Analyzing Societal Awareness and Perception of Digital Fingerprinting and Fingerprinting Countermeasures

Pascal Schramm
Technical University of Munich
pascal.schramm@tum.de

Emmanuel Syrmoudis
Technical University of Munich
emmanuel.syrmoudis@tum.de

Alexandros Markou
Technical University of Munich
alexandros.markou@tum.de

Jens Grossklags
Technical University of Munich
jens.grossklags@in.tum.de

Abstract

We explore societal awareness and perceptions related to digital fingerprinting, a stateless tracking technology increasingly used for online security, advertising, and fraud prevention, as well as to countermeasures designed to mitigate its impact. Despite its widespread application, user awareness of fingerprinting remains significantly lower compared to other tracking mechanisms, such as third-party cookies. To deepen our understanding of user perceptions, we conducted a study surveying 734 participants to assess their knowledge of fingerprinting, acceptance of its use across different applications (cybersecurity, law enforcement, user experience), and their reactions to browsing inconveniences introduced by countermeasures. Countermeasures examined include privacy-focused browsers (e.g., Tor), browser extensions, and spoofing tools. While these solutions vary in effectiveness, they often compromise usability, resulting in issues such as website breakages and prolonged CAPTCHA challenges. Privacy-conscious users demonstrated greater tolerance for such disruptions, whereas others prioritized convenience over protection.

Keywords

digital fingerprinting, browser fingerprinting, user perceptions, countermeasures

1 Introduction

In recent years, awareness about cookies and how to protect against them has grown among internet users, as a study from 2021 by Eurostat showed [17]. According to the survey, 80% of EU respondents were aware of cookies and their potential to track people's online activities. However, only slightly more than one third of those surveyed claimed to have changed their browser settings to limit the use of cookies, and even fewer used software tools to limit or block their effectiveness. After the introduction of the General Data Protection Regulation (GDPR) [63], websites using cookies are required to explicitly state the purposes for which cookies are used, and users must have the option to opt out. Additionally, commonly used browsers, such as Safari, Google Chrome, Mozilla Firefox, and Microsoft Edge, now block *third-party cookies* by default or offer tracking prevention settings to allow users to reduce their traceability on the Web [51]. The environment provided by browsers, combined with third-party cookie blockers like browser extensions, therefore, offers a wide range of relatively effective countermeasures against user tracking by cookies.

While cookies are considered to be a *stateful* tracking technology, digital fingerprinting, commonly also referred to as browser and device fingerprinting, exhibits *stateless* characteristics and, among others, uses information about the user's browser, installed plugins, fonts, and even the device's hardware and operating system specifications. Digital fingerprinting can identify users and their devices with an accuracy comparable to a biometric fingerprint used to identify humans, as Eckersley demonstrated already in 2010 [15].

Fingerprinting prevalence across the web has grown over recent years [24, 37], with applications of the tracking method ranging from cross-site tracking to enhance advertisement targeting to cyber-security mechanisms like bot detection or fraud prevention [35]. In particular, the tracking capabilities of digital fingerprinting also triggered the desire of technically capable users to better protect themselves, leading to various countermeasures against the new tracking method. They range from using multiple browsers and browser extensions, limiting JavaScript APIs, to using dedicated privacy browsers like Brave or Tor. While most countermeasures offer no comprehensive protection against fingerprinting, they also come with varying usability costs and loss of convenience during web browsing [41]. For example, frequent website breakages, infinitely repeated CAPTCHAs, and other forms of decreased usability were partly responsible for the removal of Brave's strict fingerprinting protection mode in January 2024 [7].

Current research about digital fingerprinting mainly covers the technical side of the identification technology [33, 39], limitations of countermeasures [41], and analysis of its spread on the web [18, 24, 39]. We are only aware of two studies [4, 57] providing initial insights into user perspectives regarding digital fingerprinting.

Drawing on the results of a survey study with 734 participants, our work explores, in more depth, how aware users are of digital fingerprinting and how they perceive the tracking technology and the available countermeasures. It is important to note that already Eckersley highlighted the potential of fingerprinting as a tracking mechanism that leaves no trace on the user's machine, leading to potential unawareness of the technology by users [15]. Therefore, our survey explores user awareness regarding digital fingerprinting in comparison to cookies. Further, we make use of concrete scenarios to examine users' perceptions and acceptance of different

Proceedings on Privacy Enhancing Technologies 2026(2), 397–435

https://doi.org/10.56553/popets-2026-0054

fingerprinting applications, and how users react to situations where they are confronted with a decreased browsing experience due to fingerprinting countermeasures. To that end, we formulated the following research questions:

- **RQ1** How aware are users of digital fingerprinting?
- **RQ2** How does user acceptance of digital fingerprinting differ depending on the purpose of the digital fingerprinting application?
- **RQ3** How do users react to inconveniences caused by countermeasures against digital fingerprinting?

We conducted a mixed-method online study with participants recruited via the Prolific[1] crowdwork platform and university students to answer the stated research questions. Prolific participants came from English-speaking countries (United Kingdom and United States), and the university students were recruited from a German university independent of their nationality.

Our work is the first large survey study covering in detail user perceptions (including awareness and acceptance) of digital fingerprinting countermeasures, situating users in scenarios where they decide to maintain or deactivate a fingerprinting countermeasure. The findings indicate that privacy-protecting behaviors are related to awareness of tracking technologies, while online privacy concerns and attitudes are related to the acceptability of fingerprinting. We explored responses to fingerprinting that are specific to the different application contexts, while also identifying common concerns, views, and perceptions.

The remainder of the paper is structured as follows: First, we situate our research within the literature, followed by a detailed description of the study design and deployment. We then present the results of the data analysis to answer our research questions. Finally, we discuss our findings and their potential implications.

2 Background and Related Work

In our work, we investigate user awareness and acceptance of digital fingerprinting, and further explore how users perceive the limitations of potential fingerprinting countermeasures. Below, we position our study within the existing literature on these topics.

2.1 Digital fingerprinting

In RFC 6973, Cooper et al. [10] define the term *fingerprint* as "a set of information elements that identifies a device or application instance" and *fingerprinting* as the "process of an observer or attacker uniquely identifying a device or application instance based on multiple information elements communicated to the observer or attacker" [10]. Digital fingerprinting can be split into the concepts *browser fingerprinting* and *device fingerprinting*.

Browser fingerprinting describes the process of a browser divulging information about its version, the operating system running on the machine, IP address, and further information necessary for the HTTP communication with the website. This process is known as *passive fingerprinting* since it happens instantly when an HTTP connection is established over the TCP/IP protocol. This is contrary to *active fingerprinting*, where attributes require "active discovery through a script or plugin" [43]. Properties such as supported data types (MIME types), hardware information, installed fonts, and screen resolution must be actively gathered by the website deploying fingerprinting [1].

For example, a website can probe specific JavaScript attributes or use JavaScript APIs to acquire hash strings that represent the underlying hardware features of the user's machine [16]. This procedure is called *device fingerprinting*. When such device characteristics are combined with the gathered information about the user's browser, the device can be identified with high accuracy. Commonly collected attributes include screen resolution, system fonts, time zone, and language settings. Device-specific information, such as GPU configuration and audio processing characteristics, accessed via APIs like WebGL or Canvas, can further enrich the process.

Browser and device fingerprinting can serve diverse purposes, from user tracking to enhancing online security. Laperdrix et al. highlight two primary categories of use: negative applications, such as unauthorized tracking or exploiting device vulnerabilities, and positive applications, like identifying outdated devices, fraud prevention, or bot detection [35]. For instance, fingerprinting supports paywall enforcement by identifying enrolled users [54] and enables web tracking without relying on cookies [15]. While attackers exploit device vulnerabilities to deploy targeted payloads, system administrators use similar techniques to detect and patch outdated components, ensuring network security [35]. Fingerprinting also aids in fraud detection by identifying mismatched attributes in spoofed devices [58, 64] and strengthens authentication systems by verifying device attributes during login [3]. Despite its potential for misuse, prior research highlights the dual-edged nature of fingerprinting, illustrating its capacity to undermine or improve user privacy and security.

Research documented the increasing prevalence of browser fingerprinting across the web. Fietkau et al. [18] analyzed the top 10,000 Alexa websites in 2021 using their tool FPMON and revealed that 19% employed heavily obfuscated fingerprinting scripts, with canvas fingerprinting notably prevalent. They also found that 28% of these websites collected substantial user device data, often exceeding what is necessary for regular interaction. Iqbal et al. developed FP-Inspector, a machine-learning-based tool that identifies fingerprinting scripts with high accuracy [24]. Their study showed that over 10% of the top 100,000 Alexa websites used fingerprinting, particularly on news and shopping sites, driven by targeted advertising and anti-fraud services. They also mentioned that fingerprinting has become more popular than cookies for advertising or paywall enforcement, highlighting the growing adoption of fingerprinting on the web. Providing further evidence for these trends, Li et al. [39] discovered that 66.6% of the top 10,000 TRANCO websites [37] transmitted fingerprinting data. As such, prior work highlights the pervasive nature of fingerprinting and its evolution as a tracking technique and security improvement measure.

There are no user surveys that focus primarily on digital fingerprinting applications and countermeasures. The most relevant prior work is a study by Pugliese et al. [57]. Over three years, they collected digital fingerprinting data from a self-selected group of participants, who were also invited to complete two brief optional surveys. The first survey, distributed at registration, gathered information on demographics, technical background, and privacy tool usage, while a follow-up survey nearly two years later asked

[1] www.prolific.com

about participants' awareness, concerns, and self-reported actions regarding fingerprinting.

The study's participant base was predominantly male, based in Germany, and had a strong representation of individuals with computer science experience and frequent privacy tool use. Analysis of the fingerprinting data and survey responses suggested that demographic and behavioral factors had only a marginal effect on long-term trackability. The follow-up survey revealed that most participants were already familiar with browser fingerprinting and expressed concern about it, but many felt they had limited ability to effectively protect themselves. While many had adopted privacy tools, the study did not provide a detailed assessment of countermeasure adoption or usability barriers. Instead, it highlighted persistent concerns and a sense of resignation even among privacy-sensitive users, who often perceived existing protections as insufficient or impractical for everyday use.

Another recent research project has also collected fingerprinting data associated with real web browsing behavior of users, revealing a more nuanced understanding of fingerprinting practices [52], but the authors did not collect data about user perceptions.

Berke et al. [4] analyze a dataset linking browser attributes with user demographics derived from survey responses from 8,400 US participants. Their findings suggest that fingerprinting risk is not uniform across users, it increases with age and decreases with income. The authors also showed that sensitive user information (including gender, age, and income) can be accurately predicted from browser attributes alone using machine learning.

2.2 Existing countermeasures and their limitations

Browser fingerprinting countermeasures have been studied in prior research, with a focus on their effectiveness and limitations. Unlike third-party cookies, which are often blocked by default in modern browsers, fingerprinting remains a more resilient tracking method due to its stateless nature and reliance on browser and device attributes rather than stored data [24, 69]. Iqbal et al. also highlighted browser vendors' hesitancy to implement robust built-in countermeasures because of potential web breakages caused by restricting JavaScript APIs [24].

Several countermeasures exist: **Blocking extensions** such as No-Script, Ghostery, and Privacy Badger primarily target JavaScript-based trackers. These tools can block canvas fingerprinting and other tracking scripts but are not explicitly designed to combat fingerprinting, resulting in limited effectiveness. Merzdovnik et al. noted that these tools often fail to block sophisticated fingerprinting scripts and may break website functionalities [41, 46]. More specialized tools like Canvas Defender disrupt the consistency of canvas fingerprints by adding noise to the HTML5 Canvas API. Still, they remain a partial solution as they do not address other fingerprinting methods that rely on hardware attributes, WebGL, or browser configurations. Moreover, their effectiveness diminishes when combined with broader tracking mechanisms, as fingerprinting scripts can aggregate data from multiple sources to form a composite identifier [35, 50].

Spoofing extensions offer an alternative by altering HTTP header values and JavaScript attributes, such as user-agent strings and time zones, to obscure the user's identity. However, these measures can backfire, increasing a user's uniqueness due to inconsistencies between spoofed values and actual device attributes [15, 28, 36]. Spoofing extensions can degrade website functionality, making user experiences less convenient due to overlapping website layouts, less readable fonts, or even misclassification as a potential bot [41, 61].

Privacy-focused browsers, such as Tor and Brave, represent more robust solutions. The Tor browser standardizes configurations across users, significantly reducing fingerprint uniqueness. However, deviations from its default settings can undermine its effectiveness, including deviating from the standard browser window size. Furthermore, Tor users face significant usability challenges, including slower browsing speeds, access restrictions, and limited website functionality [29, 34]. Additionally, convenient browsing functionalities like auto-fill or saved passwords are unavailable [41]. Brave's built-in fingerprinting protection, which included a strict mode for enhanced defense, was eventually discontinued in early 2024 due to low adoption and frequent web breakages [6, 7].

Information paradox: The information paradox in the context of digital fingerprinting is that measures meant to hide you can actually make you stand out if few people use them [15]. Eckersley [15] noted that many potential privacy measures (like spoofing or blocking features) only work when a lot of users share them; otherwise the countermeasure itself becomes a unique marker and contributes to a distinct fingerprint. A user trying to block fingerprinting may end up with a new, potentially unusual or rare, combination of attributes that can increase entropy instead of reducing it [15]. A concrete example is Tor Browser's attempt to bucket screen sizes. Tor locks windows to 200×100px steps and adds margins (letterboxing) to force every user into a few sizes. But if a monitor or screen size is uncommon and the user decides to maximize the screen then the resulting fingerprint may be very distinct [34, 62].

2.3 Studies on privacy vs. convenience

Prior studies explored the balance between economic utility and privacy in personalizing online services. Krause and Horvitz [30] introduced utility-theoretic methods to quantify the costs of sharing personal data against the benefits of personalization. Their algorithm for finding near-optimal trade-off solutions was evaluated using real-world search data and a user study involving over 1,400 participants. The study revealed that most participants were willing to share personal information in exchange for tangible benefits such as enhanced service efficiency. This finding parallels Acquisti and Grossklags' earlier work, demonstrating that users often sacrifice privacy for short-term convenience or utility gains [2]. These insights are relevant when considering the usability costs introduced by countermeasures against digital fingerprinting, as users may weigh such costs against their perceived privacy benefits.

A survey by Gao et al. [20] from 2014 studied people's understanding of private browsing modes. Of the 200 participants, many reported that private browsing increases personal privacy by not saving the browsing history, and some falsely assumed that the private browsing mode restricts all kinds of data collection from websites. Some respondents criticized that, like the Tor browser, no sign-in information is stored in private browsing mode, and they claimed some browsing functions, like specific plugins, did

not work correctly. Similarly, Ha et al. [22] investigated user understanding of cookies through focus groups segmented by age and technical familiarity. They found that misconceptions about cookies were widespread, and users prioritized browsing convenience over privacy, with younger participants especially resistant to the perceived effort required to manage cookies.

Nisenoff et al. [53] mapped and characterized breakage of non-ad/non-tracking website elements (e.g., missing images or non-functional buttons) caused by blocking tools. By analyzing public reviews and issue reports as well as the data from a small survey study, the authors illustrate the diversity of breakage issues and mitigation strategies by users.

Complementing prior technical work, our survey explicitly focuses on the user experience aspects of digital fingerprinting and of countermeasures against it. For instance, we confronted participants with concrete scenarios, where they were asked to react to specific countermeasure inconveniences and browsing disruptions and then indicate their likely behavior in each situation.

3 Method

To address the research questions raised in Section 1, we conducted an online questionnaire that we distributed to two batches of participants. The first batch consisted of participants from Prolific sourced from the United Kingdom and the United States. The second batch consisted of students at a German university. The subsequent subsections detail the questionnaire design, recruitment process, sample characteristics, and data analysis methodology.

3.1 Questionnaire

We first presented potential participants with information about the study. Those who consented and committed to answering attentively could proceed with the survey [21]. An additional check at the end asked participants to confirm their level of focus and active participation during the survey. Before informing the participants about the main topic of the survey, digital fingerprinting, we asked them about various security-related and privacy-related technologies they may have previously used or encountered. This was inspired by the *Privacy Behavior Index* introduced by Pugliese et al. [57] to measure an individual's privacy behavior on the web. Each participant gets an index represented by a positive integer (0 - 7), indicating the number of privacy measures previously undertaken by the participant. The *Westin Index* was used to measure participants' privacy concerns [31]. Milne et al. [48] found that privacy concern levels strongly predicted behaviors like falsifying information, refusing disclosure, or removing personal data [71]. Participants rated three statements on a five-point Likert scale, from "Strongly disagree" to "Strongly agree," with "Neither agree nor disagree" as the neutral option.

3.1.1 Awareness of tracking technologies. Our next step was to examine the participants' awareness of relevant tracking technologies, i.e., cookies and digital fingerprinting. Both questions were identically worded, offering four hierarchical options. These ranged from not knowing the respective tracking technology to being aware of it and actively using countermeasures against cookies or fingerprinting. Additionally, participants with a high awareness of fingerprinting (third or fourth level) were asked to select all applications of digital fingerprinting they were familiar with and provide further applications if they knew any.

3.1.2 Participant briefing on fingerprinting. To proceed with the survey, it was essential to ensure that participants had a basic understanding of digital fingerprinting and its potential to reveal information about them. A brief informational text was provided, offering an overview of fingerprinting, its applications, and the challenges associated with protecting against it. The explanation was designed to be accessible, avoiding technical wording, to give participants with no prior knowledge a general understanding of the concept. We wrote this description based on information from reputable online sources for privacy, including the Electronic Frontier Foundation (EFF)[2]. In the text, we used simple language and concrete examples on fingerprinting applications. We aimed to avoid tech-heavy jargon. We confirmed participants' understanding of the concepts with a knowledge assessment requiring them to select the three correct statements about digital fingerprinting from the five we listed.

3.1.3 Fingerprinting acceptance. In the next section of the questionnaire, users were presented with three areas of application of digital fingerprinting in a random order:

- *Cybersecurity*: Fingerprinting applications focusing on protecting users' online security
- *Law enforcement*: Fingerprinting as a tool to improve the effectiveness of their investigations and public safety efforts
- *User experience*: Fingerprinting applications to enrich the user experience

Each application area included six potential scenarios (e.g., prevention of online fraud, accelerated logins, and enforcing paywalls) within its scope and an open-ended question. The scenarios were derived from real-world fingerprinting applications or hypothetical fingerprinting applications implied through the technology's capabilities. For the area of cybersecurity, for instance, we asked the participants about their acceptance of fingerprinting if it is being used to prevent online fraud [26]. In the law enforcement area, we used advances in digital forensics with the help of device fingerprinting [65]; here the participants were asked about several applications of fingerprinting to support investigations or cybercrime forensics/prevention. User experience had scenarios mostly focusing on faster and better browsing experience, enhanced logins with accelerated CAPTCHA, and tailored online experiences, but also more direct applications of fingerprinting, such as online dating [12]. We selected six scenarios — including a few similar items — to capture more granular aspects of fingerprinting within each application domain while avoiding respondent overload. Each scenario was chosen to be realistic, simple, and familiar to participants.

