Cross-Jurisdictional Compliance with Privacy Laws: How Websites Adapt Consent Notices to Regional Regulations

Xander Smeets[1 [0000−0002−1773−3062]], Michele Campobasso[2 [0000−0002−5247−7711]], and Nicola Zannone[1 [0000−0002−9081−5996]]

[1] Eindhoven University of Technology
x.l.j.a.smeets@student.tue.nl, n.zannone@tue.nl
[2] Forescout Technologies
michele.campobasso@forescout.com

Abstract. Tracking cookies have been widely used for targeted advertising, raising privacy concerns due to their invasive nature. In response, jurisdictions such as the EU, UK, California, and Canada have enacted privacy laws to regulate online tracking. This study examines the compliance of 535 websites with these laws. To do so, we define a set of legal requirements and assess website compliance through region-specific simulated visits. Consistent with prior research, we find widespread privacy violations. Additionally, websites that adapt their privacy interfaces based on visitor location tend to violate EU and UK regulations more frequently while showing higher compliance with Californian requirements. No significant compliance trend was observed for Canadian regulations.

Keywords: Cookie, Consent, Cookie Banner, Legal Compliance

1 Introduction

In recent years, organizations have extensively collected user behavior data to create profiles for targeted advertising [66, 70]. However, large-scale data collection raises significant privacy concerns. To address these concerns, several jurisdictions have enacted privacy laws. For instance, California introduced the California Consumer Privacy Act (CCPA) [64], while the EU implemented the ePrivacy Directive [19] and the General Data Protection Regulation (GDPR) [20]. The ePrivacy Directive mandates user consent before placing cookies, and the GDPR establishes legal criteria for valid consent.

In response to privacy laws, many websites display *consent notices* (also known as cookie banners) asking users to accept cookies. However, research shows that these notices often fail to meet legal requirements [47, 56]. This is unsurprising, as targeted advertising—heavily reliant on cookies—remains a key revenue source for many websites [3, 40], creating incentives for manipulative consent mechanisms [61]. Most studies on privacy legislation and consent notices focus on a single jurisdiction, such as the EU [46, 56, 55] or California [68]. Moreover, little research has examined whether websites adapt privacy interfaces based on user location. Understanding whether and how websites adjust to different legal frameworks is crucial for assessing the effectiveness of privacy laws, identifying variations in compliance, and evaluating geographic disparities in user privacy protections. Investigating cross-jurisdictional compliance can

offer insights into whether companies prioritize certain regulations over others and help policymakers refine enforcement strategies.

This study aims to assess website compliance with privacy laws across four jurisdictions—the EU, the UK, California, and Canada—focusing on legal requirements for consent and privacy options. To this end, we analyze 535 websites from the EU, the UK, the US, and Canada across three categories: news, e-commerce, and government. We examine the privacy laws of these four jurisdictions to identify legal requirements on consent and privacy settings. Compliance is evaluated by simulating visits from different regions to determine adherence to these requirements. Additionally, we investigate whether websites modify their privacy interfaces based on visitor location and analyze how this behavior influences compliance.

Our main contributions are as follows:

- Our analysis of privacy regulations provides a consolidated and updated overview of the legal requirements applicable to consent notices across multiple jurisdictions.
- Our study shows that websites comply more with local regulations than with extraterritorial ones, even when laws such as the GDPR and CCPA extend beyond their borders. This highlights the challenges of enforcing extraterritorial privacy laws and their impact on compliance.
- Our results also show that websites adapt privacy options to visitor location rather than applying the strictest regulation. This suggests that privacy is primarily perceived as a compliance obligation, highlighting the need to explore incentives for stronger privacy protections.
- Our findings indicate that privacy laws defining precise interface requirements, such as the CCPA, promote more standardized privacy controls, while technology-agnostic regulations such as the GDPR result in significant variation.

The remainder of the paper is organized as follows. Section 2 discusses the legal background for privacy interfaces and prior work on privacy choices on the Internet. Section 3 introduces our research questions and describes the methodology for answering them. Section 4 provides an overview of our results and answers to the research questions. Section 5 discusses the implications of our work. Finally, Section 6 concludes the paper.

