.19$), but the collection score for this group decreased more strongly ($change = -0.5$).

6.3 User Experience & Usability

6.3.1 System Usability Scale (SUS) & Short User Experience Questionnaire (UEQ-S). Participants rated the system usability (SUS) of both prototypes similarly (*Cookie Counter*: *mean* = 74.17, digital alternative: *mean* = 77.14), which indicates that both prototypes have a "good" usability [3]. The user experience (UEQ-S) of the *Cookie Counter* was overall rated "above average" (*mean* = 1.03) [33]. Its pragmatic quality was rated with a score of *mean* = 1.53 and the hedonic quality with *mean* = 0.53 on a range from -3 to +3. The digital alternative received slightly higher overall UEQ-S scores, which nevertheless still fall into the "above average" category (*mean* = 1.20) as indicated by [33]. Its pragmatic quality ratings had a mean score of *mean* = 1.79, and its hedonic quality was rated *mean* = 0.61.

6.3.2 Additional Opinions. The final questionnaire included additional Likert-scale items about the prototypes' effects on participants' knowledge and cookie awareness, as well as their possible adaptation. Participants were neutral about being motivated to learn more about cookies or "Internet security" in the *Cookie Counter* condition ($median = 3$), while they partly agreed in the digital alternative condition ($median = 4$). They also partly agreed that they had learned something from both prototypes ($median = 4$) and agreed that the number of cookies displayed on the *Cookie Counter* was much higher than expected ($median = 5$) and were neutral for the digital alternative ($median = 3$).

Moreover, participants were neutral towards the *Cookie Counter* being annoying in everyday life ($median = 3$) and disagreed in the digital alternative ($median = 1$). Participants were neutral towards recommending both the *Cookie Counter* condition and the digital alternative condition to other people ($median = 3$) and towards still wanting to use any prototype in everyday life ($median = 3$). Finally, participants were neutral towards having often forgotten to use the *Cookie Counter* ($median = 3$) and slightly disagreed in the digital alternative ($median = 2$).

Mann-Whitney U tests showed that the *Cookie Counter* was perceived as significantly more annoying in everyday life ($U = 51.0$, $p = 0.042$). Moreover, the agreement to feeling the the number of cookies displayed was much higher than expected was also significantly larger for the *Cookie Counter* ($U = 51.5$, $p = 0.042$). The effect sizes as indicated by the rank-biserial correlation for both these comparisons were $r_{rb} = .62$.

6.4 Qualitative Feedback

6.4.1 Liked and Disliked Features. Participants of the *Cookie Counter* liked its ease of use ($n = 2$) and enjoyed the real-time feedback ($n = 2$). They also mentioned that the *Cookie Counter* raised awareness of the number of cookies used by certain websites ($n = 2$). Two participants were surprised by the large number of cookies ($n = 2$) and one enjoyed being able to delete cookies easily ($n = 1$). They criticized the *Cookie Counter* for taking up space ($n = 2$), being too large ($n = 1$), and not portable ($n = 1$). One participant disliked the automatic cookie deletion at the limit.

Participants found the digital alternative easy to use ($n = 2$) and liked that it enabled them to delete cookies easily ($n = 2$). Participants also enjoyed that it provides real-time feedback ($n = 1$) and that it *"raises awareness on how many sites are collecting information about"* (P19) them ($n = 1$). One participant also mentioned that they liked the option to set a cookie limit. However, participants also mentioned that loading websites in their browser took longer due to the extension ($n = 2$). One participant criticized that they had to revise the current number of cookies manually, as they could not see the number of cookies while using the browser, nor the limit warning. Another participant found the user interface design outdated and suggested relabeling the "delete cookies" button to "delete all cookies".

6.4.2 Allowlist Feature. Most participants in the *Cookie Counter* group did not use the allowlist function, explaining that they did not feel the need to do so ($n = 8$). The only participant who reported actively using the allowlist explained that they mostly used it to observe the domains in the drop-down menu, which was implemented so the user could select the domains they wanted to include on the allowlist and avoid being logged out. Most participants in the digital alternative felt they did not need the allowlist ($n = 3$) or did not understand its functionality ($n = 2$). One participant used it to avoid repeated logins on frequently visited websites.

