

Mitigating User Exposure to Dark Patterns in Cookie Banners Through Automated Consent

Lorenzo Porcelli(✉), Massimo Ficco, and Francesco Palmieri

Department of Computer Science, University of Salerno, Fisciano, SA, Italy
{lporcelli,mficco,fpalmieri}@unisa.it

Abstract. The General Data Protection Regulation (GDPR) has established a de facto standard for presenting consent banners to users. To comply with the GDPR, websites are required to obtain user consent before processing their personal data, both for the provision of services and the monitoring of user behavior. Despite this, the most commonly adopted paradigm involves informing and requesting user preferences when visiting a website, often without adhering to GDPR standards and including dark patterns, such as dark nudges. In this paper, we propose a Personal Information Management Service that automatically generates consent responses based on user preferences, leveraging a Large Language Model. We demonstrate the feasibility of the proposed approach in a case study involving ChatGPT.

Keywords: Personal Information Management Service (PIMS) · GDPR · Transparency and Consent Framework (TCF) · Cookie banner · Dark pattern · Nudging · Large Language Model (LLM) · Generative Pre-trained Transformer (GPT)

1 Introduction

Modern computing technologies enable the collection, manipulation, and sharing of large amounts of data. This has led to the emergence of a thriving trade in personal information. However, users are often unaware or unable to evaluate the increasingly sophisticated methods designed to collect information about them [34]. With the introduction of the General Data Protection Regulation (GDPR) [19], privacy concerns regarding online services have gained greater prominence. One of the most visible aspects of the GDPR is the emergence of cookie banners for profiling choices (also known as cookie consent notices or consent dialogs). In fact, to comply with GDPR regulations, websites are required to display cookie consent notices that provide users with information about the use of cookies and tracking practices. It should be noted that the rules outlined in the GDPR apply to the handling of personal data of individuals located in the EU, regardless of whether the processing is carried out by an entity outside of the EU. Therefore, compliance with GDPR is mandatory not

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023
O. Gervasi et al. (Eds.): ICCSA 2023 Workshops, LNCS 14105, pp. 145–159, 2023.
https://doi.org/10.1007/978-3-031-37108-0_10

only for European companies, but also for non-European entities that create software and services intended for use by EU citizens [23].

As service and content providers are required to obtain users' consent before processing their personal data, users can communicate their privacy preferences through digital signals that specify how their data will be processed. The Transparency and Consent Framework (TCF) standardized by the Interactive Advertising Bureau (IAB) is the prevailing approach for collecting user privacy signals, and it is deemed as the only GDPR consent solution designed by the industry for the industry [22]. However, several Consent Management Platforms (CMPs) that adopt this framework often do not fully or only partially comply with the requirements established by the GDPR [28]. In more detail, several studies have highlighted that:

- cookie banners on web pages do not necessarily respect people's choices [30];
- about half of EU websites violate the EU directive on cookies, installing profiling cookies before user consent [37];
- opting out is much more complicated than opting in, and especially changing or revoking previously accepted settings is very difficult [31];
- dark patterns as nudging and implicit consent are ubiquitous [32,36].

Our proposal aims to introduce a Personal Information Management Service (PIMS) as an intermediary between the user and the CMP within the Transparency and Consent Framework (TCF). The novelty of the proposed approach is the use of a Large Language Model (LLM) for generating and applying rules to enable automatic responses to cookie consent notices. By reducing user interaction with cookie banner on websites, we can effectively mitigate the potential negative effects of dark patterns and provide a seamless browsing experience for users. The latter part of this article is structured as follows. Section 2 provides an introduction to privacy preference signals. Section 3 outlines previous research in the field. In Sect. 4, we conceptually describe the proposed PIMS and place it within the TCF, and then in Sect. 5, report a practical case study. Section 6 delves into a discussion of our proposal and the results we obtained. Finally, we draw our conclusions and future works in Sect. 7.

2 Privacy Preference Signals

Hils et al. [27] identify two waves of privacy preference signals, which are digital representations of how users want their personal data to be processed. The first wave includes the Platform for Privacy Preferences (P3P), Do Not Track (DNT), and the opt-out standards of the Network Advertising Initiative (NAI). The second wave includes signals that have a legal basis, such as the Global Privacy Control (GPC) signal and the Transparency and Consent Framework (TCF). The GPC signal is based on the California Consumer Privacy Act (CCPA) and is standardized by dozens of organizations [8], while the different versions of the TCF are based on the GDPR and are standardized by the Interactive Advertising Bureau (IAB). The P3P standard was retired in 2018 [16]. Currently, only nine