Participants were asked to indicate their level of acceptance for the six scenarios involving the processing of their own fingerprint using a five-point Likert scale. Furthermore, in an open-ended question, participants were asked to share their thoughts on whether they trust the entity processing their digital fingerprint. This provided insight into users' concerns regarding fingerprint processing,

[2] https://coveryourtracks.eff.org/learn

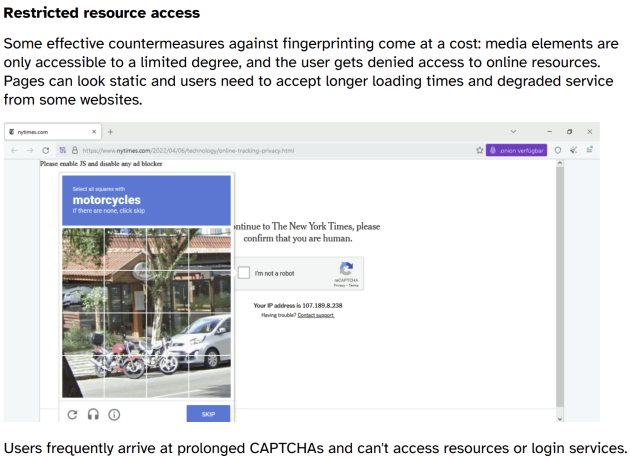


Figure 1: Example scenario – frequent display of CAPTCHAs

taking into account the specific entity involved, as well as the context and purpose of the fingerprinting.

3.1.4 Fingerprinting countermeasures. The next part of the survey explored the user perspective on fingerprinting countermeasures. An additional three-paragraph explanation was included to address the absence of countermeasures and their limitations in the earlier description of fingerprinting. This text provided participants with a brief overview of fingerprinting countermeasures, highlighting their potential to reduce user experience and introducing the *information paradox*, which suggests that specific countermeasures can potentially make a user more identifiable [15] (described in Section 2.1). We selected three fingerprinting countermeasures and presented scenarios of how the respective countermeasure could potentially decrease the browser's functionality and user experience. These countermeasures were the Tor Browser fingerprinting protection, Brave's strict fingerprinting protection method (now deprecated [7]), and lastly, browser extensions spoofing HTTP header values to decrease fingerprinting effectiveness. For each countermeasure, one specific scenario was directly presented in the survey, and a screenshot served as a point of reference for the upcoming scenarios (see Figure 1 for an example). The participants then had to decide whether they would actively turn off the protection mechanism against fingerprinting to retain lost browser functionality. The scenarios ranged from losing access to online resources and static page layouts to losing browser functionalities and website breakages. The specific countermeasures were not explicitly named. Each individual scenario included a five-point Likert scale, where participants indicated how likely they would be to turn off the countermeasure if keeping it activated resulted in a constant loss of functionality or user experience. Three scenarios were presented for each countermeasure, yielding a total of nine items to assess user perspectives on fingerprinting countermeasures.

The lead instructions were worded similarly for each countermeasure; the participant was asked to decide whether to turn it off in the specific scenario or to keep it running.

We selected these three countermeasures to cover a range of privacy vs. usability trade-offs and to offer participants realistic trade-off scenarios: Tor Browser as the strongest defence, designed to minimize fingerprint uniqueness across users, offers potentially the highest protection but also the largest impact on browsing experience. Brave's anti-fingerprinting mode is considered an intermediate option that provides substantial built-in protections while preserving more web compatibility; Brave's stricter settings reduce fingerprintability but can also break or degrade site functionality, which places it in the middle of the trade-off spectrum. Browser extensions and HTTP-header spoofers serve to illustrate a light option. These measures are easier to adopt but technically less comprehensive and can either be bypassed or even increase uniqueness [64].

3.1.5 Supporting questions. After completing the part on countermeasure scenarios, we asked if the survey had changed the participants' attitudes toward browsing the internet. Participants' demographics were collected at the end of the survey, including questions on background in information technology, work or study experience, and the browsers preferably used. This allowed us to identify users with potential prior experience with online privacy and privacy-enhancing browsers such as Brave and Tor.

The questionnaire included two attention checks to identify inattentive participants: one embedded within the standard scales and another within the demographic questions.

Before launching the study, we piloted the questionnaire on Prolific with 30 participants. Feedback and responses from the pilot informed several adjustments to enhance clarity and understandability. These included refining descriptions, simplifying complex or ambiguous wording, and reducing content to remain in scope without losing the big picture. The pilot responses were solely used to evaluate and improve the study design and were not included in the final dataset. The questionnaire is provided in Appendix D.

3.2 Recruitment

The survey was conducted in English, and the first batch was advertised in February 2024 on the scientific crowdworking platform Prolific[3]. The survey was open to anyone fluent in English living in the United Kingdom (UK) or the United States (US). Data collection ended after 301 participants finished the questionnaire. The second batch was conducted in July 2024 with 601 university students. The students were recruited from two IT-related courses held in English. Recruitment on Prolific offered monetary rewards, while university students received points toward a voluntary grade bonus. The threshold to receive the voluntary grade bonus could be reached without participation in the study. Overall, the median time to complete the survey was 24 minutes.

3.3 Sample

After filtering for inattentive participants, 753 of the 902 respondents remained in the sample. In total, 149 (16.5%) failed either both or one of the attention checks. We further excluded the responses of participants who did not want to disclose their age or entered an age below 18, which is the minimum age to participate. This left us with 734 valid responses. 261 of them were from Prolific,

[3] www.prolific.com

while the other 473 were from university students. Regarding country of residence, matching based on the Prolific record was used to update the answers of three participants. All participants who did not want to disclose their country of residence were grouped under *other* (0.4%). More than half of the participants were from Germany (61.7%). The remainder came primarily from the United Kingdom (17.7%) or the United States (17.8%). Table 18 in Appendix C shows the distribution of countries. The Prolific sample is nearly perfectly split 50/50 by UK (49.8%) and US (50.2%) participants. The university students sample is made up of a majority of German residents (95.8%) with a small number of residents from other countries. Regarding gender, 391 (53.3%) participants identified as male, 335 (45.6%) as female, one participant identified as non-binary, and seven other participants preferred to either not disclose or to self-describe their gender (< 0.1%). The age of the participants ranged between 18–77 years, with a mean age of 29.6 and a median of 24. The mean (22 vs. 43.3) and median (21 vs. 42) age among students was much younger compared to the Prolific participants. Table 19 in Appendix C displays an overview of age and gender grouped by country of residence and sample. More than 75% of the participants reported either having a college degree (or Bachelor's) or graduated from high school; further details on the level of education are displayed in Table 20, Appendix C. For the university students, we observe a big portion of 230 (48.6%) to only have a high school diploma, implying these were undergraduate students. As expected, many participants were students: 429 (58%), and 146 participants reported working full time (19.8%). Table 21 in Appendix C provides a more detailed overview of participant employment status for the respective samples. Apparently, some university students either did not want to disclose their student status or did not select the option (13.3%). We introduced a binary variable indicating *IT-related Background* to differentiate between participants who either studied or worked in an IT-related field, or not. We identified 413 participants (56.3%) from an IT-related field, 306 from a non-IT-related field (41.7%); 15 preferred not to disclose this information (2%). Details are shown in Table 22, Appendix C.

Furthermore, we asked participants to indicate the daily hours they spent online. 304 (41.3%) of the participants reported that they are online for more than 5 hours per day (Table 23, Appendix C).

To determine which users had already gained experience with either the Tor or Brave Browser (or both), the participants could select all browsers they had previously used (multiple selections allowed). From this, we created a binary variable indicating whether a participant had used a privacy-focused browser before; *Private Browser User (PBU)*. Table 24 (Appendix C) shows all previously used browsers, while Table 25 (Appendix C) indicates the proportion of participants who were identified as being a *Private Browser User (PBU)*. We classified nearly 22% of the participants as being privacy-focused browser users. The proportion was slightly larger among the participants from Prolific (24.9% vs. 19.9%).

Lastly, the measured privacy metrics, the *Westin Index* (privacy concern) and the *Privacy Behavior Index (PBI)*, are represented in Figure 10 & Table 26 and Figure 11 (Appendix C), respectively. The *Westin Index* categorizes participants according to their level of agreement with three privacy statements [31]. The majority, 517 participants, were identified as Privacy Pragmatists (70.4%), 190 as Privacy Fundamentalists (25.9%), and only 27 as Privacy Unconcerned (3.7%). Among the smaller Prolific subsample, the relative proportion of Privacy Unconcerned was higher in comparison (6.5% vs 2.1%). The behavior index had a median of 4 (Students and Prolific) and a mean of 3.96 and 3.97 for the students and Prolific participants, respectively.

3.4 Analysis

3.4.1 RQ1. To assess whether participants' awareness of fingerprinting *(FP-A)* is significantly lower than their awareness of cookies *(C-A)*, we employed a one-sided Wilcoxon signed-rank test. Further, we examined whether fingerprinting awareness significantly differed among Privacy Pragmatists, Privacy Fundamentalists, and Privacy Unconcerned based on the Westin Index. The same approach was used for participants from IT-related backgrounds versus those not coming from IT-related fields. If a significant effect was found, we applied a Tukey-Kramer post-hoc test to identify pairwise differences.

To assess the relationship between participants' awareness of fingerprinting *(FP-A)* and cookies *(C-A)*, we calculated Spearman's rank correlation coefficient. We chose Spearman's rank correlation because awareness scores are ordinally scaled and may not meet the normality assumption.

Finally, to assess which demographic factors and privacy metrics of the individual have an impact on fingerprinting awareness *(FP-A)*, we developed a series of Ordered Logistic Regression models based on the configurations described in Section 3.4.4. The same logistic models (Section 3.4.4) were also employed for participants' awareness of cookies *(C-A)*. In the regression models, we excluded participants who did not want to disclose their gender or their IT-related background. As such, for all subsequent regressions, 712 participants were considered. Further, female and non-binary participants serve as the reference group for the gender variable. The reference groups for IT-related backgrounds and privacy concerns were participants from non-IT-related fields and Privacy Fundamentalists, respectively.

3.4.2 RQ2. Regarding the second research question, covering the level of user acceptance depending on the application of digital fingerprinting, we aggregated the Likert scores from the scenarios described in Section 3.1. To validate internal consistency, we employed the Cronbach Alpha criterion. To analyze the impact of demographic factors, privacy concerns, and privacy-protecting behaviors on acceptability, we developed Ordinary Least Squares (OLS) regression models. To remain consistent with the first research question, we employed the same model configurations described in Section 3.4.4.

Sentiment analysis was used to analyze participants' responses to the three open-ended questions asked for each application area of digital fingerprinting to assess their emotional tone. We categorized words using a sentiment lexicon, the NRC lexicon [49]. The lexicon assigned them into positive or negative sentiments as well as 8 different emotions, including anger, anticipation, disgust, fear, joy, sadness, surprise, and trust [49, 72]. Sentiment ratios were analyzed to identify differences in user sentiment across use cases. Additionally, free-text responses were categorized using text mining and coded into binary variables. A 20% random sample was double-coded and tested with Cohen's Kappa to ensure reliability.

3.4.3 RQ3. For the final research question, we used exploratory factor analysis to group the countermeasure scenarios presented in Section 3.1. We verified the suitability of our data for factor analysis using the Kaiser-Meyer-Olkin (KMO) test [11]. Afterwards, the optimal number of factors was determined and aggregated, similar to the acceptance scores described in Section 3.4.2. Again, we ensured the validity of the scores for further analyses using Cronbach's Alpha. Finally, we also employed OLS regressions on the determined factors.[4] We again used the model configurations explained in Section 3.4.4. This allowed us to examine which characteristics may have influenced participants' decisions to either disable their fingerprinting countermeasure or keep it active while browsing.

3.4.4 Regression model configurations. We used the same four model configurations for all three research questions with the same independent variables, solely varying the dependent variable. We first estimated a base model, which included the demographic factors of age, gender, and IT-related background as predictors. To control for potential unobserved structural differences between subsamples, we included a dummy variable ("Sample") indicating whether a response comes from the group of paid Prolific participants or the students. Building on this, we expanded the model (one additional variable at a time) to examine the influence of additional privacy-related variables:

Base Model Includes Age, Gender, IT-related background, and Sample.

Model 1 Adds Privacy Concern *(Westin Index)*.

Model 2 Incorporates the Privacy Behavior Index *(PBI)*, evaluating whether individuals' privacy-protective behaviors influence awareness.

Model 3 Includes the binary variable Privacy-Focused Browser Usage *(PBU)* to examine if the use of privacy-focused browsers is associated with higher fingerprinting awareness.

3.5 Ethical remarks & limitations

Our institution does not require ethics approval for questionnaire-based studies. However, when conducting the study and analyzing the data, we followed standard practices for ethical research, e.g., presenting detailed study procedures, obtaining consent, and allowing to leave the study at any time.

Participation in the study was voluntary. Participants on Prolific were compensated for their participation with a monetary reward of 1.75 GBP. Therefore, the median hourly reward was 7.00 GBP, which is 17% higher than Prolific's minimum hourly rate of 6 GBP.

Student participants were rewarded for their participation with a bonus code that could be redeemed as part of a series of grade bonus tasks in their university course. This code was not stored with the collected data. The only condition for receiving the bonus code was completion of the survey.

Using two separate samples and a two-batch approach introduced potential variability in the data. However, this design mirrors real-world conditions, where participants may have different contexts or experiences, which may help generalize the findings. Overall, we find that the effects for the subsamples to be aligned for the key results of the study. We provide an overview of all effects split by sample in Appendix B.

Our samples are not representative of a broader population. Due to the study topic, our Prolific sample may be biased toward people interested in IT or technology-related fields. We tried to address this by keeping the survey teaser on Prolific relatively generic. The participation rate by the students did not differ substantially from other voluntary grade bonus tasks on other subject matters.

Additionally, the small number of Privacy Unconcerned *(Westin Index)* in the sample (only 27 of 734 participants) may have impacted the reliability of conclusions about the views and behaviors concerning this group (Table 26). It has to be noted that work by Pugliese et al. [57] recorded a similar proportion of Privacy Unconcerned participants.

The survey included a short, non-technical explanation of digital fingerprinting. Although the wording was chosen to be easy to understand for a wide and non-technical audience, certain aspects (for example, comparisons to cookies and statements about persistence) may have primed or influenced participants. Our goal was to inform and to improve understanding, but we have to acknowledge that framing effects are unavoidable.

Nowadays, Prolific participants as well as students potentially use large language models (LLMs) to reply to open-ended questions such as the acceptability scenarios described in Section 3.1.2. If we noticed an obvious case of AI-generated response during the categorization of the answers, this response was flagged as fitting none of the developed categories, as these answers do not reflect participants' genuine opinions or concerns. We acknowledge the general and growing concern of LLM usage for survey-based research.

4 Findings

This section presents all findings from our investigation on the research questions stated in Section 1. For each research question on fingerprinting awareness, acceptance, and user perception of fingerprinting countermeasures, we implemented the methods described in Section 3.4. These results provide a comprehensive view of participants' responses related to digital fingerprinting in the areas of interest.

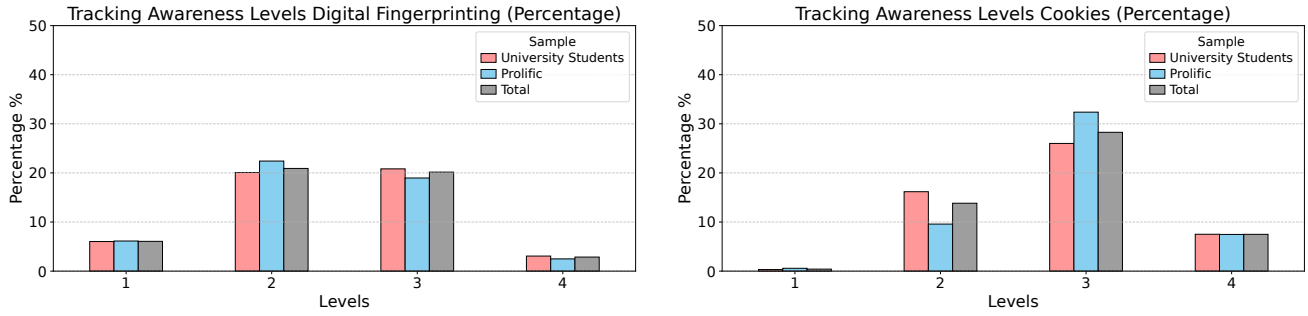
4.1 Awareness of digital fingerprinting (RQ1)

Here, we focused on a comparison of participants' awareness of digital fingerprinting with their cookie awareness, while also investigating the impact of demographic and privacy-related factors.

4.1.1 Awareness of cookies and fingerprinting. For participants' awareness of cookies and fingerprinting, we observed an overall mean awareness level of 2.86 (Students: 2.81 and Prolific: 2.93) and 2.4 (Students: 2.42 and Prolific: 2.36), respectively (min: 1 – max: 4). This corresponds to the levels described in Section 3.1. See Figure 2 for a detailed breakdown.

The Wilcoxon signed rank test revealed a statistically significant difference between the awareness levels, with fingerprinting awareness being significantly lower than cookie awareness ($p < 0.001$). We further calculated a Spearman's rank correlation coefficient of 0.40 between participants' awareness of cookies and fingerprinting. According to the guidelines from Cohen [9], this value indicates a moderate strength of association.

[4] Individuals with higher aggregated values for the factors were more likely to disable the countermeasure if the respective inconveniences in the scenarios occurred.