6.4.3 Reasons for Deleting Cookies. Most users in both groups stated that they deleted cookies after reaching a certain number ($n_{Cookie\ Counter} = 5$, $n_{DigitalAlternative} = 3$). They also mentioned deleting cookies just to try the feature out ($n_{Cookie\ Counter} = 1$, $n_{DigitalAlternative} =$). Two participants in the *Cookie Counter* group felt that they did not need to delete cookies ($n = 2$). Two participants in the digital group deleted cookies after visiting certain websites ($n = 2$) and one wished to delete cookies from specific sites only.

6.4.4 Improvements of the Prototypes. When asked how the prototypes could be improved, participants of the *Cookie Counter* group mostly suggested fixing connectivity issues ($n = 4$). One participant wished to have a *Cookie Counter* for mobile devices. Another suggestion was to integrate the cookie count into the browser menu bar, so it's always visible.

One participant from the digital alternative groups suggested implementing an audio signal when the limit is reached. Another participant wished for a solution to prevent data collection rather than just showing the number of cookies.

6.5 Logged Data

6.5.1 Browsing Behavior. Participants in the *Cookie Counter* group browsed the web for $mean = 8.44$ days, and participants in the digital alternative group for $mean = 11.29$ of the 14 study days. Correspondingly, participants in the *Cookie Counter* group also visited fewer websites overall ($mean = 837.11$) than participants in the digital alternative group ($mean = 957.14$). Nevertheless, when accounting for different active days, the average number of visited websites per active day was similar between groups ($mean_{Cookie\ Counter} = 83.18$, $mean_{DigitalAlternative} = 81.39$), indicating comparable browsing behaviors.

6.5.2 Prototype Usage. While the average number of cookie deletions varied across groups, this was largely due to outliers (see Table 2). The median values of cookie deletions indicate comparable daily cookie deletions in both groups ($median_{Cookie\ Counter} = 0.36$, $median_{digital} = 0.5$). Participants of the digital alternative groups mostly triggered cookie deletions with higher counter values ($median = 468.85$, $mean = 505.27$, $std = 427.49$) compared to participants of the *Cookie Counter* group ($median = 206.80$, $mean = 293.12$, $std = 257.82$).

Most participants in both groups did not change the cookie limit from its default value (1000). Only two participants in the *Cookie Counter* group adapted the limit (one participant twice), and one participant in the digital alternative group did so. Changes to the allowlist were recorded from three participants in each group, with most varying between 2 and 5 changes. However, one participant in the *Cookie Counter* group made 18 changes to the allowlist, and another participant from the digital alternative group applied 406 changes to the allowlist. However, that participant did not specify why they used the function in the questionnaire.

Table 2: Datalogs indicating participants' daily usage of both prototypes during the user study (i.e., per active day).

	Cookie Counter			Digital Alternative		
	Cookie Deletion	Limit Changed	Allowlist Changed	Cookie Deletion	Limit Changed	Allowlist Changed
mean	0.57	0.05	0.73	3.58	0.02	4.95
std	0.75	0.10	1.98	5.85	0.04	12.74
median	0.36	0.00	0.00	0.50	0.00	0.00

7 DISCUSSION

We discuss our findings in the context of related work, along with our observations regarding the different design features and opportunities for future research.

7.1 RQ1: Impact on Concerns, Awareness and Choices

Participants in both our study groups started with high cookie awareness ratings and internet user privacy concerns scores. This may have resulted in ceiling effects and thus potentially limited measurable increases. We believe that the high initial awareness about browser cookies of our participants is likely rooted in the omnipresence of cookie banners.

We were, therefore, only able to observe small changes. In particular, participants' cookie banner choices of both groups shifted slightly toward more cautious choices. Moreover, while participants' IUIPC scores for the *Cookie Counter* groups remained overall mostly stable, we observed a slight decrease for the digital alternative group. This points at an interesting observation. We expected both prototypes to increase participants' awareness and concerns and to encourage more privacy-preserving choices. However, we observed contrary trends in some dimensions. In particular, participants' IUIPC scores in the collection dimension decreased, and responses to the statement about third parties using cookies to collect data shifted toward more (partly) disagree responses post-study in both groups. We believe that this observation might be rooted in participants' perceived increase in knowledge about cookies, which both groups reported in the final questionnaire. Related work has reported a similar effect, showing that legal and technical knowledge about cookies can reduce corresponding threat perceptions [36].