companies [2] have publicly declared their support for the Do Not Track (DNT) signal [21], while the NAI system has over 100 AdTech members [13]. Regarding the GPC specification, it is currently still a proposal [9]. In stark contrast to the aforementioned signals, the Transparency and Consent Framework (TCF) has emerged as the dominant privacy preference signal [27], as it was proposed by the same industries that adopted it. The TCF [11] comprises several stakeholders, including publishers, CMPs, advertisers, and vendors. Users visit a publisher's website primarily to consume its content. A publisher may generate income by selling advertising spaces on its website to advertisers, which are companies that intend to display ads to users. Advertisers often collaborate with third-party vendors to help them deliver and optimize their ads. CMPs are responsible for providing consent pop-ups, storing user preferences, and offering an API to allow vendors to access data. The TCF, particularly its "Notice and Choice" paradigm utilized for capturing user signals, presents certain limitations. Firstly, it does not standardize the manner in which user consent is solicited. This has led to the emergence of various methods to obtain consent that can have an impact on the user [29]. It is well known that several CMPs display cookie banners for gathering consent that incorporate design elements intended to encourage users to provide consent [30,32,38]. This type of nudge constitutes a form of dark pattern [36]. Additionally, with the TCF, users are required to express their preferences through cookie banners every time they visit a website. As outlined in [27], it has been estimated that since 2018, users have spent over two thousand years sending TCF consent signals.

In summary, the signals proposed by AdTech (NAI and TCF) collect user preferences through a web page, whereas those suggested by privacy advocates (P3P, DNT/GPC) are collected by a browser. In the latter case, privacy preferences are obtained through a single interaction, and the browser presumes that this decision applies across the entire web. Thus, it is assumed that the user makes a single decision that has long-term effects [27]. Instead, in the former scenario, user choices remain effective until cookies are deleted or a vendor introduces a new one. Therefore, AdTech companies strive to prevent browser settings from having a binding impact.

3 Related Works

The Platform for Privacy Preferences (P3P) was the first attempt to standardize privacy preferences in a machine-readable format [15]. Based on the P3P standard, several user agents have been developed that allow users to avoid reading privacy policies every time they visit a website. One of the most popular user agents was Privacy Bird, which was a browser add-on utilizing P3P to produce a concise privacy report. It examined the P3P policies for each site the user accessed and matched them against the user's privacy preferences. When a user visited a site, the interface displayed whether the site's policies corresponded to the user's privacy preferences, did not match them, or was not P3P-enabled [24]. Another strategy was adopted by the Mozilla Firefox add-on Targeted Advertis-

ing Cookie Opt-Out (TACO), which maintained an updated list of opt-out cookies and shared them with thousands of users [20]. However, TACO was a rather drastic tool as it deleted all existing cookies. The P3P protocol quickly became obsolete due to its poor adoption by AdTech vendors. Consequently, all solutions based on the P3P standard are now obsolete. Furthermore, privacy advocates have criticized P3P, as no consequences have been established for false reporting of privacy practices [17]. Since the obsolescence of the P3P standard, privacy-focused browsers such as Mozilla Firefox have integrated alternatives such as DNT. Unfortunately, DNT suffered a similar fate as P3P, as major AdTech vendors explicitly stated that they would ignore DNT signals after Microsoft enabled the DNT signal as a default option in Internet Explorer [5]. As time passed, even pro-privacy browsers such as Firefox removed support for DNT [4]. New browsers such as Brave [7] and add-ons such as Privacy Badger [3] have already enabled the new GPC signal by default. The GPC is a solution that aims to follow the path of DNT. According to [27], there is little reason to be optimistic that AdTech vendors will widely adopt GPC signals. In fact, just as with DNT, it is likely that AdTech providers will claim that an active default signal renders the signal meaningless. However, in this last case, unlike with the DNT signal, privacy advocates can rely on CCPA, which was not available when DNT was first adopted by browsers [27].

The need for websites to comply with GDPR has led them to rely on CMPs. Thus, numerous companies have started providing "Consent as a Service" solutions to help ensure legal compliance. The availability of free solutions, like those offered by Quantcast, has significantly boosted the adoption of the TCF, similar to what Let's Encrypt [12] implemented with the adoption of HTTPS [27]. In this context, users are expected to define their preferences each time they visit a website. To address this issue, academics and industry experts have begun developing Personal Information Management Services (PIMS). PIMSes are tools designed to centralize all of a user's personal data and allow them to manage both incoming and outgoing data from a single location. At present, users typically have access to a limited range of PIMSes, which provide only basic functionality and are mainly focused on managing consent decisions. These tools are available as free browser extensions, primarily for Google Chrome and Mozilla Firefox, that work mainly by blocking cookie banners or automatically responding to requests for permission to process personal data. A significant challenge in implementing automated consent responses is the substantial variance among consent requirements across different cookie banners. Consequently, even if a browser extension is informed of user preferences, it may be unable to adequately address all website specifications [35]. In some cases, adopting harsh approaches such as "reject all" could lead to problems. For example, not granting consent for any data processing activity, such as blocking all cookies, may affect the functionality of certain websites, as the user technically appears with an unresolved request for consent. This issue can be addressed by providing minimal consent, which allows only functional cookies, i.e., first-party cookies vital to the website's operation. In late 2021, a browser extension that gained extensive popularity on various