2 Background and Related Work

2.1 Legal Frameworks

This section reviews the most relevant legislation in the EU, UK, US, and Canada.

European Union: The European Union has enacted several directives and regulations related to privacy. The most relevant to our work are the ePrivacy directive and the GDPR.

ePrivacy directive: The ePrivacy directive [19] defines obligations for telecommunications service providers. In particular, article 5(3) requires the explicit and informed consent of the users before cookies (or any other form of data) can be stored or read from their devices [16, 37, 38]. The only exception to this rule applies to cookies which are strictly necessary[3] to transmit data over the network [1] or to provide services that have been explicitly requested by the user.

[3] The necessity should be from the user's perspective, not the website's [1].

Table 1: GDPR consent aspects.

GDPR consent aspect	Description
Freely given	User should be provided with a *genuine choice* between giving and refusing consent [20, rec. (42)].
Specific	Consent should be given for *specific purposes* [20, art. 6(1)(a)]. This is usually interpreted as requiring separate consent for each of the purposes for which processing of data is desired [25].
Informed	Users should be *made aware* of the *identity of the data controller* (i.e., the organization determining how and for what purposes data is processed [20, art. 4(7)]), as well as the *purposes of the data processing* [20, rec. (42)]. In addition, the information provided to the user must be *clear and comprehensive* [25].
Unambiguous	Consent needs to be expressed through a *clear and affirmative action of the user* [25].

GDPR: The GDPR [20] grants users several privacy rights and imposes obligations on organizations processing data of individuals in the European Economic Area (EEA). One key obligation is to establish a legal basis for data processing [20, art. 6(1)], which must be one of the following: (1) consent, (2) performance of a contract, (3) compliance with a legal obligation, (4) vital interests, (5) public interest, or (6) legitimate interests. As noted before, the ePrivacy Directive mandates consent as the legal basis when storing non-essential data (e.g., cookies) on a user's device. For consent to be valid, it must be *freely given*, *specific*, *informed*, and *unambiguous* [20, art.4(11)], hereafter referred to as *GDPR consent aspects* (Table 1). Additionally, consent requests must be clearly distinguishable from other matters [20, art.7(2)], and users must be informed of their right to withdraw consent, which must be as easy as granting it [20, art. 7(3)].

United Kingdom: Despite Brexit, the privacy-related EU regulations still largely apply in the UK. For instance, Article 5 of the ePrivacy directive and article 6 of the Privacy and Electronic Communications (EC Directive) Regulations [59] have been incorporated in UK law. In addition, the UK has chosen to retain the GDPR as part of its domestic law as part of the *European Union (Withdrawal) Act* [52]. The UK has, however, made some modifications to the GDPR as it applies in the UK [58]. The resulting version of the GDPR is known as the UK GDPR [21]. For our study, the UK GDPR can be considered equivalent to the EU's GDPR.

California: The California Consumer Privacy Act (CCPA) [64], later amended by the California Privacy Rights Act (CPRA) [65], establishes privacy rights for California residents, even when temporarily outside the state [64, § 1798.140(i)]. It grants individuals control over their personal data and imposes obligations on businesses handling such information. In particular, the CCPA grants rights to delete [64, §1798.105], correct [64, §1798.106], and access [64, §1798.110] personal data. Additionally, businesses must provide a 'notice at collection'[63, § 7012(a)], informing users about data collection, its intended use, and whether the data is sold or shared. However, unlike the GDPR, which regulates data collection, the CCPA primarily governs data use after collection. This distinction is highlighted in the California Code of Regulations, which states that cookie banners alone do not satisfy opt-out requirements for data sale or sharing [63, § 7026(a)(4)]. Businesses that sell or share personal data must provide an opt-out option and inform users via a '*Do Not Sell or Share My Personal Information*' (DNSMPI) [68]) link on their homepage. Those processing *sensitive* personal information must also offer a '*Limit the Use of My Sensitive Personal Information*' link [63, §7014], though both may be combined into a single '*Your Privacy Choices*' or '*Your California Privacy Choices*' link with a designated opt-out icon [63, § 7015].

