Johnny Can't Revoke Consent Either: Measuring Compliance of Consent Revocation on the Web

Gayatri Priyadarsini Kancherla
Indian Institute of Technology Gandhinagar
Gandhinagar, India
gayatripriyadarsini@iitgn.ac.in

Nataliia Bielova
Inria Centre at University Côte d'Azur
Sophia Antipolis, France
nataliia.bielova@inria.fr

Cristiana Santos
Utrecht University
Utrecht, Netherlands
c.teixeirasantos@uu.nl

Abhishek Bichhawat
Indian Institute of Technology Gandhinagar
Gandhinagar, India
abhishek.b@iitgn.ac.in

Abstract

The EU General Data Protection Regulation (GDPR) requires websites to facilitate the right to revoke consent from Web users. Prior works have examined consent management by auditing that user choices are correctly stored, and comparing cookies set upon acceptance versus rejection to assess compliance. While these studies measured compliance of consent with respect to the various consent requirements, no prior work has studied consent revocation on the Web. Therefore, it is unclear how difficult it is to revoke consent on the websites' interfaces, and whether the revoked consent is properly stored and communicated behind the user interface.

Our work aims to fill this gap by measuring compliance of consent revocation on the Web on Tranco's top-200 websites. We found that 19.87% of websites make it difficult for users to revoke consent throughout different interfaces, 20.5% of websites require more effort than acceptance, and 2.48% do not provide consent revocation at all, thus violating EU legal requirements for valid consent. 57.5% websites do not delete the cookies after consent revocation enabling continuous illegal processing of users' data.

Further, we analyzed 281 websites implementing the IAB Europe Transparency & Consent Framework, and found 22 websites that store a positive consent despite user's revocation. Surprisingly, we found that on 101 websites, third parties that have received consent upon user's acceptance, are not informed of revocation, leading to the illegal processing of users' data by such third parties according to EU laws. Our findings emphasize the need for improved legal compliance of consent revocation, and proper, consistent, and uniform implementation of revocation communication to third-parties.

Keywords

Consent revocation, consent withdrawal, opt-out, GDPR, consent banners

Proceedings on Privacy Enhancing Technologies 2025(4), 329–347

https://doi.org/10.56553/popets-2025-0133

1 Introduction

In recent years, compliance with privacy and data protection laws on the Web has gained a lot of attention, both from the research community and regulators. The EU Data Protection framework, consisting of the General Data Protection Regulation (GDPR) [30] and ePrivacy Directive (ePD) [22] sets requirements for a legally-valid consent when tracking technologies are deployed on a website or app. Such consent is usually implemented via consent banners and must satisfy seven requirements for validity: it must be prior to any data collection, freely given, specific, informed, unambiguous, readable and accessible, and revocable [30, Art. 4(11), 7], [69, para 17]. While numerous studies have evaluated compliance of consent banners with the various consent requirements, such as the presence and visibility of the rejection button [6, 59, 63], one aspect has so far been overlooked by the research community and the regulators: the requirement of *revocable consent*, also known as consent withdrawal, which entails that the user has the option to change a prior preference regarding trackers due to the reversible nature of consent decisions [15].

According to the GDPR, users have the *right to revoke consent at any time* [30, Art. 7(3), Rec. 42]. Accordingly, websites must *facilitate* the exercise of this right [30, Art. 12(2)] by providing an option to revoke consent. Upon revoking consent, websites must subsequently comply with an additional obligation to *delete* data previously processed on the basis of that consent, and without undue delay, even if the user did not explicitly exercise their right to request data deletion [30, Art. 17(1)(b)]. This paper focuses exclusively on the right to revoke consent. Websites that do not allow consent revocation are deemed to be processing data illegally, and run the risk of being fined for not complying with the legal requirements [10, 16, 32, 64, 76].

However, it remains unclear *whether websites provide users with compliant methods to revoke their consent, whether revoked consent is properly stored by the websites behind the consent interface, and whether it is communicated to third-parties that collected users' data.* Our work aims to fill this gap by measuring the compliance of consent revocation on the Web, addressing the research questions:

RQ1: Are the revocation interfaces on websites compliant with EU data protection laws?

RQ2: Do *advertising and analytics* (AA) cookies that require consent get deleted once consent is revoked?

RQ3: Is consent stored correctly in the browser, and is it consistent across browser storage and APIs implemented by Consent Management Platforms (CMPs)?

RQ4: Are all third parties that are initially informed of "acceptance" also notified when the consent is revoked?

To address these questions, we have set up a team of several computer scientists and a legal expert to *measure compliance of consent revocation on the Web*, making the following contributions:

(1) We provide the first in-depth legal analysis of the GDPR, ePD and other legal guidelines for *consent revocation* interface, storage and communication, and establish six operational legal requirements (§3).
(2) We provide a method to audit compliance of consent revocation interfaces (§4.1), and apply our analysis on Tranco's top-200 websites identifying multiple instances of non-compliance with the legal requirements (§5).
(3) We study the effect of revoking advertising and analytics (AA) cookies, finding that on the majority of websites, revocation does not decrease the number of AA cookies, thus violating the GDPR (§6).
(4) We propose a methodology (§4.2) to evaluate revocation on websites that implement *IAB Europe Transparency and Consent Framework* (TCF) and the most popular Consent Management Platform, OneTrust. We analyze 281 such websites and evaluate the storage of consent behind the consent banner interface (§7) and the communication of revocation (§8), thereby detecting multiple non-compliant practices.
(5) Finally, we give recommendations to further improve consent revocation compliance (§9).

Table 1 summarizes the most prevalent (more than 10%) potential violations of the GDPR and ePD that we detected while analysing both the consent revocation interface, cookies, and the consent storage and sharing with third-parties. Among the top-200 websites, we find that 22.7% (36) websites are compliant with GDPR and ePD within their revocation interfaces and management of cookies (see remaining potential violations in rows 1-3), and the compliance is more common in websites that employ CMPs. We, therefore, further investigate websites with CMPs for possible non-compliance. Of the 281 with CMPs, 251 provided revocation options – among them, we further check if a positive consent is stored even after revocation and if the consent modification is communicated to third-parties that were informed of acceptance. Overall, we find that 52.6% out of 251 websites providing revocation do not have a possible violation beyond the interface, while the remaining websites either had positive consent after revocation or communicated an initial positive consent to third-parties but did not communicate negative consent after revocation (rows 4-6).

Violations within the interface and cookies in top-200 websites	**Prevalence**	**Potential Violations**
Revocation via a different interface/medium (§5)	**20.25%** (32/158)	**LR2**, **P1**, **P2**, **P3**
Two or more steps to find revocation interface vs zero steps to accept (§5)	**20.8%** (33/158)	**LR3**, **P1**, **P2**, **P3**
Data processing based on AA cookies is not stopped upon user's consent revocation(§6)	**57.5%** (69/120)	**LR4**, **P1**, **P2**
Violations beyond the interface in 281 websites with CMPs	**Prevalence**	**Potential Violations**
Positive consent after revocation (TCF-based consent string) (§7)	**16.17%** (22/136)	**LR5**, **P2**
Positive consent after revocation (OneTrust-specific consent string) (§7)	**14.47%** (22/152)	**LR5**, **P2**
Third-parties informed of consent acceptance via HTTP requests, but not informed of revocation (§8)	**74.2%** (101/136)	**LR6**, **P1**, **P2**

Table 1: Summary of most prominent potential violations of consent revocation implementation alongside its prevalence (with the number of websites with violations and the total number of websites analyzed for each case) and legal requirements (LR) and GDPR principles (P) from Section 3.

2 Background and Related Works

In this section, we provide background on different techniques for consent management and discuss prior works on compliance in the context of consent banners, opt-out, and revocation.

Consent Interfaces and Compliance. Consent banners have become a common method for obtaining consent for online tracking. Recent works [4, 14, 38, 46, 69, 75] have examined consent banners following the implementation of the GDPR and the ePD while numerous others [3, 34, 35, 53, 55, 57–59, 63, 68, 71] explored the impact of privacy regulations on consent design, and how the websites and CMPs might violate these laws, e.g., by using *dark patterns*. Tools have been proposed to help users handle consent banners automatically [2, 6, 45, 50, 67**? ? ?**]. Several works [6, 38, 49, 63] focused on automated analysis of consent banners at scale.

IAB Europe TCF and Compliance. The current "de-facto" standard for the consent banners in the EU is the IAB Europe Transparency and Consent Framework (TCF) [23]. The current TCF v2.2 [43] defines the *pre-defined purposes* for processing personal data by Consent Management Platforms (CMPs). If also defines the *format to store the user's choice*, called TCString, that includes: (a) list of enabled third-party vendors registered within the TCF; (b) list of enabled purposes among the pre-defined purposes [42]. The TCF standard *does not specify which of the purposes require user consent*. According to GDPR and ePD, only purposes that do not require user consent (and users' explicit interaction with the CMP) may be enabled in TCString by default. Matte et al. [60] analyzed which purposes in TCF v1.1 and v2.0 require consent according to the GDPR and ePD; however, this analysis was not extended to TCF v2.2, which we perform in this paper.

Once a user has made their choice on the CMP interface, the CMP is required to store the corresponding TCString in the browser (however, the specific storage mechanism is not specified in TCF v2.2), or implement an API for third-parties to check the TCString.

The TCString can be accessed via the `__tcfapi` function by third-parties in first-party context or via the JavaScript `postMessage` API to communicate with a special `__tcfLocator` iFrame. Following TCF v1.1 [51], TCString can also be shared in the outgoing HTTP requests via URL-based methods. However, TCF v2.2 does not specify any URL parameters to be used for this.

Prior works [59, 60, 70, 77] have focused on the analysis of IAB Europe TCF and its consent implementation. However, none of these works studied how CMPs manage consent revocation, which is one of the main objectives of our work.

Consent Rejection and Revocation. While multiple studies [6, 59, 63] detect and analyze the presence of a reject button on consent banners, none of the prior works evaluated the interfaces that allow *revocation* of a given consent within the EU data protection framework. Nevertheless, since the updates of the CPRA regulation in California, multiple studies have analyzed the implementation of the right to opt out of selling or sharing user data within websites. Tran et al. [73] propose a methodology to measure compliance of opt-out links' wordings automatically found on websites subject to CCPA and CPRA [8]. Liu et al. [54] measure the impact of opting out in the presence of advertisers and tracking mechanisms. Aziz et al. [3] assessed the IAB CCPA Compliance Framework (analogous to IAB TCF in Europe) and detected that opt-out signals are not honored on websites. A similar latest work by Du et al. [18] detected violations regarding withdrawal interfaces in mobile applications.

Other studies evaluated user perceptions when interacting with opt-out mechanisms. As such, Habib et al. [37] evaluated the usability of data deletion and opt-out options related to email communication and targeted advertising. Habib et al.[36] evaluated how different instructions about revocation in the banner's text impact users' ability to find revocation options.

None of these works, however, studied whether the revocation interfaces comply with the EU laws. Additionally, no prior work has shed light on whether websites correctly store and manage revoked consent, and inform all the third-parties that were previously informed of consent acceptance.

3 Legal Compliance for Revocation

The EU Data Protection Framework provides legal principles and requirements that can be applied to websites and specifically to consent revocation. The GDPR applies to the processing of personal data [5], and the ePrivacy Directive (ePD) [22] provides *supplementary* rules, particularly, for the use of tracking technologies [21]. Whenever tracking data is stored and read from the user's device, the ePD [22, Art. 5(3)] requires websites to request *user's consent* when tracking is used for *purposes* not strictly necessary for the service provided, *e.g.*, advertising [20, 29]; purposes required for a website to operate are exempted [22, Recital 66]. The way to assess with certainty whether consent is required is to analyze the *purpose* of each tracker on a given website [20, 33].