stores was "I don't care about cookies" [10]. It grants consent to either all or only necessary cookies, depending on what is easier to implement technologically for the extension. Currently, the most widely used browser extension is Ghostery [14], which relies on rules that automate interactions with cookie banners, rather than hiding them outright [6]. An alternative approach is presented by the Advanced Data Protection Control (ADPC) technical specification [1]. ADPC allows publishers to request consent using TCF or through specific consent requests while simultaneously enabling users to set general signals, such as "object to all", specific signals, such as consent to a particular request, or a combination of both. Although ADPC is still under development, a prototype is available for Firefox and Chromium-based browsers.

The growing popularity of such browser extensions may suggest that many users prefer not to receive cookie banners while visiting websites and are willing to forego the opportunity to differentiate their authorization preferences [35]. Broadly speaking, such behavior could be characterized as an instance of the Privacy Paradox phenomenon documented in the literature [25]. Many people claim to prize their privacy and express unwillingness to share personal information online. Yet, in practice, they often fail to take sufficient precautions to safeguard their data. Upon examining the history of privacy preference signals, it is unusual for both parties, i.e., websites and AdTech vendors, to embrace a signal. It is expected that investments will continue to be made in TCF signals in the future [27]. We proposed a PIMS to automatically generate rules and respond to any type of cookie banner, with the aim of reducing consent response time and preventing deceptive practices in cookie banners.

4 Methods

As mentioned earlier, one of the challenges for users when browsing online is deciding and responding to each website's initial request for permission, keeping track of all decisions, and updating them if desired. The Transparency and Consent Framework (TCF) is currently the most widely adopted specification, and projections suggest that this trend will continue in the future [27].

Our proposal involves a Personal Information Management Service (PIMS) that enforces a user's privacy policy at the time of website visit. Essentially, the user declares their privacy preferences only once in the PIMS. Afterwards, when the user visits a website, the PIMS automatically responds to consent requests according to the user's policy. A user policy reflects the user's privacy preferences, such as rejecting all cookies. To generate and apply consent rules based on user policies, we utilized a Large Language Model (LLM). A LLM is a type of language model that uses deep learning techniques, such as neural networks, to generate artificial text on a large scale. These models are trained on massive text corpora, consisting of billions of words, and are capable of processing and generating text with high precision and naturalness. The current state-of-the-art for LLMs is GPT (Generative Pre-trained Transformer), developed by OpenAI, which is based on transformer-based architectures [39]. GPT has led

to significant advancements in natural language processing, particularly in areas such as common sense reasoning, question answering, and textual entailment [33]. As shown in detail in Sect. 5, we employed ChatGPT for multiple purposes. Firstly, we analysed the content of the web page to identify the cookie banner. Then, we generated rules to interact with the cookie banner based on the user's policy.

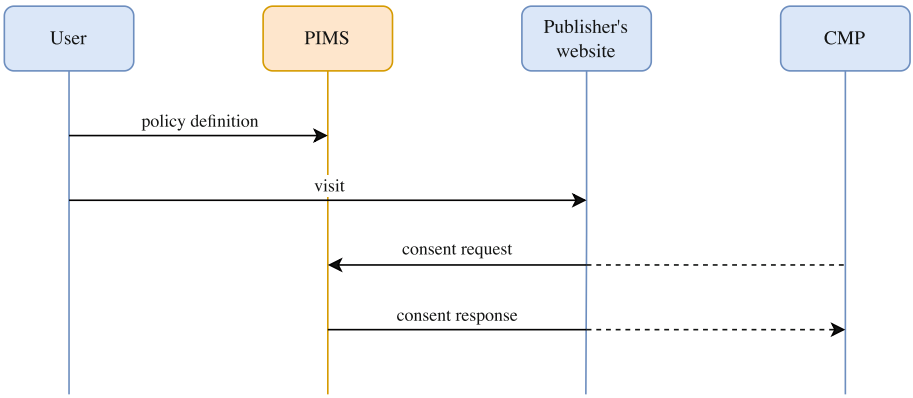

Fig. 1. The diagram illustrates how the proposed PIMS integrates and interacts within the Transparency and Consent Framework. After a user has defined his policy, the PIMS intercepts consent requests from CMPs and responds in a manner consistent with the user's policy.