It is worth noting that CCPA obligations apply only to businesses meeting at least one of the following criteria [64, §1798.140(d)(1)]: (1) annual gross revenue exceeding $25 million, (2) buying, selling, or sharing the personal information of at least 100,000 consumers, or (3) deriving at least 50% of revenue from selling or sharing personal information. Nonprofits and government agencies are exempt [44].

Canada: Canada has two privacy laws similar to those in the EU: the Personal Information Protection and Electronic Documents Act (PIPEDA) [49] and Canada's Anti-Spam Legislation (CASL) [50]. PIPEDA mandates businesses to follow privacy principles when handling personal data, while CASL regulates the installation of *'computer programs'*, including cookies. In case of conflict, CASL takes precedence [50, §2].

PIPEDA: PIPEDA applies the National Standard of Canada's personal information protection principles [49, Sched. 1] to organizations. These principles include: (1) accountability, (2) identifying purposes, (3) consent, (4) limiting collection, (5) limiting use, disclosure, and retention, (6) accuracy, (7) safeguards, (8) openness, (9) individual access, and (10) challenging compliance. The second and third principles are the most relevant for our work. The second principle requires organizations to identify and disclose the purposes for collecting and using personal information, generally before collection. Previously collected data can only be repurposed after obtaining user consent. The third principle mandates knowledgeable consent before collecting, using, or sharing personal data, similar to GDPR's informed consent. Users must be able to withdraw consent at any time, and consent cannot be a condition for accessing goods or services, aligning with EU regulations. However, unlike EU law, PIPEDA allows implied consent; for example, not checking a box can be considered valid consent [49, Sched.1, §4.3.7(b)], whereas the EU requires explicit user action (i.e., no pre-ticked boxes).

Although PIPEDA applies broadly to "organizations" [49, §4(1)], some are exempted, similar to California's CCPA. Notably, government institutions (as defined in Canada's Privacy Act [51]) are excluded. Additionally, PIPEDA does not apply to intra-provincial data activities when a province has privacy laws deemed "substantially similar" [49, §26(2)(b)]. Currently, this exemption applies in several provinces [48].

Canada's anti-spam legislation: CASL prohibits the installation of computer programs without the express consent of the owner or authorized user of a computer located in Canada [50, §8(2)]. The law defines "computer programs" broadly, covering cookies, HTML, JavaScript, and any executable code that runs via another program previously installed with consent [50, §10(8)(a)]. When expressing consent is required, users must be informed of both the purpose of the consent request [50, §10(1)(a)] and the function of the program being installed [50, § 10(3)]. Although this rule resembles the EU ePrivacy Directive, CASL presumes user consent for certain programs, including cookies, unless users explicitly indicate otherwise [50, §10(8)(b)]. In practice, this means a user is considered to have consented unless they disable cookies in their browser [10].

2.2 Consent Gathering and Enforcement

Websites use various methods to collect user consent, and these methods vary depending on regulatory frameworks in place. Common methods, especially in the EU and UK, include consent notices (e.g., Fig. 1) that inform users about the use of cookies and

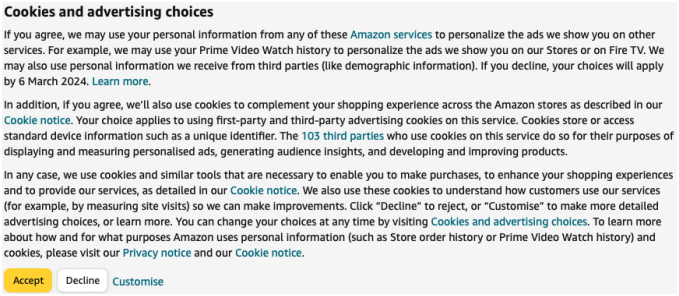

Fig. 1: `Amazon` consent notice

third-party data sharing while providing options to accept or reject cookies with different levels of granularity. Some jurisdictions rely on implied consent, treating continued site usage as agreement, while others (e.g., California) mandate opt-out mechanisms.