(a) Tracking awareness – fingerprinting

(b) Tracking awareness – cookies

Figure 2: Comparison of fingerprinting and cookie awareness levels. 1: I do not know what web cookies are / digital fingerprinting is. – 4: I am aware of web cookies / digital fingerprinting and I actively employ countermeasures against them / it

4.1.2 Factors influencing awareness of fingerprinting and cookies. Table 3 in Section A.4 presents the ordered logistic regression coefficients for regressions on participants' awareness levels for fingerprinting and cookies. The independent variables and their respective relationships with awareness are reported below:

- **Age:** We did not observe any significant relationship between an increase in age and awareness of cookies. In contrast, we found such an effect for participants' awareness of fingerprinting. Here, older users, on average, were less aware compared to younger participants ($p < 0.05$).
- **Gender:** Male participants, with one exception (fingerprinting awareness model 2), were more aware of both fingerprinting and cookies ($p < 0.05$) compared to the reference group.
- **IT-Related Background:** A background in IT showed a positive relationship with participants' awareness of cookies ($p < 0.01$) and fingerprinting awareness, as seen in the base model focused on demographics ($p < 0.05$).
- **Sample:** Awareness of fingerprinting did not significantly vary in the university sample compared to the Prolific sample, but we observed lower awareness and knowledge about cookies in the university student subsample ($p < 0.01$).
- **Privacy Concern:** We found no relationship of privacy concerns with the awareness levels for both technologies.
- **Privacy Behavior Index (PBI):** The Privacy Behavior Index (PBI) [57] is related to awareness of fingerprinting and cookies ($p < 0.01$), with the coefficient for fingerprinting being slightly larger. This means that participants engaging in more privacy-protecting online activities exhibit a higher awareness of both technologies.
- **PBU:** The same conclusion as for the Privacy Behavior Index can be drawn for users who already used a privacy-focused browser (PBU) ($p < 0.01$).

Overall, participants exhibited significantly lower awareness of digital fingerprinting compared to cookies. While IT-related backgrounds were linked to higher fingerprinting awareness, privacy concerns did not significantly relate to awareness levels. Male participants were generally more aware of both cookies and fingerprinting. A moderate correlation between fingerprinting and cookie awareness was observed. Finally, more privacy-protective behaviors and the use of privacy-focused browsers were strong predictors of higher awareness for both tracking methods.

4.2 Acceptance of digital fingerprinting depending on its application (RQ2)

The acceptance level for each fingerprinting application was measured with five-point Likert scales. After completing the scenarios from each fingerprinting application, the participants were asked open-ended questions concerning their trust, and their responses were analyzed using sentiment analysis and text mining. The application scenarios and the exact wording of the questions is presented in Appendix A.

4.2.1 Acceptance levels – descriptive statistics. Across all 734 participants, the aggregated acceptance levels (min: 1 - max: 5)[5], had an average of 3.90 for *Cybersecurity*, 3.73 for *Law Enforcement*, and 3.00 for *User Experience*. Figures 4, 5, & 6 (Appendix A) illustrate the varying level of acceptance for fingerprinting across all three use cases. Interestingly, scenario 3 (enforcing paywalls to non-paying customers) for cybersecurity and scenario 6 (dynamic price determination of services or products) for user experience strongly deviate from the pattern observable among the other scenarios. Both of the scenarios have a monetary context of fingerprinting usage.

4.2.2 Factors influencing acceptance of fingerprinting applications. Before performing the OLS regressions, the three aggregated acceptance scores were evaluated using Cronbach's alpha. The analysis yielded a Cronbach's alpha of 0.76 for the aggregated acceptance score for the cybersecurity use case, as well as 0.84 and 0.83 for the law enforcement and user experience use cases, respectively. The independent variables showed the following relationships with the acceptance scores:

- **Age:** An increase in age had a significant positive relationship with participants' acceptance when fingerprinting is used for cybersecurity purposes or law enforcement ($p < 0.01$). The score on user experience contrasts this; here, with

[5] A higher score implies an overall higher acceptance within the field of application.

increasing age, participants found it less acceptable that fingerprinting is used to enhance user experience on the web ($p < 0.05$).

- **Gender:** Being male is associated with a lower acceptance of fingerprinting when employed for cybersecurity or law enforcement, compared to the reference group ($p < 0.01$). For user experience applications, no significant relationship was determined.
- **IT-Related Background:** Regarding participants with an IT background, they exhibited a lower acceptance for scenarios when fingerprinting is employed for law enforcement purposes. This effect is significant at the 5% level in all but model 2.
- **Sample:** For all use cases, we observed higher acceptance among the sample of university students, at least at a 5% significance level.
- **Privacy Concern:** Across all three acceptance scores (with one exception), being a Privacy Pragmatist or Privacy Unconcerned was related to significantly higher acceptance scores for both groups ($p < 0.05$). The Privacy Unconcerned showed a higher coefficient in all three application areas. The overall trend is observable in all scenarios, but for cybersecurity the results are not as strongly significant as for the other two scores.
- **Privacy Behavior Index (PBI):** For all application areas, an increase in the behavior index is associated with a lower acceptance of fingerprinting ($p < 0.01$).
- **PBU:** Having worked with either the Tor or Brave Browser also decreased the acceptance rate across all three areas of application. Interestingly, the coefficient for cybersecurity has a weaker significance level compared to law enforcement and user experience ($p < 0.1$ vs. $p < 0.01$).

The complete regression tables are displayed in Table 4 (Acceptance cybersecurity), Table 5 (Acceptance law enforcement), and Table 6 (Acceptance user experience) in Appendix A.4.

4.2.3 Sentiment analysis of participants' responses across fingerprinting applications. After the initial data cleaning steps, we classified the free text responses into positive and negative with the NRC Lexicon from Mohammad and Turney [49]. We found a dominance of the frequency of negative wordings for the open-ended question concerning fingerprinting for law enforcement (1.18 vs. 1.03) and an opposite result for the user experience use case (0.42 vs. 1.30). Regarding fingerprinting used for cybersecurity, the frequencies of positive (1.00) and negative (0.41) words also painted a similar image as the law enforcement case, but here we observed an even bigger difference. See Figure 3 for an illustration.
The NRC lexicon categorizes single words into positive or negative sentiments as well as 8 different emotions [72]. The sentiment ratios were analyzed to check participants' sentiment differences regarding the varying fingerprinting applications. Table 1 shows the overall absolute values for each use case. Positive sentiment was the most dominant in all three domains. Beyond these, trust was the most prevalent emotion across all instances.

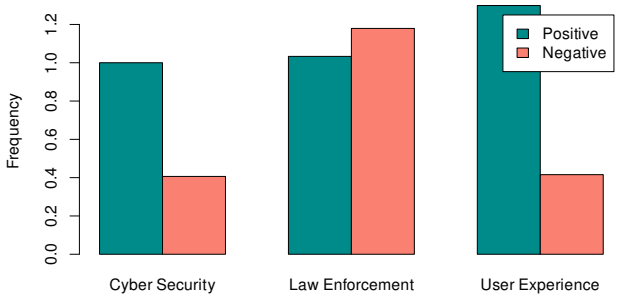


Figure 3: Frequency of positive and negative words per use case

For cybersecurity, anticipation was the second most frequent emotion, indicating a forward-looking perspective on risks and developments. In the law enforcement area, fear ranked second, suggesting concerns about security and authority. In the user experience area, anticipation was again prominent, reflecting expectations regarding usability and innovation, followed by joy, indicating positive interactions.

Table 1: Sentiment values across fingerprinting domains

Sentiment	CyberSec	LawEnf	UserExp
Positive	609	678	852
Trust	421	477	487
Negative	293	443	303
Anticipation	221	230	306
Fear	178	278	165
Anger	137	199	163
Joy	125	106	254
Sadness	90	136	93
Surprise	69	44	106
Disgust	64	106	70

Further, we applied a text mining approach, assigning the answers to the open-ended questions (described in Appendix A) into specific categories we identified. Employing trigrams and sample inspection of several answers, we identified the following categories relevant to our text analysis:

(1) Fingerprinting data used for own purposes by entity (profiling, advertising, tracking, ...)
   (a) Explicitly mentioned monetary purpose (selling data, advertising, dynamic pricing, ...)
(2) Trust in the entity to handle fingerprinting data responsibly (companies or government)
(3) Fear of data breaches/hacks (concern of data leakages or data access from third parties)

After the categories were identified, one of the authors coded all answers. Furthermore, an external coder coded a random 20% subset of the sample. We then calculated the resulting Cohen's Kappa values, representing a measurement of objectivity. For values smaller than 0.4, disagreements were discussed, the coding scheme refined, and coding conducted again for these categories. Table 9

in Appendix A displays the final Cohen's Kappa values for all categories in each fingerprinting domain. With nearly all values larger than 0.6 ("substantial agreement" or better) and none smaller than 0.4 ("moderate agreement") [32], we verified our scheme and pursued the coding.

In the cybersecurity area, respondents consistently viewed companies as primarily profit-driven, undermining trust. 34.0% of the respondents claimed that fingerprinting would be abused by firms for their own purposes, hiding behind a claim to use it for cybersecurity. Interestingly, trusting the entity to responsibly handle an individual's fingerprint was higher compared to the user experience use case (19.1%). Further, an explicit monetary intent of fingerprinting was mentioned less compared to the user experience area (16.0%). Participants emphasized that increased transparency could substantially improve confidence in these companies, like this participant, for example: "I am cautious about trusting companies to use my digital fingerprint primarily for security reasons, given the potential for misuse and lack of transparency." Many respondents further noted that trust depends on the specific firm's practices and commitment to safeguarding data, like this participant's example: "It strongly depends on the company, its reputation and its position in the marketplace of security. In case those indicators aren't positive, I definitely wouldn't trust that company."

For law enforcement, the findings are more nuanced. Here, we noticed a higher trust in the local government as a fingerprint processing entity (39.3%), and at the same significantly fewer concerns about the use of fingerprinting data for own (17.4%) or monetary purposes (1.6%) were mentioned. For German participants, there is a baseline trust in the German government – mainly because it is not seen as profit-oriented – however, participants expressed significant concerns regarding its technical capability to secure data. Here, we also observe the highest fear of data getting leaked through breaches by external entities or hacks (9.4%). The participants highlighted issues such as stereotypes, profiling, and political manipulation, and many suggested introducing stricter regulatory laws could enhance trust, like in this answer: "Mostly yes, since in Germany at least it would not be possible without reasonable suspicion in the first place. If I am informed about access to my data and the same data deletion laws apply to the government, then it is fine." Furthermore, some respondents indicated that trust levels might vary with changes in government or during election cycles: "As the state changes hands, there is no guarantee that it will be fair to potential profiles who did not vote for them in the elections. If you are a strong opposing party, you will likely be labeled a terrorist. E.g., Türkiye." This already highlights a tendency to trust official agencies like the government with a higher likelihood than companies, independently of their claim to use fingerprinting for security or enhanced user experience. However, as the last quote suggested, the participants recognized the potential to misuse or directly profile individuals in sensitive matters.

In the user experience area, the predominant views are similar to the cybersecurity use case. We observed lower trust (15.9%) and the most concerns for fingerprinting data being used for own purposes (42.9%), and from these, the highest number of participants claiming that these purposes are directly or indirectly financially motivated (30.3%). Here, respondents are skeptical of companies, primarily due to their profit-driven motives and the risk of data being sold, as this respondent noted: "I do not trust companies to use this information primarily for user experience reasons. I believe the information will be sold to third parties as it is in a company's best interest to make money, and that's one surefire way to make some quick money". Further, participants stated that companies often prioritize their own interests over those of their customers and that a lack of transparency is a critical barrier to building trust: "I already do not consent to websites collecting my data for 'user experience reasons.' Companies have been known to sell user data. This scenario would be no different." Overall, many participants reported that a higher level of trust could be achieved if companies were more transparent about their data practices, as noted in this answer: "If all use is transparent, and I am aware of it, it would be acceptable to me when used this way."

Participants showed the highest acceptance of digital fingerprinting for cybersecurity, followed by law enforcement, and the lowest for user experience. Acceptance was influenced by factors such as age, gender, IT background, privacy concerns, and use of privacy-focused browsers. Sentiment analysis revealed more positive emotions for cybersecurity and user experience, with anticipation being prominent, while law enforcement applications caused more negative sentiments, particularly fear. The findings from the coding of the open-ended questions suggested that respondents view commercial fingerprinting as largely profit-driven and opaque – fostering significant distrust – while displaying higher trust in government agencies despite concerns over their technical capabilities and potential for misuse.

4.3 User perception of inconveniences caused by fingerprinting countermeasures (RQ3)

Lastly, we examine the factors influencing users' decisions to deactivate or maintain a fingerprinting countermeasure when an associated inconvenience arises. This analysis follows a similar methodology as outlined for RQ2 in Section 3.4. The Tor Browser scenarios are described in more detail in Section 3.1. Before conducting the regressions, we performed an exploratory factor analysis to group the scenarios into two common factors.

4.3.1 Countermeasure scenarios – descriptive statistics. For all 734 participants, we solicited their propensity to deactivate a fingerprinting countermeasure when the respective inconveniences in the scenarios occurred[6]. For Brave (Figure 7, Appendix A), a common pattern in the offered scenarios can be observed, while scenario 2 (personalized search engine results) for Tor has a strong shift to "Would not disable" (Figure 8, Appendix A). A similar pattern can be detected for the Browser Extensions scenarios; here, many participants opted not to disable their fingerprinting countermeasure when encountering static-looking webpages (Figure 9, Appendix A).

4.3.2 Grouping countermeasure scenarios to factors. To evaluate if the Likert items (min:1 – max:5) from the scenarios are suitable for factor analysis, the Kaiser-Meyer-Olkin test for sampling adequacy

[6]Five-point Likert Scale: "Would definitely not disable," "Would probably not disable," "Not sure," "Would probably disable," "Would definitely disable"

Table 2: Overview of response frequencies by scenario

Scenario	Fingerprinting Usage: **Category 1(a) & 3**						Trust: **Category 2**					
	Own Purposes		Monetary		Fear of Breaches		No Trust		Indifferent		Trust	
	Count	%	Count	%	Count	%	Count	%	Count	%	Count	%
Cybersecurity	256	34.0%	125	16.6%	68	9.0%	390	51.8%	219	29.1%	144	19.1%
Law Enforcement	131	17.4%	12	1.6%	71	9.4%	315	41.8%	142	18.9%	296	39.3%
User Experience	323	42.9%	228	30.3%	30	4.0%	423	56.2%	210	27.9%	120	15.9%

was performed [11, 68]. We computed a test value of 0.796, which indicates that it is suitable to proceed with a factor analysis [42].

Afterward, we determined the optimal number of factors to group our items. We used Cattell's scree test, also known as the "elbow criterion" [5]. We obtained an optimal number of two factors, while Horn's parallel trends analysis yielded three. We decided to use only two factors because using three factors resulted in high cross-loadings for scenarios 3 and 9 while also leaving one factor to contain only two scenarios.

We conducted a factor analysis using an oblique (oblimin) rotation to identify underlying structures within the dataset. This rotation method is appropriate since it can be assumed that the factors are not independent of each other [25]. Two factors were extracted, and the factor loadings were examined to assess the strength of each variable's association with the respective factors. This approach allowed us to explore potential latent constructs that may explain the observed data patterns. Table 10 in Appendix A displays each item and the respective loadings to both factors. We assign the items to the factor where they exhibit the highest absolute loading:

- **Factor 1:** Scenarios 4 – 6 focus on disruptions in continuity, errors in operation, and missing interface elements, all of which contribute to an overarching theme of **Functionality Loss**.
- **Factor 2:** Scenarios 1 – 3 & 7 – 9 reflect both restricted access to desired content (e.g., streaming platforms, language preferences) and disruptions in the browsing experience due to non-personalized search results, malfunctioning website elements, and the need for manual intervention (e.g., disabling extensions). We labeled this factor **Restricted Access & Browsing Disruptions**.

Further, we performed regressions on the aggregated factor scores (Section 3.4.4). The scores for both factors were again validated regarding internal consistency using Cronbach's alpha. For Functionality Loss, we calculated an alpha score of 0.94; for Restricted Access & Browsing Disruptions, we found a score of 0.74. This allowed us to pursue OLS regressions on the scores, capturing participants' willingness to trade off browsing experience and functionality for enhanced fingerprinting protection. For all 712 participants considered in the regressions, we computed a mean of 3.31 for Functionality Loss and a mean of 3.20 for Restricted Access & Browsing Disruptions. For both factor scores, it has to be kept in mind that a higher score implies that the user is less willing to accept the inconveniences caused by fingerprinting countermeasures to his browsing experience. Users with a score of 1 ("Would definitely not disable") would endure functionality and convenience loss to keep their fingerprinting protection active.

4.3.3 Factors influencing the perception of fingerprinting countermeasures. We again performed the four regression models described in Section 3.4.4 on both factors to examine the impact demographic factors and online privacy concerns had on participants' willingness to deactivate fingerprinting countermeasures:

- **Age:** We did not observe any significant relationship of age (on the 5% level) with either of the countermeasure factors.
- **Gender:** We also did not record any significant relationship of gender with either of the countermeasure factors.
- **IT-Related Background:** We only found a significant relationship of background in IT with the second factor: Restricted Access & Browsing Disruptions. Participants with an IT-related background exhibited a significantly ($p < 0.05$) lower willingness to deactivate a countermeasure even if it resulted in access loss while browsing. For the first factor, no effect could be observed.
- **Sample:** We did not encounter any significant differences regarding our two samples.
- **Privacy Concern:** A significant relationship could only be observed for the second factor. Compared to Privacy Fundamentalists, Privacy Pragmatists and Privacy Unconcerned participants were significantly more likely to deactivate their countermeasures to achieve a satisfactory browsing experience and to access all resources they wanted, even though it may expose them to being fingerprinted ($p < 0.01$).
- **Privacy Behavior Index (PBI):** Participants engaging in more privacy-protective measures, as indicated by the privacy behavior index developed by Pugliese et al. [57], were also more likely to keep their fingerprinting countermeasures active and to tolerate the respective side effects. For the second factor covering Restricted Access & Browsing Disruptions, we observed a significant negative relationship at the 1% level, and for the first factor at a 5% level.
- **PBU:** In constrast to our PBI analysis, participants who had previously used Tor or Brave were less willing to accept any side effects to retain their fingerprinting protection. This relationship could only be observed for the second factor: Restricted Access & Browsing Disruptions ($p < 0.01$).

The regression tables for both factors are displayed in Section A.4, where Table 7 shows the results for Functionality Loss and Table 8 shows the results for Restricted Access & Browsing Disruptions.

As an additional exploratory analysis, we investigated if higher acceptance scores, as discussed in RQ2, were related to participants

being more likely to deactivate their countermeasures if functionality or experience were impacted. To do so, we also added the average acceptance scores (for Cybersecurity, Law Enforcement, and User Experience) to the respective *Base Model* for Factors 1 & 2. Participants who exhibited higher acceptance scores for fingerprinting being applied to enhance User Experience also showed significantly ($p < 0.001$) higher scores for Restricted Access & Browsing Disruptions as well as a higher tendency to deactivate countermeasures when confronted with Functionality Loss ($p < 0.01$). For the case in which we controlled for the average fingerprinting acceptance score when applied for Cybersecurity, we observed a significant relationship only for Functionality Loss through countermeasures ($p < 0.01$). For Law Enforcement, we did not observe any significant relationship. (This analysis is not included in the Appendix.)