To illustrate how our proposal fits within the TCF, we provide a concise overview of an eight-step use case. In this scenario, a publisher obtains consent for its specific TCF purposes independently, without partnering with vendors who require user authorization. When user X arrives at the publisher's website (step 1), the publisher contacts its CMP C using a CMP tag, which is a JavaScript tag added to publisher P's website (step 2). The CMP code then runs on the page and checks whether a Transparency and Consent (TC) String corresponding to publisher P exists in user X's local storage (step 3). The TC String is used to store, update, and exchange a user's authorization in a standardized manner. Since this is user X's first visit to publisher P, no such TC String is found. In this case, CMP C displays a cookie banner on the website, similar to the banner shown in Fig. 2 (step 4). Next (step 5), user X makes choices on the cookie banner for each purpose. Then, CMP C creates a TC String for user X-publisher P by encoding the consent information according to the standard (step 6). publisher P stores the TC String locally on user X's device (step 7). Afterward, publisher P can rely on its CMP API to decode the TC String and determine which purpose user X has allowed it to pursue (step 8). The proposed PIMS is implemented as a browser extension and interposes itself between the user and the CMP in steps 4 and 5, as shown in Fig. 1. The PIMS intercepts the CMP request and

subsequently responds on behalf of the user according to their established policy. Except for the initial stage where the user defines their own policy within the PIMS, the remaining steps described in the previous use case remain unchanged.

5 Case Study

As a case study, we generated a consent rule and applied it to the Quantcast website [18]. We assumed that the user does not want to accept any cookies. When a user accesses the Quantcast website for the first time, they are presented with the cookie banner shown in Fig. 2. It should be noted that the banner includes a dark pattern that induces the user to click the "Agree" button, highlighted in blue. If the user wishes to reject all cookies, he must first click on the "More options" button. After arriving at the screen shown in Fig. 3, two additional clicks will be required: one on the "Reject all" button, and another on the "Save & exit" button. We prompted ChatGPT to derive consent response rules and identify the location of buttons on the page, generating the necessary code for interaction. Below is an excerpt from the ChatGPT conversation, providing insights into this process. Please note that ellipses have been used to indicate omitted text for brevity.

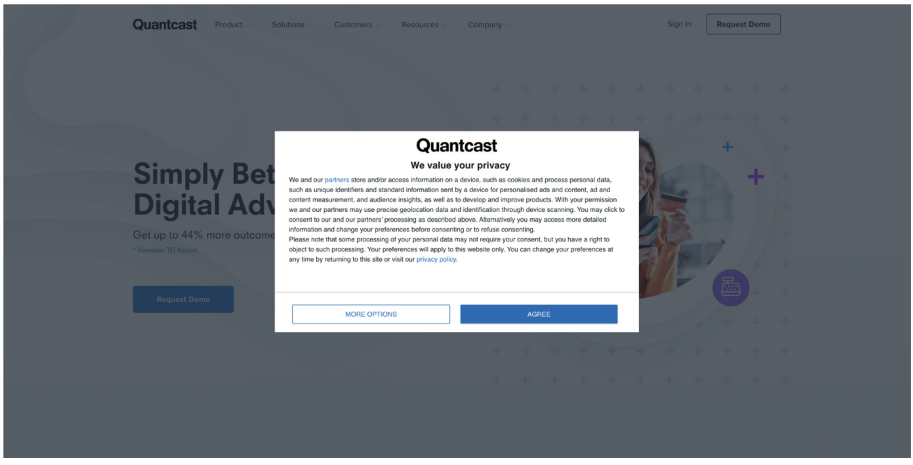

Fig. 2. The initial view of the cookie banner displayed on the Quantcast website.

Rules Generation. With the first question, we establish the context for the entire conversation. We then proceed to discuss the location of the buttons used to indicate the user's choice. Finally, we generate the JavaScript code that interacts with these buttons based on the user's policy.

Question 1. What is a cookie banner and what is its purpose?