The GDPR, as well as guidelines from the Data Protection Authorities (DPAs) and from the European Data Protection Board (EU advisory board, representing all EU DPAs) provide legal requirements for *consent revocation*. While guidelines are not legally-binding, they are part of the EU framework for data protection which we apply in this work to discern when revocation methods are compliant. A website can be held liable and fined if it fails to comply with the GDPR principles and requirements for valid consent, including revocation. Relevant *GDPR principles* are presented below and numbered with **P**, and *legal requirements for consent revocation* for websites are numbered with **LR**.

P1 (Fairness). Websites must not process personal data in a unjustifiably detrimental, discriminatory, unexpected or misleading way [30, Art.5(1)(a)], [24, para 17].

P2 (Data protection by design). Websites must implement organisational measures and safeguards efficiently to enable the exercise of the revocation right [25, para 68], [30, Art. 25(1)]; [25, para 70]. Revocation options should be provided in an objective and neutral way, avoiding any deceptive or manipulative language or design [26, 28, para 16]. If a website requires more effort to revoke than to give consent, it is deploying a dark pattern [26, para 30].

P3 (Accountability). Websites must demonstrate that revocation is performed easily and effectively [30, Arts. 5(2), 24(1), Rec. 74].

LR1 (Right to revoke consent). Users have the *right* to revoke consent at any time [30, Art. 7(3), Recital 42], and thus websites are obligated to *facilitate* the exercise of this right [30, Art. 12(2)] by providing a consent revocation option. This option to revoke consent must be clearly and distinctly recognisable. A *violation* of this requirement is the absence of revocation options, which renders consent invalid [30, Art. 4(11)] and any data processed henceforth is processed illegally, without a legal basis [30, Art. 6(1)(a)].

LR2 (Easy revocation through the same interface). Giving and revoking consent should be available through the same means/interface [26, para 115] (e.g. website, app, log-on account, etc.) since switching to another interface would require *unnecessary effort* [24, para 114]. For consent granted via a consent banner, DPAs disagree on which implementation should be recommended: the Dutch DPA only recommends that revocation should be reachable within the same website [19], while the German DPAs insist that it is inadmissible to search a privacy policy for a revocation option [17]. While the EDPB states a specific revocation solution cannot be imposed, and a case-by-case analysis is needed [27], [28, para 31-35], it recommends a permanently visible *icon* or a *link* on a standardized place [27, para 32], although not referring to its location. Few DPAs propose that such options could be displayed within the privacy or cookie policies [12, 17]. A *violation* of this requirement would be proposing revocation through another interface, contacting the website by email, asking the user to delete cookies [17, 19, 24], or using opt-out options on external websites [17].

LR3 (Easy revocation through the same effort and number of steps). Ease of revocation can be measured by the time spent and the number of actions [11], [26, para 116]. Actions can include the number of mouse clicks, keystrokes or swipe gestures to revoke, in comparison to the number of actions required to grant consent [24, para 14]; this number must be the same [19, p.8]. A *violation* could occur when consent obtained through one mouse-click, swipe or keystroke, but revoking takes more steps, it is more difficult to achieve or takes more time [26, paras 30, 114].

RQs	Collected dataset
RQ1, RQ2	**158** domains (ranked 1-200)
RQ3, RQ4	**279** domains (54 domains ranked 1-200 and 225 domains ranked 201-5k)

Table 2: Datasets used for RQs.

LR4 (Revoking requires stopping of data processing and deletion of consent-based data). The receiver of data *must stop subsequent data processing* after revocation [24, para 17]. This is especially relevant in circumstances where the controller uses a large advertising network to target individuals and track them across several websites [28, para 175]. If there is no other lawful basis justifying data processing, data receivers *must additionally delete all the data that was processed on the basis of consent*, as mandated by [30, Art. 17(1)(b)] (assuming that there is no other purpose justifying the continued retention). Such data should be deleted even in the absence of a deletion request by the user [24, para 119]. A *violation* could occur when data is still processed after revocation.

LR5 (Correct registration of consent revocation). Websites must correctly register the user consent revocation decision, and assure that the decision made by the user in the banner interface is identical to the consent that gets registered/stored by the website [30, Arts. 7(1), 30, Rec. 42], [13, 69](p.9). A *violation* occurs when a registered consent is different from the user's choice.

LR6 (Communication of revocation to third-parties). When users revoke consent, organisations need to make sure that this is communicated to other organisations that they have shared people's personal information with [19, 44]. Santos et al. [69, §5.5] also proposed that "the publisher should delete the *consent cookie* and communicate the withdrawal to all the third-parties who have previously received consent." Nevertheless, DPAs do not express specific requirements on informing third-parties. A *violation* could occur when a website does not implement the registration of consent revocation correctly, or does not communicate it to third-parties who process the data of its users [28, para 176], [9, para 85].

Another important requirement is that revoking consent cannot be detrimental to the user. If the consequences of revocation result in users being unable to access the services provided by the website, and no alternative is offered, the right to revoke consent cannot be considered free and may be deemed detrimental [10].

4 Methodology

Next, we describe our data collection and analysis methodology to address our research questions. We built a semi-automated crawler based on a Selenium-instrumented Chromium v122.0.6261.128. We used the crawler to collect data between March and June 2024, within the EU. Table 2 presents an overview of the datasets we collected, which are further explained below.

4.1 Dataset for RQ1 and RQ2

We have implemented the data collection pipeline shown in Figure 1 to capture the elements of the user interface that need to be interacted with in order to exercise consent revocation. At each stage of our analysis, we save background data to further analyze cookies, consent storage, and communication. Figure 2 presents the details of the background data collection.

4.1.1 Website selection. We analyzed the revocation interface options on Tranco top-200 domains [52, 74]. Of these, 158 domains were reachable while 42 did not display a webpage because they were either CDNs, blocked or returned failures.

4.1.2 Methodology. We collected the data (including cookies, local-storage, request-response pairs and screenshots) in a semi-automated manner as shown in Figure 1. Manual effort was required to browse and *locate* revocation options, while all technical data (cookies/storage, screenshots, logs) were collected automatically. Automating this would require robust ML/NLP models, which may not generalize well due to the diversity in UIs and revocation paths. While we manually visited and navigated the websites, the data was collected automatically in the background. We took screenshots to record the user interfaces involved in reaching a revocation option. We collected this data in four stages:

(1) *Initial landing:* We visit each website afresh with storage cleared for all websites in the browser, and collect the screenshots showing the presence of a banner.
(2) *After acceptance:* We record whether a banner is present and if an option is provided to the user to accept consent, in which case we accept all cookies.
(3) *After revocation:* After accepting consent, we check if an icon for modifying consent is visible on the page. If not, we check if an option is available in the footer or elsewhere on the main page. Finally, we check if the option is available on a different page reachable from the main page. For each of the options, we record the number of steps needed for revocation. If no option is found, we record that revocation is not possible.
(4) *After rejection:* To compare the behavior of the website after initial rejection (opt-out) with that after the consent is explicitly revoked, we clean the browser (includes clearing history, cookies, cache, passwords, form data, and site settings to ensure consistency in each measurement) and record the options to reject consent on the website. If a consent banner is present, we reject all cookies.

Amid all these steps, we also take screenshots in an automated manner at different stages by scrolling to the bottom of the pages or navigating to the settings in order to get the important information like keywords leading to revocation.

4.1.3 Analyzing interfaces for consent revocation (RQ1). Using the inputs and screenshots, we categorize the websites based on the revocation options, where such options are provided, and the number of steps required to revoke consent. We then map these categories to the legal requirements for GDPR and consent revocation (§3) to identify and measure potential violations of the law. To reduce manual bias in our analysis, labeling was conducted by one author (twice, in March and June of 2024), with category examples co-developed with a legal scholar. Several examples were jointly reviewed by both a legal expert and a computer scientist.

4.1.4 Effect of revocation on AA cookies (RQ2). In the background, we collect cookies stored in the browser at each of the four stages.

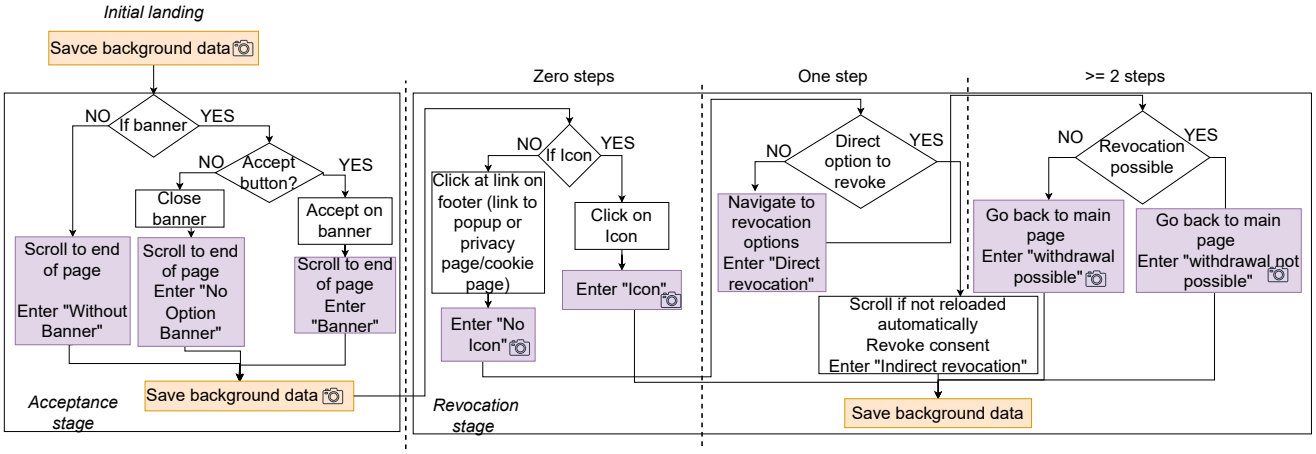


Figure 1: Data collection pipeline: to address RQ1, we collect screenshots and label a website as shown in violet boxes; for RQ2 we collect cookies at each stage and also at *Rejection stage* in a similar way (not shown in this figure).

Since only some categories of cookies require consent (see §3), we followed Bouhoula et al. [7] and consider that only cookies classified as *Advertising* or *Analytics* (AA) by CookieBlock [6] require user consent. If we detect AA cookies upon initial landing, after rejection, or after revocation, we map it to legal requirements and identify a potential violation of the law. Similarly, we analyze whether the number of AA cookies increases after revocation w.r.t. other stages of our analysis.

In this analysis, we do not include the websites without a banner because we need to compare cookies after explicit acceptance and after revocation. Websites without a banner do not allow a user to accept consent, and therefore, modifying consent on such websites would not mean "revocation" in legal terms.

4.2 Dataset for RQ3 and RQ4

In websites that allowed revocation, different methods were used to store the modified consent and communicate it over the network. Websites using CMPs normally rely on the revocation options provided by the CMPs to manage consent, which also provide a more standardized approach to consent management for websites using a specific CMP. We identify the detection methods for the use of OneTrust CMP, which is the most popular CMP on Tranco top-20k websites [39]. Additionally, prior works [59, 77] used the `__tcfapi` function provided by IAB TCF [23] to detect the presence of CMPs that implement the TCF and therefore use a standardised format for storing consent (Transparency and Consent String or TCString).

4.2.1 Identifying presence of TCF and OneTrust. We performed an automated crawl querying for `__tcfapi`, a function that must be provided to use TCF's functionalities, on the top-200 domains [74]. Out of 158 websites that were reachable, we found `__tcfapi` on 32 (20%) of websites[1]. Further, by examining websites with OneTrust and its documentation [**?**], we found that this CMP (1) stores user consent in a very specific format in a cookie named `OptanonConsent`, and (2) maintains a JavaScript variable, `OneTrustActiveGroups` (OTAG), which can be queried to get the current consent string. However, the format of the consent string accessible through these methods does not respect the IAB TCF TCString format.

4.2.2 Website selection. We use the above methods to detect websites that use TCF and OneTrust in the top-200 websites, resulting in only 56 websites with CMPs. We randomly chose an additional 1000 websites between the rank 200 and 5000; of these 1000, we detected either TCF or OneTrust on 225 websites resulting in a dataset of 281 websites for **RQ3** and **RQ4**.

