POLITECNICO DI TORINO
Repository ISTITUZIONALE

AwEE - Improving Privacy Awareness by Leveraging Gamification Principles

Original
AwEE - Improving Privacy Awareness by Leveraging Gamification Principles / Calo', L., Laudadio, L., Vetro', A., Coppola, R., Torchiano, M.. - ELETTRONICO. - (2025), pp. 411-419. (2025 International Conference on Information Technology for Social Good Antwerp (BE) 3-5 September 2025) [10.1145/3748699.3749819].

Availability:
This version is available at: 11583/3004801 since: 2026-01-09T13:33:29Z

Publisher:
ACM

Published
DOI:10.1145/3748699.3749819

Terms of use:

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright

(Article begins on next page)

02 November 2026

Check for updates

ACM DIGITAL LIBRARY | Association for Computing Machinery | acm open

Latest updates: https://dl.acm.org/doi/10.1145/3748699.3749819

RESEARCH-ARTICLE

AwEE - Improving Privacy Awareness by Leveraging Gamification Principles

LUCA CALÒ, Polytechnic of Turin, Turin, TO, Italy

LORENZO LAUDADIO, Polytechnic of Turin, Turin, TO, Italy

ANTONIO VETRO', Polytechnic of Turin, Turin, TO, Italy

RICCARDO COPPOLA, Polytechnic of Turin, Turin, TO, Italy

M. TORCHIANO, Polytechnic of Turin, Turin, TO, Italy

Open Access Support provided by:

Polytechnic of Turin

PDF Download
3748699.3749819.pdf
09 January 2026
Total Citations: 0
Total Downloads: 91

Published: 03 September 2025

Citation in BibTeX format

GoodIT '25: International Conference on Information Technology for Social Good
September 3 - 5, 2025
Antwerp, Belgium

Conference Sponsors:
SIGCAS

https://doi.org/10.1145/3748699.3749819
ISBN: 9798400720895

AwEE - Improving Privacy Awareness by Leveraging Gamification Principles

Luca Calò
Politecnico di Torino
Torino, Italy
mail@olac.eu

Lorenzo Laudadio
Politecnico di Torino
Torino, Italy
lorenzo.laudadio@polito.it

Antonio Vetrò
Politecnico di Torino
Torino, Italy
antonio.vetro@polito.it

Riccardo Coppola
Politecnico di Torino
Torino, Italy
riccardo.coppola@polito.it

Marco Torchiano
Politecnico di Torino, Italy
Torino, Italy
marco.torchiano@polito.it

Abstract

In today's digital society, companies regularly collect vast amounts of personal data from their users, raising profound privacy and ethical concerns. Yet, despite many cases of large personal data breaches being documented, most users remain unaware of the real-time flow of their information while they use online services. We describe the design and development of AwEE, a browser extension designed to address this gap by enhancing privacy awareness among users, incorporating gamification principles. It provides real-time insights during users' web browsing, highlighting requests made to companies with known issues in data handling practices. To increase user engagement, the extension incorporates various gamification elements. We detail the results of a preliminary evaluation of AwEE, conducted in an academic context. The results from such evaluation suggest that users find the tool both enjoyable and informative, demonstrating the potential of combining privacy tools with gamification to promote greater awareness and proactive privacy management. The tool is openly available on Zenodo.[1]

ACM Reference Format:
Luca Calò, Lorenzo Laudadio, Antonio Vetrò, Riccardo Coppola, and Marco Torchiano. 2025. AwEE - Improving Privacy Awareness by Leveraging Gamification Principles. In *International Conference on Information Technology for Social Good (GoodIT '25), September 03–05, 2025, Antwerp, Belgium.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3748699.3749819

1 Introduction

Today's world and society are strongly characterized by the ubiquity of digital connections and the continuous extraction of value from every human activity in the form of data.

There are now many companies that have built or adapted their business models around this extractive possibility, guaranteed by the increasing diffusion and demand for digital goods and personalized services.

Shoshana Zuboff defines the above picture as Surveillance Capitalism. This is a new form of capitalism that claims human experience as free raw material translated into data and used to manufacture predictive products that anticipate people's wants or needs. Ultimately, this provides powerful corporations the ability to manipulate and control our behaviors [32].

Nick Couldry and Ulises A. Mejias refer to this process as Data Colonialism and identify it as a key dimension of what they believe to be the current phase of capitalism's expansion [2].

This continuous flow of data and information creates concerns about the users' privacy and how ethically their data are handled, while there are various cases that shifted the public debate on these issues. Here is a non-all-inclusive list of relevant examples:

- Edward Snowden case in 2013, when the extensive monitoring and mass data collection of telephone metadata and internet communications by the NSA were made public [9];
- Cambridge Analytica in 2018, when the personal data of millions of Facebook users was obtained without their authorization to craft targeted political ads during the 2016 US presidential election campaign [10];
- The lawsuit started in 2020, that forced Google to agree to a $5 billion settlement in 2024, destroy billions of records and update its data collection practices. It alleged that the company secretly tracked users as they browsed in incognito mode, turning it into a *"mine of unaccountable information"*[12];
- The presence of additional code within the web browser integrated into the TikTok app, allowing the company to track every character typed by users, found in 2022 [29].

These kinds of concerns led to multiple attempts to legislate against the indiscriminate harvesting and usage of personal data, in order to ensure the protection of users' privacy. In this regard the European Union's General Data Protection Regulation (GDPR) [23] is the most significant and emblematic example of a unified framework to give citizens more control over their data, becoming a model for many other laws around the world.

The introduction of cutting-edge laws is only part of the changes needed for user privacy to be truly protected. It is necessary, above all, to change the habits of people, who got used to surrendering personal information in exchange for seemingly free (in terms of money) services.