The design of consent notices strongly influence user decisions, often raising concerns about legal compliance. Despite existing regulations, many websites employ deceptive or non-compliant mechanisms, driven by the profitability of targeted advertising. Research on this issue primarily examines two interconnected aspects: the use of *dark patterns* in consent interfaces and their *compliance with legal requirements*. While dark patterns are used to manipulate users into consenting, studies focusing on legal compliance assess whether organizations meet the requirements outlined in privacy laws.

Dark patterns are deceptive design techniques that nudge users toward choices favoring the organization rather than their own privacy interests. First introduced by Brignull [8, 9], these techniques have been systematically categorized in various taxonomies [24]. For instance, the consent notice in Fig. 1 exemplifies the 'interface interference' dark pattern by visually prioritizing the 'Accept' button to encourage user consent. The widespread use of dark patterns raises concerns about compliance with privacy regulations. Recognizing their manipulative nature, the European Data Protection Board (EDPB) advises against their use [17], while regulations such as the Digital Services Act [22], Digital Markets Act [23], and California's CCPA [64] explicitly prohibit them. Several studies have examined the prevalence of dark patterns on websites and their impact on user interactions with consent notices [4, 5, 28, 67]. Soe et al. [61] manually analyzed 300 news websites and found that 297 employed some form of dark pattern in their consent mechanisms. Gunawan et al. [26] compared websites and mobile apps offering the same services, revealing that every service used at least one dark pattern, with notable variations between platforms. Similarly, Habib et al. [28] found that 88% of 603 UK websites utilized at least one dark pattern. Kirkman et al. [36] developed an automated system to detect dark patterns, identifying 3,744 instances across 2,417 consent notices.

Most studies on legal compliance have primarily examined the GDPR, leaving other regulations comparatively underexplored. Santos et al. [56] define six legal requirements for cookie banner text in the EU, emphasizing clarity, specificity, and informed consent. Paci et al. [46] assessed the compliance of Android apps, categorizing consent requirements into six key aspects, including prior consent, specificity, and ease of revocation. Similarly, Santos et al. [55] identify 22 legal requirements based on the ePrivacy direc-

tive and GDPR, highlighting additional concerns such as readability and accessibility. Van Nortwick and Wilson [68] investigate compliance with the CCPA, particularly the requirement for a 'Do Not Sell My Personal Information' link on websites. Their study also considers whether or not DNSMPI links are hidden for users outside California, as well as exemptions to the CCPA.

While many studies have examined the compliance of privacy interfaces across a diverse set of popular websites, often selected using the Tranco list or market research reports [6, 27, 28, 35, 39, 47, 54, 56, 68], only a few have investigated how these interfaces vary based on user location. Dabrowski et al. [12] found that websites commonly request cookie consent only when accessed from the EU, while US visitors receive no such prompts. Rasaii et al. [54] observed a higher prevalence of consent notices for EU users compared to those outside the EU. Van Eijk et al. [18] further examined the role of top-level domains (TLDs) and found that TLDs strongly predict consent notice prevalence, whereas user location had a limited effect, except for `.com` domains where location did influence notice display. Given the discrepancies in findings, further research is needed.

Beyond improperly obtaining consent, another major privacy violation occurs when websites disregard users' choices. Several studies have examined the enforcement of user decisions, revealing that consent refusals are often mishandled [39, 47]. For example, research has shown that some websites record users as having given consent even when they have not [39]. Moreover, tracking is not limited to cookies—fingerprinting and other tracking techniques are often used even when users explicitly reject cookie-based tracking [47]. In some cases, rejecting consent has paradoxically increased the number of third parties receiving user data [47]. To counteract such practices, Bollinger et al. [6] developed CookieBlock, a browser extension that uses machine learning to categorize cookies and enforce user preferences. Privacy violations are not limited to websites—similar issues have been found in mobile applications. Several studies have shown that many Android apps share user data with third parties without first requesting consent [38, 42, 43]. Nguyen et al. [42] analyzed these violations by examining the third-party domains contacted by mobile apps, highlighting the extent of unauthorized data sharing.