4.2.3 Data collection. Figure 2 shows the data collection pipeline for **RQ3** and **RQ4**. The data is collected during all four stages of the experiment (highlighted as "Save background data" in Figure 1). We collect the consent strings (both TCString and consent variable specific to OneTrust) for further analysis of validity and consistency of consent storage (**RQ3**), and complement it with the information about scripts that access consent strings via APIs, scripts that initiate the requests and third-parties with whom consent is shared for the analysis of communication of consent (**RQ4**).

4.2.4 Collecting stored consent strings and third-parties that access them. The current TCF v2.2, does not define the specific location where the user consent should be stored; therefore, we collect all cookies and localStorage objects' values that match the TCString format. Additionally, we collect the `OptanonConsent` cookie that OneTrust uses to store a user's consent. We also inject scripts in the webpage to query `__tcfapi` and OTAG to analyze consent strings that third-parties would receive if they query these APIs and examine network logs to detect and store TCStrings shared in the requests and responses. All the collected consent strings are visualised in Figure 2 in orange color.

Third-parties can access consent strings via APIs or receive them via network requests. We capture (1) fetching of consent string via `__tcfapi` or OTAG by third-party scripts; (2) HTTP requests that contain consent strings in TCString format or OTAG. However,

[1]Similar to prior work [59], we found that `__tcfLocator` is present on only 1 website where `__tcfapi` is not present. We therefore do not test for this method here.

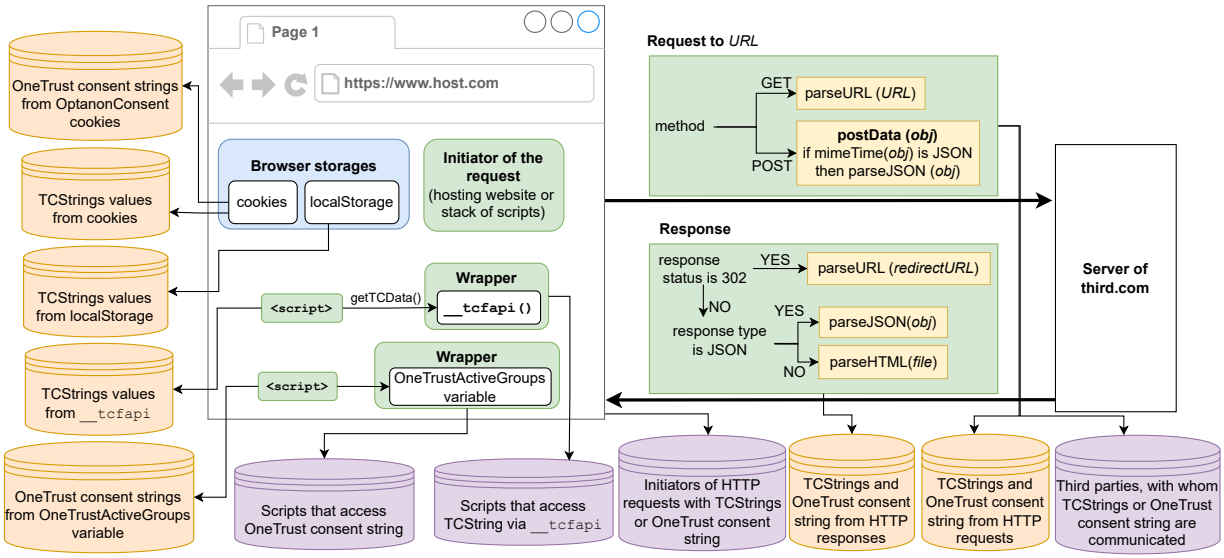


Figure 2: Data collection pipeline: to address RQ3 (validity and consistency of consent), the collected sets of consent strings are highlighted in orange, while for RQ4 (access and communication of consent to 3rd-parties), the sets of scripts parties involved in the communication of consent are highlighted in violet. The objects in green represent our methods for collecting the data, and the boxes in yellow are further described in Table 3.

some requests might not have been recorded since they do not have a well-defined format. We store all initiators and receivers of consent strings (see violet stores in Figure 2).

4.2.5 Detecting and extracting TCStrings and specific categories from OneTrust in network logs. To detect the TCString in network logs, we look at different parts of a request/response pair. Prior work [59], following TCF v1.1, has extracted TCStrings only from specific URL parameters (such as `gdpr_consent`) of outgoing HTTP requests. A follow-up work [77] checked for outgoing TCString in all URL parameters of HTTP requests and also in the HTTP cookie headers since TCF v2.2 does not specify URL parameters to be used. Following these works, when parsing URLs, we extract all query parameters, for example for a URL `https://www.site.com/zzz.jpg?ISBN=XXX&UID=ABC123`, we first extract the values `XXX` and `ABC123` and then check whether they correspond to the TCString format, according to TCF specification [41]. The orange boxes in Figure 2 represent the functions we used to extract TCStrings from different parts of the network logs that are further explained in Table 3.

Differently from prior works, our approach compares TCStrings sent in outgoing HTTP requests to third-parties with the TCStrings returned in HTTP responses, identifying cases when third-parties *modify the original TCStrings*. Since TCStrings do not have any protection mechanisms, any third-party that receives a TCString, can potentially modify it and return a different TCString back to the browser. To detect inconsistencies in TCString between requests and responses, we:

(1) search for TCString in the URL parameters for GET requests
(2) analyze the `postData` in POST requests and the response data (HTML and JSON formats) from the servers.

Func. in Fig. 2	Extracting TCString
parseURL (*URL*)	Extract all query parameters from *URL* and keep all values that match a TCString format or contain OneTrust cookie categories.
parseJSON (*obj*)	Extract all {`key:value`} pairs present in *obj* and keep all values that match a TCString format or contain OneTrust cookie categories.
parseHTML (*file*)	Extract URLs for `img`, `iframe` and `script` in *file* and parse them to extract TCStrings or OneTrust cookie categories.

Table 3: Extracting TCStrings and OneTrust consent string

(3) analyze redirected URLs in HTTP responses: if response type is JSON, we parse it; otherwise, we parse the returned HTML file to extract TCString from the script, image and iFrame elements.

We also record the request initiator to identify scripts that sent the wrong consent strings.

Compared to previous works [59, 77], our approach can uncover more instances of TCStrings because past works analyzed only specific URL parameters in GET requests and the cookies storing TCStrings apart from observing the requests made to 'getTCData' and 'getEventHandler'. We additionally collect network POST requests and responses(may be present in HTML format or JSON format) as well containing TCStrings. With our method, we detect 3,423 TCStrings in the `postData`, 52 TCStrings in JSON objects and 170 TCStrings in HTML files.

4.2.6 OneTrust-specific encoding of consent. Differently from other CMPs, OneTrust CMP does not use the TCString but uses a specific

format to store and communicate consent: the consent can be stored as key-value pairs in two locations, either in the `OptanonConsent` cookie or in the OTAG variable. The cookie values contain encoded categories of cookies (e.g., "analytics" or "advertisement"), that follow the format such as "X:1;Y:0;Z:1", where X, Y and Z indicate cookie categories and 0 or 1 indicate rejection or acceptance to use the specific category in the consent. The values of the OTAG list all the allowed cookie categories (called "active groups" in OneTrust documentation); however, the encoded format of such categories is not specified in OneTrust documentation. Our analysis of inconsistency between the `OptanonConsent` cookie value and OTAG variable (§7) revealed that when two values are not consistent, the value of `OptanonConsent` cookie contained the correct record of user consent. We therefore opted for extracting the allowed categories from the `OptanonConsent` cookies and search all such encoding (only X and Z in the example above) in the URL query parameters to record the consent strings being sent to third-parties.

However, the variable in the query parameter having the consent string is not consistent. This leads to false positives where the active groups are represented using numbers like '1', '2', and '3' or "1:1,2:0,3:0,4:1". These representations are hard to distinguish from query parameters used for purposes other than sharing consent. We manually analyzed such websites, and hence, could have missed some websites due to human error.

4.2.7 Wrappers for `__tcfapi` and OTAG. To identify `__tcfapi` access, we override the function to record all the scripts that access it. We also record what command was requested, e.g., "ping", "getTCData" or "getEventHandler". A similar approach was adopted by Matte et al. [59]. However, they observed calls made to the APIs in an older version of TCF, and their analysis did not include OneTrust. We override getter and setter methods of the OTAG variable to record which domain is writing/updating it (mostly by a designated CMP script) and reading/accessing it.

4.2.8 Communicating consent modification. We check the network logs to investigate if third-parties that received the TCString and OneTrust consent string (containing allowed cookie categories) after acceptance had also received the updated consent after revocation. We do this by checking if the requests to third-party URLs contained the TCString or OneTrust consent string either in the URL or in the POST data as described in Figure 2.

4.2.9 Identifying responsible parties. We record the initiators of all the network requests and use this information to identify which third-party script changed the consent. We match the script's domain of provenance with the CMP name decoded from the TCStrings. If the name and domain do not match, in case of inconsistencies, we manually check the domains for cases where the CMP names are either shortened or have words like 'privacy center' or 'CDN'. If we do not identify any such indicator that the third-party could be the CMP, we classify the responsible party just as a third-party.

4.3 Limitations

4.3.1 Accuracy of AA cookie classification. Even though CookieBlock [6] has better accuracy than other tools for classifying cookie purposes, it might not be entirely accurate: a website may declare some of the cookies, classified as AA, as *necessary* in their cookie policies. Such cookies, classified by CookieBlock, will be, nevertheless, labeled as AA and considered to require consent.

4.3.2 Not capturing network logs while searching for revocation option on secondary pages. When reaching the revocation settings takes multiple steps, for a few seconds, log-entries with the old consent (after acceptance) are also saved along with the network logs meant for "after revocation" stage. We remove these log-entries by searching for inconsistencies after the consent is revoked. However, the set of log-entries misclassified as "after revocation" are not checked for inconsistencies, and we may have missed a few cases similar to the ones mentioned in Table 8 in the Appendix.

4.3.3 Unable to capture access to consent when the third-parties use event listeners. Callback functions returned as an event listener by `__tcfapi` do not have a standard format or name to track the access requests made to the API. In theory, event-listeners should notify third-parties upon consent modification by initiating a network request. However, we observed that even when the third-parties registered the event listeners, there were no explicit network requests transmitting the modified consent string. Hence, we do not track API accesses when event listeners are used.

4.3.4 Determining description of purposes in OneTrust. We do not know how the purposes displayed by OneTrust or any CMP used by the website are mapped to the user's actual consent. Since there is no particular format used to store the consent string, it can vary between different CMPs and within websites using the same CMP.

4.3.5 Delay in registering user's consent. While collecting network logs to assess the communication of consent revocation to third parties, we observed (see Section A) that some websites may take time to register that a user revoked their initial consent. To account for this, we exclude cases with delays in updating consent strings from our list of violations. However, we include cases where some third parties correctly include the updated consent string in their network requests, while others still send the old consent (positive consent string). As the third-party notification happens server-side, this may result in some false-positives on our end.

4.3.6 Automation of data collection. Automating the data collection process would allow the framework to be applied more generically. While recent works [7, 47, 48] provide automated tools to select initial consent options on websites (specifically, button and toggle HTML elements) based on user choices, our analysis shows that *revoking consent may require navigating multiple links* on the page to reset the options once the initial banner is closed. Moreover, the *location of the consent modification options on websites are non-standard*, and it is not clear whether (and where) such options are present. Therefore, revocation options are difficult to find and interact with automatically (even with the use of ML/NLP models) due to the heterogeneity of revocation implementations. This is, however, an interesting future research direction but out of scope for the current work.

4.4 Data Availability and Responsible Disclosures

As described in §4.1 and Figure 1, we collect background data, screenshots, and website labels. The complete dataset, including the network logs and the crawler, is provided in the supplementary material [1]. Some examples are shown in the Appendix.