[1] https://doi.org/10.5281/zenodo.15591402

This work is licensed under a Creative Commons Attribution 4.0 International License.
GoodIT '25, Antwerp, Belgium
© 2025 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-2089-5/25/09
https://doi.org/10.1145/3748699.3749819

Against this backdrop, we propose AwEE, a browser extension that aims to become a tool to improve users' awareness about where their data goes while surfing the Internet. AwEE allows users to get a clear view of the list of HTTP requests made during their navigation. The extension highlights the requests directed to *Bad Hosts*, defined as companies that are known to adopt bad practices in handling users' data. To incentivize its use, AwEE is equipped with several gamification elements. The tool was subject to a preliminary evaluation with an experiment in an academic context. The extension was inspired by our previous work *Minos* [16]; further details can be found in Section 2.1.

The goal of this paper is to describe the development process of the AwEE browser extension and to present the experiment design and results. In Section 2 we introduce the background behind our project and present which previous work inspired us. In Section 3, we dive into the creation of our tool and provide an explanation of how the extension works. In Section 5, we describe the brief experiment we conducted to obtain a preliminary evaluation of AwEE and present the results, while in Section 4 we present a list of privacy-related browser extensions that had an impact on the AwEE development process. In Section 6 we list what we consider as possible threats to the validity of our work, and finally in Section 7 we summarize our main contributions and provide an overview of possible future improvements.

2 Background and Related Work

In this section we present some technical background to better understand the context in which AwEE was developed, along with some essential related work which served as inspiration.

2.1 Privacy Related Studies

The main motivation behind the development of AwEE is the growing amount of concerns about online privacy and the increasing spread of data-tracking policies adopted by big tech companies. This led to a growing need for tools that empower users to make informed decisions about their privacy and manage their personal information more consciously.

Several studies in the literature address privacy protection on the web. Garimella et al. compared several ad-blocking browser extensions, and assessed their ability to limit trackers, [7]. Other studies focused on the creation of new tools, such as FPMON [4] and FPNET [22], designed to measure and rate fingerprinting activity on websites. Fingerprinting is a technique that uniquely identifies users based on their browser and hardware device characteristics, allowing for pervasive tracking even without the use of cookies. JShelter [25] is a browser extension that instead aims to protect user data from these kinds of techniques. NoScript [17] is another browser extension that introduces several client-side countermeasures against web-based privacy threats.

Our main starting point for the development of AwEE is *Minos* [16], an Electron application that allows browsing the Web while logging HTTP requests. The software combines a browser with a backend tailored to record and analyze personal data transfers to countries outside the European Economic Area (EEA). The term *personal data* in this case refers to the GDPR definition: any kind of information that can lead to the identification of a natural person. Whenever a personal device makes an HTTP request to a certain server, the server can identify the device from its IP address. It follows that even the IP address of a host can be considered as personal data, and each HTTP request results in a personal data transfer. In practice, Minos identifies and logs all the HTTP requests made to a selected subset of third-country domains. The application was used to perform an analysis of the Italian Public Administration entities.

However, in AwEE, we are not directly interested in the geographic location of the target domains. In our case, the focus is on the companies which are behind such domains. We consider specific big tech companies or entities that suffered fines or are under investigation for their bad data handling practices.

2.2 Gamification

Gamification is defined as the adoption of mechanics typical of game design in a non-ludic context [3].

Many examples of works in literature focus on the impact of gamification in privacy protection. Mavroeidi et al. explored the existing connections between privacy and gamification, highlighting the need for programs that educate users on privacy by adopting gamification mechanics [19]. Other authors explored how gamification can be used in designing Privacy Training Programs [20], and highlighted the significance of paying attention to privacy when applying gamification to work environments [26].

The design of the gamification mechanics of AwEE is based on the *Octalysis Framework*, developed by Yu-kai Chou [1]. The framework can be depicted as an octagonal-shape scheme, each side representing one of the eight *Core Drives* (*CDs*). Yu-kai Chou defines them as the fundamental psychological motivators that drive every human action. They are the following: *Epic Meaning & Calling (CD 1)*, *Development & Accomplishment (CD 2)*, *Empowerment of Creativity & Feedback (CD 3)*, *Ownership & Possession (CD 4)*, *Social Influence & Relatedness (CD 5)*, *Scarcity & Impatience (CD 6)*, *Unpredictability & Curiosity (CD 7)* and *Loss & Avoidance (CD 8)*.

The *CDs* are grouped based on the type of motivation they stimulate. The *Left Brain (Extrinsic motivation)* includes drives that focus on logic, analytical thought and ownership, typically derived from the desire to obtain something (*CDs 2, 4, 6*). In contrast, the *Right Brain (Intrinsic motivation)* emphasizes creativity, self-expression, and social dynamics, and is involved in activities that are themselves rewarding (*CDs 3, 5, 7*).

In addition, the *CDs* can be classified as *White Hat Gamification (Positive)*, making people feel powerful, fulfilled, satisfied, in control of their lives and actions (*CDs 1, 2, 3*), or *Black Hat Gamification (Negative)*, which induces feelings of obsession, anxiety, and loss of control (*CDs 6, 7, 8*).

3 AwEE

AwEE is a browser extension that interactively displays the web navigation log, reporting in real-time the requests sent to known *Bad Hosts* from a blacklist, and showing related statistics. It also allows users to download the browsing log in different formats. To improve the user experience, a profile can be created, with the possibility of choosing a username and an avatar. The name "AwEE" stands for "AwarE Extension", reflecting the tool's goal of raising