Our findings reveal that participants' propensity to deactivate fingerprinting countermeasures in response to browsing inconveniences is associated with their IT-related background, privacy concerns, and prior privacy-related behaviors. While age, gender and sample origin had no significant impact, individuals with an IT-related background were more tolerant of Functionality Loss, but not of Restricted Access & Browsing Disruptions. Privacy Pragmatists and Privacy Unconcerned participants were significantly more likely to disable countermeasures to maintain browsing convenience. Further, participants who actively engaged in privacy-protective behaviors (PBI) were more likely to endure browsing disruptions to retain fingerprinting protection. Our exploratory analysis of the impact of fingerprinting acceptance also revealed significant effects, in particular, for User Experience.

5 Summary & Discussion

Our results reveal an *awareness* gap between digital fingerprinting and cookies: respondents showed significantly lower awareness of fingerprinting. This could be influenced by various factors. In comparison to cookies, digital fingerprinting is a more recently recognized technology space [10, 15], which is considerably more difficult to communicate to users due to the diversity of approaches, technologies and terminologies involved. Further, digital fingerprinting suffers from a lack of transparency due to the high relevance of server-side processing and its stateless characteristics. In addition, regulations such as the GDPR and the ePrivacy Directive [15, 57] have been mostly applied to scenarios involving cookies.

Participants with IT-related backgrounds reported higher awareness of fingerprinting, suggesting that acquiring technology literacy may often include knowledge about fingerprinting. Gender differences were consistent and notable: men were more aware of both tracking methods, similar as in prior work on gender differences in digital literacy and privacy awareness [55, 60, 66]. Awareness of fingerprinting did not significantly vary across our two samples.

In contrast to general privacy concerns, active privacy-protective behaviors (e.g., using VPNs or ad blockers) were associated with higher awareness levels. As the data are observational and cross-sectional, we cannot determine the directionality of this relationship: e.g., does higher awareness lead users to adopt protective tools, or vice versa. Future experimental work or longitudinal studies could explore such patterns in more detail [13].

Acceptance of fingerprinting varied strongly by application: it was highest for cybersecurity uses, lower for law enforcement, and lowest for user-experience applications. However, the results from the sentiment analysis and text mining differed to a certain degree. Here, the law enforcement context had the most unfavorable ratio between positive and negative word occurences, and also positive and negative sentiment occurences. The emotion of fear was also expressed more often in comparison to the other application areas. This resonates with broader concerns about surveillance and social control tools like facial recognition and predictive policing [8].

It must be noted though that positive sentiments and expressions of trust were most common across all three application areas (see Table 1). As such, our participants seemingly appreciated the beneficial uses of fingerprinting. This, however, also points to an area of improvement of our study. We did not explicitly include an application context that was more negatively loaded such as usage of fingerprinting to enhance social control mechanisms or to sidestep other anti-tracking mechanisms (e.g., to respawn cookies). This would be an important area for future work to complement our results. Across all application areas, the detailed analysis of the free-text answers revealed various points of criticism that could be useful for the design of follow-up studies. For example, many participants interpreted "user experience" claims skeptically, associating them with commercial motives (e.g., monetization or firm self-interest). This illustrates that many of our participants recognized the (policy) conundrum between using digital fingerprinting "for good" vs. the slippery slope of potential misuse and abuse.

However, from a numerical perspective, user experience scenarios generated also the largest number of positive sentiments, likely due to their more direct association with convenience rather than negative aspects such as the potential for social control. This may relate to research showing that users often trade privacy for convenience or benefits when using online services or products [2, 30].

Age did play a role in our investigation. Older participants were less aware of digital fingerprinting. Further, their acceptance of digital fingerprinting was higher for the cybersecurity area, and lower for user-experience applications. Prior research also highlights generational differences in technology contexts [27, 38, 45], and our study adds to this line of work.

Privacy Fundamentalists and users of privacy-enhancing technologies (high PBI) showed a significantly lower acceptance of fingerprinting across all application areas, especially in contexts with direct financial implications such as paywalls or dynamic pricing [23, 56]. That is, they are leaning towards the sceptical side of the aforementioned trade-off scenario between the beneficial usage of fingerprinting and potential overreach or abuse.

Men showed lower acceptance of fingerprinting in cybersecurity and law enforcement contexts compared to women and non-binary participants, a difference that aligns with research in other contexts highlighting that women have "distinct safety and security needs" [40]. The same applies to people with other gender identities and other marginalized communities [59]. On the one hand, supporting cybersecurity and law enforcement may be appreciated. On the other hand, fingerprinting also substantially increases the technical and practical hurdles for achieving anonymity online or evading trackability by unwanted parties.

Perceptions of browsing inconveniences caused by fingerprinting countermeasures varied by privacy-related factors and background. Participants engaging in more privacy-protective measures (higher PBI), were more likely to tolerate all forms of inconveniences outlined in the survey. Similarly, participants with IT-related backgrounds and Privacy Fundamentalists were more willing to tolerate at least problems with Restricted Access & Browsing Disruptions in exchange for better fingerprinting protection. However, we observed the opposite effect for users of privacy-focused browsers. This is perhaps the result of having – out of all groups – the most direct experience with such challenges, but also the practical understanding to sidestep them.

Returning to the analysis of the free-text responses, we noted that the comments by the participants further illuminated the numerical analysis meaningfully. For example, discussions around user experience often referenced personal use cases, whereas financial motives were rarely mentioned in law enforcement contexts, suggesting that monetary concerns are less central in debates about government tracking. In contrast, trust-related responses dominated the law enforcement context, seemingly reflecting more confidence in government agencies over commercial entities when it comes to online monitoring and investigative practices.

Building on seminal theoretical work [44] and applied to the context of digital fingerprinting, trust in an organization can be broken down into distinct dimensions: competence (e.g., can the organization technically protect personal data), benevolence (e.g., are users' preferences respected), and integrity/accountability (e.g., is fingerprinting transparent, lawful, and controllable). In our study, respondents referred to competence the most in the cybersecurity area. Participants accept the technical rationale but only if organizations prove they can prevent breaches. Further, (a lack of) benevolence was an important point for user experience use cases: participants overwhelmingly interpreted fingerprinting for user experience as profit-driven (42.9% own-purpose, 30.3% monetization), with many criticizing user experience being only a claim for the real intent of commercially exploiting consumer data. For law enforcement, they often referred to benevolence (39.3% trust) but then shifted attention to integrity, accountability and oversight, claiming fingerprinting must be used for non-commercial motives and demanding (legal) safeguards/protections against political misuse.

Finally, the survey itself had a notable effect on some respondents: several reported heightened concern about fingerprinting after learning about it, with comments such as: "It made me much more aware and frightened by what is collected about us", or "It made me more concerned about my security while browsing", or "I'm going to get rid of all my extensions… and be more mindful of my browsing habits." These reactions highlight how increased awareness can shift perceptions and intentions regarding protective behavior.

6 Implications & Concluding Remarks

We observed that fingerprinting acceptance is dependent on the application area, but also on the trust in the organization deploying fingerprinting. Therefore, transparent and direct communication from the implementing party would be ideal to foster understanding and acceptance, and to overcome the inherent information barriers of digital fingerprinting. Unfortunately, current disclosure practices regarding digital fingerprinting appear incomplete [47]. Likewise, attempts at self-regulation in the online tracking space have a spotty track record; see, for example, the dissolution of the W3C Tracking Protection Working Group in 2019 [70], or the recent public debates on the phasing out of third-party cookies.

The mentioned desire for transparency and control over the own fingerprint could imply adding user-facing feedback mechanisms. Prior work shows that users can benefit from real-time notification of fingerprinting attempts. For instance, Weinshel et al. [67] found that users were "surprised by how often they were tracked" and motivated to take action when shown tracking summaries. Tools like browser dashboards or indicator icons can meet this need: Firefox's privacy dashboard, for example, transparently reports how many fingerprinting attempts have been blocked [19]. Likewise, Fietkau et al. [18] designed a color-coded icon (green→yellow→red) that alerts users to extensive fingerprinting on the current page. Incorporating similar UI into more browser dashboards could increase trust and perceived control. Of course, dashboard-type approaches still place a significant burden on users to inform themselves and manage their preferences. Importantly, our study illustrates that there is a sizable number of users willing to invest time and effort in protective behaviors (PBU, PBI), or are even willing to suffer from non-trivial browsing inconveniences to evade digital fingerprinting.

Our findings shed light on users' preferences related to fingerprinting, suggesting concrete directions for countermeasure design. For example, privacy-sensitive users were less willing to accept fingerprinting, implying that automatic defaults should favor protection. Firefox, for example, has fingerprinting protection enabled by default [19]. Consistent with the participants' expressed desire for control and transparency in the open-ended questions, there are already efforts to formulate advice for marking fingerprintable features and enabling fallback behavior [14]. This involves clearly indicating when an API may aid in fingerprinting, such as through an icon or label, and ensuring that the application's functionality can gracefully degrade if those APIs are turned off [14].

In conclusion, our study of 734 participants revealed a more comprehensive picture of user perceptions of digital fingerprinting and its countermeasures. While awareness of traditional tracking methods like cookies is widespread, fingerprinting remains less well-known, especially among non-technical users. In our work, we further establish how acceptance of fingerprinting largely depends on its application area and how users react to inconveniences related to fingerprinting countermeasures.

A significant challenge highlighted by our findings is the balance between robust protection and usability. Even privacy-conscious users may abandon countermeasures if they disrupt the browsing experience. Moreover, relying solely on external tools can sometimes introduce additional risks, such as malware or even making a user more uniquely identifiable [15].

Future work should also delve deeper in the economic determinants of the ecosystem supporting digital fingerprinting to improve our understanding of the perceived and actual value of digital fingerprinting to deliver more equitable outcomes.

Acknowledgments

We thank the participants of our survey study. We further highly appreciate the constructive comments made by the anonymous reviewers that helped improve our work. We thank Maximilian J. Frank for assistance with qualitative data analysis. For an earlier version, we used a genAI tool to check for typos and improve grammatical structure. Jens Grossklags gratefully acknowledges a research gift from Google Inc.

References

[1] Gunes Acar, Marc Juarez, Nick Nikiforakis, Claudia Diaz, Seda Gürses, Frank Piessens, and Bart Preneel. 2013. FPDetective: Dusting the web for fingerprinters. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security (CCS '13)*. Association for Computing Machinery, New York, NY, USA, 1129–1140. https://doi.org/10.1145/2508859.2516674

[2] Alessandro Acquisti and Jens Grossklags. 2005. Privacy and rationality in individual decision making. *IEEE Security & Privacy* 3, 1 (2005), 26–33. https://doi.org/10.1109/MSP.2005.22

[3] Furkan Alaca and Paul C. van Oorschot. 2016. Device fingerprinting for augmenting web authentication: Classification and analysis of methods. In *Proceedings of the 32nd Annual Conference on Computer Security Applications (ACSAC '16)*. Association for Computing Machinery, New York, NY, USA, 289–301. https://doi.org/10.1145/2991079.2991091

[4] Alex Berke, Badih Ghazi, Enrico Bacis, Pritish Kamath, Ravi Kumar, Robin Lassonde, Pasin Manurangsi, and Umar Syed. 2025. How unique is whose web browser? The role of demographics in browser fingerprinting among US users. *Proceedings on Privacy Enhancing Technologies* 2025, 1 (2025), 720–758. https://doi.org/10.56553/popets-2025-0038

[5] Johan Braeken and Marcel A. L. M. van Assen. 2017. An empirical Kaiser criterion. *Psychological Methods* 22, 3 (2017), 450–466. https://doi.org/10.1037/met0000074

[6] Brave. 2024. Fingerprinting protections: Brave browser. https://github.com/brave/brave-browser/wiki/Fingerprinting-Protections

[7] Brave Privacy Team. 2024. Brave browser simplifies its fingerprinting protections. https://brave.com/privacy-updates/28-sunsetting-strict-fingerprinting-mode/

[8] Christopher G. Reddick, Akemi Takeoka Chatfield, and Patricia A. Jaramillo. 2015. Public opinion on National Security Agency surveillance programs: A multi-method approach. *Government Information Quarterly* 32, 2 (2015), 129–141. https://doi.org/10.1016/j.giq.2015.01.003

[9] Jacob Cohen. 2013. *Statistical Power Analysis for the Behavioral Sciences*. Routledge. https://doi.org/10.4324/9780203771587

[10] Alissa Cooper, Hannes Tschofenig, Bernard D. Aboba, Jon Peterson, John Morris, Marit Hansen, and Rhys Smith. 2013. *Privacy Considerations for Internet Protocols*. Request for Comments 6973. Internet Architecture Board. https://doi.org/10.17487/RFC6973

[11] Edward E. Cureton and Ralph B. D'Agostino. 2013. *Factor Analysis*. Psychology Press. https://doi.org/10.4324/9781315799476

[12] Dries Depoorter. 2025. Browser.dating. https://browser.dating/

[13] Tamara Dinev and Qing Hu. 2007. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems* 8, 7 (2007), 386–408. https://doi.org/10.17705/1jais.00133

[14] Nick Doty and Tom Ritter. 2025. Mitigating Browser Fingerprinting in Web Specifications. W3C Group Note. https://www.w3.org/TR/fingerprinting-guidance/

[15] Peter Eckersley. 2010. How unique is your web browser?. In *Privacy Enhancing Technologies*, Mikhail J. Atallah and Nicholas J. Hopper (Eds.). Springer, Berlin, Heidelberg, 1–18.

[16] Steven Englehardt and Arvind Narayanan. 2016. Online tracking: A 1-million-site measurement and analysis. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*. Association for Computing Machinery, New York, NY, USA, 1388–1401. https://doi.org/10.1145/2976749.2978313

[17] EuroStat. 2022. Safer Internet Day: Are you restricting cookies? https://ec.europa.eu/eurostat/web/products-eurostat-news/-/edn-20220208-1

[18] Julian Fietkau, Kashyap Thimmaraju, Felix Kybranz, Sebastian Neef, and Jean-Pierre Seifert. 2021. The elephant in the background: A quantitative approach to empower users against web browser fingerprinting. In *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society* (Virtual Event) *(WPES '21)*. Association for Computing Machinery, New York, NY, USA, 167–180. https://doi.org/10.1145/3463676.3485599

[19] Firefox. 2025. Firefox blocks fingerprinting. https://www.firefox.com/en-US/features/block-fingerprinting/

[20] Xianyi Gao, Yulong Yang, Huiqing Fu, Janne Lindqvist, and Yang Wang. 2014. Private browsing: An inquiry on usability and privacy protection. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society (WPES '14)*. Association for Computing Machinery, New York, NY, USA, 97–106. https://doi.org/10.1145/2665943.2665953

[21] Emily Geisen. 2022. Improve data quality by using a commitment request instead of attention checks. https://www.qualtrics.com/blog/attention-checks-and-data-quality/

[22] Vicki Ha, Kori Inkpen, Farah Al Shaar, and Lina Hdeib. 2006. An examination of user perception and misconception of internet cookies. In *CHI '06 Extended Abstracts on Human Factors in Computing Systems (CHI EA '06)*. Association for Computing Machinery, New York, NY, USA, 833–838. https://doi.org/10.1145/1125451.1125615

[23] Gerrit Hufnagel, Manfred Schwaiger, and Louisa Weritz. 2022. Seeking the perfect price: Consumer responses to personalized price discrimination in e-commerce. *Journal of Business Research* 143 (2022), 346–365. https://doi.org/10.1016/j.jbusres.2021.10.002

[24] Umar Iqbal, Steven Englehardt, and Zubair Shafiq. 2021. Fingerprinting the fingerprinters: Learning to detect browser fingerprinting behaviors. In *2021 IEEE Symposium on Security and Privacy (SP)*. 1143–1161. https://doi.org/10.1109/SP40001.2021.00017

[25] Robert I. Jennrich and P. F. Sampson. 1966. Rotation for simple loadings. *Psychometrika* 31, 3 (1966), 313–323. https://doi.org/10.1007/BF02289465

[26] Justin Trificana. 2023. How device fingerprinting improves fraud prevention: Device fingerprinting is an impactful tool for fighting fraud without gumming up the user experience. https://plaid.com/resources/identity/device-fingerprinting/

[27] Veronika Kalmus, Göran Bolin, and Rita Figueiras. 2024. Who is afraid of dataveillance? Attitudes toward online surveillance in a cross-cultural and generational perspective. *New Media & Society* 26, 9 (2024), 5291–5313. https://doi.org/10.1177/14614448221134493

[28] Navpreet Kaur, Sami Azam, Krishnan Kannoorpatti, Kheng Cher Yeo, and Bharanidharan Shanmugam. 2017. Browser fingerprinting as user tracking technology. In *2017 11th International Conference on Intelligent Systems and Control (ISCO)*. 103–111. https://doi.org/10.1109/ISCO.2017.7855963

[29] Sheharbano Khattak, David Fifield, Sadia Afroz, Mobin Javed, Srikanth Sundaresan, Vern Paxson, Steven J. Murdoch, and Damon McCoy. February 21-24, 2016. Do you see what I see? Differential treatment of anonymous users. In *Proceedings of the 2016 Network and Distributed System Security Symposium*. Internet Society, Reston, VA. https://doi.org/10.14722/ndss.2016.23342

[30] Andreas Krause and Eric Horvitz. 2010. A utility-theoretic approach to privacy in online services. *Journal of Artificial Intelligence Research* 39 (2010), 633–662. https://doi.org/10.1613/jair.3089

[31] Ponnurangam Kumaraguru and Lorrie Faith Cranor. 2005. *Privacy indexes: A survey of Westin's studies*. Technical Report CMU-ISRI-5-138. Institute for Software Research International.

[32] J. Richard Landis and Gary G. Koch. 1977. The measurement of observer agreement for categorical data. *Biometrics* 33, 1 (1977), 159–174. https://doi.org/10.2307/2529310

[33] Tomer Laor, Naif Mehanna, Antonin Durey, Vitaly Dyadyuk, Pierre Laperdrix, Clémentine Maurice, Yossi Oren, Romain Rouvoy, Walter Rudametkin, and Yuval Yarom. 2022. DrawnApart: A device identification technique based on remote GPU fingerprinting. In *Network and Distributed System Security Symposium*. https://doi.org/10.14722/ndss.2022.24093

[34] Pierre Laperdrix. 2019. *Browser fingerprinting: An introduction and the challenges ahead*. Blog. Tor. https://blog.torproject.org/browser-fingerprinting-introduction-and-challenges-ahead/

[35] Pierre Laperdrix, Nataliia Bielova, Benoit Baudry, and Gildas Avoine. 2020. Browser fingerprinting: A survey. *ACM Transactions on the Web* 14, 2, Article 8 (2020), 33 pages. https://doi.org/10.1145/3386040

[36] Pierre Laperdrix, Walter Rudametkin, and Benoit Baudry. 2015. Mitigating browser fingerprint tracking: Multi-level reconfiguration and diversification. In *Proceedings of the 10th International Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS '15)*. IEEE Press, 98–108.