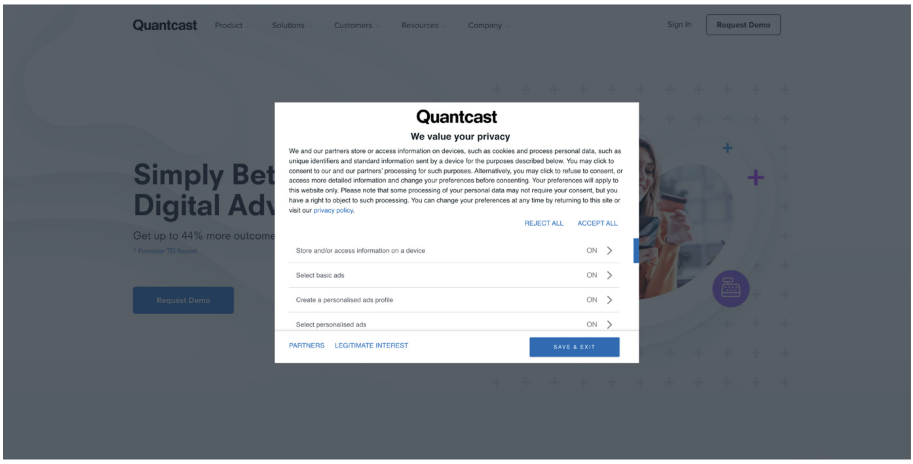

Fig. 3. The display presented upon clicking the "More options" button within the cookie banner on the Quantcast website.

Solution 1. A cookie banner is a message that appears on a website asking for a user's consent to use cookies [...] By giving users the ability to choose which cookies they allow, the banner helps protect user privacy and comply with regulations, such as the GDPR and the CCPA [...].

Question 2. I would like to reject all cookies on this page, does this banner display a button with this option?

```
[...]<div id="qc-cmp2-ui" role="dialog" aria-label="qc-cmp2-ui" aria-modal="true
     " tabindex="0" class="css-6napma"><div class="qc-cmp2-summary-section">
     [...] </div><div class="qc-cmp2-footer␣qc-cmp2-footer-overlay␣qc-cmp2-footer
     -scrolled"><div class="qc-cmp2-summary-buttons"><button mode="secondary"
     size="large" class="␣css-1hy2vtq"><span>MORE OPTIONS</span></button><button
     mode="primary" size="large" class="␣css-47sehv"><span>AGREE</span></button><
     /div> </div> </div>[...]
```

Solution 2. Based on the HTML code provided, it does not appear that there is an option to reject all cookies on the page. The only options provided are to "Agree" or to access "More options", which presumably would allow the user to customize their cookie preferences rather than reject all cookies outright. However, without actually interacting with the banner on the live website, it is possible that additional options or information may be available upon further inspection.

Question 3. Please provide me with a JavaScript code to click on the "more" button.

Solution 3. Here is an example of JavaScript code that will simulate a click on the "more" button:

```
const moreButton = document.querySelector('.qc-cmp2-summary-buttons button:first
    -of-type');
moreButton.click();
```

[...] Once the button is clicked, the banner should reveal additional options for managing the cookie preferences.

Question 4. Does this new version of the cookie banner display a button that allows to reject all cookies on this page?

```
[...]<div id="qc-cmp2-ui" role="dialog" aria-label="qc-cmp2-ui" aria-modal="true
    " tabindex="0" class="css-1irhpn0"><div class="qc-cmp2-consent-info"><div
    class="qc-cmp2-publisher-logo-container">[...]<div>[...]</div><div class="qc
    -cmp2-header-links"><button mode="link" size="small" class="␣css-8rroe4">
    REJECTALL</button><button mode="link" size="small" class="␣css-8rroe4">
    ACCEPT ALL</button></div></div></div>[...]<div class="qc-cmp2-footer␣"><
    button class="qc-cmp2-hide-desktop␣css-47sehv" mode="primary" size="large">
    SAVE &amp; EXIT</button><div class="qc-cmp2-footer-links"><button mode="link
    " size="small" class="␣css-8rroe4"aria-pressed="false">PARTNERS</button><
    button mode="link" size="small" class="␣css-8rroe4"aria-pressed="false">
    LEGITIMATE INTEREST </button></div><div class="qc-cmp2-buttons-desktop"><
    button aria-pressed="false" mode="primary" size="large"class="␣css-47sehv">
    SAVE &amp; EXIT</button></div></div></div>[...]
```

Solution 4. Yes, this new version of the cookie banner displays a button that allows to reject all cookies on the page. The button with the label "Reject all" can be used to reject all cookies on the page.

Question 5. Please provide me with a JavaScript code to click on the "Reject all" button and close the banner with the preference of rejecting all cookies.

Solution 5. Sure, here's a JavaScript code to click on the "Reject all" button and close the banner with the preference of rejecting all cookies:

```
const rejectAllButton = document.querySelector('.qc-cmp2-header-links␣button:
    first-of-type');
rejectAllButton.click();
const saveAndExitButton = document.querySelector('.qc-cmp2-footer␣button:first-
    of-type');
saveAndExitButton.click();
```

Note that, this code assumes that the structure of the HTML code for the cookie banner remains the same. If the structure changes, this code may not work as expected.