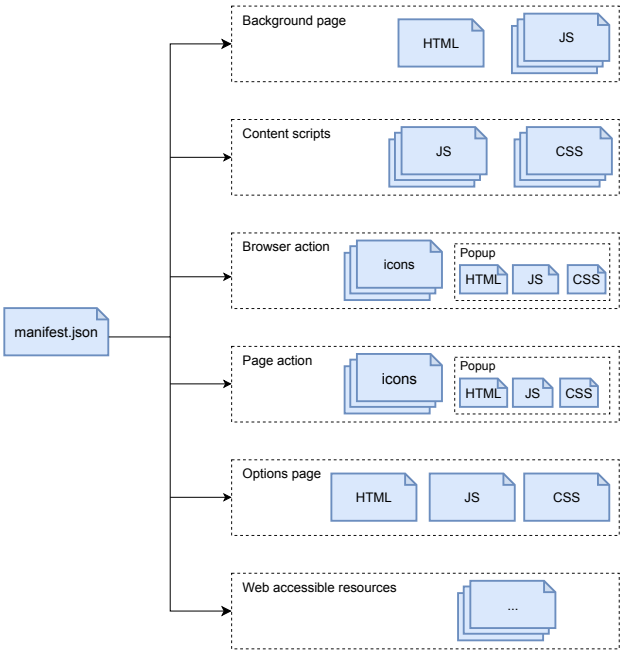


Figure 1: Anatomy of a generic Firefox extension

user awareness about privacy concerns and web threats. The goal of this section is to provide a comprehensive overview of the software, both from a technological perspective and in terms of gamification choices.

3.1 Browser Choices

The software we propose is a browser extension, specifically developed as an extension for Firefox (also called Firefox add-on), a free and open-source web browser developed by the Mozilla Foundation.

The choice of Firefox was mainly dictated by the existence of MDN Web Docs, a comprehensive documentation repository and learning resource for Firefox web developers, maintained by the Mozilla Foundation [21].

However, since according to recent statistics, Firefox is currently used by a fairly small niche of people (around 2.5%)[27], we ported the extension to Chromium. Chromium is an open-source web browser project developed and maintained primarily by Google. Most of the other popular browsers are based on this project, including examples such as Brave, Google Chrome, Microsoft Edge, and Opera.

The steps required to perform the above-mentioned porting were carried out by analyzing both the MDN documentation and the Chrome Extension Docs [8], and ensure that the extension reaches almost all browsers used nowadays.

3.2 Architecture of the extension

AwEE consists of a collection of files, packaged for distribution and installation (see Figure 1). The main files, using MDN as a reference, are:

- *manifest.json* is the only file that must be present in every extension. It contains basic metadata such as the extension's name, version, and manifest version. It provides pointers to other required files like background scripts and browser actions, specifying aspects of the extension's functionality, and it defines required permissions.
- *Background script* is the script that enables monitoring and reacting to events in the browser (*background.js*).
- *Browser Actions* in AwEE's case are an *icon* (the one for the toolbar's extension button) and popup files. A popup is a dialog linked to a toolbar button or an address bar button. When the user clicks on the button, the popup appears. If the user clicks outside the popup, it closes. The popup is defined using an HTML file (*popup.html*) and includes CSS and JavaScript files (*popup.css*, *popup.js*), similar to a standard web page.

Additional local resources are defined for AwEE operation, such as:

- *hosts.json* is a JSON file containing all *Bad Domains*, grouped by the *Bad Host* they refer to (see Section 3.3);
- *description-hosts.json* is a JSON file containing all the *Bad Hosts* descriptions, including references and news case links.

3.3 Bad Hosts

Bad Hosts are defined as companies or organizations that faced issues in managing user data, resulting in fines or ongoing investigations. As a result, *Bad Requests* turn out to be HTTP requests made to domains (we call them *Bad Domains*) that belong to a *Bad Host*.

In drafting our *hosts.json* file, we used the blacklist adopted within *Minos* as a starting point. This blacklist was compiled by volunteers from *MonitoraPA*[2], a community that maintains an automated distributed observatory on the Italian Public Administration. We then grouped the domains by their owning companies, allowing AwEE to report the specific company associated with each *Bad Request*.

To justify the classification of these companies as *Bad Hosts*, we created the *description-hosts.json* file. In this file, each *Bad Host* is linked to a brief summary of the criticisms regarding the company's management of user privacy, along with a list of related references. Additionally, we included a compilation of significant news cases concerning fines or investigations related to the *Bad Host*.

For instance, in the case of Google, the list includes the investigation by the Irish Data Protection Commission into Google's Pathways Language Model 2 (PaLM 2) to assess its compliance with EU data privacy laws [24]. Additionally, it features also a €50 million fine imposed by France's data protection authority on Google for violating the EU's General Data Protection Regulation (GDPR). The company failed to provide users with clear and accessible information about data processing for personalized advertising, which hindered informed consent [11].

3.4 GUI and Workflow

The goal of this subsection is to describe the GUI of AwEE, which is depicted in Figure 2, to guarantee an adequate understanding of the

[2]https://monitora-pa.it/

proposed software interface. Upon clicking the AwEE icon in the browser toolbar, a popup window appears for the user. The visual structure of this page is based on two main sections. Initially, when the users open the extension for the first time (or after a logout), they are presented with the *Initial UI*. The *Initial UI*, allows the user to choose an avatar from a set of options and enter a username. After selecting an avatar and entering a username, the users click on the *Submit Button* which triggers the transition to the *Main UI*. The *Main UI* provides the main interface for interacting with the extension's functionalities.

The *Main UI* includes several key components. The *User Profile* section displays the chosen avatar and username. The *Navigation Log Window* is the primary area where all HTTP requests made during browsing are listed. Users can filter these requests by using the *Search Bar*, which allows them to enter specific search terms, and the *Filter Option*, which enables filtering by domains listed in the *hosts.json* file.

Additionally, the interface includes several *Control Buttons*. The *Exit Button* logs the user out and clears its stored data, reverting back to the *Initial UI*. The *Start/Stop Button* allows the users to begin or end the recording of their web navigation activity. When recording is activated, each navigation event (HTTP request) is displayed inside the *Navigation Log Window* along with timestamps. *Bad Requests* are highlighted in red and, next to the timestamp, the name of the *Bad Host* linked to the specific HTTP request is shown. Clicking one of these red entries triggers a special *Sidebar* opening, displaying detailed data from *description-hosts.json* about the specific *Bad Host* (Figure 3). It is possible to download navigation logs in either JSON or CSV format using the *Download Buttons*, while the *Clear Button* resets the *Navigation Log Window*, clearing all displayed entries.

