Pragmatic Cybersecurity
https://www.sciltp.com/journals/pc

Article

Global Web, Local Privacy? An International Review of Web Tracking

Harry Yu [1,†,‡], Patton Yin [2,†,‡] and Sebastian Zimmeck [3,*]

[1] Department of Computer Science, Carnegie Mellon University, Pittsburgh, PA 15213, USA
[2] Department of Computer Science, Brown University, Providence, RI 02912, USA
[3] Department of Mathematics and Computer Science, Wesleyan University, Middletown, CT 06459, USA
* Correspondence: szimmeck@wesleyan.edu
† These authors contributed equally to this work.
‡ They performed their work during their studies at Wesleyan University.

How To Cite: Yu, H.; Yin, P.; Zimmeck, S. Global Web, Local Privacy? An International Review of Web Tracking. *Pragmatic Cybersecurity* **2026**, *1*(1), 5.

Received: 31 December 2025
Revised: 11 March 2026
Accepted: 17 March 2026
Published: 24 March 2026

Abstract: Web tracking by ad networks, social networks, and other third parties is privacy-invasive. To protect users' privacy, an increasing number of countries are adopting new privacy laws. However, a major reason why their application on the web is so challenging is that privacy laws are local while the web is global. To that end, we evaluate websites' tracker connections for ten countries for two sets of sites—the global Common Top 525 and the Country-specific Top 525 sites. We find that Australia and the US (California)—two of the three opt-out jurisdictions in our study—have the highest level of web tracking while opt-in jurisdictions generally have lower levels. We also find that the Common Top 525 sites have 50.5% fewer average tracker connections when accessed from EU countries compared to non-EU countries. Further, simply not interacting with cookie banners decreases trackers by 48.5% for Germany, as measured for a sample of 36 Common Top 525 sites. These results suggest that the General Data Protection Regulation and the ePrivacy Directive have a tangible effect in reducing tracking. As 28% of Common Top 525 sites show cookie banners in all ten countries, our results suggest a moderate Brussels effect. However, against the backdrop of global US ad tech practices, EU law primarily acts as a Brussels shield. Generally, we think that strong enforcement of privacy laws is key to increase user privacy on the web.

Keywords: web privacy; web tracking; cookie consent; cookie banner; web measurement; privacy law; GDPR; eprivacy directive; brussels effect

1. Introduction

The most common business model for the web is "content for data." In exchange for access to news, videos, games, and other online content, users pay with their data. Ad networks and other third parties integrated on websites track users' online activities—for example, what they like, what they purchase, or where they are located—to create user profiles, deliver targeted ads, and personalize their web experience [1]. HTTP cookies, for example, used in combination with invisible tracking pixels, are some of the most common tracking mechanisms. Their use for tracking has long been recognized as privacy-invasive, and increasingly lawmakers and regulators aim to curb the harm of web tracking with privacy laws [2] (for simplicity we refer to "privacy laws" in this study to cover both "privacy laws," such as the California Consumer Privacy Act (CCPA), and "data protection laws," such as the General Data Protection Regulation (GDPR). Similarly, we use other broad terms to cover technical terms under specific laws, e.g., "user" covers 'consumer" under the CCPA and "data subject" under the GDPR). Over the past decade lawmaking activity has picked up substantially. An increasing number of countries enacted comprehensive privacy laws that establish which personal data website operators and third parties can collect and under which conditions and with whom they can share it. Once these new laws are in place, regulators are being tasked with enforcing them. Despite this lawmaking activity, questions remain how effective privacy laws are in practice.

In order to protect users from privacy-invasive tracking on websites, two common approaches are: (1) prohibiting tracking by default, while allowing users to opt in and (2) allowing tracking by default and giving user a right to opt out. The EU's GDPR [3] and ePrivacy Directive [4] are based on the former and so is Brazil's Lei Geral de Proteção de Dados (LGPD) [5] as well as South Korea's Personal Information Protection Act (PIPA) [6], among others. In contrast, opt-out laws—most notably the CCPA and other state privacy laws in the US [7]—allow tracking by default, thus, requiring users to take action if they wish to restrict tracking. As long as users in opt-in jurisdictions do not opt in, they should be tracked less than users in opt-out jurisdictions. However, they may be subjected to a deluge of cookie banners and experience consent fatigue [8].

A major reason why the application of privacy laws on the web is so challenging is that privacy laws are local while the web is global. Different countries and regions have different privacy laws, and many have none. Different countries are also at different stages in their evolution of privacy lawmaking and enforcement. Some laws may also create spillover effects impacting regions beyond their territorial scope, for example, as website operators may decide to simplify their compliance by adhering to the strictest law that applies to their site. One notable example is the Brussels effect [9]. Overall, web users' levels of privacy can differ depending on geographic locations. Thus, we are evaluating trackers across regions to understand how different privacy laws shape tracking and consent practices locally and globally.

1.1. Research Questions

With this study we are addressing the following research questions:

RQ1. Sites Across Countries : How do users' geographic locations in different countries impact their tracker exposure?
RQ2. Global vs. Local Sites: Do globally popular sites have different tracking practices than locally popular sites?
RQ3. Potential Privacy Law Impact: How are sites' tracking and consent practices shaped by privacy laws across countries?

1.2. General Approach

We address our research questions by measuring and evaluating the tracker connections of websites in ten countries: Australia, Brazil, Canada, Germany, India, Singapore, South Africa, South Korea, Spain, and the US. The ten countries cover all continents except Antarctica. For each country, we evaluate two sets of sites: the Common Top 525 sites—a set of globally popular sites—and the Country-specific Top 525 sites—a set of popular sites in each of the evaluated countries. Website operators can ensure compliance with three primary methods: (1) not issuing tracking requests, (2) blocking data collection until obtaining user consent, or (3) allowing data collection accompanied by an indicator of the user's consent status. We focus here on the first method because it is directly observable and comparable across all site visits without requiring site-specific interactions or assumptions about third party behavior. While sites might connect to third parties and rely on them to discard data server-side, the absence of a connection guarantees that no data was shared.

1.3. Contributions

In the following, we will begin our inquiry with a discussion of related work (Section 2). Based on the synthesis of applicable privacy laws (Section 3), we then perform a privacy evaluation of websites' tracker connections in ten different countries (Sections 4 and 5) that we contextualize for the broader web ecosystem to improve its overall privacy (Section 6) (The code of our web crawler and data related to this study is publicly available under the MIT License [10]).

2. Related Work

We see our study as a contribution to the field of web privacy, especially to measurement studies with multi-country scope that evaluate the influence of the GDPR and other privacy laws on cookie consent, compliance, and how users exercise their privacy rights.

2.1. Web Privacy Measurement

Various studies have shown how third-party trackers use cookies, browser fingerprinting, and other privacy-invasive technologies to follow users in their browsing sessions across sites [11–13]. An early study in 2012 showed that most commercial sites implemented trackers by multiple parties, with some capturing over 20% of a user's browsing behavior [14]. A longitudinal study showed that from 1996 to 2016, web tracking grew in prevalence and complexity [15]. This research has been enabled by measurement platforms like FourthParty [16] and OpenWPM [12] as well as browser extensions like Disconnect [17] and Privacy Pioneer [18], the latter of which we use here as well. As privacy law-making activity picked up substantially in the late 2010s various studies aimed to quantify the impact of the GDPR and other privacy laws on web tracking. Longitudinal studies comparing sites' privacy practices before and after the time the GDPR went into effect showed an increase in cookie consent notices [19] as well as a decline in the number of third parties belonging to certain categories, though, it remained unclear whether the latter was attributable to the GDPR [20].

2.2. Impact of the GDPR and ePrivacy Directive

The GDPR aims to improve data protection online, which leads to a direct conflict with the online ad industry's real-time bidding infrastructure for ads personalization [21]. In some areas the law's impact has improved data protection on the web while in others its full impact has yet to be realized. Studies have shown that after the GDPR's enforcement, sites embedded fewer trackers [22] and reduced connections to web technology providers, which was also the case for sites intended for non-EU audiences [23]. The number of ID syncing connections also decreased, reducing information sharing between third parties [24]. However, the overall structure of the tracking ecosystem remains largely unaffected, and the GDPR may have inadvertently increased market concentration in the online ad industry, with fewer, larger companies dominating web tracking [23,24]. An early study covering the Netherlands' implementation of the ePrivacy Directive into national law concluded that it did not result in meaningful choice for users but instead caused widespread deployment of annoying banners, pop-up screens, and cookie walls [25].

Beyond the EU, the introduction of the GDPR has increased friction between jurisdictions, which is most evident in transatlantic data flows. The 2020 Schrems II ruling by the Court of Justice of the European Union [26], which invalidated the EU-US Privacy Shield, concluded that US law does not provide "essentially equivalent" protection for EU residents' data, thereby complicating third-party tracking that relies on US-based servers [27]. Despite these hurdles, the GDPR often functions as a global de facto standard as multinational companies often apply EU-level protections across their global operations to minimize technical and legal fragmentation [28]. However, work comparing EU and US cookie behavior suggests that while persistent tracking has decreased in the EU, US-based sites continue to maintain significantly higher tracking densities due to the permissive opt-out nature of US privacy laws [29].

2.3. Cookie Consent, Compliance, and Opting Out

A large body of research demonstrates widespread non-compliance with the consent requirements of the ePrivacy Directive and GDPR. Studies have consistently found that sites install tracking cookies before receiving user consent [30]. Even when consent is sought, the mechanisms are often flawed. Sites deploy consent banners with deceptive designs that nudge users towards acceptance or assume consent from inaction [31]. Many sites continue to collect data even when users explicitly reject consent [32,33]. The rise of the "consent ecosystem", dominated by a few Consent Management Platforms (CMPs), has led to standardized but often confusing and unusable consent dialogs that encourage users to "Accept All" [34,35], have no reject option [36], or include dark patterns and implied consent features [36,37]. Users also often experience consent fatigue [8]. The automation of rejecting consent can help to tip the scale towards user privacy [38]. Privacy preference signals, such as Global Privacy Control (GPC) [39,40], can mitigate this impact [41], however, have yet to be adopted broadly. Furthermore, it is a fundamental design flaw of the online ad ecosystem that it is built on the notion that sites make normal ad calls to third parties, append opt-out flags, for example of the Transparency Consent Framework [42], and leave it to the downstream third parties to respect the opt-outs by discarding the received user data [43].

2.4. Multi-country Privacy Law Comparisons

Previous studies highlight significant differences in privacy practices across jurisdictions. A key finding is that cookie behavior, cookie consent violation rates, and cookie banner implementations are highly dependent on region [44]. Sites employ fewer cookies for EU visitors compared to US visitors [29]. While the Brussels effect has been observed, i.e., EU standards being applied to sites' US visitors [29], the impact of EU law on the operations of US online services is limited [45]. Cookie banner existence even decreased when accessing European websites from the US [46]. Even within the EU, the transition to the GDPR saw inconsistent adoption of functional and usable consent mechanisms across member states [19]. Sites appear to follow notice requirements based on their expected audience, as identified by their country code top-level domain, and not individual user location, except for `.com` sites [47]. These implementation differences are mirrored by cultural variations that influence privacy concerns and the application of legal principles like transparency across borders [48–51]. To overcome the challenges of privacy self-management researchers have called for the study of alternative approaches [52]. In particular, laws can introduce structural measures that would relieve individuals from unrealistic privacy self-management expectations [53].

3. Privacy Laws and their Enforcement

We study websites in ten countries: Australia, Brazil, Canada, Germany, India, Singapore, South Africa, South Korea, Spain, and the US (California). The territorial scope of the privacy laws in these countries, whether they require opt-in or opt-out consent, and their enforcement determine their applicability and impact.