[37] 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 '19)*. https://doi.org/10.14722/ndss.2019.23386

[38] Karen Leppel and Donna W. McCloskey. 2011. A cross-generational examination of electronic commerce adoption. *Journal of Consumer Marketing* 28, 4 (2011), 261–268. https://doi.org/10.1108/07363761111143150

[39] Tianyi Li, Xiaofeng Zheng, Kaiwen Shen, and Xinhui Han. 2022. FPFlow: Detect and prevent browser fingerprinting with dynamic taint analysis. In *Cyber Security*, Wei Lu, Yuqing Zhang, Weiping Wen, Hanbing Yan, and Chao Li (Eds.). Springer Nature, Singapore, 51–67.

[40] Anastasia Loukaitou-Sideris and Camille Fink. 2009. Addressing women's fear of victimization in transportation settings. *Urban Affairs Review* 44, 4 (2009), 554–587. https://doi.org/10.1177/1078087408322874

[41] Sakchan Luangmaneerote, Ed Zaluska, and Leslie Carr. 2016. Survey of existing fingerprint countermeasures. In *2016 International Conference on Information Society (i-Society)*. 137–141. https://doi.org/10.1109/i-Society.2016.7854198

[42] Wolfgang Ludwig-Mayerhofer. 2004. Faktorenanalyse. In *ILMES – Internet-Lexikon der Methoden der empirischen Sozialforschung*. Universität Siegen. http://wlm.userweb.mwn.de/Ilmes/ilm_f3.htm

[43] Jonathan R. Mayer and John C. Mitchell. 2012. Third-party web tracking: Policy and technology. In *2012 IEEE Symposium on Security and Privacy*. 413–427. https://doi.org/10.1109/SP.2012.47

[44] Roger C. Mayer, James H. Davis, and F. David Schoorman. 1995. An integrative model of organizational trust. *The Academy of Management Review* 20, 3 (1995), 709–734. http://www.jstor.org/stable/258792

[45] Nazaria Binti Md. Aris, Ruziah A. Latif, Nurnais Safiy Binti Zainal, Khalisah Khairina Binti Razman, and Razman Bin Anuar. 2021. Factors affecting young shoppers' online shopping preference in Kelantan, Malaysia. *International Journal of Academic Research in Business and Social Sciences* 11, 14 (2021), 417–430. https://doi.org/10.6007/IJARBSS/v11-i14/9618

[46] Georg Merzdovnik, Markus Huber, Damjan Buhov, Nick Nikiforakis, Sebastian Neuner, Martin Schmiedecker, and Edgar Weippl. 2017. Block me if you can: A large-scale study of tracker-blocking tools. In *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*. 319–333. https://doi.org/10.1109/EuroSP.2017.26

[47] Julissa Milligan, Sarah Scheffler, Andrew Sellars, Trishita Tiwari, Ari Trachtenberg, and Mayank Varia. 2021. Case study: Disclosure of indirect device fingerprinting in privacy policies. In *Socio-Technical Aspects in Security and Trust*, Thomas Groß and Theo Tryfonas (Eds.). Springer International Publishing, Cham, Switzerland, 175–186. https://doi.org/10.1007/978-3-030-55958-8_10

[48] George R. Milne, Andrew J. Rohm, and Shalini Bahl. 2004. Consumers' protection of online privacy and identity. *Journal of Consumer Affairs* 38, 2 (2004), 217–232. https://doi.org/10.1111/j.1745-6606.2004.tb00865.x

[49] Saif M. Mohammad and Peter D. Turney. 2013. Crowdsourcing a word–emotion association lexicon. *Computational Intelligence* 29, 3 (2013), 436–465. https://doi.org/10.1111/j.1467-8640.2012.00460.x

[50] Mozilla. 2017. Canvas Defender: Firefox add-on that adds unique and persistent noise to a canvas element. https://addons.mozilla.org/en-US/firefox/addon/no-canvas-fingerprinting/

[51] Shaoor Munir, Sandra Siby, Umar Iqbal, Steven Englehardt, Zubair Shafiq, and Carmela Troncoso. 2023. CookieGraph: Understanding and detecting first-party tracking cookies. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*. ACM, New York, NY, USA, 3490–3504. https://doi.org/10.1145/3576915.3616586

[52] Meenatchi Sundaram Muthu Selva Annamalai, Emiliano De Cristofaro, and Igor Bilogrevic. 2025. Beyond the crawl: Unmasking browser fingerprinting in real user interactions. In *Proceedings of the ACM on Web Conference (WWW '25)*. Association for Computing Machinery, New York, NY, USA, 3896–3907. https://doi.org/10.1145/3696410.3714871

[53] Alexandra Nisenoff, Arthur Borem, Madison Pickering, Grant Nakanishi, Maya Thumpasery, and Blase Ur. 2023. Defining "broken": User experiences and remediation tactics when ad-blocking or tracking-protection tools break a website's user experience. In *32nd USENIX Security Symposium (USENIX Security '23)*. USENIX Association, Anaheim, CA, 3619–3636. https://www.usenix.org/conference/usenixsecurity23/presentation/nisenoff-broken

[54] Panagiotis Papadopoulos, Peter Snyder, Dimitrios Athanasakis, and Benjamin Livshits. 2020. Keeping out the masses: Understanding the popularity and implications of internet paywalls. In *Proceedings of The Web Conference 2020 (WWW '20)*. Association for Computing Machinery, New York, NY, USA, 1433–1444. https://doi.org/10.1145/3366423.3380217

[55] Yong Jin Park. 2013. Digital literacy and privacy behavior online. *Communication Research* 40, 2 (2013), 215–236. https://doi.org/10.1177/0093650211418338

[56] Anna Priester, Thomas Robbert, and Stefan Roth. 2020. A special price just for you: Effects of personalized dynamic pricing on consumer fairness perceptions. *Journal of Revenue and Pricing Management* 19, 2 (2020), 99–112. https://doi.org/10.1057/s41272-019-00224-3

[57] Gaston Pugliese, Christian Riess, Freya Gassmann, and Zinaida Benenson. 2020. Long-term observation on browser fingerprinting: Users' trackability and perspective. *Proceedings on Privacy Enhancing Technologies* 2020, 2 (2020), 558–577. https://doi.org/10.2478/popets-2020-0041

[58] Philip Raschke and Axel Küpper. 2018. Uncovering canvas fingerprinting in real-time and analyzing ist usage for web-tracking. In *Workshops der INFORMATIK 2018 – Architekturen, Prozesse, Sicherheit und Nachhaltigkeit*. Köllen Druck+Verlag GmbH, Bonn, 97–108.

[59] Shruti Sannon and Andrea Forte. 2022. Privacy research with marginalized groups: What we know, what's needed, and what's next. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2, Article 455 (2022), 33 pages. https://doi.org/10.1145/3555556

[60] Mustafa Saritepeci, Hatice Yildiz Durak, Gül Özüdoğru, and Nilüfer Atman Uslu. 2024. The role of digital literacy and digital data security awareness in online privacy concerns: A multi-group analysis with gender. *Online Information Review* 48, 5 (2024), 983–1001. https://doi.org/10.1108/OIR-03-2023-0122

[61] Takamasa Tanaka, Hidekazu Niibori, Shiyingxue Li, Shimpei Nomura, Hiroki Kawashima, and Kazuhiko Tsuda. 2020. Bot detection model using user agent and user behavior for web log analysis. *Procedia Computer Science* 176 (2020), 1621–1625. https://doi.org/10.1016/j.procs.2020.09.185

[62] Tor Project. 2025. Anti-Fingerprinting. https://tb-manual.torproject.org/anti-fingerprinting/

[63] European Union. 2018. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). http://data.europa.eu/eli/reg/2016/679/oj

[64] Antoine Vastel, Walter Rudametkin, Romain Rouvoy, and Xavier Blanc. 2020. FP-Crawlers: Studying the resilience of browser fingerprinting to block crawlers. In *MADWeb'20 - NDSS Workshop on Measurements, Attacks, and Defenses for the Web*, Oleksii Starov, Alexandros Kapravelos, and Nick Nikiforakis (Eds.). https://doi.org/10.14722/madweb.2020.23010

[65] VS FingerPrinting Inc. 2024. The Advantages of Digital Fingerprints in Digital Forensics. https://www.vsfingerprinting.com/post/the-advantages-of-digital-fingerprints-in-digital-forensics

[66] Maor Weinberger, Maayan Zhitomirsky-Geffet, and Dan Bouhnik. 2017. Sex differences in attitudes towards online privacy and anonymity among Israeli students with different technical backgrounds. *Information Research* 22, 4, Article 777 (2017). http://InformationR.net/ir/22-4/paper777.html

[67] Ben Weinshel, Miranda Wei, Mainack Mondal, Euirim Choi, Shawn Shan, Claire Dolin, Michelle L. Mazurek, and Blase Ur. 2019. Oh, the places you've been! User reactions to longitudinal transparency about third-party web tracking and inferencing. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19)*. Association for Computing Machinery, New York, NY, USA, 149–166. https://doi.org/10.1145/3319535.3363200

[68] Brett Williams, Andrys Onsman, and Ted Brown. 2010. Exploratory factor analysis: A five-step guide for novices. *Australasian Journal of Paramedicine* 8 (2010), 1–13. https://doi.org/10.33151/ajp.8.3.93

[69] Marissa Wood. 2019. Today's Firefox Blocks Third-Party Tracking Cookies and Cryptomining by Default. https://blog.mozilla.org/en/products/firefox/todays-firefox-blocks-third-party-tracking-cookies-and-cryptomining-by-default/

[70] World Wide Web Consortium (W3C). 2019. Tracking Protection Working Group. https://github.com/w3c/dnt

[71] Seounmi Youn. 2009. Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs* 43, 3 (2009), 389–418. https://doi.org/10.1111/j.1745-6606.2009.01146.x

[72] Zhiyong Zhang. 2018. *Text Mining for Social and Behavioral Research Using R: A Case Study on Teaching Evaluation*. University of Notre Dame, Chapter 8.1.2. https://books.psychstat.org/textmining

A Additional Material: Scenarios, Graphs, and Tables

A.1 Survey: Fingerprinting acceptance scenarios

Acceptance scenarios – cybersecurity:

(1) Detecting potential criminal access to user accounts.[7]
(2) Preventing illegal attempts to access databases comprising user information.
(3) Enforcing paywalls to non-paying customers.
(4) Leveraging Artificial Intelligence to improve fraud prevention practices.
(5) Educating the user about their account security.
(6) Reducing the amount of phishing mails.

Acceptance scenarios – law enforcement:

(1) Performing digital forensic analysis in the context of online fraud.
(2) Tracking suspicious online search queries for crime prevention.
(3) Supporting criminal investigations with evidence obtained through digital fingerprinting.
(4) Employing digital fingerprinting technology to aid in missing persons investigations.
(5) Preventing harm by inspecting online chat forums for signs of criminal activities.
(6) Controlling the rehabilitation of prisoners by tracking their online activities.

Acceptance scenarios – user experience:

(1) Accelerating user logins by bypassing CAPTCHAs.
(2) Elevating the online dating experiences with personalized and relevant matches.
(3) Relevant ad recommendations based on individual interests.
(4) Tailored websites for personalized user experience.
(5) Optimizing job search results for relevant and fulfilling career opportunities.
(6) Dynamic price determination of services or products.

A.2 Likert scales: Acceptance scenarios

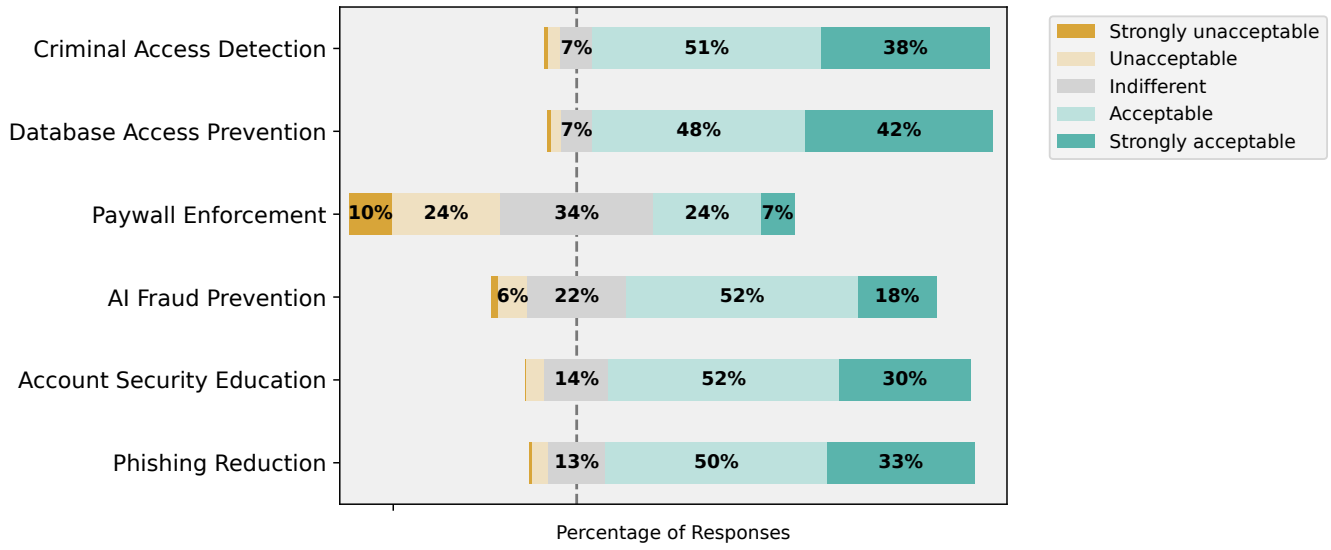


Figure 4: Fingerprinting for cybersecurity scenarios

[7] Response options: Strongly Unacceptable, Unacceptable, Indifferent, Acceptable, Strongly Acceptable.

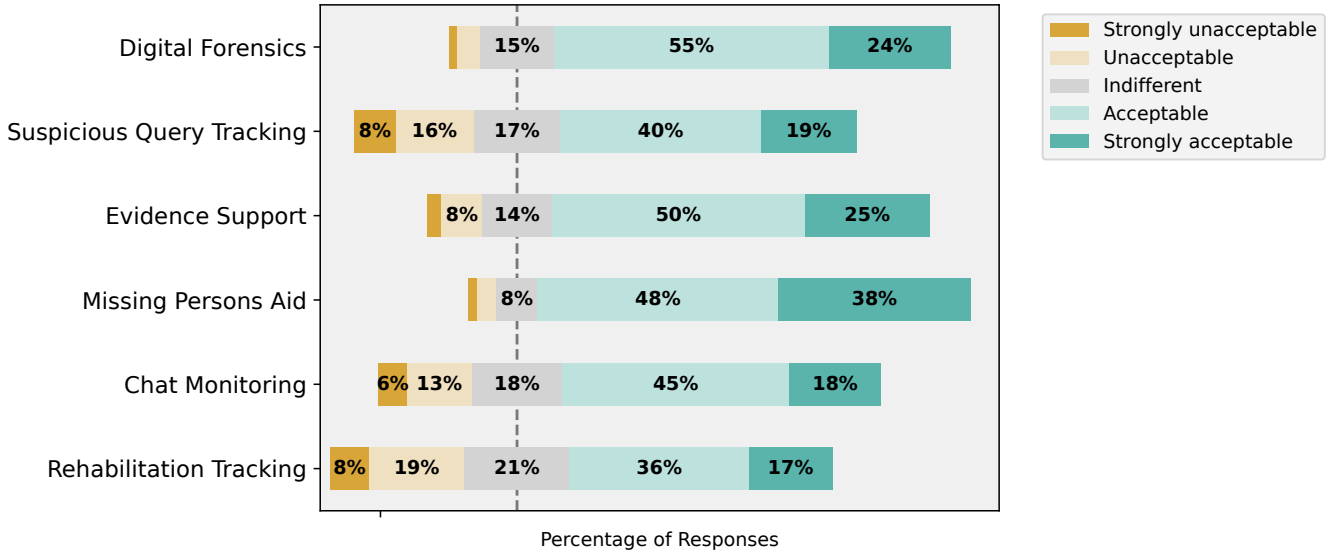


Figure 5: Fingerprinting for law enforcement scenarios

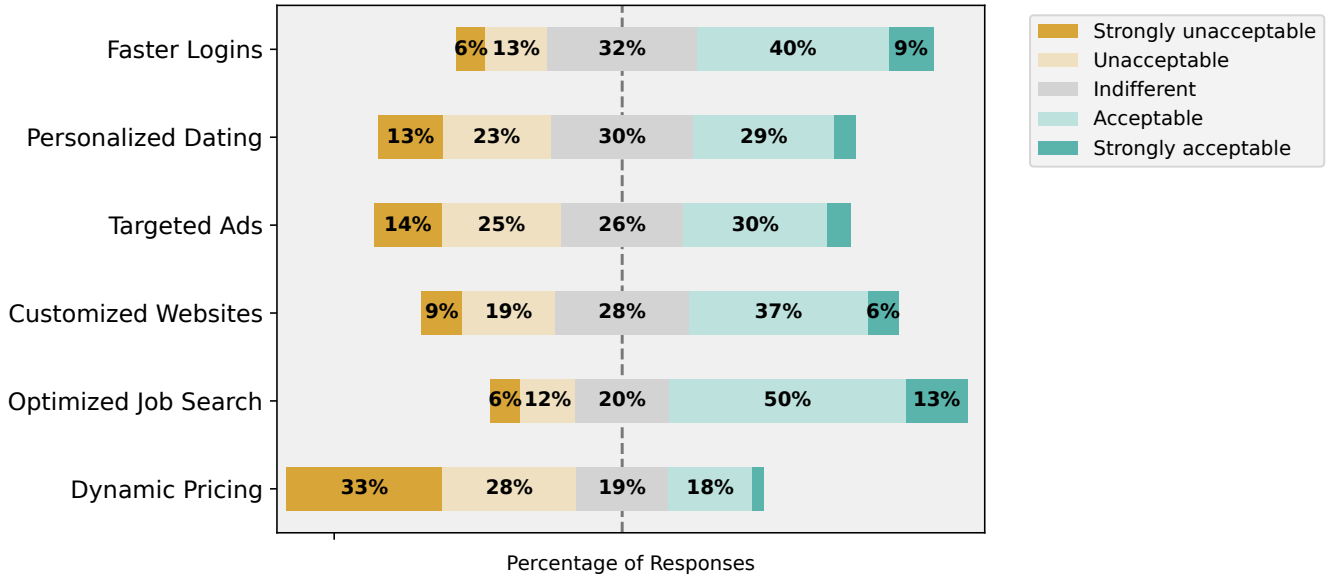


Figure 6: Fingerprinting for user experience scenarios

A.3 Likert scales: Countermeasure scenarios

Figure 7: Brave browser scenarios (1: All the progress you made in the game is lost in your next gaming session; 2: Many games do not work correctly; 3: You cannot reach the next level because a 3D element of the game's user interface is not visible)