7.2 RQ2: Usage Behavior

The following observations should be treated as exploratory, given the variability of the behavioral data and the sample size. We did not observe large changes in usage behavior between groups. The logged daily cookie deletion frequencies of both groups showed high variability, but median daily deletions were similar between groups. Neither group used the software-based customization features much (i.e., allowlist and cookie limit). Correspondingly, participants' qualitative feedback indicated that the allowlist was often perceived as unnecessary or unclear. These exploratory findings indicate that the preference for purely digital solutions observed in the majority of the overall population in related lab studies [10, 11] does not necessarily translate into actual changes in usage behavior.

The most notable difference in participants' usage patterns between groups was that participants in the digital alternative group tended to delete cookies at higher cookie-count values (higher median and mean). This observation is consistent with participants from the *Cookie Counter* group being significantly more surprised about the high number of cookies and is probably rooted in the fact that the *Cookie Counter* provided the cookie count at a glance, while participants of the digital group had to open the extension's graphical interface to see the counter.

7.3 RQ3: User Perceptions

Both prototypes were perceived as having good usability and achieved above-average user experience ratings, with the digital alternative achieving slightly higher SUS and UEQ-S scores. This is consistent with the findings from Windl et al. [42]. Qualitative feedback suggests both versions were valued for ease of use and real-time feedback and control features. The *Cookie Counter* was criticized for occupying physical space and limited portability, which are typical challenges of TaPSI [12]. The digital alternative was criticized for performance slowdowns and reduced visibility during browsing (requiring the extension to be open to check values). Correspondingly, our findings also indicated that using the *Cookie Counter* in everyday life would be significantly more annoying compared to the digital alternative. The digital alternative was criticized for its reduced directness. The perception of both prototypes was also negatively impacted by technical issues (i.e., connection loss and slowdown of website loading).

7.4 Observations on our Design Features

While our study design does not permit isolating participants' perceptions of individual design features, it nevertheless enables us to discuss several interesting observations.

The *real-time information* our tangible interface provided *directly and persistently* to participants was noticed and appreciated. This suggests that the frequently discussed information communication benefits of TaPSI [2, 12, 29, 42] also hold true in the wild. However, we were not able to confirm the assumed benefit of TaPSIs to provide *direct and intuitive control* [2, 12, 29], as participants in both conditions made only limited use of the cookie deletion functionality. Further in-the-wild research is needed to assess whether this observation also applies to other TaPSIs addressing privacy or security issues beyond the deletion of persistent cookies. Similarly, most participants did not use the available *customization features* and reported not needing them. Nevertheless, we argue that providing such options remains valuable, as individual preferences may differ. This is reflected in the fact that, while the allowlist feature was used by only a few participants overall, it was used extensively by those who did engage with it. Regarding the *metaphoric appearance of our TaPSI*, the comparison study yielded few insights, as no participants commented on it. However, two participants in the formative lab trial explicitly stated that they liked the Cookie Monster design of the initial prototype.

7.5 Opportunities for Future Research

Our design focused on the accumulation of persistent cookies and the ability to delete them, thereby emphasizing their potential risks over their functional benefits. However, decisions about cookies inherently involve a tradeoff between utility (e.g., maintaining login states) and privacy. The *Cookie Counter* may have shaped participants' awareness toward the presence and amount of persistent cookies, without equally representing the benefits associated with cookies. Hence, future research could center this trade-off more clearly and, thus, support users better in making an informed choice when it comes to the management of persistent browser cookies.

Participants felt little need for customization features, which may stem from the privacy and security issue addressed by our TaPSI (i.e., persistent cookie management) or from the fact that we implemented customization mostly at the software level to ensure that both prototypes provide the same functionalities. *Hence, we believe that an opportunity for future research is to explore more tangible, hardware-based customization and personalization features.*

We also opted for a very primitive user interaction design, as our *Cookie Counter* was primarily developed to enable exploration of our research questions. This opens up the possibility for more sophisticated interactions in future research, such as *physically communicating the current cookie count (e.g., through movement) or enabling multiple control actions by the user (e.g., deleting all persistent cookies vs. only cookies from certain domains).*

We would also like to invite future researchers to replicate and compare our results with in the wild evaluations that measure the effects of *TaPSIs addressing other security and privacy challenges on security behaviors, concerns, and choices.*

8 CONCLUSION

We investigated the potential of Tangible Privacy and Security Interfaces (TaPSI) to support users' awareness and security-related behaviors in-the-wild. Using browser cookies as a frequently encountered topic, we designed and implemented a tangible cookie management interface grounded in design recommendations from prior research. We compared this tangible solution to a functionally equivalent digital alternative in a two-week in-the-wild study.