As the date of submission, we notified 23 companies who own the domains that we explicitly mention in the main text. In sharing our findings, we took inspiration from Maass et al. [56] who showed that mentioning GDPR and its fines and sending notifications from a legal academic, significantly increases the remediation rate of website owners. We informed the owners of these domains of the potential violations via email or contact form linked to in their privacy or cookie policy pages. The emails sent are included in the supplementary material [1]. Out of these 23 contacted companies, 3 explicitly acknowledged our email and and expressed interest in improving their revocation mechanisms. Two of them requested more information or examples to better understand the potential violations. Six others reverted with automated messages conveying possible delays, instructions on account deletion, requests to redirect the email within the organization or fill a request form. We are yet to receive responses from the remaining 14 websites, even after our follow-up.

5 Revocation Interface and its Compliance

To address **RQ1**, we examined user interfaces for revoking consent and checked if they (potentially) violated EU legal requirements. We first categorize the 158 reachable websites based on their consent banners: 108 (67%) websites display a *consent banner* to the users on their first visit, 8 (5%) websites displayed a banner with *no option*, not allowing to accept or reject consent, and 45 (28%) websites did not display any banner.[2] We manually classify the 158 websites based on the interface to revoke consent: 120 (74.5%) websites provide users option to revoke consent *within the same interface* where the consent request took place, or navigates to related pages for revoking consent; 32 (19.8%) websites provided options *via different interface*, where such options are present outside the interface or medium, where the consent request took place, and 9 (5.6%) websites offer *no revocation* option.

Table 4 summarizes the results for these three categories. To further evaluate legal compliance, for websites that provide revocation *within the same interface*, we count the number of steps required to revoke consent based on Figure 1. Figure 6 (in the Appendix) shows example screenshots for each of these categories.

5.1 Results

5.1.1 Compliant revocation interface (zero or one steps). Out of the 158 websites, only 8 (5.6%) offer a persistent icon or button floating on the page, thus requiring *zero steps* to reach the revocation option. 68 (41.6%) websites offered a link option in the footer of the page, requiring *one step* to reach the revocation option. 6 (6.8%) websites showed a consent banner or icon when accessing the privacy policy page from the footer, therefore also requiring *one step* to revoke consent. All these implementations found on 82 (51%) websites (labeled as *Icon, Footer Options* and *Banner on Policy* in Table 4) *comply* with revocation GDPR principles and consent requirements (**LR1-3**) since they are presented within the same interface and require zero or one step to revoke consent. According to Habib et al. [36], users who face persistent icons are more likely to recognise a correct method to revoke consent with respect to users who saw a link in the website's footer. Therefore, even though all such implementations are compliant, only 7.4% websites with an *Icon* provide a more *usable* revocation design.

5.1.2 Two or more steps to revoke vs zero steps to accept. 35 (22.1%) websites out of 158 allow users to access the revocation option *within the same interface*, but with additional obstruction, requiring them *2 or more steps* to revoke consent. Such websites (labeled with *Options via Policy*) hid the option to revoke consent inside the "Cookie Policy" or "Privacy Policy" page. According to the majority of EU regulators, this additional effort does not allow to exercise the right of revocation in a easy and effective way even if such option is located withing the interface. Arguably, the websites requiring additional effort neither comply with **LR3** (Easy revocation through the same effort and number of steps) nor with the principles **P1** (Fairness), since websites require unjustifiable and unexpected effort, nor **P2** (Data Protection by Design), since the adopted measures are not efficient as to facilitate the revocation right but obstruct it instead, and **P3** (Accountability), since such websites are not able to demonstrate compliance with the requirement **LR3**.

5.1.3 Revocation options Via Different Interface. Overall, 32 (19.87%) websites out of 158 offered the option to revoke consent via an interface that is substantially different from the interface for users to accept consent. Figure 7 in the Appendix shows examples of websites for each of the options given.

Twenty-five websites, including `medium.com`, `discord.com` and `wikipedia.org`, suggest revocation through *browser settings* by clearing cookies or by offering opt-out links for third-party tracking or advertisement domains (labeled as *Settings or links*). Three websites – `github.io`, `archive.org` and `who.int` – suggested users to contact or email them to revoke consent or delete the data (labeled *Contact/email*).

Settings or links as well as *Contact/email* revocation options infringe the legal requirement **LR2** (Easy revocation through the same interface), since revoking consent is not made available through the *same* means or interface; and principles **P1** and **P2**, since switching to these totally different interfaces requires unnecessary and disruptive effort that is obstructive and unexpected. This leaves users in an asymmetrical relationship between giving and revoking consent, which does not permit users to exercise their revocation right. Consequently, these websites cannot be accountable for demonstrating compliance with this right (**P3**).

On one website(`tumblr.com`) privacy settings lead the user to the login page and instruct them to revoke consent *after logging-in*, which may require account creation (labeled *After login*). While this option occurs through the same website, it directs the user to a different interface. As before, this option infringes the requirement **LR2** since the option redirects users to an unrelated interface. It also infringes principles **P1** and **P2** as it forces users to take unexpected additional steps and effort – to subscribe, and thus to give

[2]This can be explained by the fact that these websites were hosted outside of the EU and did not yet implement compliance solutions with EU laws.

Banner	#	Within the Same Interface				Via Different Interface			No Revocation
		Icon	Footer Options	Banner on Policy	Options via Policy	Settings or links	After Login	Contact/ Email	No option provided
Consent banner	105	8	61	4	23	8	1	0	0
No option banner	8	0	0	0	5	3	0	0	0
Without banner	45	0	7	2	7	17	0	3	4 [+5]
Total	158	8	68	6	35	28	1	3	9

Table 4: Prevalence and type of consent revocation options on 158 websites (ranked 1-200). We use different colors to represent the level of compliance of the detected practices. Green color represents zero or one steps, yellow represents two or more steps, and pink and red represent violations of varying severity.

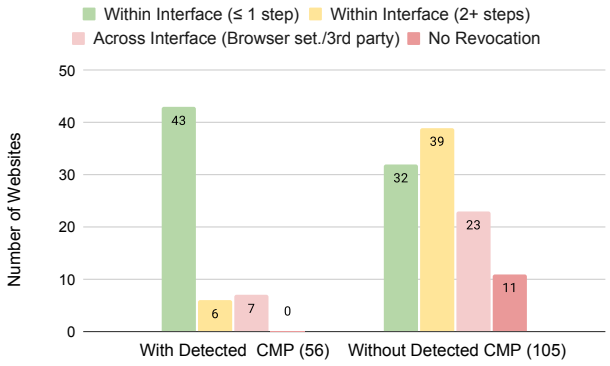


Figure 3: Revocation methods on top 158 websites

more personal data – to revoke consent. This option impedes these websites to show accountable revocation (**P3**).

5.1.4 No revocation option provided. Nine (5.6%) websites out of 158 did not provide any means to revoke consent, though they also did not display any consent banner, indicating that these websites probably did not integrate online tracking. We further analyzed these websites and found that 4 (2.48%) of them stored AA cookies making them non-complaint. These websites include `ntp.org` and `un.org`. All these 4 websites that use AA cookies infringe the legal requirement **LR1** (Right to revoke consent) and the following principles: **P1** since websites process data unjustifiably for AA purposes without a legal basis, or the knowledge or consent of users; **P2** as it does not create measures to enable the exercise of the revocation right. Consequently, these websites cannot be accountable for demonstrating compliance with this right (**P3**).

5.2 Impact of CMPs on compliance

Figure 3 shows the prevalence of different revocation options on the websites with detected CMPs *vis a vis* websites where we did not detect any CMP. 43 (77%) out of 56 websites with detected CMPs provide a compliant implementation (zero or one step) to revoke consent, while only 32 (30.5%) websites out of 105 websites without detected CMP have compliant implementation, showing overall a higher compliance rate for websites with CMPs.

Regarding non-compliant implementation, 37% (39 out of 105) websites without CMP require two steps or more to revoke consent, while only 10.7% (6 out of 56) websites with CMP needed 2 or more steps for revocation. None of the websites with CMP denied a revocation option to users, though 9 out of 105 websites without CMP offered no revocation option. In conclusion, websites with detected CMPs tend to be more compliant with revocation requirements.

6 Effect of Revocation on AA Cookies

In this section, we address **RQ2** and measure whether cookies requiring consent (Advertising and Analytics, or AA cookies) are deleted upon user's consent revocation. As described in § 4.1.3, we recorded the cookies of websites in four stages – upon initial landing, after accepting consent, after rejecting optional cookies, and after revocation. Out of the 120 websites where revocation was possible within the same interface, we find AA cookies after revocation on 69 (57.5%) websites.

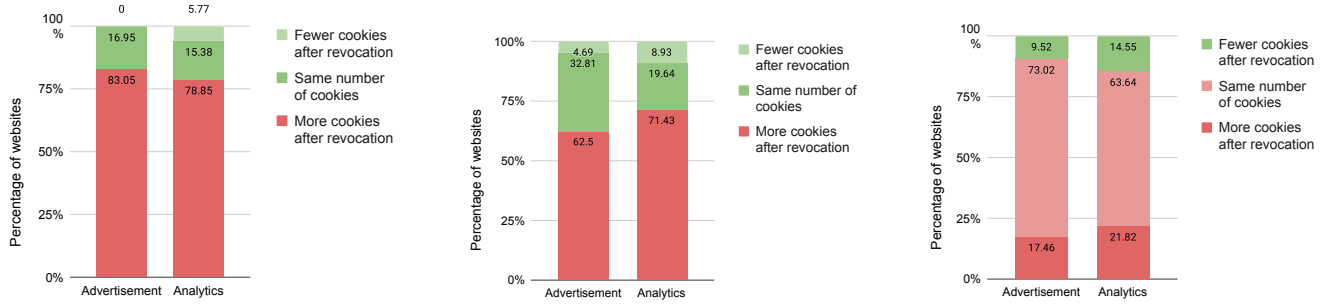
Figure 4 compares the change in the number of AA cookies on websites after revocation w.r.t. other stages. Surprisingly, the number of AA cookies increases on most websites after revocation w.r.t. initial landing and w.r.t. after rejection (see red bar in Figures 4a and 4b). Additionally, on the majority of analyzed websites, the number of AA cookies after acceptance remains the same after revocation (see pink bars in Figure 4c). Websites that *add or keep* AA cookies after consent revocation violate **LR4** (Revoking requires stopping data processing and deletion of consent-based data), **P1** and **P2**. Such AA cookies are processed unexpectedly and contrary to user's decisions, without a legal basis and are thus illegal [30, Art. 6(1)(a)].

We have further analyzed the datasets for potential violations for **RQ1** and **RQ2** by country, category of the website, or website owners. Since such subgroup analyses involve small sample sizes and are not statistically significant, we do not report them in the main text of the paper[3].

7 Validity and Consistency of Consent

In this section, we analyze how consent information is stored and shared behind a website interface, whether it is consistently stored across different storage and APIs and whether it is legally valid, thus answering **RQ3**. We analyzed 281 websites with detected CMPs to check the validity and consistency of the consent string that these CMPs implement. Together with a legal expert co-author of the paper, we analyzed 11 purposes predefined within IAB Europe TCF v2.2 [43] (see Table 9 in the Appendix). These purposes are largely consistent with those of the TCF v2.0 [60]. We determined

[3]These exploratory breakdowns are instead provided in the Appendix B for completeness.



(a) Comparison of AA cookies upon *initial landing* vs *after revocation*

(b) Comparison of AA cookies *after rejection* vs *after revocation*

(c) Comparison of AA cookies *after acceptance* vs *after revocation*

Figure 4: Change in the number of advertising and analytics (AA) cookies across different options

that purposes 2-9 require consent and demand user action to be selected, thus such purposes cannot be enabled by default in TC-String. Purposes 10-11 are exempted from this requirement and may be enabled by default. Purpose 1 is storage-based and enabled by default.

Positive consent: if the given TCString contains at least one of the purposes from 2-9, and at least one vendor in its vendor list, we consider it to contain a positive consent. Such consent is correct only within the Acceptance phase, where the user has actively selected purposes 2-9 requiring user action.