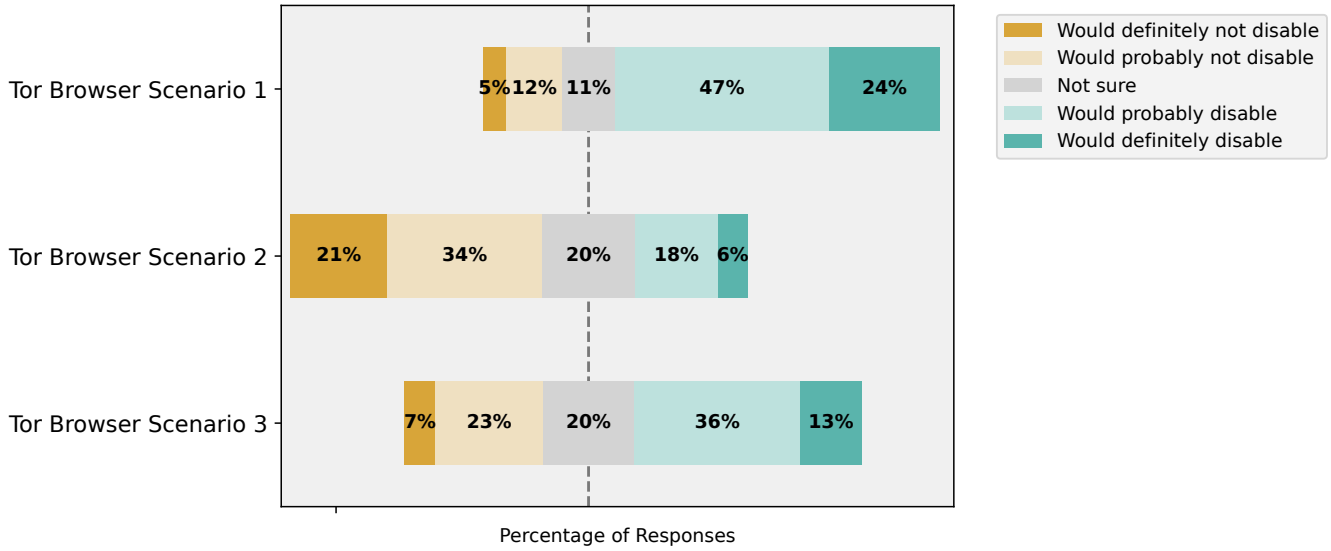


Figure 8: Tor browser scenarios (1: You can't access your favorite streaming platform; 2: Your search engine results are not personalized to match your interests; 3: You always need to manually turn off a browser extension to watch a video online)

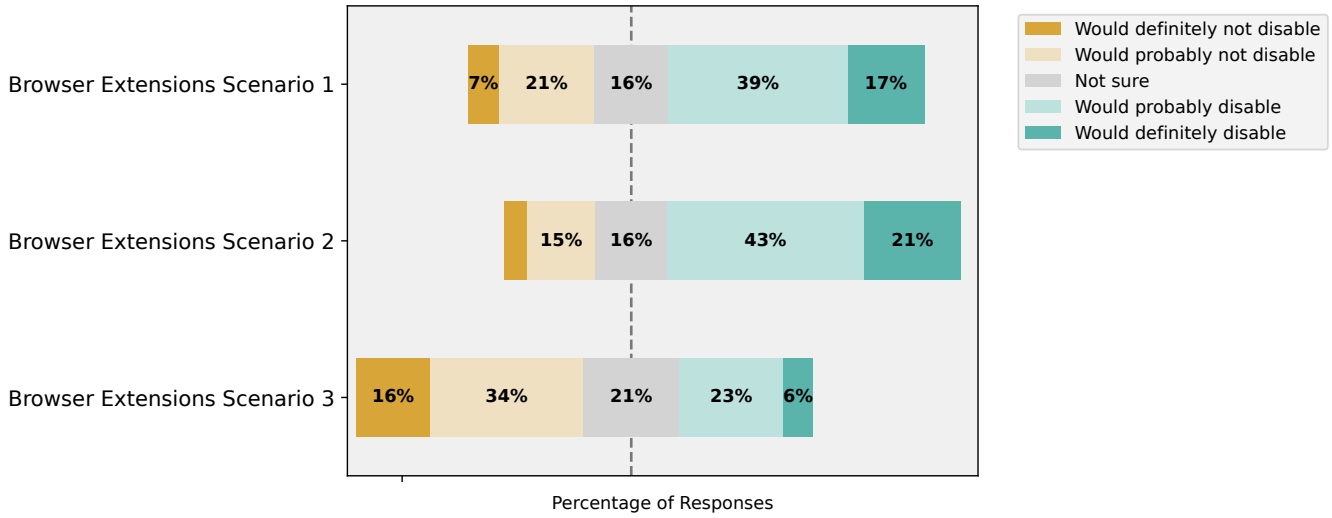


Figure 9: Browser extensions scenarios (1: Websites are not displayed in your preferred language; 2: Interactive website elements (search buttons or sliders) overlap each other and do not work; 3: Search engine results look static and less appealing)

A.4 Tables: Regression tables, Cohen's Kappa, and factor loadings

Table 3: Ordered logistic regression: Awareness fingerprinting vs. awareness cookies

Dep. Variable	Tracking Awareness Fingerprinting				Tracking Awareness Cookies			
	Base Model	**Model 1**	**Model 2**	**Model 3**	**Base Model**	**Model 1**	**Model 2**	**Model 3**
Age	-0.0195**	-0.0188**	-0.0133	-0.0138	-0.002	-0.001	0.004	0.003
	(0.008)	(0.008)	(0.008)	(0.008)	(0.009)	(0.009)	(0.009)	(0.009)
Gender	0.499***	0.489***	0.261*	0.332**	0.550***	0.553***	0.324**	0.413***
	(0.144)	(0.145)	(0.149)	(0.148)	(0.152)	(0.153)	(0.156)	(0.155)
IT-Related Background	0.326**	0.321**	0.120	0.199	1.007***	1.005***	0.845***	0.905***
	(0.161)	(0.161)	(0.165)	(0.164)	(0.172)	(0.172)	(0.175)	(0.174)
Sample	-0.461*	-0.444*	-0.195	-0.219	-0.979***	-0.972***	-0.761***	-0.780***
	(0.242)	(0.244)	(0.248)	(0.248)	(0.256)	(0.257)	(0.260)	(0.197)
Westin Index								
Privacy Pragmatists		-0.101				-0.029		
		(0.165)				(0.175)		
Privacy Unconcerned		-0.1217				-0.255		
		(0.404)				(0.406)		
Privacy Behavior Index			0.491***				0.452***	
			(0.062)				(0.061)	
PBU				1.046***				0.827***
				(0.193)				(0.197)
1/2	-2.419***	-2.472***	-0.511	-2.092***	-4.759***	-3.554***	-3.018***	-4.492***
	(0.399)	(0.409)	(0.466)	(0.405)	(0.573)	(0.581)	(0.619)	(0.576)
2/3	0.775***	0.775***	0.831***	0.792***	1.376***	1.378***	1.395***	1.387***
	(0.053)	(0.053)	(0.053)	(0.053)	(0.103)	(0.103)	(0.102)	(0.103)
3/4	0.983***	0.984***	1.046***	1.021***	1.041***	1.064***	1.107***	1.098***
	(0.060)	(0.060)	(0.059)	(0.060)	(0.044)	(0.045)	(0.046)	(0.045)
Observations	712	712	712	712	712	712	712	712
Pseudo R^2	0.015	0.015	0.057	0.034	0.042	0.043	0.082	0.055

Note: *p<0.1; **p<0.05; ***p<0.01
Standard errors are in parentheses.
Gender: Female and Non-binary as reference category.
Sample: Prolific sample participants as reference category.
Westin Index: Privacy Fundamentalists as reference category.

Table 4: OLS regression: Acceptance of fingerprinting for cybersecurity

Dep. Variable	**Acceptance Fingerpinting Cybersecurity**			
	Base Model	**Model 1**	**Model 2**	**Model 3**
Age	0.010***	0.009***	0.009***	0.010***
	(0.003)	(0.003)	(0.003)	(0.003)
Gender	-0.144***	-0.139***	-0.114**	-0.126***
	(0.044)	(0.044)	(0.044)	(0.045)
IT-Related Background	-0.068	-0.064	-0.043	-0.052
	(0.049)	(0.049)	(0.049)	(0.049)
Sample	0.191***	0.176**	0.160**	0.164**
	(0.74)	(0.074)	(0.074)	(0.075)
Westin Index				
Privacy Pragmatists		0.085*		
		(0.050)		
Privacy Unconcerned		0.259**		
		(0.119)		
Privacy Behavior Index			-0.051***	
			(0.017)	
PBU				-0.102*
				(0.055)
Const	3.601***	3.563***	3.811***	3.639***
	(0.118)	(0.121)	(0.137)	(0.120)
Observations	712	712	712	712
R^2	0.045	0.053	0.057	0.050
Adj. R^2	0.040	0.045	0.500	0.043

Note: *p<0.1; **p<0.05; ***p<0.01
Standard errors are in parentheses.
Gender: Female and Non-binary as reference category.
Sample: Prolific sample participants as reference category.
Westin Index: Privacy Fundamentalists as reference category.

Table 5: OLS regression: Acceptance of fingerprinting for law enforcement

Dep. Variable	**Acceptance Fingerprinting law enforcement**			
	Base Model	**Model 1**	**Model 2**	**Model 3**
Age	0.010***	0.008**	0.009***	0.009***
	(0.003)	(0.003)	(0.003)	(0.003)
Gender	-0.386***	-0.370***	-0.323***	-0.343***
	(0.056)	(0.056)	(0.057)	(0.057)
IT-Related Background	-0.230***	-0.219***	-0.178***	-0.194***
	(0.063)	(0.062)	(0.063)	(0.064)
Sample	0.0334***	0.294***	0.270***	0.271***
	(0.096)	(0.095)	(0.095)	(0.097)
Westin Index				
Privacy Pragmatists		0.224***		
		(0.064)		
Privacy Unconcerned		0.549***		
		(0.152)		
Privacy Behavior Index			-0.106***	
			(0.022)	
PBU				-0.237***
				(0.070)
Const	3.561***	3.458***	4.001***	3.649***
	(0.153)	(0.155)	(0.175)	(0.154)
Observations	712	712	712	712
R^2	0.100	0.124	0.129	0.114
Adj. R^2	0.094	0.116	0.123	0.108

Note: *p<0.1; **p<0.05; ***p<0.01
Standard errors are in parentheses.
Gender: Female and Non-binary as reference category.
Sample: Prolific sample participants as reference category.
Westin Index: Privacy Fundamentalists as reference category.

Table 6: OLS regression: Acceptance of fingerprinting for user experience

Dep. Variable	**Acceptance Fingerpinting user experience**			
	Base Model	**Model 1**	**Model 2**	**Model 3**
Age	0.001	-0.002	-0.000	-0.000
	(0.004)	(0.003)	(0.004)	(0.004)
Gender	-0.107*	-0.072	-0.0455	-0.068
	(0.061)	(0.060)	(0.062)	(0.062)
IT-Related Background	-0.067	-0.047	-0.016	-0.034
	(0.068)	(0.066)	(0.068)	(0.069)
Sample	0.286***	0.212**	0.224**	0.229**
	(0.103)	(0.101)	(0.103)	(0.105)
Westin Index				
Privacy Pragmatists		0.411***		
		(0.068)		
Privacy Unconcerned		0.786***		
		(0.161)		
Privacy Behavior Index			-0.103***	
			(0.023)	
PBU				-0.217***
				(0.076)
Const	2.886***	2.686***	3.315***	2.997***
	(0.165)	(0.164)	(0.190)	(0.167)
Observations	712	712	712	712
R^2	0.023	0.085	0.049	0.034
Adj. R^2	0.018	0.077	0.043	0.028

Note: *p<0.1; **p<0.05; ***p<0.01
Standard errors are in parentheses.
Gender: Female and Non-binary as reference category.
Sample: Prolific sample participants as reference category.
Westin Index: Privacy Fundamentalists as reference category.

Table 7: OLS regression: Functionality loss caused by fingerprinting countermeasures

Dep. Variable	**Functionality Loss**			
	Base Model	**Model 1**	**Model 2**	**Model 3**
Age	-0.007	-0.008	-0.008	-0.007
	(0.006)	(0.006)	(0.006)	(0.006)
Gender	-0.065	-0.046	-0.020	-0.052
	(0.097)	(0.098)	(0.099)	(0.099)
IT-Related Background	-0.188*	-0.180*	-0.150	-0.177
	(0.108)	(0.108)	(0.110)	(0.110)
Sample	-0.190	-0.218	-0.236	-0.209
	(0.164)	(0.165)	(0.165)	(0.167)
Westin Index				
Privacy Pragmatists		0.155		
		(0.110)		
Privacy Unconcerned		0.092		
		(0.264)		
Privacy Behavior Index			-0.075**	
			(0.038)	
PBU				-0.073
				(0.122)
Const	3.7803***	3.697***	4.093***	3.807***
	(0.262)	(0.269)	(0.304)	(0.266)
Observations	712	712	712	712
R^2	0.010	0.013	0.016	0.011
Adj. R^2	0.005	0.005	0.009	0.004

Note: *p<0.1; **p<0.05; ***p<0.01
Standard errors are in parentheses.
Gender: Female and Non-binary as reference category.
Sample: Prolific sample participants as reference category.
Westin Index: Privacy Fundamentalists as reference category.

Table 8: OLS regression: Restricted access & browsing disruptions caused by fingerprinting countermeasures

Dep. Variable	Restricted Access & Browsing Disruptions			
	Base Model	Model 1	Model 2	Model 3
Age	0.001	-0.001	-0.001	-0.001
	(0.003)	(0.003)	(0.003)	(0.003)
Gender	0.011	0.029	0.075	0.061
	(0.059)	(0.059)	(0.059)	(0.060)
IT-Related Background	-0.152**	-0.141**	-0.098	-0.110*
	(0.066)	(0.065)	(0.066)	(0.066)
Sample	0.163	0.123	0.098	0.090
	(0.100)	(0.099)	(0.099)	(0.101)
Westin Index				
Privacy Pragmatists		0.226***		
		(0.066)		
Privacy Unconcerned		0.480***		
		(0.159)		
Privacy Behavior Index			-0.109***	
			(0.023)	
PBU				-0.279***
				(0.073)
Const	3.146***	3.038***	3.598***	3.250***
	(0.159)	(0.162)	(0.182)	(0.160)
Observations	712	712	712	712
R^2	0.010	0.032	0.041	0.030
Adj. R^2	0.004	0.023	0.035	0.023

Note: *p<0.1; **p<0.05; ***p<0.01
Standard errors are in parentheses.
Gender: Female and Non-binary as reference category.
Sample: Prolific sample participants as reference category.
Westin Index: Privacy Fundamentalists as reference category.

Table 9: Cohen's Kappa for text mining categories

Nr.	Category	Cybersecurity	Law Enforcement	User Experience
1	Fingerprint used for own purposes by entity	0.746	0.442	0.762
1a	Explicitly mentioned monetary purpose	0.758	0.429	0.784
2	Trust in the entity to handle fingerprint responsibly	0.968	0.958	0.965
3	Fear of data breaches/hackers	0.669	0.664	0.793

Table 10: Factor loadings for countermeasure scenarios (Oblimin rotation and absolute values smaller than 0.2 omitted)

Nr.	Scenario	Factor 1	Factor 2
1	You can't access your favorite streaming platform	0.261	0.364
2	Your search engine results are not personalized to match your interests		0.566
3	You always need to manually turn off a browser extension to watch a video online		0.625
4	All the progress you made in the game is lost in your next gaming session	0.869	
5	Many games do not work correctly	0.922	
6	You cannot reach the next level because a 3D element of the game's user interface is not visible	0.950	
7	Websites are not displayed in your preferred language		0.534
8	Interactive website elements (search buttons or sliders) overlap each other and do not work		0.582
9	Search engine results look static and less appealing		0.629

B Variable Significances in Both Samples – University Students vs. Prolific Participants

Table 11: Significance and sign of predictors across all model specifications – fingerprinting awareness

	Prolific (N=253)				University Students (N=459)				Combined (N=712)			
Variable	Base	M1	M2	M3	Base	M1	M2	M3	Base	M1	M2	M3
Age	*(-)				***(-)	***(-)	***(-)	***(-)	**(-)	**(-)		
Gender	***(+)	***(+)	***(+)	***(+)					***(+)	***(+)	*(+)	**(+)
IT-Related Background	**(+)	**(+)		*(+)					**(+)	**(+)		
Westin–Privacy Pragmatist												
Westin–Privacy Unconcerned												
Privacy Behavior Index			***(+)				***(+)				***(+)	
SafeBrowserUser				***(+)				***(+)				***(+)
Sample			/				/			*(-)	*(-)	

Note. Empty cell indicates no significant effect in that model. Base Model = Age, Gender, IT-Related Background (Sample for Combined); M1 adds Westin typology; M2 adds Privacy Behavior Index; M3 adds SafeBrowserUser. Significance: $^{*}p < 0.1$, $^{**}p < 0.05$, $^{***}p < 0.01$. "(+)"/"(–)" shows the sign of the estimated coefficient.

Table 12: Significance and sign of predictors across all model specifications – cookie awareness

	Prolific (N=253)				University Students (N=459)				Combined (N=712)			
Variable	Base	M1	M2	M3	Base	M1	M2	M3	Base	M1	M2	M3
Age									*(-)	*(-)	*(-)	
Gender	***(+)	***(+)	*(+)	**(+)	**(+)	**(+)		*(+)	***(+)	***(+)	**(+)	***(+)
IT-Related Background	**(+)	**(+)			***(+)	***(+)		***(+)	***(+)	***(+)	***(+)	***(+)
Westin–Privacy Pragmatist												
Westin–Privacy Unconcerned												
Privacy Behavior Index			***(+)				***(+)				***(+)	
SafeBrowserUser				**(+)				***(+)				***(+)
Sample			/				/		***(-)	***(-)	***(-)	***(-)

Note. Empty cell indicates no significant effect in that model. Base Model = Age, Gender, IT-Related Background (Sample for Combined); M1 adds Westin typology; M2 adds Privacy Behavior Index; M3 adds SafeBrowserUser. Significance: $^{*}p < 0.1$, $^{**}p < 0.05$, $^{***}p < 0.01$. "(+)"/"(–)" shows the sign of the estimated coefficient.