Our findings suggest that both the tangible interface and the digital alternative were perceived similarly in terms of usability and user experience, leading to only small changes in participants' reported awareness, privacy concerns, and cookie-related choices. However, the persistent and real-time physical display of the cookie count was positively noticed by participants and perceived as more surprising than the corresponding information provided by the digital alternative. At the same time, the tangible interface was seen as potentially more annoying in daily life.

Our work contributes empirical insights from one of the first in-the-wild comparisons of a purposefully designed TaPSI and a digital baseline. It thus refines existing assumptions about the unique benefits and challenges of tangible privacy and security interfaces by investigating them in an ecologically valid setting.

ACKNOWLEDGMENTS

We would like to thank Dominik Liesfeld, Egesa Vrapi and Timo Krapf for their efforts in developing the initial concept and implementation of the Cookie Counter. Moreover, we would like to thank all our study participants for their input. This project has been funded by the European Union – NextGeneration EU and the dtec.bw – Center for Digitization and Technology Research of the Bundeswehr (MuQuaNet and Voice of Wisdom).

REFERENCES

[1] Claudia Ziegler Acemyan, Philip Kortum, Jeffrey Xiong, and Dan S. Wallach. 2018. 2FA Might Be Secure, But It's Not Usable: A Summative Usability Assessment of Google's Two-factor Authentication (2FA) Methods. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 62, 1 (Sept. 2018), 1141–1145. https://doi.org/10.1177/1541931218621262 Publisher: SAGE Publications Inc.

[2] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J. Lee. 2020. Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy. *Proc. ACM Hum.-Comput. Interact.* 4, CSCW2 (Oct. 2020), 116:1–116:28. https://doi.org/10.1145/3415187

[3] Aaron Bangor, Philip Kortum, and James Miller. 2009. Determining what individual SUS scores mean: adding an adjective rating scale. *J. Usability Studies* 4, 3 (May 2009), 114–123.

[4] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101. https://doi.org/10.1191/1478088706qp063oa

[5] John Brooke. 1996. *SUS – a quick and dirty usability scale.* Taylor & Francis, 189–194.

[6] 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

[7] Varun Chandrasekaran, Suman Banerjee, Bilge Mutlu, and Kassem Fawaz. 2021. PowerCut and Obfuscator: An Exploration of the Design Space for Privacy-Preserving Interventions for Smart Speakers. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, 535–552. https://www.usenix.org/conference/soups2021/presentation/chandrasekaran

[8] Lorrie Faith Cranor. 2022. Cookie monster. *Commun. ACM* 65, 7 (June 2022), 30–32. https://doi.org/10.1145/3538639

[9] Sarah Delgado Rodriguez, Sarah Elisabeth Winterberg, Franziska Bumiller, Felix Dietz, Florian Alt, and Mariam Hassib. 2025. XSec Companions: Exploring the Design of Cybersecurity Companions. In *2025 European Symposium on Usable Security (EuroUSEC)*. 204–220. https://doi.org/10.1109/EuroUSEC69254.2025.00028

[10] Sarah Delgado Rodriguez, Sarah Prange, Lukas Mecke, and Florian Alt. 2024. Act2Auth – A Novel Authentication Concept based on Embedded Tangible Interaction at Desks. In *Proceedings of the Eighteenth International Conference on Tangible, Embedded, and Embodied Interaction* (Cork, Ireland) *(TEI '24)*. Association for Computing Machinery, New York, NY, USA, Article 12, 15 pages. https://doi.org/10.1145/3623509.3633360

[11] Sarah Delgado Rodriguez, Sarah Prange, Christina Vergara Ossenberg, Markus Henkel, Florian Alt, and Karola Marky. 2022. PriKey – Investigating Tangible Privacy Control for Smart Home Inhabitants and Visitors. In *Nordic Human-Computer Interaction Conference (NordiCHI '22)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3546155.3546640