3.1. Territorial Scope

Typically, website operators and third parties are subject to the privacy laws of their jurisdiction. However, many laws also have extraterritorial application. For example, the GDPR not only applies to controllers and processors established in the EU but also to those outside it if they offer goods or services to, or monitor the behavior of, data subjects within the EU (GDPR, Article 3(2)). Similarly, the ePrivacy Directive applies to the processing of personal data in public communications networks in the European Community, i.e., EU, regardless of who does the processing (ePrivacy Directive, Article 3(1)). In the US, the CCPA applies to any for-profit entity that does business in the State of California and that has annual gross revenues in excess of twenty-five million dollars, annually buys, sells, or shares the personal information of 100,000 or more consumers or households, or derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information (CCPA, Section 1798.140(d)(1)). Generally, all privacy laws in our study protect users within their jurisdiction regardless of where the data processing takes place (See the Australian Privacy Act 1988, Article 5B (1A) and (3), Brazil's LGPD, Article 3, India's Digital Personal Data Protection (DPDP) Act, 2023, Article 3, and South Africa's Protection of Personal Information Act (POPIA), Section 3. While Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) is silent on the matter, courts interpret the law to apply where there is a "real and substantial link" to Canada [54]. Similar guidance is provided by governmental regulators in Singapore [55] and South Korea [56]). We ensure applicability of a jurisdiction's privacy law by accessing sites from a Virtual Machine (VM) server located inside it.

3.2. Consent Type

Most privacy laws require user consent for web tracking; many in form of opt-in consent and some in form of opt-out consent. Opt-in laws require website operators to obtain consent from users before collecting any personal data or sharing it with third parties, such as in the case of non-essential cookies for advertising or analytics. Users in opt-out jurisdictions, on the other hand, can be tracked until they exercise their right to opt out. Thus, without any user interaction we expect lower levels of tracking in opt-in jurisdictions (by "opt-in jurisdiction" and "opt-out jurisdiction" we refer to the type of *consent* a user is required to give. We do not mean to refer to other legal bases for personal data processing, for example, legitimate interest per GDPR, Article 6(1)(f). Under EU law we focus here on consent because the Court of Justice of the European Union held that a user "cannot reasonably expect that the operator [...] will process that user's personal data, without his or her *consent*, for the purposes of personalised advertising" (emphasis added) [57]. Furthermore, the ePrivacy Directive's requirement for prior consent per Article 5(3) applies to the access of information on a user-s device—a technical prerequisite for web tracking—thereby requiring an opt-in consent before any data collection can occur [58,59]).

3.2.1. Opt-In Jurisdictions

Germany, Spain, Brazil, India, South Korea, Singapore, and South Africa are opt-in jurisdictions. For Germany and Spain, the ePrivacy Directive requires consent as the legal basis for all cookies that are not strictly necessary for the operation of a website (ePrivacy Directive, Article 5(3)). Access to user information is only allowed on the condition that the user is provided with clear and comprehensive information about the purposes of the processing and is offered the right to refuse such processing. The Court of Justice of the European Union further specified the law in its Planet49 decision reasoning that pre-checked boxes are insufficient and that users must be notified how long cookies will be stored on their devices and whether or not third parties may have access to those [58].

For Brazil the LGPD enumerates the legal bases for processing personal data in Article 7 and requires user consent as the default basis for processing personal data via tracking cookies. Brazil's National Data Protection Authority published guidance against using cookie banners with pre-selected authorization options or the adoption of tacit consent mechanisms, such that by continuing to browse a site a user is assumed to give consent [60]. This is also true for India, whose DPDP Act, 2023 requires consent to be "unambiguous with a clear affirmative action" (DPDP Act, 2023, Article 6(1)). Similarly, opt-in consent is required per Article 22(1)(No.7) of South Korea's PIPA as well as per regulatory guidance in Singapore [61] and South Africa [62].

3.2.2. Opt-Out Jurisdictions

Australia, Canada, and the US (California) are opt-out jurisdictions. The Office of the Australian Information Commissioner issued guidance on the use of tracking pixels according to which organizations should enable users to opt-out of receiving targeted online ads using tracking pixels, for example, by deploying a banner or pop-up when a user first visits a site [63]. Similarly, the Privacy Commissioner of Canada issued guidance on the use of opt-out consent for online behavioral advertising requiring that users are notified and no sensitive information is involved [64]. In the US the CCPA operates on an opt-out basis for the selling and sharing of personal information, the latter of which includes communicating a consumer's personal information to a third party for cross-context behavioral advertising (CCPA, Section 1798.140(ah)(1)). Websites must provide a "Do Not Sell or Share My Personal Information" link and honor GPC opt-out preference signals [65].

3.3. Privacy Law Enforcement

For enforcing users' privacy rights, especially, consent choices, we distinguish jurisdictions with high, medium, and low enforcement activity (Table 1).

Table 1. Germany and Spain are the only countries in our study with high enforcement activity.

Country	**Consent Type**	**Enforcement**	**Major Enforcement Actions**	**Primary Privacy Law**
Germany & Spain	Opt-in	High	EU-wide 833 fines for insufficient legal basis for data processing (€3,011,611,435)	GDPR, ePrivacy Directive
Australia	Opt-out	Medium	Meta Cambridge Analytica settlement ($50,000,000)	Privacy Act 1988
Canada	Opt-out	Medium	Meta Cambridge Analytica investigation	PIPEDA
South Korea	Opt-in	Medium	Meta investigation (approximately $15,000,000)	PIPA
US (California)	Opt-out	Medium	Individual enforcement actions by the California Attorney General and the CPPA	CCPA
Brazil	Opt-in	Low	Sanctions mostly for data breaches, not tracking	LGPD
India	Opt-in	Low	No major enforcement actions	DPDP Act, 2023
Singapore	Opt-in	Low	No major enforcement actions	PDPA
South Africa	Opt-in	Low	No major enforcement actions	POPIA

3.3.1. High Enforcement Activity

Germany and Spain, which represent the EU jurisdictions in our study, are high enforcement jurisdictions. They have a strong and active regulatory environment related to tracking and user consent. Especially, Germany has a long privacy law and enforcement tradition dating back to the 1970s. The German Data Protection Authorities are among the most active in the EU and enforce privacy laws broadly. For example, in a recent case brought by the Data Protection Authority of Lower Saxony against a web publisher the Administrative Court Hannover decided that the use of the options "Accept all", "Accept & close x", and "Settings" is insufficient for valid consent and that the use of Google Tag Manager requires consent [66]. The Spanish Data Protection Authority is also very active and recently fined the automotive company SEAT for placing non-technical cookies without user consent and failing to stop such placement after consent withdrawal [67]. As of March 2026, the EU has issued a total of 833 fines against companies on the ground of insufficient legal basis for data processing for a total of €3,011,611,435 [68].

3.3.2. Medium Enforcement Activity

Australia, Canada, South Korea, and the US (California), also have engaged in enforcing applicable privacy laws. However, their enforcement activities are generally not broad-based but instead focused on individual high-profile cases. We categorize them as medium enforcement jurisdictions. The Office of the Australian Information Commissioner issued guidance on the use of tracking pixels [63] and settled a civil case with Meta on the sharing of user data with Cambridge Analytica for $50,000,000 [69]. The Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia also investigated Meta and found various consent shortcomings as well as a failure to safeguard users' personal data [70]. South Korea's Personal Information Protection Commission found similar consent violations for Meta [71]. Under the CCPA the California Attorney General most recently brought a case against Disney for not properly opting out users, including via GPC, resulting in a $2,750,000 settlement [72]. Similar major actions involved Healthline [73] and Sephora [74]. Together with the Colorado and Connecticut Attorneys General the California Attorney General recently conducted a privacy enforcement sweep [75]. The new California Privacy Protection Agency (CPPA) also recently brought its first major enforcement actions against PlayOn Sports and Ford for not letting users opt out from tracking and adding unnecessary friction to the opt-out process, respectively [76,77].

3.3.3. Low Enforcement Activity

Brazil, India, Singapore, and South Africa are low enforcement jurisdictions. These countries are either at the beginning of their privacy lawmaking and enforcement activities (Brazil and India) or have not engaged much in enforcement despite their privacy laws being effective for more than a decade (Singapore and South Africa). Brazil's LGPD is closely modeled after the GDPR. However, the National Data Protection Authority is still in the early stages of its enforcement activities. While it has started issuing sanctions, those focus on foundational issues, such as responding to data breaches, rather than violations of user consent choices on websites [78]. It is noteworthy that the first violations came, for the most part, from the public sector [78]. India's DPDP Act, 2023 is even more recent than that of Brazil and enforcement has yet to begin. Both Singapore's PDPA and South Africa's POPIA date back more than a decade and have not been strongly enforced as to users' privacy rights and consent choices.

4. Methodology

We conducted a country-localized web crawl using ten identically provisioned VM servers, one per country, to visit for each country the Common Top 525 and Country-specific Top 525 sites, derived from the Tranco list [79] (We used the Tranco list version of 27 November 2023, available at https://tranco-list.eu/list/Q9Z84).

4.1. Common and Country-Specific Top 525 Sites

1. Common Top 525 Sites: This list contains the 525 most popular sites taken directly from the Tranco list. All 525 sites have a `.com` top level domain.
2. Country-specific Top 525 Sites: To identify the most popular sites in a country we used sites' country code top-level domains. For example, we classified a site with `.de` domain as a German site.

We chose not to create a separate Country-specific Top 525 list for the US because a substantial portion of the Common Top 525 sites are already US-based. In addition, most US sites commonly use the `.com` top-level domain instead of the country-specific `.us` top-level domain, which, thus, would not accurately reflect the most popular sites in the US. When preparing the crawl list for each country we started top-down in the Tranco list and manually loaded each site to ensure its availability or redirection to a loading site. If a site failed to load, the browser returned an error page, or required human verification, we did not include the site and evaluated the next one until we arrived at 525 sites for a list. We chose this number of sites to crawl to ensure a statistically meaningful sample for each country given that some sites' analyses may fail. In total, we prepared nine Country-specific Top 525 site lists and one Common Top 525 site list that doubles as Country-specific Top 525 list for the US. Thus, our study covers $9 \times 1,050 + 525 = 9975$ sites across ten countries, corresponding to $525 \times 9 + 525 = 5250$ unique sites.

4.2. VM Server Locations

To ensure that the privacy laws of the ten countries we examine applies, we performed our crawls via the Google Cloud Platform on ten different VM servers located in the respective countries. Each VM was identically configured with 4 vCPUs, 16 GB of memory, 50 GB of storage, and the Windows operating system to ensure consistent performance across countries. Table 2 shows the VM servers' geographic locations.

Table 2. List of VM servers and their geographic locations.

Country	Continent	City
Australia	Oceania	Sydney
Brazil	South America	São Paulo
Canada	North America	Toronto
Germany	Europe	Berlin
India	Asia	New Delhi
Singapore	Asia	Singapore
South Africa	Africa	Johannesburg
South Korea	Asia	Seoul
Spain	Europe	Madrid
US (California)	North America	Los Angeles

4.3. Setup and Crawl Overview

We deployed our crawler with a Selenium WebDriver [80] on Firefox Nightly with Enhanced Tracking Protection disabled [81]. The crawler then installed the Privacy Pioneer browser extension [18], observed each site for 60 seconds (Figure A1), and persisted web requests and responses via a REST API to a local MySQL database [82]. Based on the Disconnect Tracker Protection lists [17], Privacy Pioneer labeled third-party connections into advertising, analytics, and social categories by matching request URLs against the URLs on the lists. Figure 1 illustrates our automated web crawling pipeline.