2.3 Gaps in Prior Work

Most prior studies have primarily focused on the requirements imposed by the EU's ePrivacy Directive and GDPR. While some works have examined privacy regulations outside the EU, they typically analyze non-EU legislation in isolation rather than in conjunction with EU laws. As a result, little is known about how websites adapt their privacy interfaces when serving users in different regulatory environments. Investigating these differences is important for assessing whether websites tailor their privacy practices to the legal obligations of the user's jurisdiction, or maintain a uniform approach irrespective of user location. To the best of our knowledge, only a few studies have explored the impact of user location on privacy interfaces. Notably, Van Eijk et al. [18] examined regional differences in consent notices but focused primarily on visual characteristics, such as notice presence, height, word count, and button/link counts, leaving a more detailed analysis for future work. Similarly, Rasaii et al. [54] investigated how user location affects consent notices and the availability of CCPA-mandated DNSMPI links but did not comprehensively assess compliance with broader CCPA requirements.

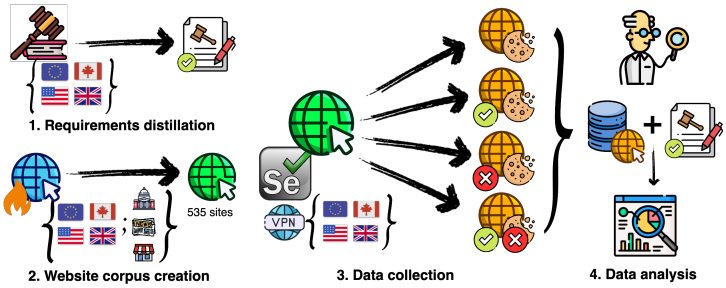

Fig. 2: A schematic overview of the methodology.

By systematically analyzing privacy interfaces and compliance across multiple jurisdictions, our study offers insights into how regulatory frameworks influence website behavior. If privacy interfaces and compliance levels vary significantly across countries, this suggests that regulatory requirements play a dominant role in driving privacy practices rather than a website's internal privacy policies or user-centric commitments. Understanding such patterns is valuable for regulators evaluating the impact of different legal frameworks, and for users and consumer associations assessing how companies handle privacy across jurisdictions.

3 Methodology

The gap identified in the previous section leads us to the following research questions:

RQ1 *To what extent do the origin and category of websites determine whether they present different privacy-related interfaces to visitors from different regions?*

RQ2 *To what extent do the origin and category of websites determine whether they comply with the requirements posed by the privacy legislation that applies by virtue of the location of their visitors?*

RQ3 *If websites present different privacy-related interfaces to visitors from different regions, are they more likely to comply with privacy regulations?*

These questions aim to provide an understanding of how user location influences the privacy mechanisms displayed by websites.

Fig. 2 shows an overview of the methodology used to answer the research questions. First, we distilled a set of requirements to be met by websites from privacy regulations and prior work (Section 3.1). Then, we created a corpus of websites (Section 3.2). Next, we collected data on the websites in our corpus from the perspective of each region (Section 3.3). Finally, we analyzed each website's compliance with the identified requirements and used regression models to answer our research questions (Section 3.4).

3.1 Requirements Distillation

From the legal frameworks discussed in Section 2.1, we obtained the requirements from the associated privacy laws and prior work. The requirements were initially defined by one of the authors and iteratively refined with the other authors until a consensus was

Table 2: Requirements applying to sites under EU privacy laws.