[12] Sarah Delgado Rodriguez, Maximiliane Windl, Florian Alt, and Karola Marky. 2025. The TaPSI Research Framework - A Systematization of Knowledge on Tangible Privacy and Security Interfaces. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25)*. Association for Computing Machinery, New York, NY, USA, Article 923, 28 pages. https://doi.org/10.1145/3706598.3713968

[13] Verena Distler, Matthias Fassl, Hana Habib, Katharina Krombholz, Gabriele Lenzini, Carine Lallemand, Lorrie Faith Cranor, and Vincent Koenig. 2021. A Systematic Literature Review of Empirical Methods and Risk Representation in Usable Privacy and Security Research. *ACM Trans. Comput.-Hum. Interact.* 28, 6, Article 43 (Dec. 2021), 50 pages. https://doi.org/10.1145/3469845

[14] Youngwook Do, Nivedita Arora, Ali Mirzazadeh, Injoo Moon, Eryue Xu, Zhihan Zhang, Gregory D. Abowd, and Sauvik Das. 2023. Powering for Privacy: Improving User Trust in Smart Speaker Microphones with Intentional Powering and Perceptible Assurance. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, 2473–2490. https://www.usenix.org/conference/usenixsecurity23/presentation/do

[15] Youngwook Do, Jung Wook Park, Yuxi Wu, Avinandan Basu, Dingtian Zhang, Gregory D. Abowd, and Sauvik Das. 2022. Smart Webcam Cover: Exploring the Design of an Intelligent Webcam Cover to Improve Usability and Trust. *Proc.*

ACM Interact. Mob. Wearable Ubiquitous Technol. 5, 4, Article 154 (Dec. 2022), 21 pages. https://doi.org/10.1145/3494983

[16] Youngwook Do, Yuxi Wu, Gregory D Abowd, and Sauvik Das. 2026. Physically-intuitive Privacy and Security: A Design Paradigm for Building User Trust in Smart Sensing Environments. *arXiv preprint arXiv:2604.00312* (2026).

[17] Thomas Franke, Christiane Attig, and Daniel Wessel. 2019. A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) Scale. *International Journal of Human–Computer Interaction* 35, 6 (2019), 456–467. https://doi.org/10.1080/10447318.2018.1456150

[18] Nor Anisah Amir Hamzah, Anis Safiyyah Adnan, and Norsaremah Salleh. 2025. Exploring cookies vulnerabilities: awareness, privacy risks and exploitation. *International Journal of Electrical and Computer Engineering (IJECE)* 15, 6 (2025), 5792–5803. https://doi.org/10.11591/ijece.v15i6.pp5792-5803

[19] Philip Hausner and Michael Gertz. 2021. Dark patterns in the interaction with cookie banners. *arXiv preprint arXiv:2103.14956* (2021). https://doi.org/10.48550/arXiv.2103.14956

[20] Nari Kim, Juntae Kim, Bomin Kim, and Young-Woo Park. 2021. The Trial of Posit in Shared Offices: Controlling Disclosure Levels of Schedule Data for Privacy by Changing the Placement of a Personal Interactive Calendar. In *Proceedings of the 2021 ACM Designing Interactive Systems Conference* (Virtual Event, USA) *(DIS '21)*. Association for Computing Machinery, New York, NY, USA, 149–159. https://doi.org/10.1145/3461778.3462073

[21] Michael Kretschmer, Jan Pennekamp, and Klaus Wehrle. 2021. Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web. *ACM Trans. Web* 15, 4, Article 20 (July 2021), 42 pages. https://doi.org/10.1145/3466722

[22] Chiara Krisam, Heike Dietmann, Melanie Volkamer, and Oksana Kulyk. 2021. Dark Patterns in the Wild: Review of Cookie Disclaimer Designs on Top 500 German Websites. In *Proceedings of the 2021 European Symposium on Usable Security* (Karlsruhe, Germany) *(EuroUSEC '21)*. Association for Computing Machinery, New York, NY, USA, 1–8. https://doi.org/10.1145/3481357.3481516

[23] Kat Krol, Eleni Philippou, Emiliano De Cristofaro, and Angela Sasse. [n. d.]. "They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking. https://www.ndss-symposium.org/ndss2015/ndss-2015-usec-programme/they-brought-horrible-key-ring-thing-analysing-usability-two-factor-authentication-uk-online/

[24] Bettina Laugwitz, Theo Held, and Martin Schrepp. 2008. Construction and evaluation of a user experience questionnaire. In *Symposium of the Austrian HCI and usability engineering group*. Springer, 63–76. https://doi.org/10.1007/978-3-540-89350-9_6

[25] Victor Le Pochat, Tom Van Goethem, Samaneh Tajalizadehkhoob, Maciej Korczyński, and Wouter Joosen. 2019. Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation. In *Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS 2019)*. https://doi.org/10.14722/ndss.2019.23386

[26] 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. https://doi.org/10.1287/isre.1040.0032

[27] 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* (1947), 50–60.

