Measuring Compliance of Consent Revocation on the Web

Gayatri Priyadarsini Kancherla
IIT Gandhinagar, India
gayatripriyadarsini@iitgn.ac.in

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

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

Abhishek Bichhawat
IIT Gandhinagar, India
abhishek.b@iitgn.ac.in

The General Data Protection Regulation (GDPR) and the ePrivacy Directive (ePD) set out the requirements for obtaining a valid consent when tracking technologies are used on a website. While numerous studies assessed the compliance of consent, one key aspect has been largely overlooked by the research community: **consent revocation**. According to the GDPR (Art. 7(3), Rec. 42), users have the right to withdraw their consent at any time. Consequently, websites are required to offer a straightforward way to revoke consent. However, it remains unclear whether websites actually provide users with compliant methods to revoke their consent, whether revoked consent is properly recorded, and whether this decision is effectively communicated to third-parties that previously collected the user's data.

We analysed **consent revocation mechanisms and its compliance on 200 most popular websites**. Our legal-empirical research paper identifies multiple violations reported below:

- 49% of websites offer non-compliant revocation interfaces,
- 66% fail to store or communicate consent revocation correctly,
- 57% of websites continue to store tracking cookies after consent has been revoked.

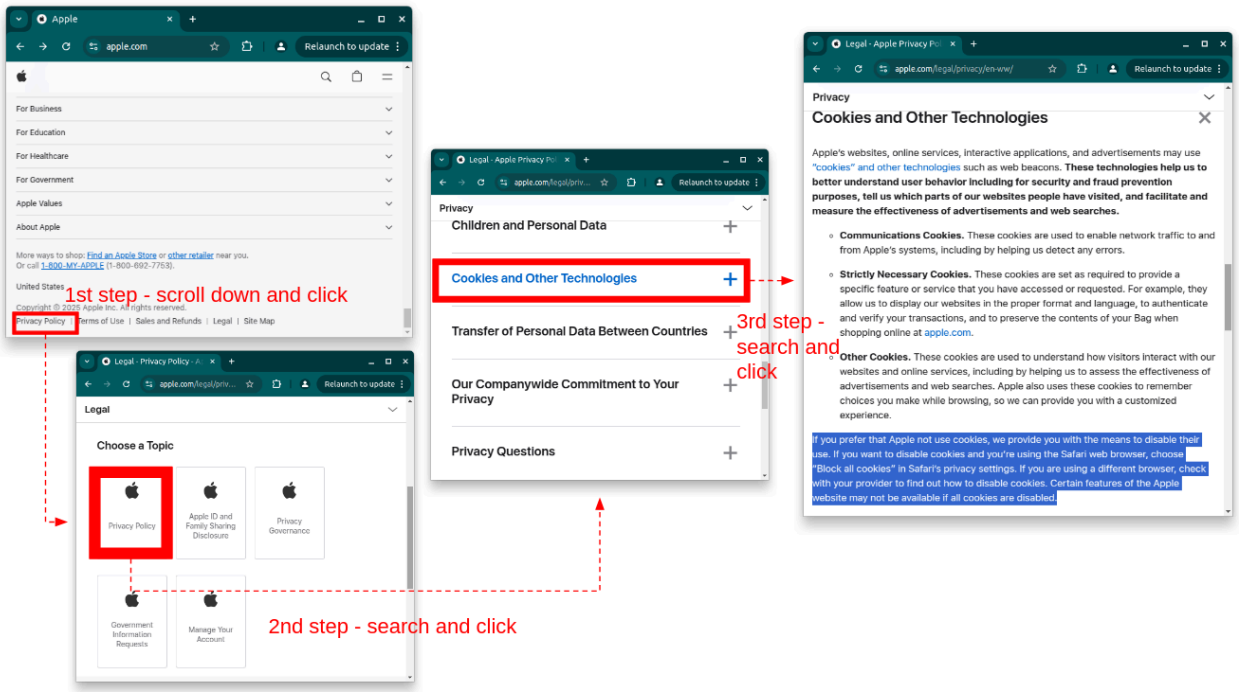
This academic paper is accepted for publication at the top-tier international computer science conference Privacy Enhancing Technologies (PETS 2025), and is going to be presented in Washington DC, USA in 14-19 July 2025.

49% websites offer non-compliant revocation interfaces

By analysing the revocation interface, we have found that only 51% (82 of 158 websites) provide a compliant solution for consent revocation: persistent icon floating on the page or a link option in the footer of the page. On the remaining 49% of websites, revocation mechanism is absent (6%), different and more complex than the initial consent interface (20%) or requires more than 2 user actions to revoke versus 1 action to accept consent (22%), all detailed below.