Browser Extension Setup. We implement our PIMS as a browser extension specifically designed for Mozilla Firefox. The extension consists primarily of two files: the manifest file (shown in Listing 1.1) and the script that executes the auto-consent rule (defined in Listing 1.2). To simplify the execution flow, we include a contextual menu item that allows the user to close the browser extension with a single click, as demonstrated in Listing 1.3. In a real-world scenario, this additional feature would not be necessary, as the code in Listing 1.2 would be invoked directly at the end of the page loading process.

Listing 1.1. manifest.json

```
{
    "manifest_version": 2,
    "name": "Autoconsent",
    "version": "1.0",
    "permissions": [
        "activeTab",
        "contextMenus"
    ],
    "background": {
        "scripts": [
            "background.js"
        ]
    }
}
```

Listing 1.2. autoconsent.js

```
var moreOptionsButton = document.querySelector('.qc-cmp2-summary-buttons button:
    first-child');
moreOptionsButton.click();

setTimeout(function () {
    const rejectAllButton = document.querySelector('.qc-cmp2-header-links button
        :first-of-type');
    const saveAndExitButton = document.querySelector('.qc-cmp2-footer button[
        mode="primary"]');

    if (rejectAllButton && saveAndExitButton) {
        rejectAllButton.click();
        saveAndExitButton.click();
    }
}, 500);
```

Listing 1.3. background.js

```
browser.contextMenus.create({
    id: "autoconsent",
    title: "Autoconsent"
});

browser.contextMenus.onClicked.addListener((info, tab) => {
    if (info.menuItemId === "autoconsent") {
        browser.tabs.executeScript({
            file: "autoconsent.js"
        });
    }
});
```

Rules Execution. After installing the browser extension, the user can apply their policy to all the pages they visit. In this particular use case, the PIMS performs the following actions: it first clicks on the "More options" button, then selects the "Reject all cookies" option from the new screen, and finally closes the banner by clicking the "Save & exit" button. Figure 4 displays the contextual menu item that was introduced in Listing 1.3. It is important to note that this menu item was added solely for demonstration purposes. Its purpose is to highlight the actions of the browser extension and make the presence of the cookie banner noticeable. In an actual scenario, the browser extension would

remove the cookie banner quickly after the page has loaded, without the need for user intervention.

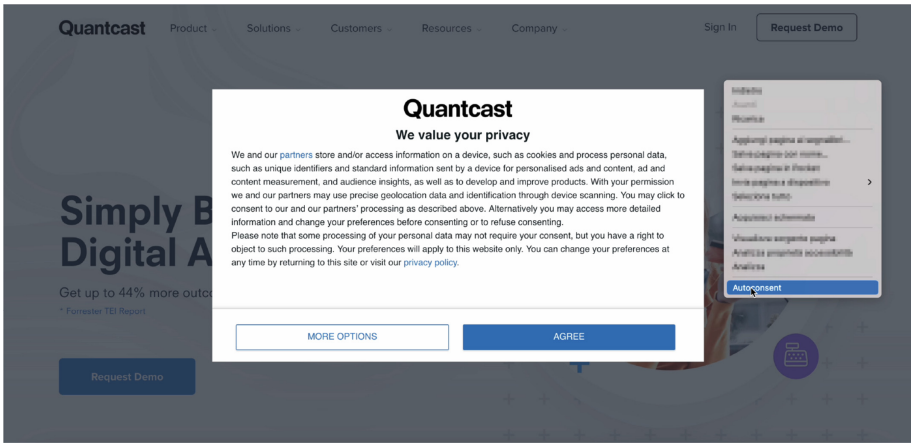

Fig. 4. Screenshot demonstrating the automatic invocation of the automated consent response by the browser extension. It is important to note that this action is purely for descriptive purposes, as in reality, it is executed automatically without requiring any user intervention.

6 Discussion and Results

The increasing adoption of GDPR-compliant consent management by websites has led to a de facto standard in the presentation of cookie banners to users. However, despite the existence of standardized frameworks like the TCF, managing and controlling authorizations remains a complex process. It is important to note that the TCF itself does not guarantee GDPR compliance. In many cases, cookie banners are designed to optimize the chances of obtaining user consent [35]. A study conducted by Nouwens et al. [32], which analyzed the top five CMPs on the top 10,000 websites in the UK, revealed the prevalence of dark patterns and implied consent. Only 11.8% of the CMPs met the minimum requirements based on European law.