[28] Karola Marky, Martin Schmitz, Verena Zimmermann, Martin Herbers, Kai Kunze, and Max Mühlhäuser. 2020. 3D-Auth: Two-Factor Authentication with Personalized 3D-Printed Items. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376189

[29] Vikram Mehta, Daniel Gooch, Arosha Bandara, Blaine Price, and Bashar Nuseibeh. 2021. Privacy Care: A Tangible Interaction Framework for Privacy Management. *ACM Trans. Internet Technol.* 21, 1, Article 25 (Feb. 2021), 32 pages. https://doi.org/10.1145/3430506

[30] Ryo Minakawa and Tetsuji Takada. 2017. Exploring alternative security warning dialog for attracting user attention: evaluation of "Kawaii" effect and its additional stimulus combination. In *Proceedings of the 19th International Conference on Information Integration and Web-based Applications & Services (iiWAS '17)*. Association for Computing Machinery, New York, NY, USA, 582–586. https://doi.org/10.1145/3151759.3151846

[31] Nadim Nachar et al. 2008. The Mann-Whitney U: A test for assessing whether two independent samples come from the same distribution. *Tutorials in quantitative Methods for Psychology* 4, 1 (2008), 13–20.

[32] Ken Reese, Trevor Smith, Jonathan Dutson, Jonathan Armknecht, Jacob Cameron, and Kent Seamons. 2019. A Usability Study of Five {Two-Factor} Authentication Methods. 357–370. https://www.usenix.org/conference/soups2019/presentation/reese

[33] Martin Schrepp, Andreas Hinderks, and Jörg Thomaschewski. 2014. Applying the User Experience Questionnaire (UEQ) in Different Evaluation Scenarios. In *Design, User Experience, and Usability. Theories, Methods, and Tools for Designing the User Experience (Lecture Notes in Computer Science, Vol. 8517)*, Aaron Marcus (Ed.). Springer International Publishing, Cham, USA, 383–392. https://doi.org/10.1007/978-3-319-07668-3_37

[34] Sujay Shalawadi, Katrina Hvítklett, Anna Stentoft Ries, Aisho Mohamed Ali, and Florian Echtler. 2026. DataCrumb: A Physical Probe for Reflecting on Background Web Tracking. In *Proceedings of the Twentieth International Conference on Tangible, Embedded, and Embodied Interaction* (Chicago, IL, USA) *(TEI '26)*. Association for Computing Machinery, New York, NY, USA, Article 39, 11 pages. https://doi.org/10.1145/3731459.3773336

[35] Andreas Sotirakopoulos, Kirstie Hawkey, and Konstantin Beznosov. 2011. On the challenges in usable security lab studies: lessons learned from replicating a study on SSL warnings. In *Proceedings of the Seventh Symposium on Usable Privacy and Security* (Pittsburgh, Pennsylvania) *(SOUPS '11)*. Association for Computing Machinery, New York, NY, USA, Article 3, 18 pages. https://doi.org/10.1145/2078827.2078831

[36] Joanna Strycharz, Edith Smit, Natali Helberger, and Guda van Noort. 2021. No to cookies: Empowering impact of technical and legal knowledge on rejecting tracking cookies. *Computers in Human Behavior* 120 (2021), 106750. https://doi.org/10.1016/j.chb.2021.106750

[37] Andrew F. Tappenden and James Miller. 2009. Cookies: A deployment study and the testing implications. *ACM Trans. Web* 3, 3, Article 9 (July 2009), 49 pages. https://doi.org/10.1145/1541822.1541824

[38] Jessica J Thill. 2000. The Cookie Monster: From Sesame Street to Your Hard Drive. *SCL Rev.* 52 (2000), 921. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/sclr52&section=45