1. Different interface to revoke consent

⚖️ **Legal requirement:** Revoking consent must be as easy as giving it and accessible through the *same interface.* Users shouldn't have to search throughout privacy policies, send emails, or visit external sites to revoke consent. Such complex interfaces are considered non-compliant.

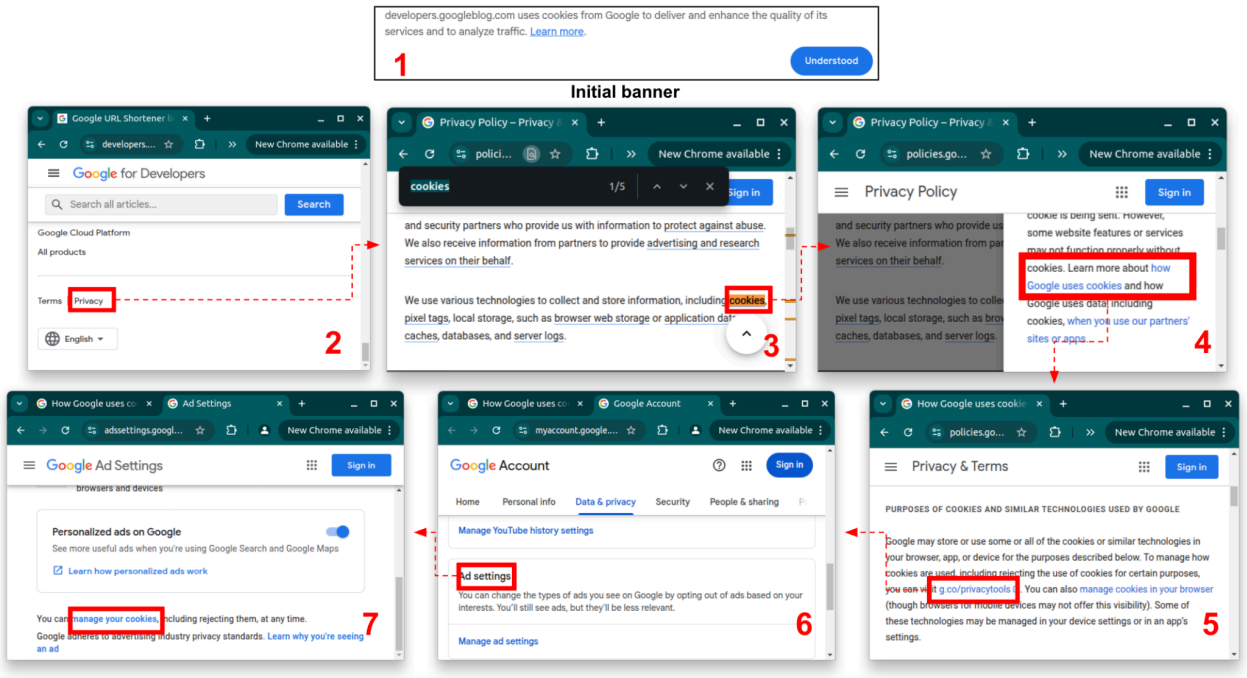


Consent revocation on https://apple.com, accessed on 20th May 2025. The user can only revoke consent by visiting a privacy policy page and searching for "cookie", where the only available options are to delete cookies from the browser settings to revoke consent.

📊 **Results:** 20% websites (32 out of 158) provide consent revocation through interfaces that differ from the initial consent banner. This practice increases the burden on users, who must spend additional effort to understand and navigate these different interfaces. We observed revocation options that require users to delete cookies from the browser settings, contact website owners via email, or redirect the user to third-party platforms, such as youronlinechoices.eu or aboutads.info. One website, tumblr.com, even required users to log in before they could revoke their consent. These violations are found on popular websites such as apple.com, wordpress.org, medium.com, and discord.com.

2. More effort to revoke consent than to give consent

⚖️ **Legal requirement:** Revoking consent must be as easy as giving it, which means it should entail the *same level of effort*. The number of steps and actions, like clicks or gestures for revoking consent must match those used to grant consent. Any other more complex mechanism is considered potentially non-compliant.



Consent revocation on http://goo.gl, accessed on 20th May 2025. The user can only revoke consent by visiting a privacy policy page and searching for "cookies" (Step 3), to further look for an option to revoke consent. In Step 7, the user finally reaches the link to open a banner.

📊 **Results:** 22% websites (35 out of 158) allow to revoke consent using the same interface used to collect consent. However, while the consent banner to grant permission appears immediately upon visiting the site, revoking consent typically requires navigating through t*wo or more steps* to access the revocation interface. These violations are found on popular websites of big tech such as goog.gl, twitter.com, google.com and tiktok.com.