The collapsible *Sidebar*, initially hidden, can be opened by clicking on the red *Bad Hosts button*. The *Sidebar* provides two alternative contents based on the context. The *Default content* shows detailed information about *Bad Hosts*, basically displaying details contained inside the *description-hosts.json* file. On the other hand, the *Alternative content* shows additional insights related to AwEE's functionalities, and includes a list of recommended links to improve user's knowledge and awareness about privacy (some examples: *Privacy Guides* [13], *EFF* [5], *Digital Defense* [28]).

Throughout the interface, various *Counters* are also available. The *Log Counter* tracks the total number of HTTP requests and the *Bad Requests Counter* tracks how many of these requests were made to *Bad Hosts*. Meanwhile, *Best Score* and *Best Scorer* indicators highlight the highest number of *Bad Requests* logged by a single user and display that user's name.

Finally, on the bottom of the GUI, a *Progress Bar* visually represents the percentage of *Bad Requests* out of the total number of HTTP requests made.

3.5 Gamification Techniques

In this subsection, we describe the gamification-related additions to the extension, listing some of the techniques conceived by Yu-Kai Chou that we implemented. We refer to Section 2.2 for details involving the *Octalysis* framework's *CDs*.

- *Engaging Narrative* is a technique (triggering *CD 1*) that uses storytelling to provide context and meaning to an experience. We harness the power of this method by introducing a dedicated page (the *Alternative Content* in the *Sidebar*) that tells about *"AwEE, the AwarE Extension Kitty"*. By briefly describing it, we provide users with a compelling context that makes interacting with the tool more meaningful.
- *Leaderboard* is a technique for motivating users by ranking them based on actions that lead to desired outcomes, and that triggers *CD 2*. Effective *Leaderboards* create what's called *Urgent Optimism* by positioning users within reach of immediate improvement. We implemented a *micro-leaderboard* in the form of the record reporting the user who discovered the highest number of *Bad Requests* on the local machine where the extension is installed (see Figure 4). This allows users to compare their current performances only with their past sessions or with a small group of users from the same PC, instead of comparing against an overwhelming number of other people.
- *Build-from-scratch* is a technique that triggers *CD 4*. It engages users by involving them in the creation process of a product or service rather than simply handing over a premade experience. We effectively apply this technique giving the possibility, before starting to use the extension's functionalities, to select an avatar from a set of three options, each featuring AwEE the kitty but with different accessories (see Figure 5). This initial decision empowers users with a feeling of control and personalization from the very start, but it prevents them from feeling overwhelmed because of too much choice.
- *Dynamic Feedback* is a technique that enhances user engagement by providing immediate, personalized responses as users perform desired actions. This triggers *CD 3* (based on what they do, users see custom feedback) and *CD 7* (makes users want to find out what the next *Dynamic Feedback* will be). We implemented the technique by modifying users' selected avatar appearance in real-time: if users trigger a certain number of *Bad Requests* while they are navigating, the avatar's expression changes dynamically to reflect increasing levels of anger (see Figure 5). This visual feedback is linked to three thresholds of the number of *Bad Requests*. Moreover, the extension's *Navigation log window* displays all HTTP requests as they occur, highlighting *Bad Requests* in red for clear visual emphasis.
- *Monitor Attachment* is a method that encourages users to develop a sense of ownership by constantly overseeing the state of a system. When users regularly monitor progress such as by tracking numerical values or statuses, they naturally become more invested in its improvement, triggering *CD 4* [1]. We implemented this technique by giving users two critical counters in real time: one tracking all HTTP requests and the other specifically counting *Bad Requests* (see Figure 6). Additionally, a *Progress Bar* (Yu-Kai Chou defines it as a free-standing technique, triggering *CD 2*) displays the percentage of *Bad Requests* out of the total HTTP Requests, offering clear and immediate insight into the system's current state (see Figure 7).