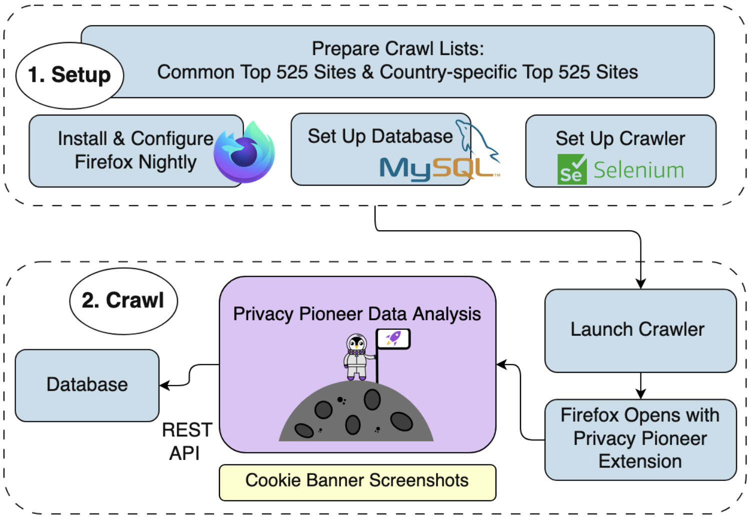
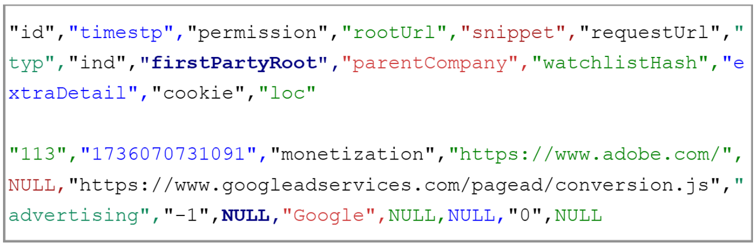

1. Setup
Prepare Crawl Lists:
Common Top 525 Sites & Country-specific Top 525 Sites
Install & Configure Firefox Nightly
Set Up Database
MySQL
Set Up Crawler
Selenium
2. Crawl
Privacy Pioneer Data Analysis
Launch Crawler
Database
REST API
Firefox Opens with Privacy Pioneer Extension
Cookie Banner Screenshots

Figure 1. Overview of our web crawling pipeline implemented and run on a separate VM server for each country.

4.4. Entries

Throughout this study, we use the term "entry" to refer to a unique record of an HTTP request for a tracking purpose, e.g., advertising, recorded by Privacy Pioneer. We refer to a "tracker connection" as the action that produces an entry. We use the number of entries as a proxy to quantify potential data sharing for a particular purpose with third parties. Figure 2 shows an advertising entry.



```
"id","timestp","permission","rootUrl","snippet","requestUrl","
typ","ind","firstPartyRoot","parentCompany","watchlistHash","e
xtraDetail","cookie","loc"

"113","1736070731091","monetization","https://www.adobe.com/",
NULL,"https://www.googleadservices.com/pagead/conversion.js","
advertising","-1",NULL,"Google",NULL,NULL,"0",NULL
```

Figure 2. An example entry recorded by Privacy Pioneer. Upon visiting https://www.adobe.com/ ("rootUrl"), the site loaded Google's conversion script ("requestUrl" = https://www.googleadservices.com/pagead/conversion.js). The entry is an advertising entry, i.e., labeled "typ" = `advertising`, "parentCompany" = `Google`, and "cookie" = `0` (no cookie recorded).

For clarity, if a site makes multiple requests to the same domain (i.e., the same top- and second-level domain) for the same purpose (e.g., for analytics to https://google-analytics.com), we count it as a single entry. Connections to different domains (i.e., a different top- or second-level domain) are counted as distinct entries even if they are for the same purpose and belong to the same company (e.g., https://connect.facebook.net and https://www.facebook.com). However, different subdomains of the same top- and second-level domain (e.g., https://ads.google.com and https://analytics.google.com) are counted as one entry. A single HTTP request can contain multiple entries.

4.5. Accuracy Test Results

To ensure that it produces accurate results we tested our pipeline in its entirety—VM environment, crawler, and Privacy Pioneer extension—under conditions mimicking a real crawl. Table 3 shows the accuracy test results, which indicate reliable performance.

Table 3. Accuracy test results for $n = 10$ sites. (TP = True Positive, FN = False Negative, and FP = False Positive).

Category	TP	FN	FP	Precision	Recall	F1
Analytics	43	3	0	1.00	0.93	0.97
Advertising	126	0	0	1.00	1.00	1.00
Social	17	0	0	1.00	1.00	1.00

We randomly selected ten sites from a subset of 100 sites for our test (The 100 sites contain five randomly selected sites from each Country-specific Top 525 list and 50 sites with a high likelihood of performing browser fingerprinting and other privacy-invasive practices that we identified via BuiltWith [83]. Thus, the list is intended to identify practices beyond this study. For purposes of this study the sampling strategy of the 100 sites is less relevant as we focus here on the sites' integration of advertising, analytics, and social functionalities, which are common on many sites). We performed our test on the US VM. Given the uniformity of our setup across all countries, we have no reason to believe that performance would differ across countries. For each site, we downloaded the HTTP Archive (HAR) files containing complete records of all network requests and responses during the test crawl. These HAR files served as the basis for establishing the ground truth that we manually evaluated against the entries Privacy Pioneer flagged during the accuracy test run (Further details of our methodology—including its limitations—are described in Appendix A).

5. Results

RQ1. Users' Geographic Location Is a Key Factor for Tracker Exposure Level: Given the identical Common Top 525 sites for each country, we find different levels of tracker exposure. For the US (California) and Australia—two of the three opt-out jurisdictions in our study—sites have the highest level with 11.7 and 11.2 average entries per site, respectively, while opt-in jurisdictions generally have lower levels, especially, Spain and Germany with 5.3 and 4.2 average entries per site, respectively (Section 5.1.3).

RQ2. Globally Popular Sites Have a More Elevated and Narrower Tracker Range than Locally Popular Sites: Notably, only 44.6% of German Country-specific Top 525 sites establish any tracker connection at all, while at the high end 96.0% of Australian sites do so (Figure 3). The number of average entries per site for the Country-specific Top 525 sites ranges from 0.9 to 14.1, while the range for the Common Top 525 sites is narrower and overall more elevated with 4.2 to 11.7 average entries per site (Section 5.1.3).

RQ3. EU Law Appears to Reduce Tracking in EU Countries but Not as Much in Other Countries: The Common Top 525 sites have 50.5% fewer average tracker connections when accessed from EU countries compared to non-EU countries (Section 5.1.3), suggesting that the GDPR and ePrivacy Directive have a tangible effect in reducing tracking. Further, simply not interacting with cookie banners decreases tracker connections by 48.5% for Germany, as measured for a sample of 36 Common Top 525 sites (Section 5.2.4). As 28% of Common Top 525 sites show cookie banners in all ten countries (Section 5.2.3), our results suggest a moderate Brussels effect. However, against the backdrop of global US ad tech practices, EU law mainly acts as a Brussels shield.

5.1. Tracker Connections

Overall, we successfully crawled 95.1% (9488/9975) sites across ten countries. The success rates of the Common and Country-specific Top 525 sites are similar. For the Country-specific Top 525 sites (including the Common Top 525 sites for the US counted as Country-specific Top 525 sites) we successfully crawled 94.9% (4984/5250) unique sites. Unless mentioned otherwise, to ensure comparability for our analysis of the Common Top 525 sites we will use only the 80% (420/525) sites that we crawled successfully in all ten countries.

5.1.1. Overall Tracker Connections and Background

Table 4 shows the percentages of entries identified and recorded across different categories. Table 5 shows the percentages of sites that connect to a third party in a category at least once. While Table 4 reflects the overall volume of tracker connections that sites in our dataset make to trackers in the various categories, Table 5 reflects their presence on the sites. With 69.4% of sites establishing an analytics connection, analytics is the most prevalent tracker category. However, comparing 55,079 connections to advertising trackers to 19,760 analytics connections, the volume of the former is approximately 2.8 times of the latter. This difference may be the result of underlying functional and economic reasons.

Table 4. Entry-level counts ($n = 84,170$) for all successfully crawled Country-specific and Common Top 525 sites ($n = 9488$).

Category	Entries Count	% of Entries
Advertising	55,079	65.4%
Analytics	19,760	23.5%
Social	9331	11.1%

Table 5. Site-level counts ($n = 8347$) for successfully crawled Country-specific Top 525 sites, with Common Top 525 sites for the US ($n = 4984$).

Category	Sites Count	% of Sites
Advertising	3060	61.4%
Analytics	3460	69.4%
Social	1827	36.7%

Advertising trackers generally need to engage in more fine-grained tracking with more frequent connections as operators try to learn as much as possible about a user to serve relevant ads. Analytics trackers, on the other hand, may only request a user agent string once and otherwise may not require frequent connections. There is also an incentive for site operators to integrate multiple ad networks to maximize ad revenue while multiple analytics services would quickly lead to a duplication of functionality. While social connections have the lowest level in both measurements, the industry is much more concentrated with only four parent companies—Facebook, LinkedIn, X, and reddit—in the top 30 trackers while both the advertising and analytics categories have a long tail (Section 5.2.4). Overall, given their prevalence and volume, advertising trackers create the highest level of privacy risks for users.

5.1.2. Percentage of Sites with Tracker Connections

Figure 3 shows the percentage of sites in a country that make at least one advertising, analytics, or social tracker connection.

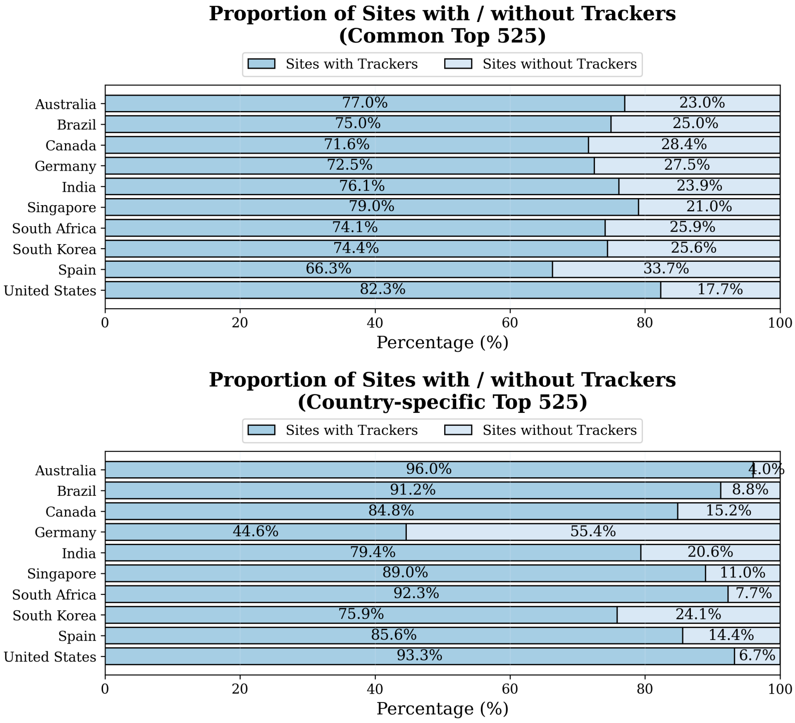
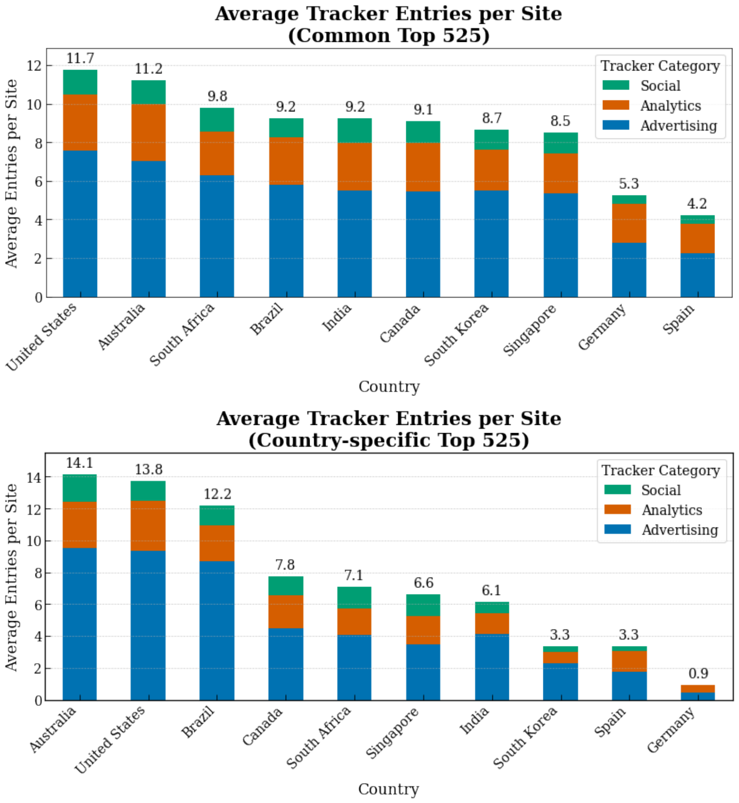


Figure 3. For the Common Top 525 sites (**top**) the percentages of sites with tracker connections across countries have a much smaller range compared to the Country-specific Top 525 sites (**bottom**). To ensure that data from different countries are comparable in the Common Top 525 sites we only include sites that we crawled successfully in all countries ($n = 420$ for each country), which is also the reason for the different percentages for the US in the Common and Country-specific Top 525 sites.