3. Absence of a revocation mechanism

⚖️ **Legal requirement:** Users have the right to revoke their consent at any time. This means websites must make it easy for users to revoke consent by providing a clear, visible, and accessible way to do so. If a website doesn't offer this right though a visible accessible mechanism, or hides it in a way that makes it hard to find it, then consent becomes invalid. As a result, any personal data the website continues to process without consent violates the GDPR lawfulness principle.

📊 **Results:** 6% websites (9 out of 158) did not provide any means to revoke consent, and 4 of them had advertising and analytics cookies that require consent. These violations are found on popular websites such as un.org (United Nations), vk.com (Russian Social network) and weibo.com (Chinese Social network).

66% of websites fail to store or communicate consent revocation

By analysing storage and communication of consent revocation behind the interface, we have found two main types of violations: on 25% of websites (47 out of 191) there was *inconsistency in registering the revoked consent*. Additionally, 74% of websites (100 out of 136) communicated consent acceptance to third-parties but *did not communicate consent revocation to all of them*.

1. Incorrect registration of consent revocation

⚖️ **Legal requirement:** Websites are required to record user's decision when they revoke consent. This means that whatever choice the user makes in the consent revocation interface, it should be recorded accordingly by the website and stored in the browser. If a website stores a different choice (for example, storing “accept” when the user clicked “reject”), that is a violation of data protection rules.

We analysed consent stored in the browser or accessed it through specific APIs, using our interpretation of both positive[1] consent (when user accepts all) and negative consent (when user rejects all), to verify whether websites store and communicate the user’s choice correctly.

📊**Results:** 12.5% websites (17 out of 136) using CMPs that implement IAB Europe Transparency and Consent Framework, and 14.5% websites (22 out of 152) using OneTrust CMP *store a positive consent even after the user revoked consent*.
We explored the reason for such violation and found that many websites simply *do not update their consent storage when the user revokes consent:* 9.3% websites (15 out of 136) using IAB TCF-based CMPs and 10.5% websites (16 out of 152) using OneTrust CMP.
These violations are found on popular websites such as msn.com, cisco.com, and forbes.com.

[1] Positive (“accept all”) consent**:** if the observed IAB TCF TCString contains at least one of the purposes 2-9, and at least one vendor present in the vendor list of TCString, we consider it to contain a positive consent. Such consent is correct only when the user actively selects such purposes or clicks the “accept all” button, since these purposes require user explicit consent.
Negative (“reject all”) 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 visit to the website, after the user clicks “reject all” or after revoking consent, we consider consent to be registered correctly.
OneTrust-specific consent: OneTrust CMP has its own format for storing consent, in a specific OTAG variable accessible via JavaScript, or in a specific “OptanonConsent” cookie, where purposes are encoded within those elements, as per OneTrust specification. Since OneTrust does not provide an explicit specification for the meaning of these purposes, we cannot analyse which ones require consent. We therefore assume that a OneTrust consent string (OTAG variable or OptanonConsent cookie) contains a negative consent if it matches the value observed upon the initial visit to the website, and a positive consent if the value contains more purposes than at the initial visit.

2. Not communicating consent revocation to all third-parties

⚖️ **Legal requirement:** When a user revokes consent, the website must communicate this decision to all third parties with whom the data was shared. While regulators haven't provided guidance on *how to notify third parties*, failing to inform these third parties constitutes a violation of data protection law.

Third parties can get informed of the status of user consent via two mechanisms: either they use APIs provided by the CMPs within the browser to access consent decisions, or they can be informed via HTTP requests with consent decisions sent to such third party servers.

📊 **Results:** We found that many third parties are not informed when users revoke consent. On 9.6% of websites (23 out of 238), at least one third party that actively used the API to retrieve positive consent after user acceptance, *did not use the API again to get informed about the user's consent revocation.* Additionally, on 74% of websites (101 out of 136), at least one third party that received consent through an HTTP request after acceptance, *did not receive the information about consent revocation*[2]. These violations are found on popular websites such as cnn.com, wsj.com, and bbc.com.

57% websites continue to store advertising and analytics cookies even after consent has been revoked

⚖️ **Legal requirement:** Any organization that collected or received data based on consent must *stop processing* it upon receiving a revocation request. Unless another valid legal basis exists, all data obtained through consent must be *deleted*, even if the user does not request its deletion.

📊 **Results:** 57% of websites (69 out of 120) failed to delete analytics and advertising cookies after the user revoked consent. These violations are found on popular websites such as microsoft.com, twitter.com, amazon.com, youtu.be and linkedin.com.

[2] On websites that allow revoking consent, we found that third parties often received consent information (like TCStrings of IAB TCF or OneTrust-specific consent records) in outgoing HTTP requests (in URLs or request data).