Table 13: Significance and sign of predictors across all model specifications – acceptance of fingerprinting for cybersecurity purposes

	Prolific Sample (N=253)				University Students (N=459)				Combined Sample (N=712)			
Variable	Base	M1	M2	M3	Base	M1	M2	M3	Base	M1	M2	M3
Age	***(+)	***(+)	***(+)	***(+)	***(+)	***(+)	**(+)	**(+)	***(+)	***(+)	***(+)	***(+)
Gender	***(–)	***(–)	**(–)	***(–)	*(–)				***(–)	***(–)	**(–)	***(–)
IT-Related Background												
Westin – Privacy Pragmatist										*(+)		
Westin – Privacy Unconcerned		***(+)								**(+)		
Privacy Behavior Index							***(–)				***(–)	
SafeBrowserUser								***(–)				*(–)
Sample			/				/		**(+)	**(+)	**(+)	**(+)

Note. Empty cell indicates no significant effect in that model. Base Model = Age, Gender, IT-Related Background (Sample for Combined); M1 adds Westin typology; M2 adds Privacy Behavior Index; M3 adds SafeBrowserUser. Significance: $^{*}p < 0.1$, $^{**}p < 0.05$, $^{***}p < 0.01$. "(+)"/"(–)" shows the sign of the estimated coefficient.

Table 14: Significance and sign of predictors across all model specifications – acceptance of fingerprinting for law enforcement purposes

	Prolific Sample (N=253)				University Students (N=459)				Combined Sample (N=712)			
Variable	Base	M1	M2	M3	Base	M1	M2	M3	Base	M1	M2	M3
Age	**(+)		**(+)	**(+)	**(+)	**(+)	**(+)	*(+)	***(+)	**(+)	***(+)	***(+)
Gender	***(-)	***(-)	***(-)	***(-)	***(-)	***(-)	***(-)	***(-)	***(-)	***(-)	***(-)	***(-)
IT-Related Background	*(-)			*(-)	***(-)	***(-)	***(-)	***(-)	***(-)	***(-)	***(-)	***(-)
Westin – Privacy Pragmatist		***(+)								***(+)		
Westin – Privacy Unconcerned		***(+)				*(+)				***(+)		
Privacy Behavior Index			***(-)				***(-)				***(-)	
SafeBrowserUser								***(-)				***(-)
Sample			/				/		***(+)	***(+)	***(+)	***(+)

Note. Empty cell indicates no significant effect in that model. Base Model = Age, Gender, IT-Related Background (Sample for Combined); M1 adds Westin typology; M2 adds Privacy Behavior Index; M3 adds SafeBrowserUser. Significance: $^{*}p < 0.1$, $^{**}p < 0.05$, $^{***}p < 0.01$. "(+)"/"(–)" shows the sign of the estimated coefficient.

Table 15: Significance and sign of predictors across all model specifications – acceptance of fingerprinting for user experience purposes

	Prolific Sample (N=253)				University Students (N=459)				Combined Sample (N=712)			
Variable	Base	M1	M2	M3	Base	M1	M2	M3	Base	M1	M2	M3
Age												
Gender					***(-)	**(-)	**(-)	**(-)	*(-)			
IT-Related Background												
Westin – Privacy Pragmatist		***(+)				***(+)				***(+)		
Westin – Privacy Unconcerned		***(+)				**(+)				***(+)		
Privacy Behavior Index			***(-)				***(-)				***(-)	
SafeBrowserUser								***(-)				***(-)
Sample			/				/		***(+)	**(+)	**(+)	***(+)

Note. Empty cell indicates no significant effect in that model. Base Model = Age, Gender, IT-Related Background (Sample for Combined); M1 adds Westin typology; M2 adds Privacy Behavior Index; M3 adds SafeBrowserUser. Significance: $^{*}p < 0.1$, $^{**}p < 0.05$, $^{***}p < 0.01$. "(+)"/"(–)" shows the sign of the estimated coefficient.

Table 16: Significance and sign of predictors across all model specifications – functionality loss caused by fingerprinting countermeasures

	Prolific Sample (N=253)				University Students (N=459)				Combined Sample (N=712)			
Variable	Base	M1	M2	M3	Base	M1	M2	M3	Base	M1	M2	M3
Age		*(-)	*(-)									
Gender												
IT-Related Background	***(-)	***(-)	**(-)	**(-)					*(-)	*(-)		
Westin – Privacy Pragmatist												
Westin – Privacy Unconcerned												
Privacy Behavior Index											**(-)	
SafeBrowserUser												
Sample			/				/					

Note. Empty cell indicates no significant effect in that model. Base Model = Age, Gender, IT-Related Background (Sample for Combined); M1 adds Westin typology; M2 adds Privacy Behavior Index; M3 adds SafeBrowserUser. Significance: $^{*}p < 0.1$, $^{**}p < 0.05$, $^{***}p < 0.01$. "(+)"/"(–)" shows the sign of the estimated coefficient.

Table 17: Significance and sign of predictors across all model specifications – restricted access & browsing disruptions caused by fingerprinting countermeasures

	Prolific Sample (N=253)				University Students (N=459)				Combined Sample (N=712)			
Variable	Base	M1	M2	M3	Base	M1	M2	M3	Base	M1	M2	M3
Age												
Gender												
IT-Related Background	**(-)	**(-)	*(-)	*(-)					**(-)	**(-)		*(-)
Westin – Privacy Pragmatist		**(+)				**(+)				***(+)		
Westin – Privacy Unconcerned		**(+)				*(+)				***(+)		
Privacy Behavior Index			***(-)				***(-)				***(-)	
SafeBrowserUser				**(-)				***(-)				***(-)
Sample			/				/					

Note. Empty cell indicates no significant effect in that model. Base Model = Age, Gender, IT-Related Background (Sample for Combined); M1 adds Westin typology; M2 adds Privacy Behavior Index; M3 adds SafeBrowserUser. Significance: $^{*}p < 0.1$, $^{**}p < 0.05$, $^{***}p < 0.01$. "(+)"/"(–)" shows the sign of the estimated coefficient.

C Tables and Figures – Demographics and Privacy Metrics

Table 18: Country of residence by sample

Country of Residence	Prolific	University	Total
Germany	0 (0.0%)	453 (95.8%)	453 (47.4%)
US	131 (50.2%)	0 (0.0%)	131 (13.7%)
UK	130 (49.8%)	0 (0.0%)	130 (13.6%)
Other	0 (0.0%)	4 (0.8%)	4 (0.4%)
China	0 (0.0%)	3 (0.6%)	3 (0.3%)
Czech Republic	0 (0.0%)	2 (0.4%)	2 (0.2%)
Spain	0 (0.0%)	2 (0.4%)	2 (0.2%)
Austria	0 (0.0%)	1 (0.2%)	1 (0.1%)
Belarus	0 (0.0%)	1 (0.2%)	1 (0.1%)
Colombia	0 (0.0%)	1 (0.2%)	1 (0.1%)
Indonesia	0 (0.0%)	1 (0.2%)	1 (0.1%)
No answer	0 (0.0%)	1 (0.2%)	1 (0.1%)
Slovakia	0 (0.0%)	1 (0.2%)	1 (0.1%)
Taiwan	0 (0.0%)	1 (0.2%)	1 (0.1%)
Turkey	0 (0.0%)	1 (0.2%)	1 (0.1%)
Vietnam	0 (0.0%)	1 (0.2%)	1 (0.1%)
Total	261 (100%)	473 (100%)	734 (100%)

Table 19: Age and gender by country of residence and sample

Residence	Age		Gender			
	Mean	Median	Fem.	Male	Non-b	Not disclose
Germany	21.98	21	184	264	0	5
Other	22.85	23	10	9	0	1
UK	41.62	41	69	61	0	0
US	44.82	43	72	57	1	1
Sample						
Prolific	43.2	42	141	118	1	1
University	22	21	194	273	0	6

Table 20: Level of education distribution in samples

Level of Education	Prolific	University	Total
College graduate (Bachelor's or equivalent degree)	115	175	290
Doctoral degree	2	0	2
High school diploma	34	230	264
Less than high school	1	0	1
Master's degree	42	21	63
Other, please specify	1	8	9
Prefer not to say	3	6	9
Professional degree after college (e.g., law, medicine)	3	0	3
Some college	53	31	84
Vocational training	7	2	9
SUM	**261**	**473**	**734**

Table 21: Employment status distribution by sample

Employment Status	Prolific	University	Total
Disabled	5	0	5
Employed full-time	141	4	145
Employed full-time, Student	1	5	6
Employed part-time	44	31	75
Employed part-time, Student	0	94	94
Homemaker	7	0	7
Other Employment	5	1	6
Prefer not to say	3	2	5
Retired	18	0	18
Student	8	291	299
Student, Disabled	0	1	1
Unemployed NOT looking for work	2	3	5
Unemployed NOT looking for work, Disabled	1	0	1
Unemployed NOT looking for work, Student	0	7	7
Unemployed looking for work	26	12	38
Unemployed looking for work, Student	0	22	22
SUM	**261**	**473**	**734**

Table 22: IT-related background by sample

IT-Related Background	University	Prolific	Total
No	121	185	306
Prefer not to Say	8	7	15
Yes	344	69	413
SUM	**473**	**261**	**734**

Table 23: Time spent online by sample

Time Spent Online	University	Prolific	Total
Less than 1 hour	1	0	1
1 - 2 hours	19	20	39
2 - 3 hours	59	40	99
3 - 4 hours	96	44	140
4 - 5 hours	108	43	151
More than 5 hours	190	114	304

Table 24: Browser usage by sample

Browser	Prolific	University	Total
Firefox	184	243	427
Opera	71	127	198
Tor Browser	44	66	110
Safari	156	385	541
Chrome	253	431	684
Microsoft Edge	171	263	434
Brave	39	46	85
Other	11	47	58

Table 25: Privacy browser users by sample

	University		Prolific		Total	
	n	%	n	%	n	%
No	379	80.1%	196	75.1%	575	78.3%
Yes	94	19.9%	65	24.9%	159	21.7%

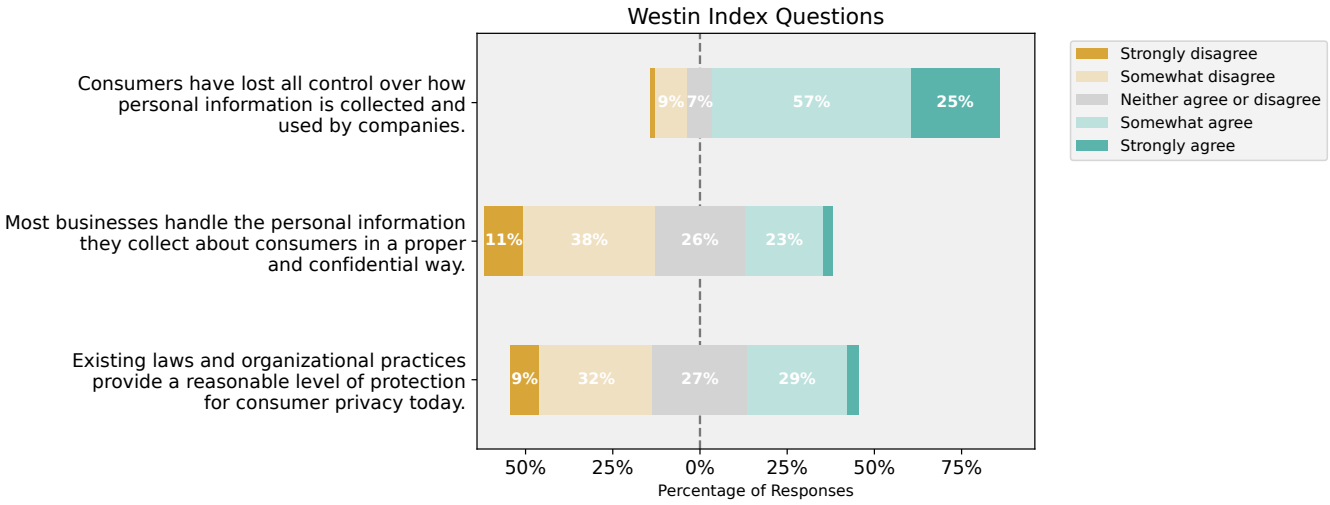


Figure 10: Westin Index – responses

Table 26: Westin Index category distribution by sample

	Prolific		University		Total	
	n	%	n	%	n	%
Privacy Fundamentalist	68	26.1%	122	25.8%	190	25.9%
Privacy Pragmatist	176	67.4%	341	72.1%	517	70.4%
Privacy Unconcerned	17	6.5%	10	2.1%	27	3.7%
SUM	**261**	**100%**	**473**	**100%**	**734**	**100%**

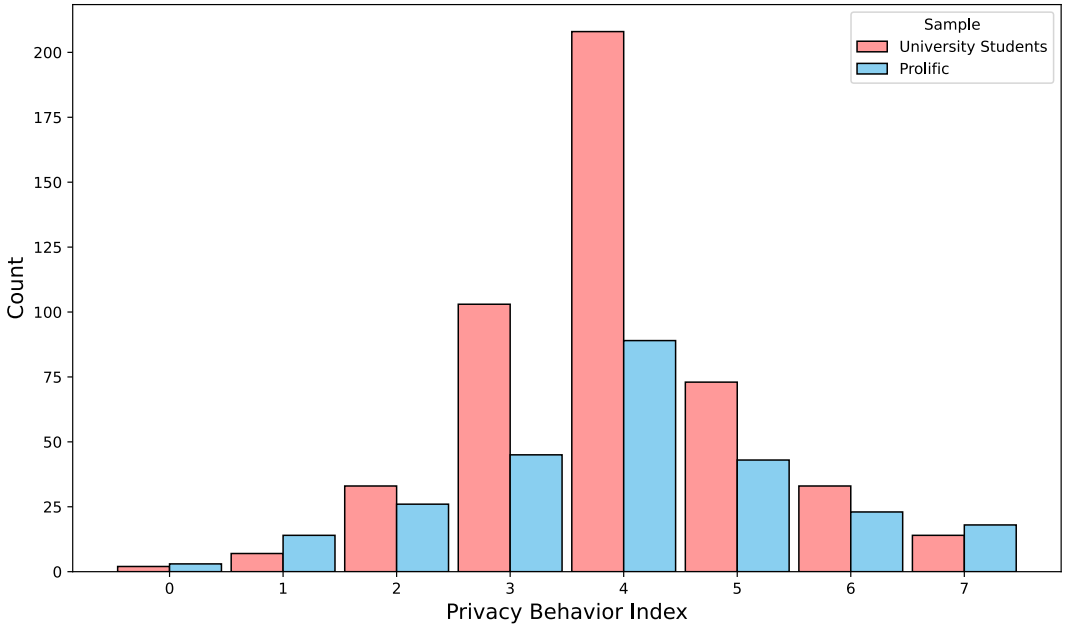


Figure 11: Privacy Behavior Index – distribution of categories among samples

D Questionnaire

We care about the quality of our data. In order for us to get the most accurate measures of your knowledge and opinions, it is important that you thoughtfully provide your best answers to each question in the study.

- **Will you provide your best answers to each question in this study?**
  - ○ I will provide my best answers.
  - ○ I will NOT provide my best answers.
  - ○ I cannot promise either way.

- **Which of the following technologies have you used or encountered?**
  (Select the answers that apply.)
  - □ Enabling "Do Not Track" in the browser settings.
  - □ Using the Tor Browser.
  - □ Using private mode in browsers (privacy or incognito mode).
  - □ Deleting cookies.
  - □ Denying third-party cookies.
  - □ Using the Brave Browser.
  - □ Deactivating JavaScript.

- **Indicate your level of agreement regarding the following statements:**
  (Select the answers that apply.)
  - – Consumers have lost all control over how personal information is collected and used by companies.
  - – Most businesses handle the personal information they collect about consumers in a proper and confidential way.
  - – Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.
  - ○ Strongly disagree
  - ○ Somewhat disagree
  - ○ Neither disagree nor agree
  - ○ Somewhat agree
  - ○ Strongly agree

- **Web Cookies**
  (Which of the following statements is applicable to your knowledge of web cookies?)
  - ○ I do not know what web cookies are.
  - ○ I have heard of web cookies before, but I do not know how they work and how they are applied.
  - ○ I am aware of web cookies, their functionality, and their applications.
  - ○ I am aware of web cookies and I actively employ countermeasures against them.
- **Digital Fingerprinting**
  (Which of the following statements is applicable to your knowledge of digital fingerprinting?)
  - ○ I do not know what digital fingerprinting is.
  - ○ I have heard of digital fingerprinting before, but I do not know how it works and how it is applied.
  - ○ I am aware of digital fingerprinting, its functionality, and its applications.
  - ○ I am aware of digital fingerprinting and I actively employ countermeasures against it.

- **Tell us a bit about your browsing preferences and what you care about while browsing the internet.**
  (Do you agree or disagree with the following statements?)
  - – My browsing experience significantly decreases when I can't access all the websites I want to.
  - – I often access my browsing history to find websites I visited in previous browsing sessions.
  - – When I download and install applications, it needs to be fast, and I don't want to bother selecting the correct file for my operating system.
  - – I care about fast loading speeds while browsing on the Internet.
  - – I only use one browser for all my online activities.
  - – I am annoyed by lengthy login procedures and want to access my accounts anytime without restrictions.
  - – CAPTCHAs slow down my productivity and browsing speed.
  - – My browsing experience significantly decreases when videos or other media elements do not load.
  - ○ Strongly disagree
  - ○ Somewhat disagree
  - ○ Neither disagree nor agree
  - ○ Somewhat agree
  - ○ Strongly agree
  - ○ Don't know

Digital Fingerprinting
(We would like to inform you about digital fingerprinting technology as covered in this study. Please read the description carefully.)

What is digital fingerprinting?
Digital fingerprinting is the process where a script or website collects small pieces of information about a user's device, assembling them into a unique "fingerprint" of the user's device. To generate a digital fingerprint, characteristics unique to an individual, their browser, and their hardware setup, including data like screen resolution and installed fonts, are gathered.

What can a digital fingerprint reveal?
Digital fingerprints can reveal insights into a user's online activities and interests, enabling tracking across websites and apps. This information may expose personal characteristics such as political affiliation, sexual orientation, education level, income bracket, etc. Unlike cookies, digital fingerprints are stable identifiers the user cannot delete. They may also be linked to a user's real-life identity based on logins to various online services.