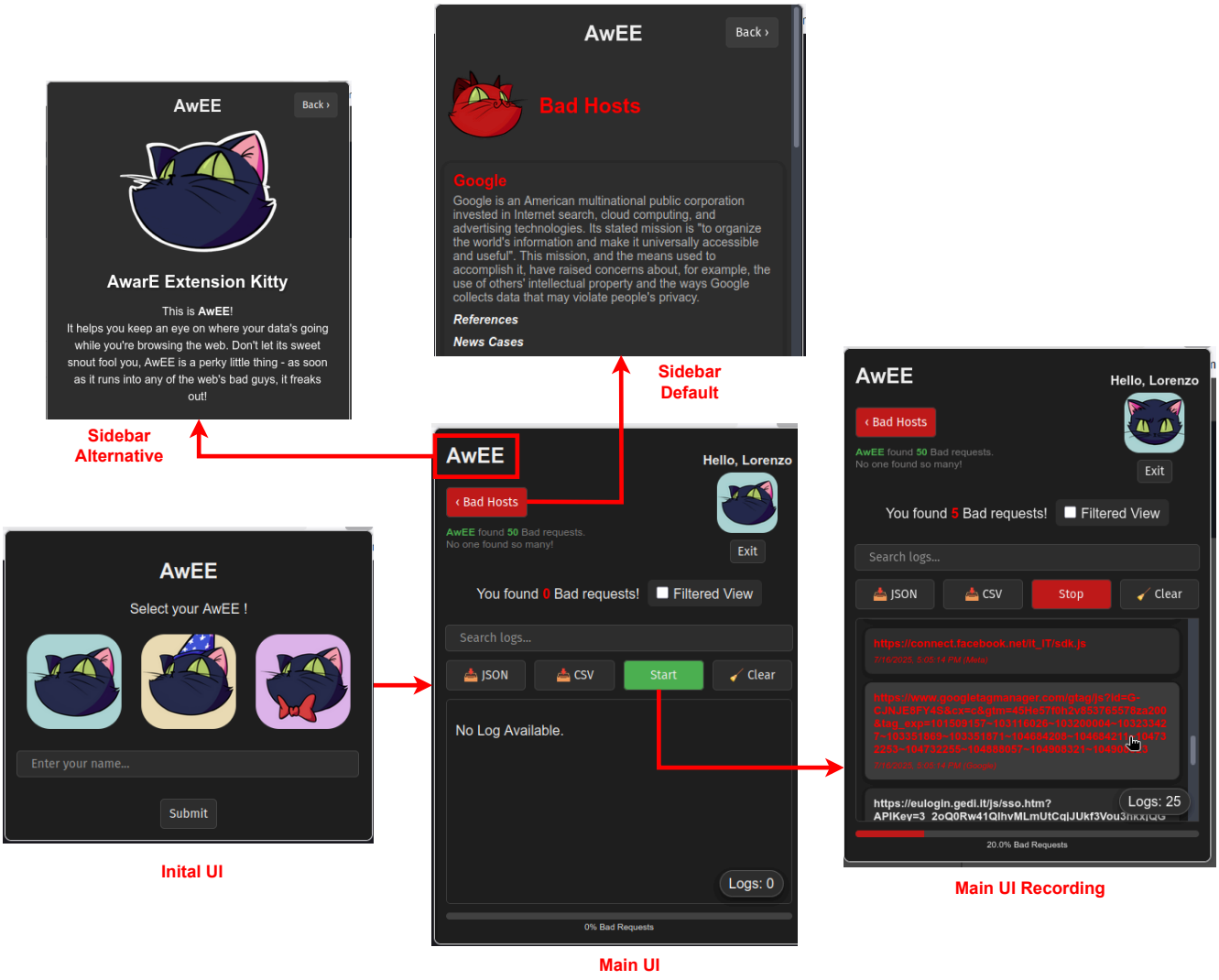


Figure 2: Awee Interaction Workflow

We report in Figure 8 the output of the *Octalysis Tool*, a project evaluation tool available on Yu-kai Chou's website, that allows checking for compliance with the Octalysis Framework[3].

This representation provides a visual assessment of our solution, showing that we focused especially on *Left Brain* and on *White Hat Gamification*. It follows that in addition to enhancing the above-mentioned areas, possible future improvements can be made particularly in the *CDs* of *Right Brain* and *Black Hat Gamification*.

4 Comparison with existing tools

There are several browser extensions available online that inspired AwEE, especially the ones allowing content blocking or providing information about user data sent to the servers of visited pages. The purpose of this section is to list and describe the most important ones, also providing insights into how they influenced the development of AwEE.

NoScript: It allows JavaScript and other potentially harmful content to be executed only on trusted websites of user choice [18]. For every visited page, NoScript analyzes the DOM to identify active content such as scripts and multimedia objects. It detects the visited domains and compares them with three different sets of domains: a whitelist containing trusted domains whose scripts can be loaded, a blacklist containing domains considered dangerous, and a set of predefined rules. The lists are stored in the browser's local storage (JavaScript API provided by web browsers to store data that persists after the browser is closed) and can be modified by the user through the GUI. Additionally, the same GUI also