ID	Requirement	GDPR consent aspect	Sources
EU01	A consent notice should contain a visibly highlighted link to the privacy/cookie policy.	Informed	[2, 17]
EU02	The consent notice text should be readable.	Informed	[17, 55]
EU03	The purposes for which cookies are being stored should be explicitly mentioned in the consent notice/privacy policy.	Informed	[2, 13, 17]
EU04	Expiration date of cookies should be disclosed to users when obtaining consent.	Informed	[17, 71]
EU05	Third party sharing should be disclosed to users when obtaining consent.	Informed	[17, 71]
EU06	Links to privacy policy of third party should be provided.	Informed	[17, 71]
EU07	Controller's identity is present in privacy policy.	Informed	[14, 55]
EU08	What cookies are being stored is present in the cookie policy.	Informed	[14]
EU09	The existence of the right to withdraw consent should be present in the notice.	Informed	[14]
EU10	Emotional language should not be used.	Informed	[17]
EU11	The legal basis for processing must be mentioned.	Specific	[13]
EU12	Consent must be given separately for each purpose.	Specific	[15, 17, 55]
EU13	The accept and reject mechanisms should be displayed using the same type of form element, and at the same level of the consent notice.	Freely given	[17]
EU14	If a form element is highlighted, it must be the most restrictive one (i.e. the most privacy-friendly one).	Freely given	[15]
EU15	Rejection of consent should be as easy as giving consent.	Freely given	[15, 17]
EU16	There should be no pre-selected boxes in any level of the consent notice.	Freely given	[17, 55, 71]
EU17	Legitimate interest should not be used as a legal basis for storing non-necessary cookies.	Freely given	[16, 37, 38, 42, 43]
EU18	The font size in a consent notice should be readable.	Unambiguous	[17]
EU19	Conditional tense should not be used in a consent notice.	Unambiguous	[17]
EU20	After withdrawing consent, non-necessary cookies should not be present.	Unambiguous	[14]
EU21	A consent notice should produce a visual effect when interacted with.	Unambiguous	[17]
EU22	If consent is declined, no non-necessary cookies should be placed.	Freely given	[17]
EU23	No non-necessary cookies should be placed without user interaction.	Freely given	[6, 17, 55]
EU24	Consent must be withdrawable via the same electronic interface.	Freely given	[14, 55]
EU25	A site's content must be accessible without providing consent. (e.g. no cookie walls)	Freely given	[17, 55]

reached. These requirements, outlined in Tables 2, 3, and 4, served as the foundation for systematically evaluating websites' compliance with privacy obligations.

3.2 Website Corpus Creation

For our study, we built a corpus of websites based on two properties: geographic *origin* and *category*. We selected sites from the countries covered in the legal requirements analysis (Section 2.1) to examine compliance with different regulations. The included websites span over three categories—*news*, *government*, and *e-commerce*—to explore how the type of organization affects compliance. These categories were selected based on their distinct business model: news websites often rely on advertising revenue, e-commerce platforms use tracking to personalize product recommendations, and government websites are typically non-profit. Government websites serve as a baseline in our study, as they are expected to adhere more closely to their country's legal privacy frameworks.

We built our corpus using country- and category-specific lists of popular websites provided by PressGazette and market research firms Semrush and SimilarWeb.[4] These sources yielded 1025 unique websites across all countries and categories. To assess the reliability of this list, we used Cloudflare Gateway to check whether each website exists and whether its origin and category match the original classification. Due to limited access to Cloudflare's API, we developed a configurable DNS resolver that selectively queried

[4] We excluded sources, like the Tranco list, that lack information on website origin or category.

Table 3: Requirements applying to sites under Californian privacy laws.