Across all countries, between 17.7% and 33.7% of the Common Top 525 sites do not connect to any tracker. However, for the Country-specific Top 525 sites this range is 4.0% to 55.4%. Compared to the other countries, Germany has a significantly higher percentage of sites that make no tracker connection. In contrast, Australia, Brazil, South Africa, and the US each have fewer than 10% of sites not making such connections. This disparity suggests that the potential privacy risks associated with tracker connections differ between global and local sites. Depending on which types of sites users visit, they are exposed to quite different levels of tracking.

5.1.3. Average Number of Entries per Site

Figure 4 shows the average number of entries across countries. For most countries (South Africa, India, Canada, South Korea, Singapore, Germany, and Spain) it is greater in the Common Top 525 sites than in the Country-specific Top 525 sites. The Country-specific Top 525 sites show a greater range from 0.9 to 14.1 compared to the Common Top 525 sites, which have a range from 4.2 to 11.7. In the Country-specific Top 525 sites Australia exhibits over 14 times more average entries than Germany. However, for all countries except one (Germany), the percentage of sites making at least one tracker connection is greater in the Country-specific Top 525 sites (Figure 3). For the Common Top 525 sites, on average, EU countries have 50.5% fewer entries (4.8) than non-EU countries (9.7).


Average Tracker Entries per Site (Common Top 525)

Average Tracker Entries per Site (Country-specific Top 525)

Figure 4. For both the Common Top 525 sites (**top**) and the Country-specific Top 525 sites (**bottom**), sites in the EU—Germany and Spain—have the lowest number of average entries. Australia and the US have the highest. (Common Top 525 sites: $n = 420$ for each country, Country-specific Top 525 sites: $n = 4984$ for all countries.)

Despite the differences in entry averages between the Common and Country-specific 525 sites, the overall ranking of countries across these two distributions remains generally consistent. However, there are a few notable individual differences. South Korea's Country-specific Top 525 sites exhibit far fewer average entries than their Common Top 525 counterparts placing it on par with Spain. Conversely, Brazil's country-specific sites have more average entries than those of Canada, South Africa, Singapore, India, and South Korea—countries that are comparable to Brazil for in the Common Top 525 sites. Overall, the following pattern emerges for the number of average entries per site across the Common and Country-specific Top 525 sites:

- High: Australia, US (California).
- Medium: Brazil, Canada, India, Singapore, South Africa, South Korea.
- Low: Germany, Spain.

5.2. Cookie Banner Deployment

We evaluate the deployment of cookie banners on Common and Country-specific Top 525 sites. Independently of whether a jurisdiction requires opt-in consent or gives users a right to opt-out, generally all laws require notice.

5.2.1. Tracker Connections by Sites with and Without Cookie Banners

Figure 5 shows the average number of entries in the advertising, analytics, and social categories for the Common and Country-specific Top 525 sites split into sites with and without a cookie banner. For the Common Top 525 sites, those without a banner have more average entries than sites with a banner. This trend holds for all countries. Sites without a banner have on average 9.6 entries, which is 26.3% more than the 7.6 average entries we observe for sites with a banner. This difference is primarily due to more advertising entries. While Germany and Spain have a comparatively lower level of average entries, the trend of higher percentages for sites without a banner holds for them as well.

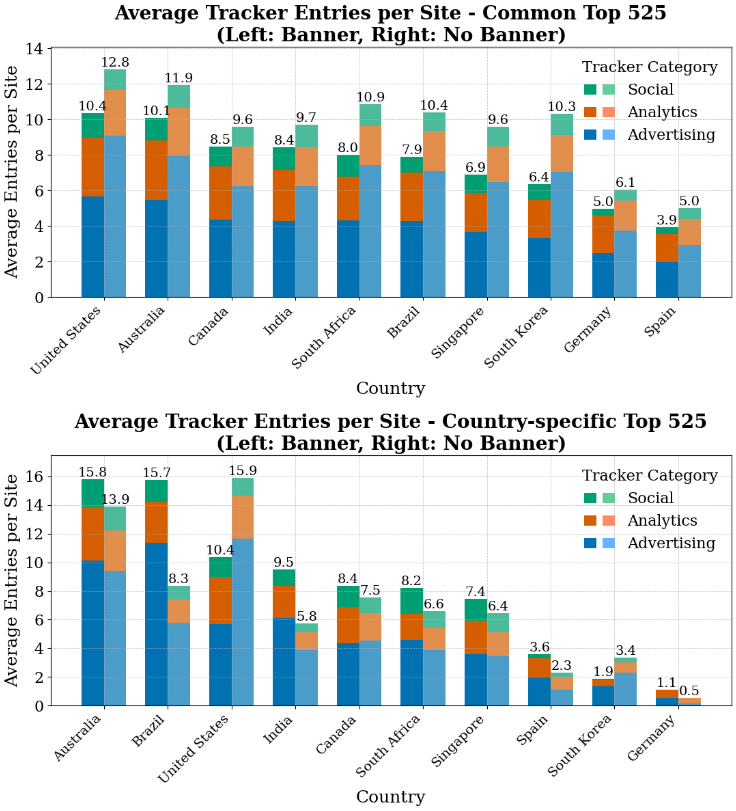


Figure 5. The Common Top 525 sites (**top**) with a banner have fewer average entries than sites without. However, this trend is reversed for the Country-specific Top 525 sites (**bottom**) except for the US (California) and South Korea. (Common Top 525 sites: $n = 420$ for each country, Country-specific Top 525 sites: $n = 4,984$ for all countries.)

This finding suggests higher levels of non-compliance for sites without a cookie banner. It is expected that sites without a banner would not connect to third parties (or only connect to third parties that do not require consent). However, our finding suggest the opposite: sites without a banner are more likely to violate applicable privacy laws as they generally connect to advertising trackers at higher rates. From a user's perspective, not seeing a banner is less disruptive but also more privacy-invasive as sites share the user's personal data "silently".

Comparing banner and non-banner sites for the Country-specific Top 525 sites, we see the opposite trend compared to the Common Top 525 sites: non-banner sites generally have fewer average entries than banner sites indicating less broad privacy risk. In particular, we observe a substantial decrease in average entries for non-banner sites for Germany (54.5%), Brazil (47.1%), India (38.9%), and Spain (36.1%). However, while the average number of entries for non-banner sites is lower, there still can be a high level of non-compliance as the banner requirement applies regardless of how many tracker connections a site makes as long it is at least one.

5.2.2. Cookie Banner Deployment Across Countries

For the Common Top 525 sites we observe substantially different distributions of cookie banner deployment between EU and non-EU countries. Germany and Spain have the highest percentage of sites with cookie banners with 73.8% and 72.9% of sites, respectively. In contrast, the sites in the remaining eight non-EU countries have substantially lower percentages of cookie banner deployment ranging narrowly from 36.7% to 46.2%. Figure 6 shows the proportion of cookie banner deployment for both the Common and Country-specific Top 525 sites.

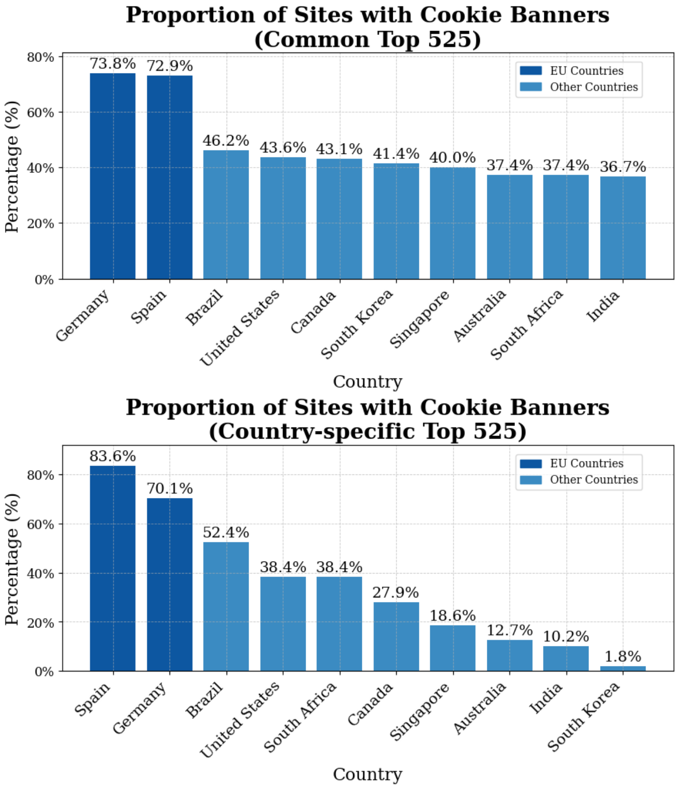


Figure 6. For the Common Top 525 sites the percentage of sites with cookie banners is in a narrow range across two sets of sites with one set consisting of the EU countries, Germany and Spain, and the other of the remaining countries (**top**). The banner distribution for the Country-specific Top 525 sites has a much larger range (**bottom**). (Common Top 525 sites: $n = 420$ for each country, Country-specific Top 525 sites: $n = 4984$ for all countries.)

For the Country-specific Top 525 sites, we see a much larger range across countries. For half of the countries the ranking by cookie banner deployment remains comparable to the Common Top 525 sites. Spain and Germany continue to exhibit the highest banner percentages. Brazil and the US (California) continue to rank third and fourth, respectively. South Africa shows only a minimal percentage difference between the two distributions. However, for Canada, Singapore, Australia, India, and, in particular, South Korea, we observe substantially lower rates of banner deployment. On average, the percentage of sites with banners across these five countries drops from 39.7% to only 14.2%. South Korea represents the most extreme case with only 1.8% of sites with cookie banners. These significantly lower levels of banners could indicate lower levels of privacy law compliance.

For South Korea, for example, 75.9% of the Country-specific Top 525 sites connect to at least one tracker (Figure 3). At the same time, only 1.8% of sites deploy a cookie banner. Thus, even though South Korea's privacy law mirrors the GDPR's requirement for opt-in consent, there may be a substantial compliance gap. The higher and approximately uniform rates of cookie banner deployment among the non-EU Common Top 525 sites could be based on the Brussels effect. Some site operators of globally popular sites may be simplifying their compliance obligations by EU cookie requirements for all their sites. We can gain further insight into the strategies of site operators' deployment of cookie banners across countries by examining the Common Top 525 sites in this regard.