[3]https://www.yukaichou.com/octalysis-tool/

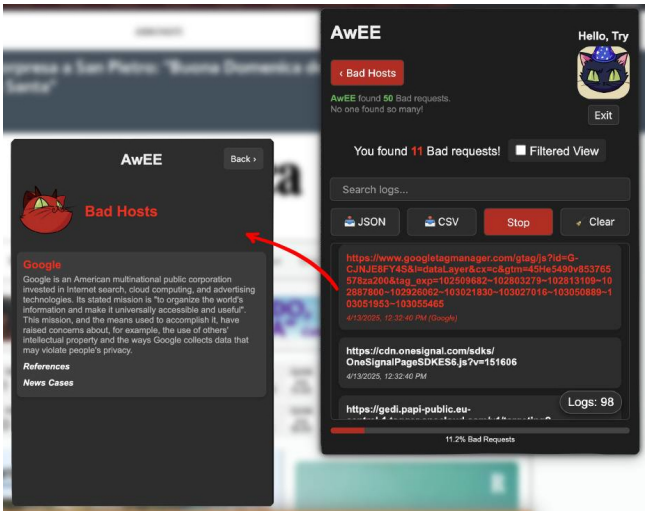


Figure 3: Check of a Bad Host during navigation

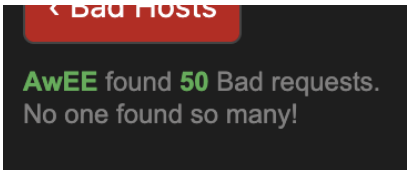


Figure 4: Micro-leaderboard record

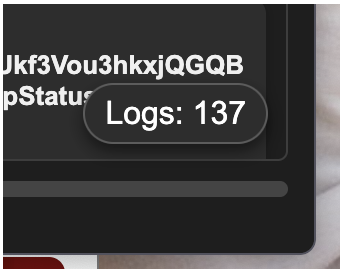


(a) avatar 1 (b) avatar 2 (c) avatar 3

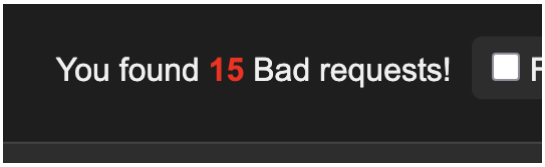


(d) angry level 1 (e) angry level 2 (f) angry level 3

Figure 5: Avatar selection and dynamic change



(a) HTTP requests counter



(b) Bad Requests counter

Figure 6: Counters

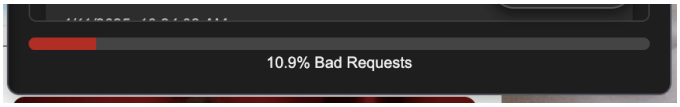


Figure 7: Progress Bar

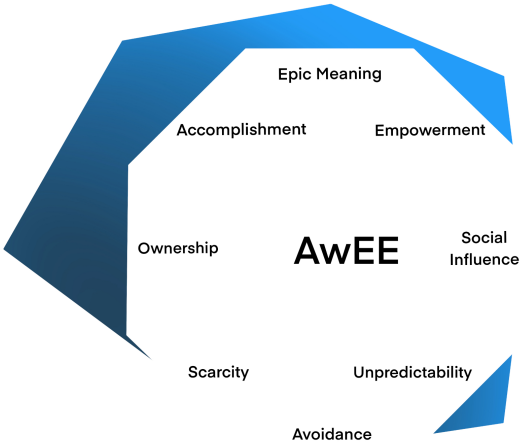


Figure 8: AwEE's Octalysis analysis

allows blocking or authorizing other specific types of content within the pages, such as media. In the implementation of AwEE, it served as a reference for how to incorporate a blacklist within a browser extension.

Privacy Badger: Made by the Electronic Frontier Foundation (EFF), it blocks third-party trackers during the navigation [6]. It does not rely on a human-curated list of domains or URLs to block. Instead, it uses an algorithmic approach to define if a domain is tracking the user or not. The extension keeps track of the third-party domains (domains different from the one explicitly visited by the user) that embed images, scripts and advertising in the pages visited by the user. Privacy Badger looks for tracking techniques like uniquely identifying cookies, local storage cookies and canvas fingerprinting. If it observes the same third-party host tracking on three separate sites, Privacy Badger will automatically disallow content

Extension	Blacklist	Tracking Detection	Fingerprinting Detection	Gamification
NoScript	✓			
Privacy Badger		✓		
uBlock Origin	✓			
FPMON			✓	
AwEE	✓			✓

Table 1: Extensions Characteristics Comparison Table

from that third-party tracker. This means that what is considered a tracker is determined by the domain's actions, not by human judgments.

uBlock Origin: Content blocking extension that allows to block ads, trackers, and fingerprinting scripts. It uses by default publicly available static blacklists permitting the user to easily choose which of them to enable or disable [14]. It features two different modes: a Basic Mode, consisting of a simple popup interface for plug-and-play and default configuration installations, and an Advanced Mode, which instead includes an interactive, point-and-click interface that allows users to adjust specific settings for individual websites [15]. From a visual point of view, this second mode introduces a lateral sidebar within the popup interface, which displays additional content to the user, for interactive per-site settings.
This specific feature was a major inspiration for part of the AwEE's popup interface, in which the use of a sidebar, employed for multiple purposes depending on the context, turns out to be critical.

FPMON: It allows to measure and rate fingerprinting activity on any website in real-time [4]. The authors of this software first classified the Javascript functions typically used to fingerprint a device. Then, they implemented a mechanism that intercepts and records these functions without altering the default runtime behavior, by modifying the Javascript runtime environment with code injections. In the end, they designed two ways to present results to the user. First, through the browser extension icon, that represents a human fingerprint whose color changes according to the level of fingerprint activity detected. Second, through a detailed view of the overall analysis visible as a popup after pressing the icon. In addition, the top 3 script files that enabled most fingerprinting features are shown.

5 Evaluation Experiment

In this section, we present a detailed overview of the evaluation experiment conducted to assess AwEE's effectiveness and user engagement. The evaluation took place during an Educational Guidance day organized at Politecnico Di Torino, Italy. The main purpose of this event was to offer advice to students in their last year of high school and to students completing their bachelor's degrees (on separate days). The focus was on university programs, career opportunities, and insights into how the Politecnico di Torino operates [4] [5].

[4]https://www.polito.it/en/education/applying-studying-graduating/choosing-a-degree-programme/polito-open-days-bachelor-s-degree
[5]https://www.polito.it/en/education/applying-studying-graduating/choosing-a-degree-programme/polito-open-days-master-s-degree-programmes

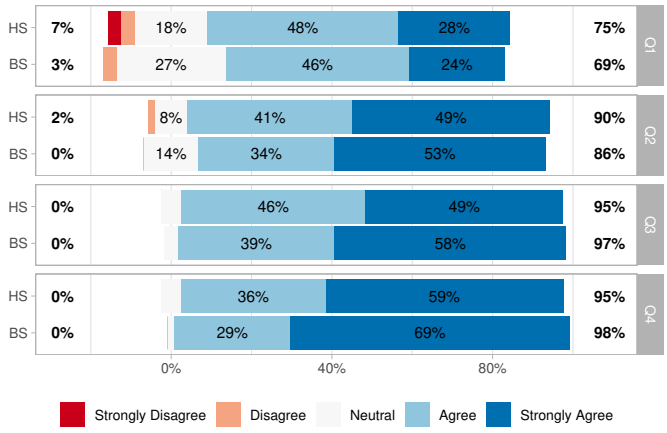


Figure 9: Results of the questionnaire

Despite the event not being designed specifically for the evaluation of AwEE, we saw it as an ideal opportunity to gather voluntary feedback from the attendees. With this in mind, we submitted a brief questionnaire to gather insights from participants who chose to answer. A total of 120 participants took part in the evaluation, 61 of them were high school students and 59 were bachelor students.

5.1 Evaluation Method

Participants were introduced to AwEE and asked to use it during their web browsing. After interacting with the extension for a short period, each participant completed a questionnaire to assess their experience. The questionnaire consisted of 4 statements and the participant had to assign their level of agreement with each of them. Statements were designed to measure user engagement, ease of use, and the impact of the extension on their perceptions of data privacy.