A limited number of tools are currently available to assist users in making and managing authorization decisions. These tools have certain drawbacks, including increased page loading time, and some even conflict with the website's functionality. The main difference between our proposal and other browser extensions is that our PIMS automates the process of creating and enforcing user policies. This ensures scalability and adaptability to customized cookie banners. A PIMS that interacts with websites, leveraging a signal type that is already widely adopted by AdTech vendors, is a fair compromise between privacy advocates

who seek a long-term solution and AdTech vendors who oppose default options incorporated into browsers. In addition, responding automatically to requests for consent, i.e., without requiring direct involvement from users in the consent process, brings several benefits, including circumventing obscure models such as nudges that induce users to accept all cookies, and a considerable reduction in the technical time required to declare one's preferences. In [26], it was estimated that on average, it takes a user at least 30 s to define their preferences on dialog windows and submit them. As we have previously highlighted in our case study, simply choosing to reject all cookies can also require up to three clicks on two different screens.

7 Conclusion and Future Works

In this study, we addressed the issue of managing user consent while visiting a website. We presented a PIMS that generates rules for automatic consent based on a user policy. Our approach eliminates some of the dark patterns found in cookie banners, which frequently encourage users to consent to all cookies. Additionally, it reduces the time spent by users in expressing their preferences on every website they visit. To demonstrate the practicability of our approach, we conducted a case study where we used ChatGPT to create rules based on a user policy. Subsequently, we implemented these rules in a browser extension that enables automatic consent when visiting a website. Our use of the GPT model proved effective in accurately identifying banners and buttons and providing relevant actions aligned with the user's preferences. The proposed browser extension is capable of enforcing policies and closing banners in less than one second from the page's load.

An effective implementation of the proposed PIMS should include a set of rules to address the consent requests received from the primary CMPs. Subsequently, users themselves can contribute to the expansion of a shared database of consent rules by declaring their own policies and browsing the internet. This way, users with similar policies who visit the same website can utilize a rule already available in the shared database. If cookie banners change or a specific rule is absent from the database, the PIMS will generate a new rule and share it with the user in the database. Moreover, this work could be extended in several directions. A more advanced PIMS would track all site authorizations for data processing and periodically propose updates to the user's privacy preferences. Updates made within the PIMS to the user's preferences would be automatically communicated to all other entities processing the user's data. The PIMS could also request information on the data stored by a specific website and request its deletion. Another possible extension would be to develop a user-centric approach that enables the average user to comprehend cookie policies and, based on their preferences, define their own policy. This could be achieved by examining the user's behavior and automatically inferring a policy. Once validated by the user, the PIMS would apply the policy automatically during navigation. Furthermore, in other contexts, a tool similar to our proposal could be useful in identifying

and notifying websites that offer non-compliant cookie banners, including those where no banner is displayed on the website.

Acknowledgments. This work was partially supported by project SERICS (PE00000014) under the NRRP MUR program funded by the EU - NGEU.

Conflicts of Interest. The authors declare no conflict of interest.

References

1. Advanced Data Protection Control (ADPC). https://www.dataprotectioncontrol.org/. Accessed 7 May 2023
2. All about Do Not Track. https://allaboutdnt.com/companies/. Accessed 7 May 2023
3. Announcing Global Privacy Control in Privacy Badger. https://www.eff.org/gpc-privacy-badger. Accessed 7 May 2023
4. DNT - HTTP. https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/DNT. Accessed 7 May 2023
5. "Do Not Track" set to "on" by default in Internet Explorer 10-IAB response. https://www.iab.com/news/do-not-track-set-to-on-by-default-in-internet-explorer-10iab-response/. Accessed 7 May 2023
6. Ghostery autoconsent. https://github.com/ghostery/autoconsent. Accessed 7 May 2023
7. Global Privacy Control, a new privacy standard proposal by the Brave web standards team. https://brave.com/web-standards-at-brave/4-global-privacy-control/. Accessed 7 May 2023
8. Global Privacy Control (GPC). https://globalprivacycontrol.org/. Accessed 7 May 2023
9. Global Privacy Control (GPC) specification proposal. https://privacycg.github.io/gpc-spec/. Accessed 7 May 2023
10. I don't care about cookie. https://www.i-dont-care-about-cookies.eu/. Accessed 7 May 2023
11. IAB Europe Transparency & Consent Framework policies. https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/. Accessed 7 May 2023
12. Let's Encrypt. https://letsencrypt.org/. Accessed 7 May 2023
13. Network Advertising Initiative (NAI). https://thenai.org/. Accessed 7 May 2023
14. Never consent by Ghostery. https://www.ghostery.com/blog/never-consent-by-ghostery. Accessed 7 May 2023
15. The Platform for Privacy Preferences 1.0 (P3P1.0) specification. https://www.w3.org/TR/P3P/. Accessed 7 May 2023
16. The Platform for Privacy Preferences 1.1 (P3P1.1) specification. https://www.w3.org/TR/P3P11/. Accessed 7 May 2023
17. Pretty poor privacy: An assessment of P3P and internet privacy. https://archive.epic.org/reports/prettypoorprivacy.html. Accessed 7 May 2023
18. Quantcast. https://www.quantcast.com/. Accessed 7 May 2023
19. 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). https://eur-lex.europa.eu/eli/reg/2016/679/oj. Accessed 7 May 2023