ID	Requirement	Sources
US01	If information is shared with third parties, the website should show a 'Do Not Sell or Share My Personal Information' link in the header or footer of the homepage.	[64, § 1798.135(a)(1)] [63, § 7015(a)] [63, § 7013(c)]
US02	Before or at the moment of collecting users' personal information, (a link to) a notice at collection should be provided to them.	[63, § 7012(c)]
US03	If the notice at collection is provided using a link to a privacy policy, then the link should bring the user to the part of the privacy policy containing the required information.	[63, § 7012(f)]
US04	The notice at collection should include a list of the categories of personal information which is gathered.	[63, § 7012(e)(1)]
US05	The notice at collection should include the purposes for which (categories of) personal information are collected and used.	[63, § 7012(e)(2)]
US06	The notice at collection should describe whether each category of information is sold or shared.	[63, § 7012(e)(3)]
US07	The notice at collection should include the retention period for each category of personal information (or the criteria used to determine that period).	[63, § 7012(e)(4)]
US08	If the business sells or shares personal information, the notice at collection should include a link to a notice of right to opt-out of sale/sharing.	[63, § 7012(e)(5)]
US09	The notice at collection should include a link to the business's privacy policy.	[63, § 7012(e)(6)]
US10	If the business uses and/or discloses sensitive personal information, the website should show a 'Limit the Use of My Sensitive Personal Information' link in the header or footer of the homepage.	[64, § 1798.135(a)(1)] [63, § 7014(c)]
US11	A business should provide an email address for submitting requests to delete, correct, and know if it operates exclusively online. Otherwise, it should provide both a toll-free telephone number and a website-based method for submitting such requests.	[64, § 1798.130(a)(1)(A, B)] [63, § 7020(a, b)]
US12	The user should not be required to create an account to exercise the right to opt-out of sale/sharing.	[64, § 1798.135(c)(1)] [63, § 7026(c)]
US13	The user should not be required to create an account to exercise the right to limit the use and disclosure of sensitive personal information.	[64, § 1798.135(c)(1)] [63, § 7027(d)]
US14	The business should not discriminate against the user for exercising their rights.	[64, § 1798.125(a)(1)]

Table 4: Requirements applying to sites under Canadian privacy laws.

ID	Requirement	Sources
CA01	The purposes for which personal information is collected shall be made available to users at/ before the time of collection of personal information.	[49, Sched. 1, § 4.2.3]
CA02	Consent must be obtained for the collection, use and disclosure of personal information.	[49, Sched. 1, § 4.3.1]
CA03	Consent must not be required as a condition of the supply of a product or service (beyond what is required to fulfil the explicitly specified, and legitimate purposes).	[49, Sched. 1, § 4.3.3]
CA04	Consent must be withdrawable at any time (subject to legal or contractual restrictions and reasonable notice).	[49, Sched. 1, § 4.3.8]
CA05	Cookies which are legally placed by a third party should not technically present themselves as first-party cookies.	[45]

websites in specific Cloudflare categories, enabling us to retrieve data for all candidate sites. We excluded websites that were inaccessible or whose origin or category did not align with the initial classification (e.g., a US website popular in Canada). This resulted in a final set of 535 unique websites, distributed by origin and category as shown in Table 5.

3.3 Data Collection

We assume that websites must comply with the privacy laws of the country where the user is physically located at the time of access, which is typically determined using their IP address. Accordingly, we assess the compliance of a website with a given law if the user's IP address originates from the country where the law applies. To this end, we accessed the websites in our corpus using an IP address from each country through a VPN. For every location, we collected the source code of the webpage and video recordings demonstrating and navigating the consent notices and privacy policy on every website. Additionally, we stored the cookies present on the website, categorized by type, such as necessary, analytics, or advertising. For the EU and UK, we recorded the cookies at multiple stages:

Origin	Category			Total
	News	E-commerce	Government	
EU	90	67	58	215
UK	30	30	34	94
US	30	34	58	122
Canada	30	38	36	104
Total	180	169	186	535

Table 5: An overview of the number of sites from each origin and category.

(i) before any user interaction, *(ii)* after giving consent, *(iii)* after rejecting consent, and *(iv)* after giving consent, withdrawing it, and refreshing the page. For California, we captured cookies after giving consent and observed the website's response to the Global Privacy Control signal [53]. For Canada, we collected cookies after giving consent and after opting out of cookies. This comprehensive data collection provided the foundation for evaluating how websites from different countries comply with privacy regulations.

We recall that the CCPA does not apply to non-profit organizations, government agencies, or websites that fail to meet any of the criteria specified in Section 2.1. Websites that do not meet these criteria were removed from the data collection process when websites were visited using an IP address from California. To determine whether a website was owned by a non-profit or government organization, we manually reviewed the website content. We also evaluated whether the website had at least 100,000 visitors from California using Semrush data [68] and whether its owning organization had annual revenues exceeding $25 million by gathering from freely available corporate records and online resources, including market research firms and Wikipedia. This approach ensured that our analysis focused solely on websites subject to the CCPA's jurisdiction.