[39] Pierre Tholoniat, Kelly Kostopoulou, Peter McNeely, Prabhpreet Singh Sodhi, Anirudh Varanasi, Benjamin Case, Asaf Cidon, Roxana Geambasu, and Mathias Lécuyer. 2024. Cookie Monster: Efficient On-Device Budgeting for Differentially-Private Ad-Measurement Systems. In *Proceedings of the ACM SIGOPS 30th Symposium on Operating Systems Principles* (Austin, TX, USA) *(SOSP '24)*. Association for Computing Machinery, New York, NY, USA, 693–708. https://doi.org/10.1145/3694715.3695965

[40] Catherine S. Weir, Gary Douglas, Tim Richardson, and Mervyn Jack. 2010. Usable security: User preferences for authentication methods in eBanking and the effects of experience. *Interacting with Computers* 22, 3 (May 2010), 153–164. https://doi.org/10.1016/j.intcom.2009.10.001 Conference Name: Interacting with Computers.

[41] Margaret Wilson. 2002. Six views of embodied cognition. *Psychonomic Bulletin & Review* 9, 4 (December 2002), 625—636. https://doi.org/10.3758/bf03196322

[42] Maximiliane Windl, Alexander Hiesinger, Robin Welsch, Albrecht Schmidt, and Sebastian S. Feger. 2022. SaferHome: Interactive Physical and Digital Smart Home Dashboards for Communicating Privacy Assessments to Owners and Bystanders. *Proc. ACM Hum.-Comput. Interact.* 6, ISS (Nov. 2022), 586:680–586:699. https://doi.org/10.1145/3567739

A LAB TRIAL: DEMOGRAPHICS AND USAGE LOGS

	Age	Gender	Job Field	Daily Browser Usage	Daily Private Browsing	Cookie Deletions
T1	28	m	Civil Engineering	7h	2h	9
T2	28	f	Human Resources	12h	3h	6
T3	28	f	Law	8h	1h	1
T4	27	m	Research	12h	1h	11
T5	28	f	Education	2.5h	2h	7
T6	28	f	Law Enforcement	8h	2h	9
			Average	**8.25**	**1.83**	**7.17**

Table 3: Demographics and *Cookie Counter* usage logs per participant of our lab trial.

B LIST OF WEBSITE CATEGORIES

- Social media & Communication
- Shopping & E-Commerce
- News, Information
- Entertainment & Streaming
- Search & Portals
- Productivity & Professional

- Finance & Legal
- Health & Wellbeing
- Travel, Dining & Booking
- Government & Education
- Technical/Infrastructure & Utilities
- Local/Browser
- Other

C ADDITIONAL DEMOGRAPHICS OF IN-THE-WILD STUDY PARTICIPANTS

Group	Mean	SD	Min - Max
Cookie Counter	34.78	16.99	21-58
Digital Alternative	37.00	18.79	21-66
All	35.75	17.22	21-66

(a) Participants' Age

Field of Work	*Cookie Counter*	Digital	All
Technology, IT & Engineering	2	2	4
Art, media & culture	2	0	2
Trade, service & gastronomy	1	1	2
Administration, Law & Finance	0	1	1
Production, construction & logistics	2	1	3
None	2	2	4

(b) Participants' Field of Work

Table 4: These tables provide an overview of the age and field of work of the 16 participants in our in the wild study.

D CATEGORIES OF WEBSITES VISITED DURING THE IN THE WILD-STUDY

Cookie Counter Website Category	Visits	Digital Alternative Website Category	Visits
Other	3632	Other	1867
Search & Portals	1316	Entertainment & Streaming	1478
Shopping & E-Commerce	728	Search & Portals	1061
Travel, Dining & Booking	509	Local & Browser	659
Local & Browser	301	Shopping & E-Commerce	493
Entertainment & Streaming	268	Social Media & Communication	307
Government & Education	241	News & Information	222
News & Information	164	Productivity & Professional	203
Productivity & Professional	157	Government & Education	117
Social Media & Communication	125	Travel, Dining & Booking	93
Finance & Legal	40	Finance & Legal	82
Health & Wellbeing	26	Health & Wellbeing	3
		Technical/Infrastructure & Utilities	2

Table 5: Logged visits per website category.

E SUPPLEMENTARY MATERIAL

Please note that you can find additional visual representations of our prototypes and the content of the German version of our study questionnaire in the supplementary materials.