20. Targeted Advertising Cookie Opt-out (TACO). https://addons.mozilla.org/en-us/firefox/addon/targeted-advertising-cookie-op/. Offline
21. Tracking Preference Expression (DNT). https://www.w3.org/TR/tracking-dnt. Accessed 7 May 2023
22. Transparency & Consent Framework (TCF). https://iabeurope.eu/transparency-consent-framework/. Accessed 7 May 2023
23. Campanile, L., Iacono, M., Mastroianni, M.: Towards privacy-aware software design in small and medium enterprises. In: 2022 IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, International Conference on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), pp. 1–8 (2022). https://doi.org/10.1109/DASC/PiCom/CBDCom/Cy55231.2022.9927958
24. Cranor, L.: P3P: making privacy policies more useful. IEEE Secur. Priv. **1**(6), 50–55 (2003). https://doi.org/10.1109/MSECP.2003.1253568
25. Gerber, N., Gerber, P., Volkamer, M.: Explaining the privacy paradox: a systematic review of literature investigating privacy attitude and behavior. Comput. Secur. **77**, 226–261 (2018). https://doi.org/10.1016/j.cose.2018.04.002, https://www.sciencedirect.com/science/article/pii/S0167404818303031
26. Hils, M., Woods, D.W., Böhme, R.: Measuring the emergence of consent management on the web. In: Proceedings of the ACM Internet Measurement Conference, IMC 2020, pp. 317–332. Association for Computing Machinery, New York (2020). https://doi.org/10.1145/3419394.3423647
27. Hils, M., Woods, D.W., Böhme, R.: Privacy preference signals: past, present and future. Proc. Priv. Enhanc. Technol. **4**, 249–269 (2021)
28. Kretschmer, M., Pennekamp, J., Wehrle, K.: Cookie banners and privacy policies: measuring the impact of the GDPR on the web. ACM Trans. Web **15**(4) (2021). https://doi.org/10.1145/3466722
29. Machuletz, D., Böhme, R.: Multiple purposes, multiple problems: a user study of consent dialogs after GDPR. Proc. Priv. Enhanc. Technol. **2**, 481–498 (2020)
30. Matte, C., Bielova, N., Santos, C.: Do cookie banners respect my choice?: measuring legal compliance of banners from IAB Europe's transparency and consent framework. In: 2020 IEEE Symposium on Security and Privacy (SP), pp. 791–809 (2020). https://doi.org/10.1109/SP40000.2020.00076
31. Mehrnezhad, M., Coopamootoo, K., Toreini, E.: How can and would people protect from online tracking? Proc. Priv. Enhanc. Technol. **1**, 105–125 (2022)
32. Nouwens, M., Liccardi, I., Veale, M., Karger, D., Kagal, L.: Dark patterns after the GDPR: scraping consent pop-ups and demonstrating their influence. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, CHI 2020, pp. 1–13. Association for Computing Machinery, New York (2020). https://doi.org/10.1145/3313831.3376321
33. Radford, A., Narasimhan, K., Salimans, T., Sutskever, I., et al.: Improving language understanding by generative pre-training. https://cdn.openai.com/research-covers/language-unsupervised/language%5Funderstanding%5Fpaper.pdf
34. Schwartz, P.M.: Property, privacy, and personal data. Harv. Law Rev. **117**(7), 2056–2128 (2004). http://www.jstor.org/stable/4093335
35. Skiera, B., Miller, K., Jin, Y., Kraft, L., Laub, R., Schmitt, J.: The Impact of the General Data Protection Regulation (GDPR) on the Online Advertising Market. Bernd Skiera (2022)
36. Thaler, R.H.: Nudge, not sludge. Science **361**(6401), 431–431 (2018). https://doi.org/10.1126/science.aau9241

37. Trevisan, M., Stefano, T., Bassi, E., Marco, M., et al.: 4 years of EU cookie law: results and lessons learned. Proc. Priv. Enhanc. Technol. **2019**(2), 126–145 (2019)
38. Utz, C., Degeling, M., Fahl, S., Schaub, F., Holz, T.: (Un)informed consent: studying GDPR consent notices in the field. In: Proceedings Of The ACM Conference On Computer And Communications Security, pp. 973–990 (2019)
39. Vaswani, A., et al.: Attention is all you need. Adv. Neural Inf. Process. Syst. **30** (2017)