What are the various uses of digital fingerprints?
Online service providers use digital fingerprints for multiple purposes. Companies use them to personalize advertisements, enhance user experiences, and boost security by identifying and blocking

potentially fraudulent login attempts. Service providers may utilize digital fingerprints to track cybercriminals and other malicious actors based on information from service providers.

Can I protect myself against fingerprinting?
Despite the widespread use of digital fingerprinting, general user awareness about it is not as high as with cookies. Unlike cookies, it is much harder to individually protect yourself against browser fingerprinting; available countermeasures are only effective to a limited degree and have the potential to substantially reduce convenience while browsing.

- **Which of the following statements describe what you know about digital fingerprinting?**
  (Check all that apply.)
  - ☐ It is a technology to check which immigrants and travelers should be admitted when crossing national borders.
  - ☐ It is a technology that could be used to detect potentially fraudulent login attempts on websites.
  - ☐ It is a technology to track online activities of users.
  - ☐ It is a technology to identify users based on the characteristics of their browsers, applications, devices, and network connections.
  - ☐ It is a technology to identify a person based on biometrics (e.g., facial features, fingerprints, irises).
  - ☐ None of the above.

- **Cybersecurity through digital fingerprinting focuses on protecting users' security. How acceptable would you find the usage of digital fingerprinting in the following use cases:**
  (Select the answers that apply.)
  - – Detecting potential criminal access to user accounts.
  - – Preventing illegal attempts to access databases comprising user information.
  - – Enforcing paywalls to non-paying customers.
  - – Leveraging Artificial Intelligence to improve fraud prevention practices.
  - – Educating the user about their account security.
  - – Reducing the amount of phishing mails.
  - ○ Strongly unacceptable
  - ○ Unacceptable
  - ○ Indifferent
  - ○ Acceptable
  - ○ Strongly acceptable
- **Imagine your digital fingerprint is now being collected for cybersecurity purposes. Indicate your level of agreement with the following statements about your digital fingerprint:**
  (Select the answers that apply.)
  - – I would like to get notifications when my digital fingerprint is collected.
  - – I would like to disclose my digital fingerprinting preferences in my device's settings (e.g., DoNotFingerprint button).
  - – I would like to be notified and provided with a reason when my digital fingerprint is collected.
  - – I would like to have the option to consent or decline the collection of my digital fingerprint on the website.
  - ○ Strongly disagree
  - ○ Disagree
  - ○ Neither agree or disagree
  - ○ Agree
  - ○ Strongly agree
- **Do you trust companies to use your digital fingerprint primarily for security reasons? State your thoughts.**
  [Textarea]

- **Law enforcement today is embracing digital fingerprinting as a tool to improve the effectiveness of their investigations and public safety efforts. How acceptable would you find the usage of digital fingerprinting in the following use cases:**
  (Select the answers that apply.)
  - – Performing digital forensic analysis in the context of online fraud.
  - – Tracking suspicious online search queries for crime prevention.
  - – Supporting criminal investigations with evidence obtained through digital fingerprinting.
  - – Employing digital fingerprinting technology to aid in missing persons investigations.
  - – Preventing harm by inspecting online chat forums for signs of criminal activities.
  - – Controlling the rehabilitation of prisoners by tracking their online activities.
  - ○ Strongly unacceptable
  - ○ Unacceptable
  - ○ Indifferent
  - ○ Acceptable
  - ○ Strongly acceptable
- **Imagine your digital fingerprint is now being collected for law enforcement purposes. Indicate your level of agreement with the following statements about your digital fingerprint:**
  (Select the answers that apply.)
  - – I would like to get notifications when my digital fingerprint is collected.
  - – I would like to have the option to consent or decline the collection of my digital fingerprint on the website.
  - – I would like to be notified and provided with a reason when my digital fingerprint is collected.
  - – I would like to disclose my digital fingerprinting preferences in my device's settings (e.g., DoNotFingerprint button).
  - ○ Strongly disagree
  - ○ Disagree
  - ○ Neither agree or disagree
  - ○ Agree
  - ○ Strongly agree

- **Do you trust your local government to handle your digital fingerprint in a responsible way? State your thoughts.**
  [Textarea]

- **Companies often state that they employ digital fingerprinting to enrich the user experience. How acceptable would you find the usage of digital fingerprinting in the following use cases:**
  (Select the answers that apply.)
  - Accelerating user logins by bypassing CAPTCHAs.
  - Elevating the online dating experiences with personalized and relevant matches.
  - Relevant ad recommendations based on individual interests.
  - Tailored websites for personalized user experience.
  - Optimizing job search results for relevant and fulfilling career opportunities.
  - Dynamic price determination of services or products.
  - Strongly unacceptable
  - Unacceptable
  - Indifferent
  - Acceptable
  - Strongly acceptable
- **Imagine your digital fingerprint is now being collected for user experience purposes. Indicate your level of agreement with the following statements about your digital fingerprint:**
  (Select the answers that apply.)
  - I would like to get notifications when my digital fingerprint is collected.
  - I would like to have the option to consent or decline the use of my digital fingerprint on the website.
  - I would like to get notified and provided with a reason when my digital fingerprint is collected.
  - I would like to disclose my digital fingerprinting preferences in my device's settings (e.g., DoNotFingerprint button).
  - Strongly disagree
  - Disagree
  - Neither agree or disagree
  - Agree
  - Strongly agree
- **Do you trust companies to use your digital fingerprint primarily for user experience reasons? Could you think of other potential applications of fingerprinting regarding user experience? State your thoughts.**
  [Textarea]

Countermeasures against fingerprinting
(Please carefully read the text about countermeasures to combat fingerprinting:)

Mitigating digital fingerprinting-based tracking presents challenges. Unlike cookies that browsers can block, browsers by default struggle to prevent digital fingerprinting effectively. Fingerprinting countermeasures risk breaking functionality on various websites when attempting to prevent a site from accessing information such as screen dimensions, installed fonts, or hardware information on your machine.

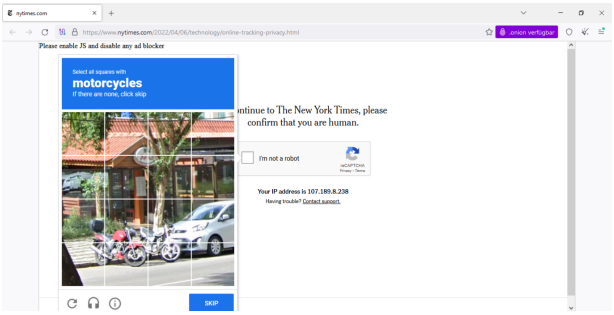
Available countermeasures range from browser extensions to special browsers designed for privacy on the web. While they all come at some usability cost, which will be evaluated on later pages of this survey, their effectiveness regarding protection against fingerprinting differs. Paradoxically, some countermeasures even increase a user's fingerprintability, making the user's device or browser even more distinguishable.

All countermeasures follow the same approach, trying to make the user less identifiable. Standard techniques are altering browser attributes, blocking potential fingerprinting scripts, or turning off certain APIs, which can be used to obtain details about the browser or device running the browser.

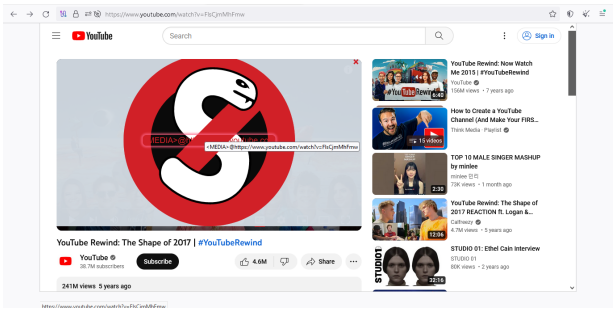
Countermeasures against fingerprinting
(Please carefully read the text about countermeasures to combat fingerprinting:)

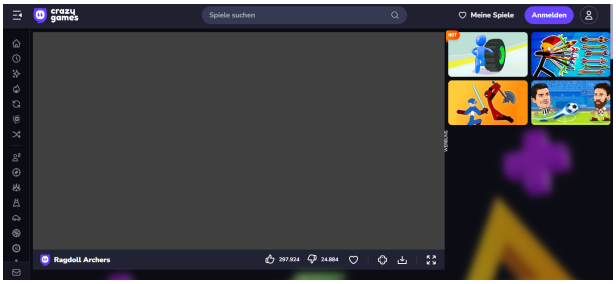
Restricted resource access

Some effective countermeasures against fingerprinting come at a cost: media elements are only accessible to a limited degree, and the user gets denied access to online resources. Pages can look static and users need to accept longer loading times and degraded service from some websites.



Users frequently arrive at prolonged CAPTCHAs and can't access resources or login services.





Accessing videos or media resources requires manual user intervention.

- **Imagine you are browsing the web with active fingerprinting protection**
  (Would you consider turning your fingerprinting protection off in the following cases? "Would not disable" means that you continue to browse the web with active fingerprinting protection. "Would disable" means that you turn off your fingerprinting protection to eliminate the given side effect.)

  – You can't access your favorite streaming platform.
  – Your search engines results are not personalized to match your interests.
  – You always need to manually turn off a browser extension to watch a video online.
  ○ Would definitely not disable
  ○ Would probably not disable
  ○ Not sure
  ○ Would probably disable
  ○ Would definitely disable

Countermeasures against fingerprinting
(Please read the provided text carefully.)

Unavailability of Browser Games

Countermeasures intervening with Graphic APIs cause some online services, like online graphic design tools or browser games, to be unavailable to users.

The sliding images above show how a countermeasure breaks the functionality of browser games.

- **Imagine you are playing an online browser game with active fingerprinting protection.**
  (Would you consider turning your fingerprinting protection off in the following cases? "Would not disable" means that you continue to browse the web with active fingerprinting protection. "Would disable" means that you turn off your fingerprinting protection to eliminate the given side effect.)

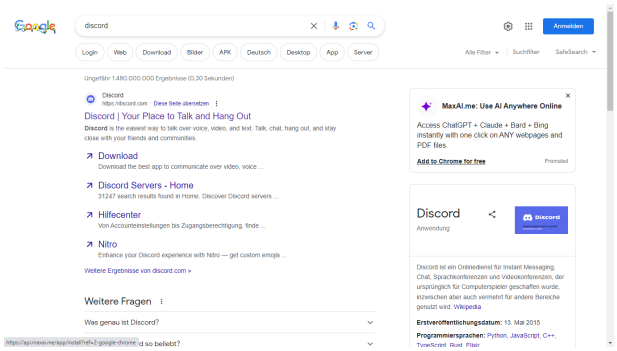
  – All the progress you made in the game is lost in your next gaming session.
  – Many games do not work correctly.
  – You cannot reach the next level, because a 3D element of the game's user interface is not visible.
  ○ Would definitely not disable
  ○ Would probably not disable
  ○ Not sure
  ○ Would probably disable
  ○ Would definitely disable

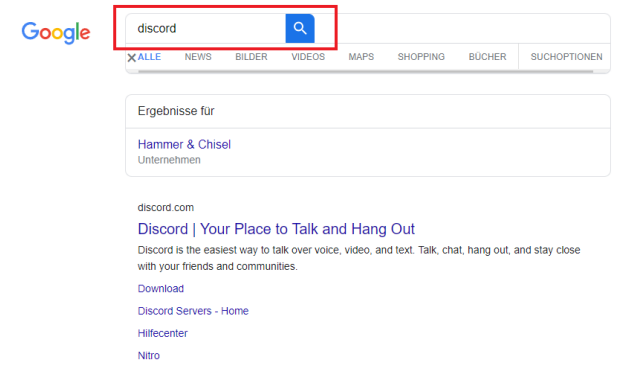
Countermeasures against fingerprinting
(Please carefully read the text about countermeasures to combat fingerprinting.)

Static and less appealing webpages

Some countermeasures randomize browser attributes to conceal the actual fingerprint, this process is called spoofing. Others block scripts associated with known trackers, reducing traceability.

While these countermeasures only reduce the effectiveness of fingerprinting to a limited degree, they also come with some usability issues:





The first screenshot shows the Google search with no spoofing extension activated, while the second screenshot depicts a browser with a browser extension enabled. Some extensions can cause webpage design elements to disappear, overlap, or have an incorrect size.

- **Imagine you are browsing the web with active fingerprinting protection**
  (Would you consider turning your fingerprinting protection off in the following cases? "Would not disable" means that you continue to browse the web with active fingerprinting protection. "Would disable" means that you turn off your fingerprinting protection to eliminate the given side effect.)

  – Websites are not displayed in your preferred language.
  – Interactive website elements (search buttons or sliders) overlap each other and do not work.
  – Search engine results look static and less appealing.
  ○ Would definitely not disable
  ○ Would probably not disable
  ○ Not sure
  ○ Would probably disable
  ○ Would definitely disable

- **Countermeasures and usability**
  (Now that you know what fingerprinting does and how typical countermeasures affect a browser's usability, consider the following scenarios: Imagine your digital fingerprint is captured, and now you need to choose. Would you apply protection mechanisms against fingerprinting if they cause the following side effects: "Definitely not" means you don't want to use a countermeasure if it causes the respective side effect. "Definitely" means you are definitely willing to accept the respective side effect for better fingerprinting protection.)

  – A website you want to visit isn't available, as the website host blocks your browser.
  – Your browsing history is never saved.
  – You need to manually select the correct installer file for a software tool because your browser, by default, provides you with a file for the wrong operating system.
  – Clicking a link and reloading a page takes triple the usual time.
  – Please select probably not in this question.
  – You need separate browsers for online shopping, working, and chatting in a forum.
  – You want to log into your online banking system, and it detects you as a potential bot and denies access.
  – You want to access online resources, but the CAPTCHA to identify you as human appears multiple times, denying you fast access.
  – You want to watch a video on a news site, but it does not load.
  ○ Definitely not
  ○ Probably not
  ○ Possibly
  ○ Probably
  ○ Definitely

- **Did our survey change your attitude concerning browsing on the internet?**
  ○ Yes
  ○ If Yes: How did your attitude change? [Textarea]
  ○ No

Finally, please tell us a bit more about yourself.

- **How old are you right now?**
  [Textarea] / Prefer not to say
- **Which is the country you're currently living in?**

  – Apsny
  – Afghanistan
  – Albania
  – Antarctic
  – Algeria
  – American Samoa
  – Andorra
  – Angola
  – Anguilla
  – Antigua and Barbuda
  – Argentina
  – Armenia
  – Aruba

  - Australia
  - Austria
  - Azerbaijan
  - Bahamas
  - Bahrain
  - Bangladesh
  - Barbados
  - Belarus
  - Belgium
  - Åland Islands
  - Belize
  - Benin
  - Bermuda
  - Bhutan
  - Bolivia
  - Caribbean Netherlands
  - Bosnia and Herzegovina
  - Botswana
  - Brasil
  - Bouvet Islands
  - British Virgin Islands
  - Brunei
  - British Indian Ocean Territory
  - Bulgaria
  - Burkina Faso
  - Burma
  - Burundi
  - Cambodia
  - Cameroons
  - Canada
  - Cape Verde
  - Cayman Islands
  - Central African Republic
  - Chad
  - Chile
  - China (People's Republic of China)
  - Christmas Island
  - Cocos Islands
  - Colombia
  - Comoros
  - Republic of the Congo
  - Democratic Republic of the Congo
  - Cook Islands
  - Costa Rica
  - Côte d'Ivoire
  - Croatia
  - Cuba
  - Curaçao
  - Cyprus
  - Czech Republic
  - Denmark
  - Djibouti
  - Dominica
  - Dominican Republic
  - East Timor
  - Ecuador
  - Egypt
  - El Salvador
  - Equatorial Guinea
  - Eritrea
  - Estonia
  - Ethiopia
  - Falkland Islands
  - Faroe Islands
  - Federated States of Micronesia
  - Fiji
  - Finland
  - France
  - French Guiana
  - French Polynesia
  - French Southern Territories
  - Gabon
  - Gambia
  - Georgia
  - Germany
  - Ghana
  - Gibraltar
  - Greece
  - Greenland
  - Grenada
  - Guadeloupe
  - Guam
  - Guatemala
  - Guernsey
  - Guinea
  - Guinea-Bissau
  - Guyana

  ...

  - No answer

- **Which of the following web browsers have you used?** *(Check all that apply.)*
  - ☐ Firefox
  - ☐ Opera
  - ☐ Tor browser
  - ☐ Safari
  - ☐ Chrome
  - ☐ Microsoft Edge
  - ☐ Brave
  - ☐ Other, please tell us: [Textarea]
- **Which of the following items is different from the others?**
  - ○ Mercedes
  - ○ Audi
  - ○ Toyota
  - ○ BMW
  - ○ Microsoft
  - ○ Tesla
- **Have you studied or worked in an IT-related field?**
  - ○ Yes
  - ○ No
  - ○ Prefer to not disclose
- **What is the highest level of education you have completed?**

- Less than high school
- High school diploma
- Vocational training
- Some college
- College graduate (Bachelor's or equivalent degree)
- Master's degree
- Doctoral degree
- Professional degree after college (e.g., law, medicine)
- Other, please specify: [Textarea]
- Prefer not to say

- **What is your current employment status?**
  (Check all that apply.)
  - ☐ Employed full-time
  - ☐ Employed part-time
  - ☐ Unemployed looking for work
  - ☐ Unemployed NOT looking for work
  - ☐ Homemaker
  - ☐ Student
  - ☐ Retired
  - ☐ Disabled
  - ☐ Other, please specify: [Textarea]
  - ☐ Prefer not to say
- **What is your gender?**
  - Male
  - Female
  - Non-binary
  - Prefer to self-describe: [Textarea]
  - Prefer not to disclose
- **How much time do you spend online on a daily basis?**
  (Select the range of hours.)
  - less than 1 hour
  - 1-2 hours
  - 2 - 3 hours
  - 3 - 4 hours
  - 4 - 5 hours
  - more than 5 hours

- **When answering the questions in the study, did you follow the provided instructions?**
  (Please answer honestly. Your answer has NO consequences for you or the compensation you will receive.)
  - I answered all questions according to the provided instructions.
  - I sometimes chose random answer options because I was not motivated to answer the question or did not know how to answer it.
  - I often chose random answer options because I wanted to finish as quickly as possible.
- **Could you complete the questionnaire without distractions?**
  (Please answer honestly. Your answer has NO consequences for you or the compensation you will receive.)
  - I completed the study with full attention.
  - I was sometimes distracted (by people, noise, etc.).
  - I was often distracted (by people, noise, etc.).
- **Is there anything else you would like to tell us?**
  [Textarea]