The statements were:

Q1: *I believe that my perceptions on data transfers to big tech companies have changed.*
Q2: *The Graphical User Interface was clear and understandable.*
Q3: *I found the interaction with the extension enjoyable.*
Q4: *I found the extension easy to use.*

Statements Q2, Q3 and Q4 were obtained by adapting the System Usability Scale [31] to our context, while Q1 is a domain-specific one.

For each of the four statements, there were 5 possible answers following a classic Likert scale structure [30], ranging from *Strongly Disagree* to *Strongly Agree*.

5.2 Results

Figure 9 shows the results of the questionnaire. Answers from high school students are labeled with **HS**, while answers from bachelor's degree students were labeled with **BS**.

The results from the questionnaire provide valuable insights into the effectiveness of AwEE in achieving its goals of improving privacy awareness and engaging users through gamification. As is clear from looking at Figure 9, more than 69% (41 out of 59)

of bachelor students and more than 75% (46 out of 61) of high school students answered *Agree* or *completely Agree* to the **Q1**. This means that the majority of participants believe that the use of AwEE changed their awareness of data transfers to big tech companies. So, it shows that the tool can work as a first step towards improving privacy awareness among users.

Furthermore, the majority of both bachelor's and high school students agreed that the interface was clear and easy to understand, the extension was enjoyable to use, and its overall usability was high (with regard to **Q2**, **Q3** and **Q4**). This suggests that AwEE's design is fairly intuitive and accessible, while its functionalities are quite self-explanatory and pleasant to use.

In addition to the questionnaire, participants were encouraged to provide free-form feedback on their experience with AwEE. Here are the key points from their comments:

- A couple of students mentioned that the bright red text used inside the GUI (for example to highlight Bad Requests or their counter) made it harder for them to read the information in the log. In their opinion, it generally worsens the readability of the interface.
- Several participants were surprised that companies such as Apple, TikTok, Temu, OpenAI, Xiaomi, or Huawei were not considered *Bad Hosts*. This suggests that a potential future improvement could involve expanding the list of *Bad Hosts* evaluating the inclusion of these companies and others.
- Some users suggested incorporating a log of JavaScript execution during browsing, similar to what FPMON (see Section 2.1) does.
- A couple of students mentioned that seeing the full HTTP requests in the log, especially when it's long and complicated, might confuse users who don't know what an HTTP request is. Instead of displaying the entire request, they suggested that the extension could just indicate the target host of the request.

6 Threats to validity

Although AwEE shows promise as a privacy awareness tool, several factors limit the strength and generalizability of our results. First of all, the way we identify *Bad Hosts*. Maintaining a list that includes all the companies subject to criticism about their data management involves a lot of effort. Continuously researching every new privacy incident, fine, or legal ruling is a labor-intensive process. It also runs the risk of being highly biased by what the contributors to this list think and what their priorities are.

Our preliminary feedback from users also has its limitations. In the context in which we offered the questionnaire, participants were aware that they were helping to test a new tool and may have been inclined to offer positive comments, showing confirmation bias. To avoid overwhelming the students, and not to shift the focus too much from the main objectives of the event, we also kept the survey extremely short. Thus, while we got a useful snapshot of first impressions, we could not explore participants' opinions more deeply.

Finally, regarding AwEE's gamification features, certainly our "micro-leaderboard" offers a too limited local leaderboard to stimulate meaningful competition. Moreover, the short narrative of *"AwEE, the Aware Extension Kitty"* is located in the *Sidebar* and exploring it is not essential or particularly stimulating concerning the usage of the extension. As also reported in Section 3.5 we neglected the *Right Brain* and *Black Hat* motivators which, according to Yu-Kai Chou, can greatly increase long-term engagement. Without improving these kind of motivators, we may have difficulty sustaining user interest beyond the initial novelty.

7 Conclusions and Future improvements

This paper contributes a novel approach to enhancing privacy awareness by presenting a new browser extension with integrated gamification mechanics, called AwEE. We designed, implemented, and preliminarily evaluated the extension, assessing both its usability and its ability to shift users' perceptions about data transfers to big tech companies. The tool logs HTTP requests made by users during their navigation, highlighting which of them refer to *Bad Hosts* taken from a blacklist. Users are motivated thanks to several gamification elements such as interactive statistics, dynamic avatar feedback, a micro-leaderboard, and a simple customization of user profile.

However, there are several areas where AwEE could be further improved to enhance its functionalities and its capability to commit users. AwEE currently relies on a static blacklist to identify *Bad Hosts*. A potential improvement would be to explore alternative methods to automatize the recognition of *Bad Hosts*. Another possibility is the introduction of a server-based backend. Although keeping everything local on the user's device guarantees privacy, a server-based system could enable better user account customization, more extensive leaderboards, sharing and communication features between users. However, this approach would require to implement a GDPR-compliant privacy policy to ensure the safe handling of user data, and managing the server infrastructure would add complexity and potential costs. Additional gamification mechanics can also be implemented in the tool. For example, introducing a background story involving characters representing privacy-conscious entities could transform AwEE into a fully immersive experience. Consequently, introducing the ability to unlock new customizable avatars as users reach milestones would add a layer of personalization and curiosity.

A point assignment system could be implemented, where users earn *privacy points* for taking actions that contribute to their privacy awareness and lose them for acting risky.

Another valuable feature could be the option for users to create, and possibly share, personalized blacklists and whitelists of websites or companies they trust, or don't trust. Finally, we could evaluate to modify some aspects of AwEE's GUI to improve its readability.

By focusing on these areas, AwEE could continue to evolve as a powerful tool for promoting privacy awareness while keeping users motivated and engaged in safeguarding their personal data.

Acknowledgments

We would like to thank Noemi Calò for designing and creating the mascot of our project, *"AwEE, the AwarE Extension Kitty"*. Her contribution added a distinctive element to our work, and we appreciate her support.