Negative consent: if only purposes 1, 10 or 11 are enabled in the TCString, we conclude that it contains negative consent because none of these purposes require any user action as per our legal analysis. Consequently, if such TCString is present upon *initial landing*, or *after rejection* or *after revocation* stage, we consider consent to be registered correctly.

For the consent strings extracted from OTAG variable, or from `OptanonConsent` cookie, we follow the OneTrust specification [**?**] and extract purpose numbers from its "groups" parameters. Since we do not have a specification for the meaning of these purposes, we cannot analyze which ones require consent. We therefore assume that a consent string contains a *negative consent* if it matches the value observed upon the *initial landing* stage, and a *positive consent* if the value contains more purposes than at *initial landing*.

7.1 Results

7.1.1 Positive consent upon initial landing, after rejection and after revocation. We first analyze if the TCStrings returned by `__tcfapi` can be considered as a "baseline" in our comparison, i.e., whether such TCStrings are valid. For this purpose, we analyzed whether the `__tcfapi` returns a positive consent at three stages: Initial landing, Rejection and Revocation, as shown in Table 5.

After Rejection and Initial landing: Only two prior works [59, 77] analyzed whether positive consent is stored or returned by APIs upon Initial landing and After Rejection. Compared to previous works, we found very few cases where positive consent is present after rejection in websites implementing the TCF (only 3 websites out of 150). In contrast, 10 websites, out of 164, store positive consent *after rejection* with OTAG.

After Revocation: We detected multiple websites where a *positive consent is present after revocation*, which has not been studied in previous works. In the websites with the TCF, 17 (12.5%) out of 136 websites provide positive consent in the `__tcfapi`, 12 (11.9%) out of 101 websites store a positive consent in a cookie, and 8 (25%) out of 32 websites store a positive consent in a localStorage. In the websites using OneTrust, we observe 22 (14.5%) out of 152 websites with positive consent returned by OTAG , and 13 (10%) out of 130 websites with positive consent in the `OptanonConsent` cookie. Positive consent constitutes potential violations of **LR5** (Correct Consent Registration) which entails that the registered consent must be identical to the user's choice in the user interface; and of the principle **P2** since websites did not implement technical measures and safeguards to assure that revocation is done efficiently.

7.1.2 Consent strings are often not updated after revocation. Since positive consent persisted post-revocation in many cases, we examined whether consent strings were properly updated (Table 5). Among websites using `__tcfapi`, 15 (9.3%) did not update the consent string, while 11 (10.9%) and 7 (21.9%) failed to update the TCString in cookies and localStorage, respectively. Notably, `sourceforge.com` lacked a banner, initially stored negative consent, but changed it to positive upon revocation. `ft.com` updated only the "consentScreen" parameter, keeping positive consent intact. For websites using OTAG, 16 (10.5%) out of 152 failed to update consent post-revocation. Additionally, six websites modified only some purposes while still retaining positive consent. Interestingly, `cisco.com`, `opendns.com`, and `webex.com` added one purpose to the consent string after revocation.

7.1.3 Inconsistency among consent strings between browser storage and APIs. Table 6 shows the number of websites where the TCString found in the cookies and localStorage is not consistent with the TC-String returned by the `__tcfapi`, and where the `OptanonConsent` cookie does not match the consent value returned by the OTAG. Such mismatches result in either an incorrect storage of consent or incorrect functioning of the APIs, and result in wrong consent being returned to third-parties. Five websites implementing the TCF returned different TCStrings from `__tcfapi` and the TCString stored in the cookie after revocation. In 2 of such websites, (`freep.com`

Storage method or API	Number of websites			Positive consent		
	Total using the method	Rejection possible	Revocation possible	Initial landing	After rejection	**After revocation**
`__tcfapi`	163	150	136	1	2	**17** (15 not updated)
TCF Cookies	127	104	101	0	0	**12** (11 not updated)
TCF localStorage	41	31	32	0	1	**8** (7 not updated)
OTAG	176	164	152	0	10	**22** (16 not updated)
`OptanonConsent` Cookies	131	130	130	0	0	**13** (10 not updated)

Table 5: Websites where consent strings in browser storage and returned by APIs were positive in different phases.

Browser storage vs. API	# websites
TCF cookie vs. `__tcfapi`	5 (100)
TCF localStorage vs. `__tcfapi`	3 (32)
OT cookie vs. OTAG	4 (130)

Table 6: Inconsistent consent strings across browser storages and APIs after revocation. The numbers in brackets show the number websites that used both the storage and the API.

and `megaphone.com`) the TCString in the cookie was not updated, and still contained a positive consent, while the TCString returned by the `__tcfapi` was properly updated into a negative consent. In the website `aol.com`, while the `__tcfapi` returned a positive consent, the value in the cookie stores negative consent.

In three websites (`reuters.com`, `manchestereveningnews.co.uk` and `portfolio.com`), the TCString returned by `__tcfapi` showed negative consent, while the TCString stored in the localStorage remained unchanged, i.e, it contained positive consent. On websites implementing OneTrust, we observed 4 mismatches between OTAG and `OptanonConsent` cookie value, where the cookies stored a negative consent and were shared on the network. This mismatch can lead to the incorrect consent being shared to third-parties.

These mismatches between consent strings across browser storage and APIs can be due to the fact that websites do not consistently update the storage and APIs when users revoke consent. Consequently, websites do not correctly register consent, as they are obligated to, thus, infringing the consent requirement **LR5**. Moreover, **P2** is not also complied with since websites do not implement technical measures to assure that revocation is done efficiently.

7.1.4 Inconsistency between consent returned via `__tcfapi` and consent shared on the network. We compare consent strings from `__tcfapi` with the consent strings found in outgoing network requests and incoming responses for two stages: Acceptance and Revocation. We consider the cases where the TCString returns the correct consent, i.e, a negative consent in case of revocation.

We investigate inconsistencies in the consent strings shared to and received from the third-parties, which, in turn, helps identify the responsible party for such inconsistencies. Previous works have only partially analyzed such inconsistency [59, §VIII.A], where positive consent was found to be sent within a specific `gdpr_consent` URL parameter on websites where `__tcfapi` did not contain a positive consent string. We however observed that the consent can be shared via differently named URL parameter as well. Additionally, the consent string can be sent in the POST data as part of the request as well. We find different inconsistencies on 8 distinct websites out of the 136 websites where revocation is possible.

These inconsistencies could arise due to: (1) delay in updating the consent after user revokes consent; (2) some scripts not being updated about revocation in consent; (3) introducing/using a different TCString. We do not consider delay in sending the updated consent as a violation since it is implementation specific. However, there are 8 websites where we observe inconsistencies causing possible violations. Out of these 8 websites, 4 of them (`forbes.com`, `time.com`, `n-tv.de` and `cadenaser.com`) had a different TCString on the network while `deadline.com`, `kotaku.com`, `manchestereveningnews.co.uk` and `walesonline.co.uk`, we observed that the old positive consent string was shared on the network by some scripts even after revocation. Details regarding these inconsistencies can be found in Appendix A.

The detected mismatches between consent strings returned by `__tcfapi` and the TCString shared on the network (Table 8) lead to an incorrect registration of consent revocation by websites and also by the implemented CMPs. Consequently, websites do not comply with **LR5** since they do not correctly register user revocation, as they are obligated to, in order to assure that the registered consent is identical to the user's choice in the user interface. As a result, a single TCString does not serve as a proof of revocation, which should consist of a negative consent. Moreover, the principle **P2** is also not complied with since websites did not implement technical measures to assure that revocation is done efficiently.

8 Communicating Consent Revocation to Third-parties

Next, we address **RQ4** and investigate if all the third-parties that were informed of the consent acceptance (either by accessing APIs or via HTTP requests) are also informed of consent revocation.

8.1 Results

8.1.1 Not all third-parties are informed of revocation by accessing consent via APIs. To examine which third-parties access the APIs implemented by CMPs, we override the implementation of `__tcfapi` and OTAG (see §4.2.4). Overall, we found 23 (9.6%) websites out of 238 where at least one third-party accessed the API to fetch positive consent after acceptance, but did not access the API to fetch revoked consent. Among these, on 163 websites where `__tcfapi` is implemented (see Table 5), on 14 (8.6%) websites at least one third-party requests the `__tcfapi` with the command "getTCData"

% 3rd-parties not informed	Number of websites
< 25%	1
≥ 25 to < 50%	5
≥ 50 to < 75%	15
≥ 75 to < 100%	35
100%	45

Table 7: Percentage of third-parties informed of acceptance but not informed of the revocation in 101 websites.

after acceptance but not after revocation[4]. Out of 176 websites that support OTAG, on 13 (7.4%) websites at least one third-party accesses the OTAG variable after accepting, but not after revocation. On 4 of these 13 websites, scripts from the third-party domain `ads-static.conde.digital` read the value of the variable, indicating that this variable can be used to know the consent choice given for AA purposes, since this domain is present in EasyList [31].

CMPs expose APIs to third-parties to access consent information making them responsible for requesting access to consent and for being informed on updates. Therefore, a proper implementation of event listeners by the website or by CMPs is necessary to inform third-parties about consent revocation, since consent can be updated multiple times in a single user session. We discuss about the standardization of the event-listeners in §9.

8.1.2 Not all third-parties are informed of the consent revocation via HTTP requests. On each website where consent revocation is possible, we detected third-parties that are informed of consent information via the TCStrings and One Trust consent string in the URL or postData (see §4.2.4). We then detect third-parties informed of consent after acceptance but not informed of revocation.

Of the 136 websites that implement `__tcfapi` and support revocation, 101 (74.2%) websites contain at least one third-party that was informed of consent after acceptance, but not after revocation via HTTP requests. Moreover, on 68 of these websites, third-parties that were not informed about revocation set cookies through the "Set-Cookie" HTTP header, and thus, did not stop processing user's data after revocation. Table 7 shows the percentage of third-parties not informed of consent after revocation. Surprisingly, 45 (44.5%) websites did not inform *any* of the detected third-parties, while 35 (34.6%) of them did not inform more than 75% of included third-parties. Figure 5 shows most prevalent third-parties that were not informed of the revoked consent via HTTP requests but were informed of consent acceptance. These websites include the big ad-tech industry actors `doubleclick.net`, `criteo.com` and `adnxs.com`. Interestingly, 73.77% of all third-party domains that do not receive a communication about consent revocation are present in EasyList [31] and therefore participate in advertising or tracking.

Of the 152 websites that provide revocation and implement OneTrust, we observed that allowed categories from the `OptanonConsent` cookie (see §4.2.5) are rarely shared with third-parties, i.e., only on 8 websites OneTrust allowed categories were sent to third-parties after acceptance, and 6 sent the allowed categories

[4]In the latest version of TCF, there is an option for third-parties to add an event-listener for consent update. However, since the implementation of this API is not standard, we could not intercept calls to it.

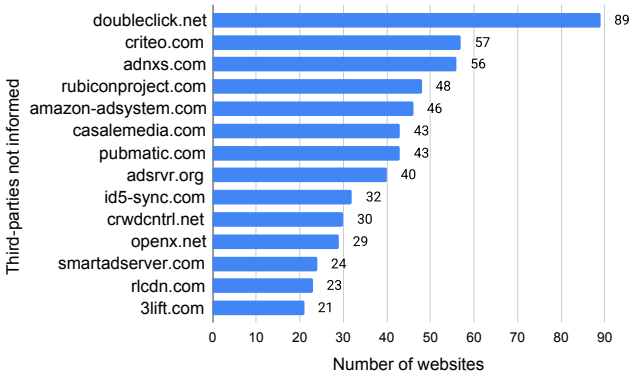


Figure 5: Top 15 third-parties not informed of the revoked consent via HTTP requests and the number of websites including these scripts but not informing them of revocation.

after revocation. Interestingly, all third-party requests with allowed categories were made to Google Analytics (`www.google-analytics.com`) and Google Tag Manager (`gtm.elementor.com`). According to the official OneTrust documentation, the categories are communicated to the Google Tag Manager for it to manage consent and third parties [66]). We therefore conclude that OneTrust CMP may delegate the consent communication to the GTM framework and not send the allowed categories to third-parties by itself.