5.2.3. Sites' Multi-country Cookie Banner Strategies

Based on the directly comparable Common Top 525 sites, we can discern three major strategies: site operators deploy banners (1) everywhere, (2) nowhere, or (3) in two or three countries. Figure 7 illustrates these strategies. The x-axis values show the number of countries in which a site displays a cookie banner while the y-axis shows the count of such sites. For example, the leftmost bar shows that 119 sites display cookie banners in all ten countries. The rightmost bar, on the other hand, shows that 97 sites do not show a cookie banner in any country. We observe a clear pattern for the majority of sites: if site operators choose to deploy a cookie banner, they will do so in either all countries or in two or three countries.

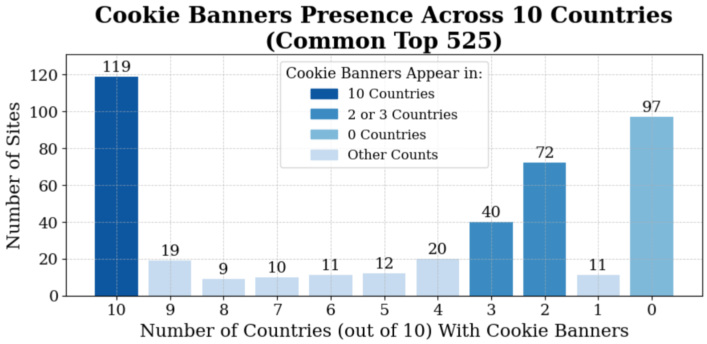


Figure 7. Cookie banners across ten countries for the Common Top 525 sites ($n = 420$ for each country). 28% (119/420) of sites show cookie banners in all ten countries. As previous findings suggest [36,37], CMPs have substantial potential impact on cookie banner and tracker settings. Our findings point to their prominent role as well. During our crawl we observed 23.6% (990/4200) connections to OneTrust, as indicated by a request to https://geolocation.onetrust.com.

Tables 6 and 7 show the sets of countries for which site operators deploy cookie banners in exactly two or three countries, respectively. Notably, almost all sites in the two-country set deploy banners only for their German and Spanish sites. Site operators seem to put strong emphasis on compliance with the EU jurisdictions Spain and Germany. This pattern suggests that compliance efforts in this regard are primarily driven by the GDPR and the ePrivacy Directive. While comparable consent requirements exist in several non-EU jurisdictions, including Brazil, South Korea, and, most recently, India, we do not yet observe any major impact by those. However, for site operators that deploy cookie banners in exactly three countries, the set consisting of Brazil, Germany, and Spain is the second-most common (Table 7). Increased enforcement of the LGPD could lead to further progress. The same is true for opt-out notices under the CCPA that are part of the most common set of three countries with 16 sites.

Table 6. Common Top 525 sites deploying banners in exactly two countries ($n = 72$ for each country).

Country Set	Sites
Germany and Spain	68
Australia and South Korea	1
Brazil and Germany	1
Germany and US (California)	1
Germany and India	1

Table 7. Common Top 525 sites deploying banners in exactly three countries ($n = 40$ for each country).

Country Set	Sites
Germany, Spain and US (California)	16
Brazil, Germany and Spain	10
Germany, South Korea and Spain	5
Canada, Germany and Spain	4
Germany, South Africa and Spain	3
Australia, Germany and Spain	1
Singapore, South Africa and Spain	1

5.2.4. Impact of Cookie Banner Consent and Inactivity

Based on a random sample of 50 sites from the Common Top 525 sites for Germany, Spain, and the US, from which we exclude 14 sites that did not load properly in at least one country, we determine the impact of cookie consent and inactivity. Figure 8 shows the 30 parent companies with the highest entry counts for Germany and the US (See Appendix A.2 for details on how we derive parent companies). In particular, trackers in the advertising and social categories are substantially reduced (Table 8), while the rate of analytics trackers, apart from those of Google and Microsoft, shows a smaller reduction. Overall, Microsoft's tracker rate was reduced the most. As the set of top 30 parent companies is very similar across countries—with Google, Facebook, LinkedIn, Microsoft, Adobe, and X dominating the industry—any privacy improvements in their practices would have broad impact for many users.

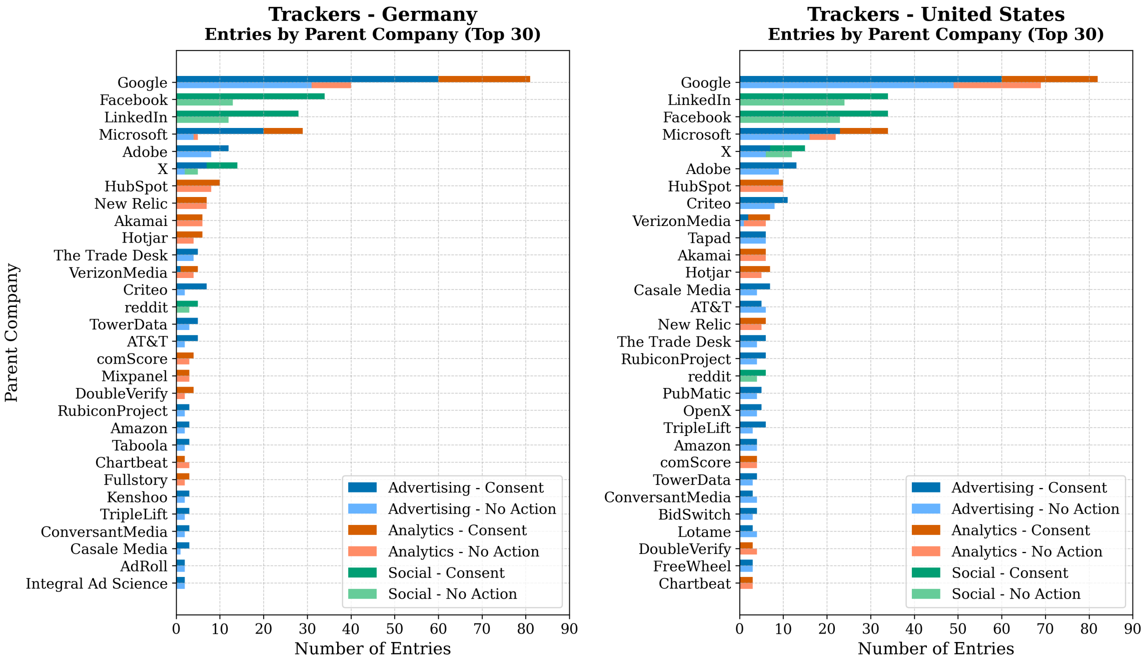


Figure 8. For Germany (**left**) the number of tracker connections upon not interacting with cookie banners is often reduced by at least half compared to consenting. The difference is substantially less pronounced for the US (**right**). Our measurement for Spain (Figure A2) exhibits a similar trend as for Germany. (Common Top 525 sites: $n = 36$ for each country.) Figure A3 shows the distribution of parent companies for the Country-specific Top 525 countries.

Table 8. The percentage decrease of trackers when taking no action compared to consenting calculated for the data in Figure 8. The overall decrease refers to advertising, analytics, and social categories combined.

Country	Advertising	Analytics	Social	Overall
Germany	-51.7%	-34.5%	-58.1%	-48.5%
US (California)	-20.8%	-11.7%	-30.5%	-21.1%

Comparing across countries, we observe much fewer tracker connections for Germany and Spain upon inactivity than for the US. This observation aligns with the opt-in requirements of the GDPR and ePrivacy Directive. If followed, both laws in combination create a twofold effect: The ePrivacy Directive prevents sites from setting cookies as Article 5(3) gives users a right to refuse accessing or storing information on the user's terminal equipment. The GDPR requires sites to obtain users' consent before initiating the network connection to trackers' servers, which would transmit users' IP addresses, that is, personal data under the GDPR. As the CCPA permits tracking until users opt out, it is plausible that we observe a smaller tracker difference rate between consent and inactivity for the US (California). Opt-in jurisdictions are inherently more privacy-protective.

6. Discussion

Our results have broader implications for protecting web users' privacy and evolving the online ad ecosystem towards a more privacy-protective system that supports the free and open web for its users.

6.1. Challenges for Users, Website Operators, and Lawmakers and Regulators

Overall, our results show that geographic location is a key factor for the level of web tracking to which a user is exposed. This geographic fragmentation creates distinct challenges for three main groups: (1) users, (2) website operators, and (3) lawmakers and regulators. Addressing these challenges in a coordinated and integrated approach is crucial for improving web privacy overall.

Currently, users experience different levels of privacy protections depending on applicable law, its enforcement, and implementation. For example, only 44.6% of German Country-specific Top 525 sites establish a tracker connection while 93.3% of US sites do so (Figure 3). In general, EU users benefit from stronger legal protections but also face a higher frequency of cookie banners (Figure 6), which can create usability challenges and undermine the very purpose of meaningful consent. Users outside the EU—even in countries with strong privacy laws—often receive much less effective legal protection from tracking. In many cases users are purposely misled via dark patterns [37]. Automating user rights, for example, via GPC [39,40], which has been shown to be effective in reducing the number of intractable cookies [41], can increase users' privacy protection while at the same time prevent the degradation of usability.

For website operators it can be a complex and costly endeavor to ensure privacy compliance with all applicable laws in the geographically fragmented legal landscape. They can implement robust controls for the EU while adopting a more permissive tracking approach elsewhere (Figure 7). This bifurcated strategy, however, may become increasingly untenable as more countries adopt privacy laws with local nuances. The challenge is to develop a scalable compliance architecture for the web that respects local laws without creating an unmanageable patchwork of different rules for website operators. That is the challenge that CMPs identified as their business case and that, for example, the Interactive Advertising Bureau is responding to with its Global Privacy Platform [84]. These aggregation solutions can help operators' to make their sites compliant if they reflect the law adequately, especially, in their default settings, and are easy and cost-effective to implement.

For lawmakers and regulators the challenge is to draft laws and regulations that are easy to implement and practical to enforce. Ideally, laws and regulations would converge across jurisdictions to reduce compliance overhead. While such convergence may happen naturally on a practical level, it can also be explicit. For example, for the right to opt out per the Texas Data Privacy and Security Act, operators are only required to support a technology if they use it for "complying with similar or identical laws or regulations of another state" (Texas Data Privacy and Security Act, Section 541.055(e)(4)). This provision illustrates how lawmakers and regulators can support the convergence of privacy laws across different jurisdictions. It also illustrates how laws and regulations can leave sufficient room for new privacy technology, for example, encompassing GPC.

6.2. The Leading Role of the EU: Brussels Shield and Brussels Effect

Our study serves as yet another example of the leading role the EU plays in shaping web privacy. Our results suggest that the GDPR and ePrivacy Directive are not merely laws on the books but have a tangible effect on reducing tracker connections. When accessed from Germany and Spain, on average, the Common Top 525 sites made 50.5% fewer tracker connections compared to non-EU countries (Section 5.1.3). Also, simply not interacting with cookie banners decreased tracker connections by 48.5% for Germany (Table 8). These findings illustrate that under EU law privacy is protected by default.

The effect of EU law also appears to be reflected in the deployment of cookie banners. For the Common Top 525 sites we observed a trimodal distribution: sites tend to show banners in either (1) all countries, (2) primarily EU countries, or (3) no countries (Figure 7). For the 28% of Common Top 525 sites showing cookie banners in all countries our results suggest a moderate Brussels effect. However, for many global sites (Figure 6) and third party operators (Figure 8) the effect is localized to EU jurisdictions, meaning the law acts as a Brussels shield for EU users but does not broadly improve privacy for the rest of the world. Thus, while the EU is playing a leading role in the adoption of consent mechanisms, its influence is also limited by geo-fencing.

6.3. Enforcement as a Driver of Privacy Evolution

Our results suggest that enacting a new privacy law by itself is insufficient to improve web privacy. Rather, it is the combination of privacy lawmaking, regulatory rulemaking, and active enforcement that is most impactful. Various countries in our study are at different evolutionary stages of developing their privacy enforcement regime (Section 3.3). Germany and Spain represent a mature stage with high regulatory awareness and active Data Protection Authorities and courts. Brazil, on the other hand, is at an earlier stage. While its LGPD mirrors the GDPR, it is still developing its enforcement capacity and has yet to build and apply an enforcement infrastructure that motivates and polices compliance. As an illustration, we found the percentage of Common Top 525 sites with tracker connections for Brazil to be similar to the percentages for Germany and Spain (Figure 3). However, the proportion of sites deploying cookie banners is substantially lower (Figure 6). This discrepancy points to a gap between the law as written and its practical enforcement.