References

[1] Yu-kai Chou and Erik von Mechelen. 2016. *Actionable gamification: beyond points, badges, and leaderboards.* Octalysis Media, Fremont, CA.

[2] Nick Couldry and Ulises Ali Mejias. 2019. *The costs of connection: how data is colonizing human life and appropriating it for capitalism.* Stanford University Press, Stanford, [California].

[3] Sebastian Deterding, Rilla Khaled, Lennart Nacke, and Dan Dixon. 2011. Gamification: Toward a definition. *Proceedings of CHI 2011 Workshop Gamification: Using Game Design Elements in Non-Game Contexts* (Jan. 2011), 6–9.

[4] Julian Fietkau, Kashyap Thimmaraju, Felix Kybranz, Sebastian Neef, and Jean-Pierre Seifert. 2021. The Elephant in the Background: A Quantitative Approachto Empower Users Against Web Browser Fingerprinting. (Nov. 2021), 167–180. https://doi.org/10.1145/3463676.3485599

[5] Electronic Frontier Foundation. 2025. EFF - Surveillance Self-Defense. https://www.eff.org/pages/surveillance-self-defense.

[6] Electronic Frontier Foundation. 2025. Privacy Badger. https://privacybadger.org/.

[7] Kiran Garimella, Orestis Kostakis, and Michael Mathioudakis. 2017. Ad-blocking: A Study on Performance, Privacy and Counter-measures. (2017), 259–262. https://doi.org/10.1145/3091478.3091514

[8] Google. 2025. Chrome Extensions Docs. https://developer.chrome.com/docs/extensions.

[9] The Guardian. 2013. Edward Snowden: the whistleblower behind the NSA surveillance revelations. https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

[10] The Guardian. 2018. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[11] The Guardian. 2019. Google fined record £44m by French data protection watchdog. https://www.theguardian.com/technology/2019/jan/21/google-fined-record-44m-by-french-data-protection-watchdog.

[12] The Guardian. 2024. Google to destroy billions of private browsing records to settle lawsuit. https://www.theguardian.com/technology/2024/apr/01/google-destroying-browsing-data-privacy-lawsuit.

[13] Privacy Guides. 2025. Privacy Guides. https://www.privacyguides.org/en/.

[14] Raymond Hill. 2025. uBlock Origin - Free, open-source ad content blocker. https://ublockorigin.com/.

[15] Raymond Hill. 2025. uBlock Origin Github Repo. https://github.com/gorhill/uBlock.

[16] Lorenzo Laudadio, Antonio Vetrò, Riccardo Coppola, Juan Carlos De Martin, and Marco Torchiano. 2024. Personal Data Transfers to Non-EEA Domains: A Tool for Citizens and An Analysis on Italian Public Administration Websites. *arXiv.org* (2024).

[17] Giorgio Maone. 2009. Hardening the Web with NoScript. *login Usenix Mag.* 34 (2009). https://www.usenix.org/publications/login/december-2009-volume-34-number-6/hardening-web-noscript

[18] Giorgio Maone. 2025. NoScript: block scripts and own your browser! https://noscript.net/.

[19] Aikaterini-Georgia Mavroeidi, Angeliki Kitsiou, and Christos Kalloniatis. 2020. The Role of Gamification in Privacy Protection and User Engagement. In *Security and Privacy From a Legal, Ethical, and Technical Perspective*. IntechOpen. https://doi.org/10.5772/intechopen.91159

[20] Aikaterini-Georgia Mavroeidi, Angeliki Kitsiou, and Christos Kalloniatis. 2021. Gamification: A Necessary Element for Designing Privacy Training Programs. In *The Role of Gamification in Software Development Lifecycle*, Christos Kalloniatis (Ed.). IntechOpen, Rijeka, Chapter 1. https://doi.org/10.5772/intechopen.97420

[21] Mozilla. 2025. MDN Web Docs. https://developer.mozilla.org/en-US/.

[22] Sebastian Neef. 2022. Uncovering Fingerprinting Networks. An Analysis of In-Browser Tracking using a Behavior-based Approach. https://doi.org/10.48550/arXiv.2210.11300 arXiv:2210.11300 [cs].

[23] The European Parliament and the Council of the European Union. 2016. 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. (2016).

[24] Politico. 2024. Google hit with European privacy probe over its AI system. https://www.politico.eu/article/google-hit-with-european-privacy-probe-over-its-artificial-intelligence-system/.

[25] Libor Polčák, Marek Saloň, Giorgio Maone, Radek Hranický, and Michael McMahon. 2023. JShelter: Give Me My Browser Back. https://doi.org/10.48550/arXiv.2204.01392 arXiv:2204.01392 [cs].

[26] Daniele Ruggiu, Blok , Vincent, Coenen , Christopher, Kalloniatis , Christos, Kitsiou , Angeliki, Mavroeidi , Aikaterini-Georgia, Milani , Simone, , and Andrea Sitzia. 2022. Responsible innovation at work: gamification, public engagement, and privacy by design. *Journal of Responsible Innovation* 9, 3 (Sept. 2022), 315–343. https://doi.org/10.1080/23299460.2022.2076985 Publisher: Routledge _eprint: https://doi.org/10.1080/23299460.2022.2076985.

[27] Statcounter. 2025. Browser Market Share Worldwide April 2025. https://gs.statcounter.com/browser-market-share#monthly-202504-202504-bar.

[28] Alicia Sykes. 2024. Digital Defense. https://digital-defense.io/.

[29] The New York Times. 2022. TikTok Browser Can Track Users' Keystrokes, According to New Research. https://www.nytimes.com/2022/08/19/technology/tiktok-browser-tracking.html.

[30] Wikipedia. 2025. Likert Scale. https://en.wikipedia.org/wiki/Likert_scale.

[31] Wikipedia. 2025. System usability scale. https://en.wikipedia.org/wiki/System_usability_scale.

[32] Shoshana Zuboff. 2018. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (1st ed.).