8.1.3 Failure to communicate consent revocation results in unlawful data processing. Our findings indicate that third-parties are not informed about consent revocation. This fact entails that these tracking- and advertising-based third-parties may continue to *unlawfully* process user's personal data even after users have revoked consent on the website's interface, since they were not updated of the user's decision by the website. Consequently, websites from both cases (communication of the TCString via API and HTTP requests) are in potential violation with **LR6** (Communication of withdrawal to third-parties) that demands websites to communicate consent revocation to the third-parties. The continuous unexpected processing of user's data after revocation infringes the fairness principle **P1** and the data protection by design principle **P2** due to the lack of technical measures and safeguards efficiently enabling the exercise of the revocation right by websites.

9 Recommendations

In this section, we also propose recommendations to regulators for enhancing the implementation of consent revocation and ensuring legal compliance, in the light of our findings.

R1. Need to unify EU requirements for consent revocation interface. Our research shows that websites implement revocation inconsistently across the Web (see Table 4). For example, the text placed in the website footer differs across websites (e.g., "Cookie Settings", "Privacy Settings", but also "EU Privacy"), and in many cases does not mention revocation. It is even harder to locate revocation links within privacy policies that are labelled with text such as "How do I control cookies and how my data is used?", or "Managing our analytics cookies". The vague and ambiguous representation of

these options misleads the users and prevents them from exercising the revocation right which should be clearly and distinctly recognisable (see **LR1**). Icons, that are supported by regulators and are easy to locate, use different visualisations, which may also confuse the user. EU DPAs should propose *unified interface requirements describing the interface, location, and wordings of revocation.* An inspiration can be taken from CPRA regulation in California, where three acceptable wordings are proposed, which simplifies locating it with automated means to measure compliance [73].

R2. Need to standardize consent storage. We observed various inconsistencies in storing the TCStrings and OneTrust consent strings (see §7). This is due to the usage of different storage options that are not updated simultaneously when consent is revoked. We *invite regulators to establish standards for consent storage, and implement security measures to protect the integrity of consent strings.*

Additionally, under the Same-Origin Policy (SOP) [**?**], any third-party script included directly on a webpage has access to all first-party persistent storage mechanisms, including cookies and localStorage. This requires the website developers to trust that the third party scripts being included will not do anything malicious. As shown in Table 5, out of 136 websites that implemented IAB TCF, we found that the TCString was stored in first-party cookies on 122 websites (89.6%). Due to the SOP policy, any third-party script running on these pages can potentially *modify* these TCStrings, for example, by rewriting a TCString that initially doesn't allow any data processing into a TCString that allows the processing of data for all purposes and vendors registered in IAB TCF. The unauthorized modification of consent strings can render consent invalid and trigger the violation of the security principle (Article 5(f) GDPR).

R3. Need to standardize consent communication via event listeners. Our results show that only 43 out of 163 websites had third-parties installing event listeners in order to be updated about the change in consent decisions (see §8.1.1). While OneTrust suggests developers to add event listeners to synchronize consent updates when integrating advertising systems [66], our results show that IAB Europe TCF does not standardize event listeners, prompting every CMP to propose their own solution. This makes it harder for third-parties to adapt to different implementations across websites, placing the burden on them along with legal consequences (for continuous processing of personal data), without offering a practical solution to ensure compliance. We therefore recommend standard-setting bodies like IAB Europe TCF to standardize the implementation of event listeners and the callback functions returned by event listeners to inform third-parties about consent revocation. We also propose *regulators to take a position on the means of communicating consent to third-parties.* We believe that event listeners are able to provide reasonable means for communicating revocation decisions, and help in the allocation of responsibility to collect valid consent by third-parties present on a website.

R4. Need to regulate consent communication via HTTP requests. The *most prevalent violation* we detected indicates that 74.2% of websites do not properly inform all third-parties about consent revocation when the HTTP request method is used (see §8.1.1). Our result shows that this concrete way of informing third-parties exempts big advertising actors, such as `doubleclick.net` and `criteo.com` (see Figure 5) from any responsibility regarding data deletion when users revoke consent. Moreover, these third-parties only receive positive consent from the majority of websites and consequently, while illegally processing data from users who revoked consent, these companies can falsely demonstrate evidence of compliance to regulators by providing a *false proof of consent.* We therefore propose that *EU regulators express their position regarding how websites should inform third-parties*, and whether HTTP requests is an acceptable method, since our findings demonstrate that this approach leads to the most prevalent violations.

10 Conclusion

In this work, we propose a framework to audit compliance of consent revocation on the Web. Using this framework, we found multiple instances of violations of the EU Data Protection law while analyzing interfaces of revocation, including the use of different interfaces (19.87%) and additional effort required to revoke than to accept (20.5%). Violations were also observed on the usage of cookies and storing positive consent despite user's revocation. Surprisingly, on 74% of websites, third-parties that received consent upon user's acceptance, were not informed of users' revocation, leading to the illegal processing of users' data by such third-parties.

While the compliance analysis in this paper is specific to the EU, we believe that this paper provides insights on how websites handle revocation in general. Given that websites may behave differently under different jurisdictions, additional data collection may be needed. Nevertheless, we believe that our methodology for analyzing both revocation interfaces and behind the interface functionality (consent storage and communication to third-parties) can still be used to detect potential violations of other regulations.

Our findings emphasize the need for consistent legal compliance of consent revocation, and proper and uniform implementation of revocation communication and data deletion practices.

Acknowledgments

We thank the anonymous reviewers for their insightful comments. This work has been supported by the ANR 22-PECY-0002 IPoP (Interdisciplinary Project on Privacy) project of the Cybersecurity PEPR, the TULIP project of the ANR MRSEI program 2023, and the Inria International Chair funding, and in part by the SERB grant no. SRG/2023/000075 and the PMRF Fellowship.

References

[1] 2025. Supplementary Material for Measuring Compliance of Consent Revocation on the Web. https://github.com/Gayatri-Priyadarsini/Measuring-Compliance-of-Consent-Revocation-on-the-Web.
[2] CAVI AU. 2022. Consent-O-Matic. https://consentomatic.au.dk/.
[3] Muhammad Abu Bakar Aziz and Christo Wilson. 2024. Johnny Still Can't Opt-out: Assessing the IAB CCPA Compliance Framework. *Proc. Priv. Enhancing Technol.* 2024, 4 (2024), 349–363. https://doi.org/10.56553/popets-2024-0120
[4] Nataliia Bielova, Cristiana Santos, and Colin M Gray. 2024. Two worlds apart! Closing the gap between regulating EU consent and user studies. *Harvard Journal of Law & Technology (JOLT)* 37 (2024).
[5] European Data Protection Board. 2007. Opinion 4/2007 on the concept of personal data (WP 136), adopted on 20.06.2007. https://ec.europa.eu/justice/article-29/documentation/opinionrecommendation/files/2007/wp136_en.pdf
[6] Dino Bollinger, Karel Kubicek, Carlos Cotrini, and David Basin. 2022. Automating Cookie Consent and GDPR Violation Detection. In *31st USENIX Security*

Symposium. 2893–2910.
[7] Ahmed Bouhoula, Karel Kubicek, Amit Zac, Carlos Cotrini, and David Basin. 2024. Automated, Large-Scale Analysis of Cookie Notice Compliance. In *USENIX Security Symposium*.
[8] California State Legislature. 2018. California Consumer Privacy Act of 2018. https://oag.ca.gov/privacy/ccpa
[9] CJEU-C-129/21-2022 2022. Judgment in Case C-129/21 Proximus NV v Gegevensbeschermingsautoriteit. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CJ0129
[10] CNIL. 2023. Délibération de la formation restreinte n°SAN-2023-024 du 29 décembre 2023 concernant la société YAHOO EMEA LIMITED. https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000048967251.
[11] Commission Nationale de l'Informatique et des Libertés (CNIL). 2020. Recommandation "cookies et autres traceurs". https://www.cnil.fr/sites/default/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf
[12] Danish DPA (Datatilsynet). 2021. Quick Guide on the use of cookies. https://www.datatilsynet.dk/Media/F/8/Behandling%20af%20personoplysninger%20om%20hjemmesidebes%C3%B8gende.pdf
[13] Data Protection Commission (DPC). 2020. Guidance Note: Cookies and other Tracking Technologies. https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20tracking%20technologies.pdf
[14] Martin Degeling, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. 2019. We Value Your Privacy... Now take some cookies: Measuring the GDPR's impact on web privacy. In *Proceedings of the 26th Network and Distributed System Security Symposium*.
[15] Directorate General Justice, European Commission. 2013. Working Document 02/2013 providing guidance on obtaining consent for cookies. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf [Online; accessed 2025-02-25].
[16] Italian DPA. 2024. Provvedimento del 6 giugno 2024 [10029424] against Eni Plenitude S.p.A. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10029424.
[17] DSK-DPA-cookies-2021 2021. Guidance from the Conference of Independent Data Protection Supervisory Authorities of the Federal Government and the States of 20 December 2021 (OH Telemedia 2021, V.1.1). https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf, accessed on 2024.09.03.
[18] Xiaolin Du, Zhemin Yang, Jiapeng Lin, Yinzhi Cao, and Min Yang. 2024. Withdrawing is believing? Detecting Inconsistencies between Withdrawal Choices and Third-party Data Collections in Mobile Apps . In *2024 IEEE Symposium on Security and Privacy (SP)*. 735–751.
[19] DutchDPA-revocationDoc-2024 2024. Explanation of the standard of the AP on the withdrawal of consent for cookie banners 01 March 2024. https://www.autoriteitpersoonsgegevens.nl/documenten/normuitleg-ap-over-intrekken-van-toestemming-bij-cookiebanners, accessed on 2024.09.03.
[20] European Data Protection Board (EDPB). 2013. Opinion 03/2013 on purpose limitation (WP 203). Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.
[21] European Data Protection Board (EDPB). 2019. Opinion 5/2019 on the Interplay between the ePrivacy Directive and the GDPR, in Particular Regarding the Competence, Tasks and Powers of Data Protection Authorities. https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf
[22] ePD-09 2009. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0136, accessed on 2019.10.31.
[23] IAB Europe. 2025. TCF - Transparency & Consent Framework - IAB Europe. https://iabeurope.eu/transparency-consent-framework/.
[24] European Data Protection Board. 2020. Guidelines 05/2020 on consent under Regulation 2016/679. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.
[25] European Data Protection Board. 2020. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0 Adopted on 20 October 2020. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf
[26] European Data Protection Board. 2022. Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them. https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en
[27] European Data Protection Board. 2023. Report of the work undertaken by the Cookie Banner Taskforce. https://edpb.europa.eu/our-work-tools/our-documents/report/report-work-undertaken-cookie-banner-taskforce_en.
[28] European Data Protection Board. 2024. Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, Adopted on 17 April 2024. https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf.
[29] European Data Protection Board (EDPB), Article 29 Working Party. 2012. Opinion 04/2012 on Cookie Consent Exemption (WP 194).
[30] European Parliament and Council of the European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council. https://data.europa.eu/eli/reg/2016/679/oj
[31] Famlam Fanboy, MonztA and Khrin. 2023. EasyList. https://easylist.to/. Accessed on 12 March 2023.
[32] Danish Agency for Digital Government. 2023. Danish Agency for Digital Government Decision against Meta. https://gdprhub.eu/images/b/bb/Paabud-til-meta-platforms.pdf.
[33] Imane Fouad, Cristiana Santos, Feras Al Kassar, Nataliia Bielova, and Stefano Calzavara. 2020. On Compliance of Cookie Purposes with the Purpose Specification Principle. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. 326–333. https://doi.org/10.1109/EuroSPW51379.2020.00051
[34] Julia Giese and Martin Stabauer. 2022. Factors That Influence Cookie Acceptance: Characteristics of Cookie Notices That Users Perceive to Affect Their Decisions. In *9th International Conference on HCI in Business, Government and Organizations*. 272–285.
[35] Colin M. Gray, Cristiana Santos, Nataliia Bielova, Michael Toth, and Damian Clifford. 2021. Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. Article 172, 18 pages.
[36] Hana Habib, Megan Li, Ellie Young, and Lorrie Cranor. 2022. "Okay, Whatever": An Evaluation of Cookie Consent Interfaces. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. Article 621, 27 pages.
[37] Hana Habib, Yixin Zou, Aditi Jannu, Neha Sridhar, Chelse Swoopes, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2019. An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 387–406.
[38] Maximilian Hils, Daniel W. Woods, and Rainer Böhme. 2020. Measuring the Emergence of Consent Management on the Web. In *Proceedings of the ACM Internet Measurement Conference (IMC '20)*. 317–332.
[39] Maximilian Hils, Daniel W. Woods, and Rainer Böhme. 2021. Privacy Preference Signals: Past, Present and Future. *Proceedings on Privacy Enhancing Technologies* 4 (2021). https://petsymposium.org/2021/files/papers/issue4/popets-2021-0069.pdf
[72]]i-dont-care-about-cookies I dont care about cookies [n. d.]. I don't care about cookies 3.5.0. https://www.i-dont-care-about-cookies.eu/.
[41] IAB. 2024. GDPR-Transparency-and-Consent-Framework/TCFv2/IAB Tech Lab - Consent string and vendor list formats v2.md at master - InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework. https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/TCFv2/.
[42] IAB. 2025. Index - Global Vendor List. https://register.consensu.org/Translation.
[43] IAB. 2025. TCF Policies - TransparencyConsentFramework_Policies_Version 2024-06-3.5.0.docx. https://iabeurope.eu/transparency-consent-framework-file/TCF%20Policies%20-%20TransparencyConsentFramework_Policies_Version%202024-06-3.5.0.pdf.
[44] Information Commissioner's Office (ICO). 2020. Call for views on "consent or pay" business models. https://ico.org.uk/cookies-call-for-views-202403
[45] Vitor Jesus and Harshvardhan J. Pandit. 2022. Consent Receipts for a Usable and Auditable Web of Personal Data. *IEEE Access* 10 (2022), 28545–28563. https://doi.org/10.1109/ACCESS.2022.3157850
[46] Georgios Kampanos and Siamak F. Shahandashti. 2021. Accept All: The Landscape of Cookie Banners in Greece and the UK. In *ICT Systems Security and Privacy Protection*. 213–227.
[47] Rishabh Khandelwal, Thomas Linden, Hamza Harkous, and Kassem Fawaz. 2021. PriSEC: A Privacy Settings Enforcement Controller. In *30th USENIX Security Symposium (USENIX Security 21)*. 465–482.
[48] Rishabh Khandelwal, Asmit Nayak, Hamza Harkous, and Kassem Fawaz. 2023. Automated cookie notice analysis and enforcement. In *Proceedings of the 32nd USENIX Conference on Security Symposium*. Article 63, 18 pages.
[49] D. Kirkman, K. Vaniea, and D. W. Woods. 2023. DarkDialogs: Automated Detection of 10 Dark Patterns on Cookie Dialogs. In *2023 IEEE 8th European Symposium on Security and Privacy (EuroSP)*. 847–867.
[50] Oksana Kulyk, Annika Hilt, Nina Gerber, and Melanie Volkamer. 2018. "This Website Uses Cookies": Users' Perceptions and Reactions to the Cookie Disclaimer. In *3rd European Workshop on Usable Security*.
[51] IAB Tech Lab and IAB Europe. 2018. GDPR consent passing for URL-based services: Transparency and consent framework. https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master.
[52] 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 Network and Distributed System Security Symposium*.
[53] Ronald Leenes and Eleni Kosta. 2015. Taming the cookie monster with Dutch law – A tale of regulatory failure. *Computer Law & Security Review* 31 (03 2015). https://doi.org/10.1016/j.clsr.2015.01.004
[54] Zengrui Liu, Umar Iqbal, and Nitesh Saxena. 2024. Opted Out, Yet Tracked: Are Regulations Enough to Protect Your Privacy? *Proc. Priv. Enhancing Technol.* 2024,