The example of the EU shows that privacy reform is best accompanied by investment in the institutional and procedural infrastructure for providing guidance, monitoring compliance and, if necessary, acting on violations. However, learning from other countries' efforts is not a one-way-street. For example, currently GPC has significantly more adoption in the US compared to the EU. California [85], Colorado [86], Connecticut [87], New Jersey [88], and Oregon [89] recognize GPC as a valid opt-out mechanism enforcing it accordingly [72–75]. With its Digital Omnibus [90] the EU is now moving towards the adoption of privacy preference signals as well. Adopting what works in other jurisdictions, in particular, when it comes to enforcement, does not only allow jurisdictions to profit from experiences others already made but also avoids fragmentation and contributes to the global convergence of privacy mechanisms and their enforcement.

6.4. Maintaining a Free and Open Web

Finally, we must acknowledge that a major driving force behind the web's privacy problem is the ad-financed online economy. Web tracking is the result of economic incentives in the online ad industry, which funds a large portion of the free content and services on the web available today and likely in the future. Thus, in our view, the policy challenge is not to eliminate online ads altogether but to ensure that they are transparent, fair, and privacy-preserving. Evolving the web into an inherently privacy-protective system while maintaining the underlying economic benefits of its ad ecosystem is a delicate balancing act. Future efforts must ensure that the web remains free and open without requiring users to trade their privacy for access to content.

7. Conclusions

Across ten countries and 9,488 websites, the results of our study suggest that users' geographic location is a key factor for their tracker exposure level. We find that the global Common Top 525 sites visited from EU jurisdictions—governed by the GDPR and ePrivacy Directive—exhibit 50.5% fewer tracker connections than sites from non-EU jurisdictions. Viewed in light of the EU's regulatory activities, these findings suggest that privacy laws with active enforcement can meaningfully limit tracking, whereas laws that do not yet have regulatory follow-through, such as Brazil's LGPD, appear to be less effective. While our results suggest a moderate Brussels effect for cookie banner deployment on global sites, EU law primarily acts as a Brussels shield against the backdrop of global US ad tech practices.

Looking ahead, we want to extend this study in various directions. First, longitudinal measurements can help gauging where future enforcement actions are necessary and where past enforcement actions have led to tangible privacy protections for users. Second, we want to extend our measurements from manual consent mechanisms to privacy preference signals, such as GPC. Third, a closer integration of privacy laws into the technological structure of the web, for example, by means of web standards is desirable. Overall, we want to evolve the web into an inherently privacy-preserving system that protects its users but also maintains and extends its free and open nature.

Author Contributions

H.Y.: data curation, investigation, methodology, software, validation, visualization, writing—original draft preparation; P.Y.: data curation, investigation, methodology, software, validation, visualization, writing—original draft preparation; S.Z.: conceptualization, investigation, methodology, software, validation, visualization, writing—original draft preparation, writing—reviewing and editing. All authors have read and agreed to the published version of the manuscript.

Funding

This research was funded by Google under the Research Scholar Program (project title "Privacy Pioneer: Automating the Creation of Privacy Labels for Websites").

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

Data related to this study is publicly available under the MIT License [10].

Acknowledgments

We would like to thank our anonymous reviewers for their detailed and valuable feedback that helped us to improve our paper substantially. We would also like to thank Nina Taft and Hamza Harkous of Google's Applied Privacy Research group for the discussions and support of this project. Brian Tang shared his expertise on cookie consent violations, for which we thank him kindly. We would finally like to thank Wesleyan University, its Department of Mathematics and Computer Science, and the Anil Fernando Endowment for their additional support. Conclusions reached or positions taken are our own and not necessarily those of our supporters, its trustees, officers, or staff.

Conflicts of Interest

The authors declare no conflict of interest.

Use of AI and AI-Assisted Technologies

No AI tools were utilized for this paper.

Appendix A. Methodology Details

Appendix A.1. Setup and Crawl Details

1. Crawl Environment Setup: For each country, we crawled sites from the Common Top 525 and Country-specific Top 525 sites. We configured the required components on each country's VM, including the Firefox Nightly browser (We used the Firefox Nightly build of 1 January 2024, available at https://ftp.mozilla.org/pub/firefox/nightly/2024/01/ 2024-01-01-23-15-40-mozilla-central/), a local MySQL database, and the Selenium-based [80] crawler.
2. Automated Web Crawl: On each VM, the crawler is launched alongside the MySQL server. The crawler opens Firefox Nightly, installs the Privacy Pioneer extension [18], and visits each URL in the crawl list. During each visit:
   (a) Privacy Pioneer monitors HTTP requests in real time.
   (b) Requests up to 100,000 characters in length are parsed and classified to detect site connection events.
   (c) All identified events are logged into the SQL database through a REST API.
   (d) In a separate step, the crawler takes a screenshot of the site to detect cookie banners.
   (e) After a fixed observation window of 60 seconds, the crawler proceeds to the next site.
   (f) Once crawling is complete, we manually export the collected data for our data analysis.

We chose Firefox because our pipeline relies on Privacy Pioneer (Appendix A.2), an existing browser extension only implemented for Firefox. Using Firefox therefore ensured compatibility with that prior system and allowed us to preserve methodological continuity with the underlying measurement framework. We disabled Firefox's Enhanced Tracking Protection [81] to avoid browser-level tracker blocking. To store the collected data we created on each VM a local SQL database [82]. After the crawler gathers entries from crawled sites the REST API inserts the data into the database. We performed our crawl from 5–24 January 2025. We observed the traffic for each site for 60 seconds (Figure A1). Excluding the US (California), crawling the sites on the Common Top 525 and Country-specific Top 525 sites lists took between 19.6 and 21.6 hours for each country (For the US (California) crawling the Common Top 525 sites took 10.9 h).

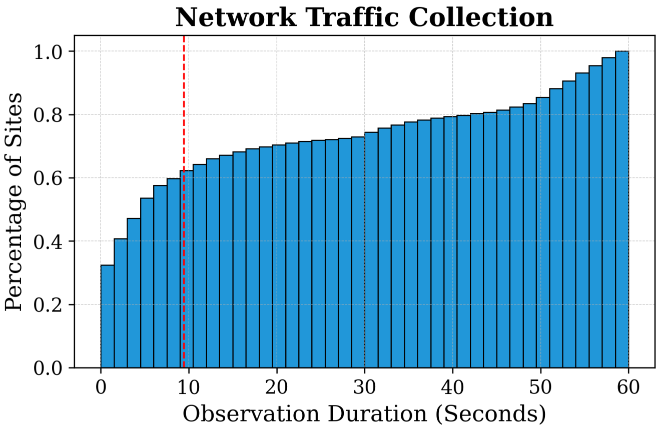


Figure A1. 60% of sites made no further request after ten seconds of observation. After that time, for the sites in total, the number of requests became much more infrequent before picking up slightly towards the end. Thus, we believe that we captured a meaningful amount of network traffic for most sites.

If a site's SSL/TLS certificate was invalid, improperly configured, or it did not have certificate at all, our crawler would flag the site for an `InsecureCertificateError` (Table A1).

Table A1. `InsecureCertificateError` counts and percentages for all sites (All), Country-specific Top 525 sites (Specific), and Common Top 525 sites (Common). For the US (California) the Common Top 525 sites double as Country-specific Top 525 sites.

Country	**Error Count** **All (Specific, Common)**	**Error %** **All (Specific, Common)**
South Africa	12 (10, 2)	1.1% (1.9%, 0.4%)
Singapore	8 (6, 2)	0.8% (1.1%, 0.4%)
India	6 (5, 1)	0.6% (1.0%, 0.2%)
Spain	6 (4, 2)	0.6% (0.8%, 0.4%)
Brazil	5 (4, 1)	0.5% (0.8%, 0.2%)
Canada	4 (4, 0)	0.4% (0.8%, 0.0%)
South Korea	4 (3, 1)	0.4% (0.6%, 0.2%)
US (California)	2 (2, 2)	0.4% (0.4%, 0.4%)
Australia	2 (1, 1)	0.2% (0.2%, 0.2%)
Germany	1 (1, 0)	0.1% (0.2%, 0.0%)

Appendix A.2. Tracker Categorization with Privacy Pioneer

We perform the analysis of whether a site connects to a third-party tracker with Privacy Pioneer [18], an open-source browser extension that we install in Firefox Nightly. The categorization into advertising, analytics, and social categories cover, respectively, third-party ad tracking, site visitor measurement (e.g., of users' geographic regions), and social media integrations. Privacy Pioneer identifies whether a site belongs to a particular category based on rule-based matching of request URLs against the Disconnect Tracker Protection lists [17], from which it also retrieves the "parent company" of the domain. We use the parent-company labels to aggregate individual tracker domains into company-level entities in our analysis, for example, for comparing the most prevalent parent companies across countries and when reporting company-level tracker rates (Section 5.2.4) (Privacy Pioneer has additional analysis functionality, for example, identifying if a site collects location data or performs browser fingerprinting, which, however, we do not consider for purposes of our study here).

Appendix A.3. Cookie Banner Identification and Interaction

To identify sites with cookie banners our crawler automatically saves screenshots for all sites it visits. We then filter for the presence of cookie banners by manually checking all screenshots. We consider a site to have a cookie banner if it presented a visible notice that informed users about data collection or sharing practices or explicitly requested user consent for such. As long as the site provided some on-screen notice of data collection, sharing, or cookie settings we counted it as a cookie banner. Our crawler only took screenshots of each site without interacting with any cookie banner. In EU jurisdictions, Germany and Spain, this scenario represents a refusal to consent while, for example, in the US (California) it represents being opted in. For a random sample of 36 sites from the Common Top 525 sites in three countries, we also manually interacted with the cookie banners to compare the effects of consent and inactivity (Section 5.2.4).

Appendix A.4. Limitations

Our findings should be interpreted in light of various limitations. First, our VM approach provides a controlled environment but cannot fully represent the local tracking experiences of real users. Further, except for our manual interaction with the cookie banners for a sample of sites in our dataset, our methodology only captures data from initial site loads without user interaction, which may trigger additional trackers or may make sites behave differently than what we observed. Our evaluation is based on crawling a limited set of sites for a limited set of countries using top-level domains as a heuristic for identifying country-specific sites. We cannot determine whether a country's privacy law is causing the tracking behavior that we observe but only whether the two correlate. Our approach measures tracker connections rather than data collection. Some of these connections may not be actually privacy-invasive, for example, because the incoming data and its related logs are immediately deleted by the receiving site. However, we can be sure that data was not sent if there was no connection. Our evaluation is based on Privacy Pioneer's rule-based URL classification that matches request URLs against the Disconnect Tracker Protection block lists [17]. We rely on the correctness of the list's tracker categorization and do not capture tracker connections beyond the list. We also consider server-side connections beyond the scope of our study.