1 (2024), 280–299. https://doi.org/10.56553/popets-2024-0016
[55] Eryn Ma and Eleanor Birrell. 2022. Prospective Consent: The Effect of Framing on Cookie Consent Decisions. In *Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems*. Article 400, 6 pages.
[56] Max Maass, Alina Stöver, Henning Pridöhl, Sebastian Bretthauer, Dominik Herrmann, Matthias Hollick, and Indra Spiecker. 2021. Effective Notification Campaigns on the Web: A Matter of Trust, Framing, and Support. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, 2489–2506. https://www.usenix.org/conference/usenixsecurity21/presentation/maass
[57] Dominique Machuletz and Rainer Boehme. 2020. Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR. In *Proceedings on Privacy Enhancing Technologies Symposium*, Vol. 2. 481–498.
[58] Arunesh Mathur, Mihir Kshirsagar, and Jonathan Mayer. 2021. What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Article 360, 18 pages.
[59] Célestin Matte, Nataliia Bielova, and Cristiana Santos. 2020. Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework. In *2020 IEEE Symposium on Security and Privacy (SP)*, Vol. 1. 791–809.
[60] Célestin Matte, Cristiana Santos, and Nataliia Bielova. 2020. Purposes in IAB Europe's TCF: which legal basis and how are they used by advertisers?. In *APF 2020 - Annual Privacy Forum*. Lisbon, Portugal, 1–24. https://inria.hal.science/hal-02566891
[72]]sop-mdn mozilla.org contributors. [n. d.]. Same-origin policy. https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy.
[72]]ninja-cookies Ninja Cookie [n. d.]. Download Ninja Cookie - MajorGeeks. https://www.majorgeeks.com/files/details/ninja_cookie.html.
[63] Midas Nouwens, Ilaria Liccardi, Michael Veale, David R. Karger, and Lalana Kagal. 2020. Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. *CoRR* abs/2001.02479 (2020). arXiv:2001.02479 http://arxiv.org/abs/2001.02479
[64] NOYB. 2024. Consent Banner Report - Overview of EU and national guidelines on dark patterns. https://noyb.eu/sites/default/files/2024-07/noyb_Cookie_Report_2024.pdf.
[72]]onetrust-dev OneTrust [n. d.]. OneTrust Developer Portal. https://developer.onetrust.com/.
[66] OneTrust. 2024. Cookie Consent Integration with Google Tag Manager | MyOneTrust. https://my.onetrust.com/s/article/UUID-301b21c8-a73a-05e8-175a-36c9036728dc?language=en_US.
[67] Harshvardhan Pandit, Christophe Debruyne, Declan O'Sullivan, and David Lewis. 2019. GConsent - A Consent Ontology Based on the GDPR. In *The Semantic Web (ESWC 2019)*. Springer, 270–282. https://doi.org/10.1007/978-3-030-21348-0_18
[68] Iskander Sanchez-Rola, Matteo Dell'Amico, Platon Kotzias, Davide Balzarotti, Leyla Bilge, Pierre-Antoine Vervier, and Igor Santos. 2019. Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control. In *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security* (Auckland, New Zealand) *(AsiaCCS '19)*. 340–351.
[69] Cristiana Santos, Nataliia Bielova, and Célestin Matte. 2020. Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners. *Technology and Regulation (TechReg)* (2020), 91–135. https://doi.org/10.26116/techreg.2020.009.
[70] Michael Smith, Antonio Torres-Agüero, Riley Grossman, Pritam Sen, Yi Chen, and Cristian Borcea. 2024. A Study of GDPR Compliance under the Transparency and Consent Framework. In *Proceedings of the ACM on Web Conference 2024* (Singapore, Singapore). 1227–1236.
[71] Than Htut Soe, Oda Elise Nordberg, Frode Guribye, and Marija Slavkovik. 2020. Circumvention by Design - Dark Patterns in Cookie Consent for Online News Outlets. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society* (Tallinn, Estonia) *(NordiCHI '20)*. Article 19, 12 pages.
[72]]super-agent superagent [n. d.]. superagent – My WordPress Blog. https://superagent.com/.
[73] Van Hong Tran, Aarushi Mehrotra, Marshini Chetty, Nick Feamster, Jens Frankenreiter, and Lior Strahilevitz. 2024. Measuring Compliance with the California Consumer Privacy Act Over Space and Time. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Article 785, 19 pages.
[74] Tranco. 2023. Information on the Tranco list with ID LYLP4. https://tranco-list.eu/list/LYLP4/.
[75] Martino Trevisan, Stefano Traverso, Eleonora Bassi, and Marco Mellia. 2019. 4 Years of EU Cookie Law: Results and Lessons Learned. In *Proceedings on Privacy Enhancing Technologies 2019*.
[76] Polish DPA (UODO). 2019. Decision ZSPU.421.3.201 against ClickQuickNow Sp. z o. o. https://uodo.gov.pl/decyzje/ZSPR.421.7.2019.
[77] Mingxue Zhang, Wei Meng, You Zhou, and Kui Ren. 2024. CSChecker: Revisiting GDPR and CCPA Compliance of Cookie Banners on the Web. In *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering* (Lisbon, Portugal). Article 174, 12 pages.

Appendix

A Inconsistency between consent returned via `__tcfapi` and consent shared on the network

Table 8 presents different types of inconsistencies we have observed in our analysis, grouped by the reason for such inconsistency. We observed three types of inconsistencies in the requests and responses: (1) due to delay in updating the consent after user revokes consent; (2) due to introducing/using a different TCString; (3) due to some scripts not being updated about revocation in consent.

Cases where the consent was not updated immediately are the requests sent to third-parties and containing the TCString before user update. We also investigate the time difference between the user update event and when the old consent was still being sent on the network. We additionally observe cases where some URL parameters were updated while some variable in the POST data containing the old consent and taking few seconds to be updated. Examples include `cnn.com, idnes.cz,independent.co.uk`.

Cases where a completely different TCString was shared on the network, include two websites `forbes.com` and `time.com`, where the CMP's server sends a TCString in the response to a request made by the CMP's script. This TCString is not the same as the one returned by the `__tcfapi` and contains additional vendors and purposes. We however don't observe this TCString being shared to other third-parties. We observe this behavior both after acceptance and after revocation. In case of `time.com`, we observed 13 different TCStrings. We also observe one case where a completely different TCString with additional legitimate interests in `n-tv.de` w.r.t the TCString retuned by the `__tcfapi` after both in case of after acceptance and after revocation. In this case, the TCString was hard-coded in a first-party script and sent to a third-party. In case of `cadenaser.com`, a third-party server sends a different TCString in response to a third-party script request. However it was not further sent to other third-parties. We also want to point out here that we observe four cases where the ConsentScreen parameter in the TCString is changed. However it does not affect the user's consent in any way, hence is not relevant for the discussion.

Finally, we also observe cases where the scripts do not use the updated consent. While in `deadline.com`, all the requests use the old consent, in two websites, `manchestereveningnews.co.uk` and `walesonline.co.uk` some scripts send requests with the updated consent while the one script (signal-beacon.s-onetag.com/beacon.min.js) still sends the old consent on the network. Upon further investigation, we found that this script is used by the CMP but is not the one responsible for updating consent when the user takes action to do so. Table 8 also shows that localStorage was not updated while the cookies and `__tcfapi` was. It's possible that the script used the value from local storage instead, resulting in an outdated consent being sent. However, there is no evidence to support this.

B Cross-Dimensional Analysis of Potential Violations

To contextualize privacy violations across multiple dimensions across the top 200 websites, we conducted a detailed analysis by

Responsible party	Website	Reason for inconsistency
3rd-party (CMP) Ketch Kloud, Inc.	forbes.com	*Different TCString:* number of vendor consents and number of vendor legitimate purposes increased in TCString on the network w.r.t to the TCString returned by the `__tcfapi`.
3rd-party (CMP) Ketch Kloud, Inc.	time.com	*Different TCString:* number of vendor consents, number of vendor legitimate purposes and number purpose consent increased in TCString on the network w.r.t TCString returned by the `__tcfapi`. 13 different TCStrings received in the responses.
1st-party	n-tv.de	*Hardcoded TCString:* String hardcoded in 1st-party script, sent in the request to 3rd-party. The TCString had additional purpose legitimate interests (5) and vendor legitimate interests (3).
3rd-party (CMP) Didomi	cadenaser.com	Third-party sends a different TCString w.r.t TCString returned by TCString in the response to a request made by a TP which was informed of the correct (TCString returned by `__tcfapi`) in previous requests.
1st-party	deadline.com	Old, non-updated (after acceptance) consent is shared via network requests even after revocation.
3rd-party (kinja-static.com)	kotaku.com	Third-party script was loaded after the consent was updated (from the previous stages, both in case of after acceptance and revocation), but it still used the wrong consent.
3rd-party (CMP) InMobi PTE Ltd	manchester-eveningnews.co.uk, walesonline.co.uk	Although all the requests sent an updated consent after revocation, signal-beacon.s-onetag.com/beacon.min.js script continues to send the positive consent (old consent-after acceptance)

Table 8: Inconsistencies in consent strings shared over the network

Purpose	Name	Repeated from v2.0	Requires Consent
1	Store and/or access information on a device	= 1	✓
2	Use limited data to select advertising	Looks new but related to no. 2 = "Select basic ads"	✓
3	Create profiles for personalised advertising	= 3	✓
4	Use profiles to select personalised advertising	= 4	✓
5	Create profiles to personalise content	= 5	(✓) Not clear: in principle, this purpose can be legitimized under a legitimate interest, but it would fail the this test.
6	Use profiles to select personalised content	= 6	(✓) Not clear: in principle, this purpose can be legitimized under a legitimate interest, but it would fail the legitimate interest test.
7	Measure advertising performance	= 7	✓
8	Measure content performance	= 8	✓
9	Understand audiences through statistics or combinations of data from different sources	New language but looks like the former purpose no. 9, "Apply market research to generate audience insights"	✓
10	Develop and improve services	= 10	It is not specific, and so we cannot derive its legal basis. X but in principle it could rely on LI though it could fail the LI test
11	Use limited data to select content	New	X

Table 9: IAB TCF purposes in v2.2 in the TCString and the applicable legal basis. The "Requires Consent" column sums up our analysis. The "Repeated from v2.0." column compares the purposes of versions v2.0 and v2.2. We add parentheses if exceptions occur. You can find the descriptions of all the purposes in the supplementary material [1].

categorizing each of the 158 websites based on three attributes: functional category, country of origin, and owning organization. This classification enabled a deeper understanding of how compliance varies not just across sectors but also geographically and

		Within the Same Interface				Via Different Interfaces					No Revocation
Banner	**No. of Websites**	**Icon or Button (0 Steps)**	**Footer Options (1 Step)**	**Banner on Policy (1 step)**	**Options through Policy Page (≥ 2 steps)**	**Browser set., 3rd-party links**	**After Login**	**Contact/ Email**	**Paywalls**	**Option mentioned but doesn't work**	**No revocation**
Consent Banner	54	4	27	3	18	2	0	0	0	0	0
No Option Banner	8	0	0	0	5	2	1	0	0	0	0
No Banner	43	0	2	5	7	17	0	3	0	0	4 [+5]
Total	105	4	29	8	30	21	1	3	0	0	9

Table 10: Prevalence and type of consent revocation options on 105 websites (rank 1-200) *without* detected CMPs

		Within the Same Interface				Via Different Interfaces					No Revocation
Banner	**No. of Websites**	**Icon or Button (0 Steps)**	**Footer Options (1 Step)**	**Banner on Policy (1 step)**	**Options through Policy Page (≥ 2 steps)**	**Browser set., 3rd-party links**	**After Login**	**Contact/ Email**	**Paywalls**	**Option mentioned but doesn't work**	**No revocation**
Consent Banner	54	5	36	3	3	6	1	0	0	0	0
No Option Banner	0	0	0	0	5	2	1	0	0	0	0
No Banner	2	0	0	0	0	0	0	0	0	0	0
Total	56	5	38	3	3	6	1	0	0	0	0

Table 11: Prevalence and type of consent revocation options on 56 websites (rank 1-200) *with* detected CMPs

institutionally. We found that 49% of websites showed potential violations related to consent interfaces, while 66% had potential violations related to cookie practices, discussed in Sections 5 and 6 respectively. A total of 114 of the 158 had either or both of these violations.

Category-based patterns. The analysis revealed that among more represented categories, Non-profit organizations had the highest violation rate at 92.9%, followed by News & Media (84.2%) and Business Services (83.3%). Even traditionally well-regulated sectors such as Government (80.0%) and Education (66.7%) showed high non-compliance. The Technology category, which constituted the largest share of the dataset (60 websites), exhibited a violation rate of 63.3%, highlighting widespread issues even among digital services. Blog/Personal, Health & Medical, and Sports categories each had only one website represented, and all of them exhibited violations.

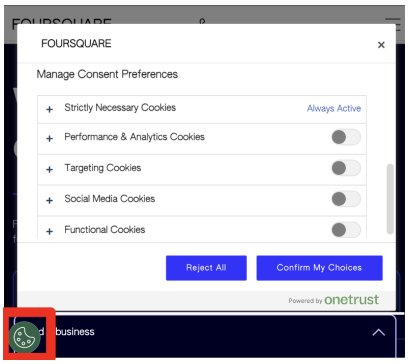
		Within the Same Interface				Via Different Interfaces					No Revocation
Banner	**No. of Websites**	**Icon or Button (0 Steps)**	**Footer Options (1 Step)**	**Banner on Policy (1 step)**	**Options through Policy Page (≥ 2 steps)**	**Browser set., 3rd-party links**	**After Login**	**Contact/ Email**	**Paywalls**	**Option mentioned but doesn't work**	**No revocation**
Consent Banner	214	33	125	0	26	9	0	3	11	3	7
No Option Banner	0	0	0	0	0	0	0	0	0	0	0
No Banner	11	0	8	0	0	1	0	0	0	0	2
Total	225	33	133	0	26	10	0	3	11	3	9

Table 12: Prevalence and type of consent revocation options on 200 to 5000 ranked websites *with* detected CMPs

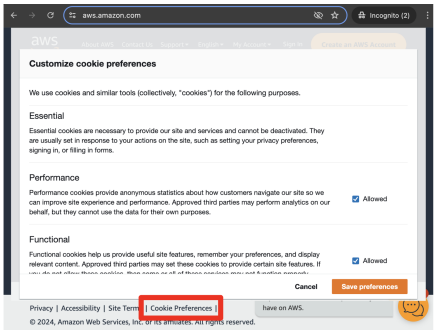
Country-based analysis. The analysis identified the United States as the most represented and highest-risk country, with 113 websites and a violation rate of 77%. Great Britain followed with an 83.3% violation rate across 6 websites, and the EU, though only represented by 2 sites, showed a 100% violation rate. "Not Found" entries—websites with indeterminate location—had a significant presence (31 sites, 61.3% violation rate).

Organization-level analysis. We found widespread non-compliance among both major tech companies and less identifiable entities. Google LLC had the highest number of violations (11 out of 11 sites), with other large organizations such as Apple Inc., Amazon.com, Inc., Twitter, and Twitch also having a violation in each website within these 158 websites.

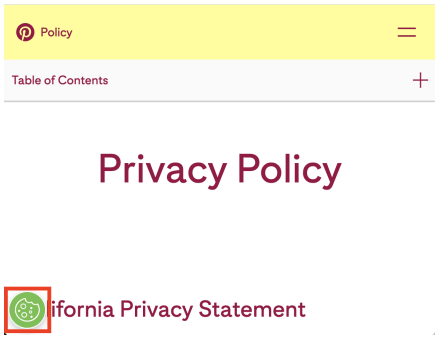
The "Not Found" group—websites with unidentified ownership had 67% of websites having a violation. Microsoft Corporation and Automattic, Inc. showed partial compliance having 5 out of the 10 websites having a violation. These results highlight that privacy violations are not limited to fringe actors but are prevalent even among high-profile and widely-used platforms.



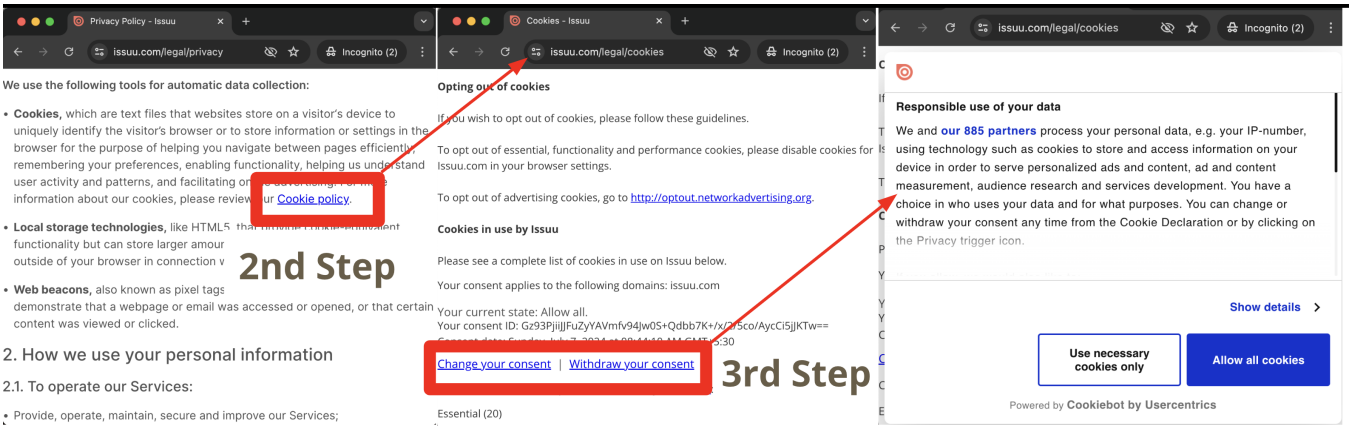
(a) Persistent icon on foursquare.com



(b) Footer options on aws.com

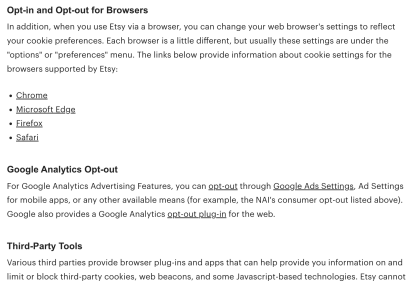


(c) Banner on the policy page on pinterest.com

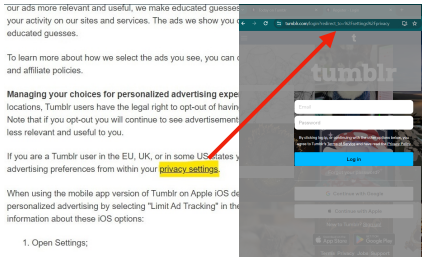


(d) Options on other pages on issuu.com

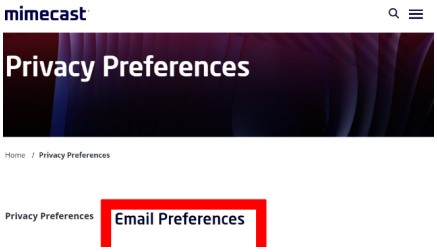
Figure 6: Revocation options within the interface on websites. (Screenshots collected between March and June 2024)



(a) Browser settings or 3rd-party links on etsy.com



(b) Consent options after login on tumblr.com



(c) Contact/Email on mimecast.com

Figure 7: Websites with revocation options via different interfaces or no revocation options (Screenshots collected between March and June 2024)