Appendix B. Additional Figures

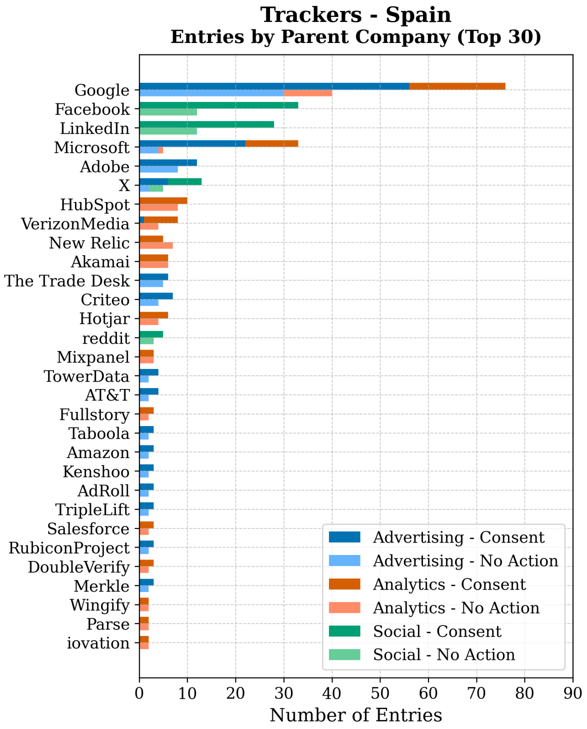


Figure A2. For Spain the number of network connections upon not interacting with cookie banners is often reduced by at least half compared to consenting to the data collection.

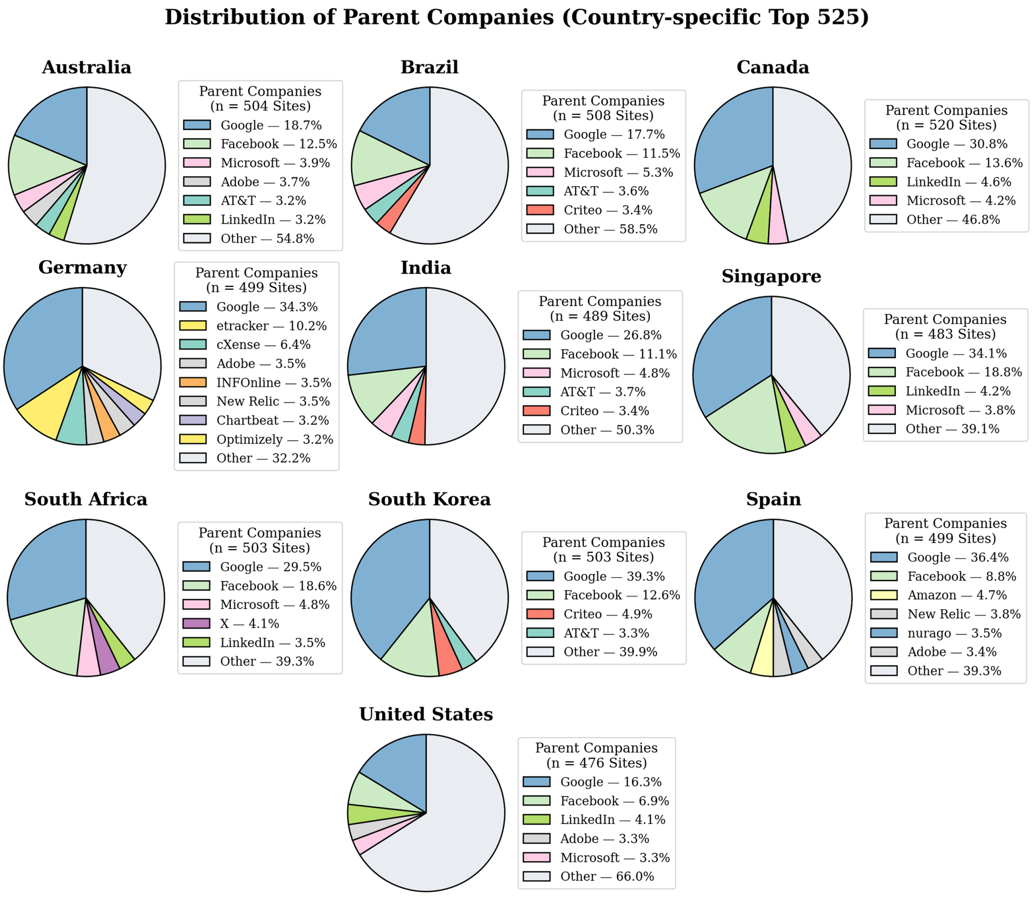


Figure A3. Parent companies for the country-specific Top 525 sites.

References

1. Weinshel, B.; Wei, M.; Mondal, M.; et al. Oh, the Places You've Been! User Reactions to Longitudinal Transparency About Third-Party Web Tracking and Inferencing. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, London, UK, 11–15 November 2019; pp. 149–166.
2. Bujlow, T.; Carela-Español, V.; Solé-Pareta, J.; et al. A Survey on Web Tracking: Mechanisms, Implications, and Defenses. *Proc. IEEE* **2017**, *105*, 1476–1510.
3. European Parliament and Council of the European Union. Regulation (EU) 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation). Available online: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (accessed on 11 March 2026).
4. European Parliament and Council of the European Union. Directive 2009/136/EC of 25 November 2009 Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, and Regulation (EC) No 2006/2004 on Cooperation between National Authorities Responsible for the Enforcement of Consumer Protection Laws. Available online: https://eur-lex.europa.eu/eli/dir/2009/136/oj/eng (accessed on 11 March 2026).
5. Coordination for the Improvement of Higher Education Personnel (CAPES). About the LGPD. 2023. https://www.gov.br/capes/en/access-to-information/privacy-and-personal-data-protection/about-the-lgpd (accessed on 11 March 2026).
6. Korea Legislation Research Institute. Personal Information Protection Act. Korea Legislation Research Institute Website. 2023. Available online: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=62389&lang=ENG (accessed on 11 March 2026).
7. California Department of Justice. California Consumer Privacy Act (CCPA). California Department of Justice website. 2024. Available online: https://oag.ca.gov/privacy/ccpa (accessed on 11 March 2026).
8. Choi, H.; Park, J.; Jung, Y. The role of privacy fatigue in online privacy behavior. *Comput. Hum. Behav.* **2018**, *81*, 42–51.
9. Bradford, A. The Brussels Effect. *Northwestern Univ. Law Rev.* **2015**, *107*, 1–68.
10. Privacy Tech Lab. Privacy-Pioneer-Web-Crawler. Available online: https://github.com/privacy-tech-lab/privacy-pioneer-web-crawler (accessed on 11 March 2026).
11. Acar, G.; Juarez, M.; Nikiforakis, N.; et al. FPDetective: Dusting the Web for Fingerprinters. In Proceedings of the ACM Conference on Computer and Communications Security (CCS), Berlin, Germany, 4–8 November 2013; pp. 1129–1140.
12. Englehardt, S.; Narayanan, A. Online Tracking: A 1-million-site Measurement and Analysis. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS), Vienna, Austria, 24–28 October 2016; pp. 1388–1401.
13. Englehardt, S.; Reisman, D.; Eubank, C.; et al. Cookies That Give You Away: The Surveillance Implications of Web Tracking. In Proceedings of the 24th International Conference on World Wide Web (WWW), Florence, Italy, 18–22 May 2015; pp. 289–299.
14. Roesner, F.; Kohno, T.; Wetherall, D. Detecting and Defending Against Third-Party Tracking on the Web. In Proceedings of the 9th USENIX Symposium on Networked Systems Design and Implementation, San Jose, CA, USA, 25–27 April 2012; pp. 155–168.
15. Lerner, A.; Kornfeld Simpson, A.; Kohno, T.; et al. Internet Jones and the Raiders of the Lost Trackers: An Archaeological Study of Web Tracking from 1996 to 2016. In Proceedings of the 25th USENIX Security Symposium, Austin, TX, USA, 10–12 August 2016; pp. 997–1013.
16. Mayer, J.R.; Mitchell, J.C. Third-Party Web Tracking: Policy and Technology. In Proceedings of the 2012 IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 20–23 May 2012; pp. 413–427.
17. Disconnect, Inc. Disconnect Tracker Protection Lists. 2025. Available online: https://github.com/disconnectme/disconnect-tracking-protection (accessed on 11 March 2026).
18. Zimmeck, S.; Goldelman, D.; Kaplan, O.; et al. Website Data Transparency in the Browser. In Proceedings on Privacy Enhancing Technologies, Online, 15–20 July 2024; pp. 211–234.
19. Degeling, M.; Utz, C.; Lentzsch, C.; et al. We Value Your Privacy ··· Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. In Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, 24–27 February 2019.
20. Sørensen, J.K.; Kosta, S. Before and After GDPR: The Changes in Third Party Presence at Public and Private European Websites. In Proceedings of The Web Conference (WWW '19), San Francisco, CA, USA, 13–17 May 2019; pp. 1590–1600.
21. Veale, M.; Zuiderveen Borgesius, F. Adtech and Real-Time Bidding under European Data Protection Law. *Ger. Law J.* **2022**, *23*, 226–256.
22. Solomos, K.; Ilia, P.; Ioannidis, S.; et al. Clash of the Trackers: Measuring the Evolution of the Online Tracking Ecosystem. 2020. Available online: https://arxiv.org/abs/1907.12860 (accessed on 11 March 2026).
23. Peukert, C.; Bechtold, S.; Batikas, M.; et al. European Privacy Law and Global Markets for Data. 2020. Available online: https://doi.org/10.3929/ethz-b-000406601 (accessed on 11 March 2026).
24. Urban, T.; Tatang, D.; Degeling, M.; et al. Measuring the Impact of the GDPR on Data Sharing in Ad Networks. In

Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (AsiaCCS '20), Taipei, Taiwan, 5–9 October 2020; pp. 222–235.

25. Leenes, R.; Kosta, E. Taming the Cookie Monster with Dutch Law—A Tale of Regulatory Failure. *Comput. Law Secur. Rev.* **2015**, *31*, 317–335.
26. Court of Justice of the European Union. C-311/18, Data Protection Comm'r v. Facebook Ire. Ltd. & Schrems. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62018CJ0311&from=EN (accessed on 11 March 2026).
27. Rubinstein, I.; Margulies, P. Risk and Rights in Transatlantic Data Transfers: EU Privacy Law, U.S. Surveillance, and the Search for Common Ground. *Conn. L. Rev.* **2022**, *54*, 391–456.
28. Birnhack, M.D.; Mundlak, G. The Brussels effect(s) and the rise of a privacy profession. *Int. Data Priv. Law* **2025**, *15*, 138–155.
29. Dabrowski, A.; Merzdovnik, G.; Ullrich, J.; et al. Measuring Cookies and Web Privacy in a Post-GDPR World. In Proceedings of the International Conference on Passive and Active Measurement (PAM 2019), Puerto Varas, Chile, 27–29 March 2019; Volume 11419, pp. 258–270.
30. Trevisan, M.; Traverso, S.; Bassi, E.; et al. 4 Years of EU Cookie Law: Results and Lessons Learned. In Proceedings on Privacy Enhancing Technologies (PoPETs 2019), Online, 16–20 July 2019; pp. 126–145.
31. Matte, C.; Bielova, N.; Santos, C. Do Cookie Banners Respect My Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework. In Proceedings of the 2020 IEEE Symposium on Security and Privacy (IEEE S&P '20), San Francisco, CA, USA, 18–21 May 2020; pp. 791–809.
32. Bollinger, D.; Kubicek, K.; Cotrini, C.; et al. Automating Cookie Consent and GDPR Violation Detection. In Proceedings of the 31st USENIX Security Symposium (USENIX Security'22), Boston, MA, USA, 10–12 August 2022; pp. 2893–2910.
33. Bouhoula, A.; Kubicek, K.; Zac, A.; et al. Automated Large-Scale Analysis of Cookie Notice Compliance. In Proceedings of the 33rd USENIX Security Symposium (USENIX Security'24), Philadelphia, PA, USA, 14–16 August 2024; pp. 1723–1739.
34. Hils, M.; Woods, D.W.; Böhme, R. Measuring the Emergence of Consent Management on the Web. 2020. Available online: https://informationsecurity.uibk.ac.at/pdfs/HWB2020_Consent_Management_IMC.pdf (accessed on 11 March 2026).
35. Machuletz, D.; Böhme, R. Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR. In Proceedings on Privacy Enhancing Technologies (PoPETs 2020), Virtual, 13–17 July 2020; pp. 481–498.
36. Nouwens, M.; Kristensen, J.B.; Maalt, K.; et al. A Cross-Country Analysis of GDPR Cookie Banners and Flexible Methods for Scraping Them. In Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems, Yokohama, Japan, 26 April–1 May 2025.
37. Nouwens, M.; Liccardi, I.; Veale, M.; et al. Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20), Honolulu, HI, USA, 25–30 April 2020; pp. 1–13.
38. Khandelwal, R.; Linden, T.; Harkous, H.; et al. PriSEC: A Privacy Settings Enforcement Controller. In Proceedings of the 30th USENIX Security Symposium, Online, 11–13 August 2021; pp. 465–482.
39. Hausladen, K.; Wang, O.; Eng, S.; et al. Websites' Global Privacy Control Compliance at Scale and over Time. In Proceedings of the 34th USENIX Security Symposium (USENIX Security 2025), Seattle, WA, USA, 13–15 August 2025; pp. 5837–5856.
40. Zimmeck, S.; Wang, O.; Alicki, K.; et al. Usability and Enforceability of Global Privacy Control. In Proceedings of the 23rd Privacy Enhancing Technologies Symposium (PETS 2023), Lausanne, Switzerland, 10–15 July 2023; pp. 265–281.
41. Rasaii, A.; Dao, H.; Feldmann, A.; et al. Intractable Cookie Crumbs: Unveiling the Nexus of Stateful Banner Interaction and Tracking Cookies. *arXiv* **2025**, arXiv:2506.11947.
42. IAB Europe. TCF—Transparency & Consent Framework. Available online: https://iabeurope.eu/transparency-consent-framework/ (accessed on 11 March 2026).
43. Zimmeck, S. Opting Out May Not Prevent Websites from Collecting Your Data. 2021. Available online: (accessed on 11 March 2026).
44. Tang, B.; Bui, D.; Shin, K.G. Navigating Cookie Consent Violations Across the Globe. In Proceedings of the 34th USENIX Conference on Security Symposium, Seattle, WA, USA, 13–15 August 2025.
45. Frankenreiter, J. Cost-Based California Effects. *Yale J. Regul.* **2022**, *39*, 1155–1217.
46. Ogut, A.; Turanlioglu, B.; Metiner, D.C.; et al. Dissecting Privacy Perspectives of Websites Around the World: "Aceptar Todo, Alle Akzeptieren, Accept All. . ." In Proceedings of the 33rd USENIX Security Symposium, Philadelphia, PA, USA, 14–16 August 2024; pp. 2849–2863.
47. Eijk, R.V.; Asghari, H.; Winter, P.; et al. The Impact of User Location on Cookie Notices (Inside and Outside of the European Union). *arXiv* **2021**, arXiv:2110.09832.
48. Bellman, S.; Johnson, E.J.; Kobrin, S.J.; et al. International Differences in Information Privacy Concerns: A Global Survey of Consumers. Available online: https://business.columbia.edu/sites/default/files-efs/imce-uploads/CDS/1172.pdf (accessed on 11 March 2026).
49. Fleming, P.; Bayliss, A.P.; Edwards, S.G.; et al. The role of personal data value, culture and self-construal in online privacy behaviour. *PLoS ONE* **2021**, *16*, e0253568.

50. Hua, J.; Wang, P. Cultural differences in privacy protection: A case study of DiDi privacy violations. *Issues Inf. Syst.* **2023**, *24*, 304–319.
51. Xu, M.; Žiga Jug.; TamoLarrieux, A. A cross-cultural analysis of transparency: the interplay of law, privacy policies, and user perceptions. *Int. Data Priv. Law* **2024**, *14*, 197–222.
52. Birrell, E.; Rodolitz, J.; Ding, A.; et al. SoK: Technical Implementation and Human Impact of Internet Privacy Regulations. In Proceedings of the 2024 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2024; pp. 673–696.
53. Solove, D.J. The Limitations of Privacy Rights. *Notre Dame Law Rev.* **2023**, *98*, 975–1036.
54. Practical Law Canada Commercial Transactions. The Extra-Territorial Reach of PIPEDA: T. (A.) v. Globe24h.com. Available online: https://ca.practicallaw.thomsonreuters.com/w-005-9407?transitionType=Default&contextData=(sc.Default)&firstPage=true (accessed on 11 March 2026).
55. Personal Data Protection Commission Singapore. Advisory Guidelines on Key Concepts in the Personal Data Protection Act. Available online: https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/ag-on-key-concepts/advisory-guidelines-on-key-concepts-in-the-pdpa-17-may-2022.pdf (accessed on 11 March 2026).
56. Personal Information Protection Commission. Guidelines on Applying the Personal Information Protection Act to Foreign Business Operators. Available online: https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS217&mCode=D010030000&nttId=10059 (accessed on 11 March 2026).
57. EUR-Lex. Judgment of the Court (Grand Chamber) of 4 July 2023. Meta Platforms Inc and Others v Bundeskartellamt. Request for a Preliminary Ruling from the Oberlandesgericht Düsseldorf. 2023. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62021CJ0252 (accessed on 11 March 2026).
58. EUR-Lex. Judgment of the Court (Grand Chamber) of 1 October 2019. Bundesverband der Verbraucherzentralen und Verbraucherverbände— Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH. Request for a Preliminary Ruling from the Bundesgerichtshof. 2019. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62017CJ0673 (accessed on 11 March 2026).
59. Zuiderveen Borgesius, F.J. Personal data processing for behavioural targeting: which legal basis? *Int. Data Priv. Law* **2015**, *5*, 163–176.
60. Autoridade Nacional de Proteção de Dados. Cookies e proteção de dados pessoais. Available online: https://www.gov.br/ anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf (accessed on 11 March 2026).
61. Personal Data Protection Commission Singapore. Advisory Guidelines on The Personal Data Protection Act (PDPA) for Selected Topics. Available online: https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/ag-on-selected-topics/advisory-guidelines-on-the-pdpa-for-selected-topics-(revised-may-2024).pdf (accessed on 11 March 2026).
62. Information Regulator South Africa. Guidance Note on Direct Marketing. Available online: https://inforegulator.org.za/wp-content/uploads/2020/07/GUIDANCE-NOTE-ON-DIRECT-MARKETING-IN-TERMS-OF-THE-PROTECTION-OF-PERSONAL-INFORMATION-ACT-4-OF-2013-POPIA.pdf (accessed on 11 March 2026).
63. Office of the Australian Information Commissioner. Tracking pixels and privacy obligations. Available online: https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/tracking-pixels-and-privacy-obligations (accessed on 11 March 2026).
64. Office of the Privacy Commissioner of Canada. Guidelines on privacy and online behavioural advertising. Available online: https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/tracking-and-ads/gl_ba_1112/ (accessed on 11 March 2026).
65. State of California Department of Justice. CCPA Enforcement Case Examples. Available online: https://oag.ca.gov/privacy/ccpa/enforcement (accessed on 11 March 2026).
66. Verwaltungsgericht Hannover. Urt. v. 19.03.2025, Az.: 10 A 5385/22. Available online: https://voris.wolterskluwer-online.de/browse/document/230df5cf-d76c-4561-9499-e44445a96f11 (accessed on 11 March 2026).
67. Agencia Española de Protección de Datos. Procedimiento Nº: EXP202309901 (PS/00284/2024. Available online: https://www.aepd.es/documento/ps-00284-2024.pdf (accessed on 11 March 2026).
68. CMS. GDPR Enforcement Tracker. Available online: https://www.enforcementtracker.com/?insights (accessed on 11 March 2026).
69. Office of the Australian Information Commissioner. Landmark settlement of $50m from Meta for Australian users impacted by Cambridge Analytica incident. Available online: https://www.oaic.gov.au/news/media-centre/landmark-settlement-of-$50m-from-meta-for-australian-users-impacted-by-cambridge-analytica-incident (accessed on 11 March 2026).
70. Office of the Privacy Commissioner of Canada. Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia. Available online: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/ (accessed on 11 March 2026).
71. Werner, J. South Korea's PIPC Fines Meta for Unauthorized Use of Sensitive Data and Privacy Violations. Available online: https://babl.ai/south-korea-pipc-fines-meta-for-unauthorized-use-of-sensitive-data-and-privacy-violations/ (accessed on 11 March 2026).
72. State of California Department of Justice. California Won't Let It Go: Attorney General Bonta Announces $2.75 Million Settlement with Disney, Largest CCPA Settlement in California History. Available online: https://oag.ca.gov/news/press-

releases/california-wont-let-it-go-attorney-general-bonta-announces-275-million (accessed on 11 March 2026).

73. State of California Department of Justice. Attorney General Bonta Announces Largest CCPA Settlement to Date, Secures $1.55 Million from Healthline.com. Available online: https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-largest-ccpa-settlement-date-secures-155 (accessed on 11 March 2026).
74. State of California Department of Justice. Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act. Available online: https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement (accessed on 11 March 2026).
75. Connecticut Office of the Attorney General. Connecticut, California and Colorado Announce Joint Investigative Privacy Sweep. Available online: https://portal.ct.gov/ag/press-releases/2025-press-releases/connecticut-california-and-colorado-announce-joint-investigative-privacy-sweep (accessed on 11 March 2026).
76. California Privacy Protection Agency. Youth Sports Media Company to Pay $1.10 Million Fine, Change Practices Over Privacy Violations. Available online: https://privacy.ca.gov/2026/03/youth-sports-media-company-to-pay-1-1-million-fine-change-practices-over-privacy-violations/ (accessed on 11 March 2026).
77. California Privacy Protection Agency. Ford to Change Practices, Pay Fine for Adding Unnecessary Friction to Opt-Out Process. Available online: https://privacy.ca.gov/2026/03/ford-to-change-practices-pay-fine-for-adding-unnecessary-friction-to-opt-out-process/ (accessed on 11 March 2026).
78. Luz, J.C.J. Lessons from Brazilian DPA sanctions to date. Available online: https://iapp.org/news/a/lessons-from-brazilian-dpa-sanctions-to-date (accessed on 11 March 2026).
79. Le Pochat, V.; Van Goethem, T.; Tajalizadehkhoob, S.; et al. Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation. *arXiv* **2018**, arXiv:1806.01156.
80. Selenium Project. WebDriver. Available online: https://www.selenium.dev/documentation/webdriver/ (accessed on 11 March 2026).
81. Mozilla Support. Enhanced Tracking Protection in Firefox for Desktop. Available online: https://support.mozilla.org/en-US/kb/enhanced-tracking-protection-firefox-desktop (accessed on 11 March 2026).
82. Oracle Corporation. MySQL Installer for Windows. Available online: https://dev.mysql.com/downloads/installer/ (accessed on 11 March 2026).
83. BuiltWith Pty Ltd. BuiltWith Technology Lookup. Available online: https://builtwith.com/ (accessed on 11 March 2026).
84. IAB Tech Lab. Global-Privacy-Platform. Available online: https://github.com/InteractiveAdvertisingBureau/Global-Privacy-Platform (accessed on 11 March 2026).
85. Becerra, X. Available online: https://twitter.com/AGBecerra/status/1354850758236102656 (accessed on 11 March 2026).
86. Colorado Department of Law. Universal Opt-Out Shortlist. Available online: https://coag.gov/uoom/ (accessed on 11 March 2026).
87. Office of the Attorney General. The Connecticut Data Privacy Act. Available online: https://portal.ct.gov/ag/sections/privacy/the-connecticut-data-privacy-act (accessed on 11 March 2026).
88. New Jersey Division of Consumer Affairs. New Jersey Data Privacy Law FAQs. Available online: https://www.njconsumeraffairs.gov/ocp/Pages/NJ-Data-Privacy-Law-FAQ.aspx (accessed on 11 March 2026).
89. Oregon Department of Justice. Consumer Privacy. Available online: https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/privacy/ (accessed on 11 March 2026).
90. European Commission. Digital Omnibus Regulation Proposal. Available online: https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal (accessed on 11 March 2026).