We accessed all websites using Google Chrome, with the collection process partially automated using Python and Selenium [62]. Automation handled tasks such as navigation, cookie management, and data recording, while manual supervision ensured completeness and data quality, for example, verifying that all relevant elements were captured. Cookie data was primarily collected using the CookieBlock browser extension [6], which categorizes cookies by type (e.g., necessary, analytics, advertising). For technical reasons, some data was manually gathered using the 'Get cookies.txt' browser extension [34].

3.4 Data Analysis

This section details how we measured our constructs (*differences in privacy interfaces* and *compliance with requirements*) and the regression models used in the analysis.

Differences in privacy interfaces: To assess whether privacy-related interfaces differ based on a visitor's country, we examine three criteria. First, we check if the website is accessible in some countries but not others. Second, we evaluate whether a consent notice is displayed to visitors from certain countries but not to others. Third, we analyze whether a "Do Not Sell or Share My Personal Information" link is visible to visitors from specific countries. The accessibility of the website, as well as the presence of a consent notice or "Do Not Sell" link, is determined through visual inspection. The difference in the privacy interface is expressed as a binary variable: 1 if a country-level difference is identified in at least one of the three criteria, and 0 otherwise.

Compliance with requirements: To evaluate the compliance of websites with legal and normative privacy expectations, we operationalized the requirements in Section 3.1

Table 6: Equations for the regression models used to describe the results.

Model	Equation
Model 1	$difference = \beta_0 + \beta_1 \cdot category + \beta_2 \cdot origin$
Model 2	$compliance = \beta_0 + \beta_1 \cdot category + \beta_2 \cdot origin$
Model 3	$compliance = \beta_0 + \beta_1 \cdot category + \beta_2 \cdot origin + \beta_3 \cdot difference$

by defining concrete assessment criteria grounded in prior work. Each requirement was assessed through visual inspection, HTML source analysis, or automated tool support, depending on its nature. Visual inspection was used to evaluate interface elements such as the presence of a cookie wall (EU25), required information (e.g., EU03, EU04, EU07, EU09), and the visual display and placement of buttons (e.g., EU13, EU14). HTML source analysis helped identify structural elements like the presence of specific links (e.g., EU01, EU06) or font size (EU18). Automated tools supported criteria involving text analysis. For example, the readability of consent notices (EU02) was assessed using the `textstat` Python library and the Flesch-Kincaid Grade Level, with scores of 8.5 or lower considered acceptable [41, 69]. Sentiment neutrality (EU10) was evaluated using the NLTK library, with an absolute compound score below 0.65 indicating neutral phrasing [32]. A full overview of the criteria and their assessment methods is provided in [60]. Each requirement was labeled as *satisfied*, *not satisfied*, or *not applicable*. Requirements were considered not applicable when the website's context rendered them irrelevant. For example, requirements concerning consent notice presentation (e.g., font size) do not apply to websites that do not display such notices. To address ambiguous or borderline cases, we adopted an iterative refinement process in which the authors discussed any unclear interpretations of the requirements. These discussions led to refinements of the criteria and ensured they were applied consistently across all websites. To quantify compliance, we computed a *compliance ratio* for each website, defined as the number of satisfied requirements divided by the total number of applicable requirements (i.e., excluding those marked as not applicable). All applicable requirements contributed equally to the ratio.

Regression analysis: To address the research questions outlined in Section 3, we defined three regression models, summarized in Table 6. Model 1 investigates RQ1 by examining how the origin and category of a website influence the presence of differences in the consent notice shown when the website is accessed from different locations. Model 2 focuses on RQ2 by exploring the relationship between the compliance ratio and the origin and category of websites. Model 3 addresses RQ3, analyzing whether the presence of differences is a predictor of a website's compliance ratio, while also using the origin and category of websites as control variables to ensure the reliability of the results.

For RQ2 and RQ3, we further analyze compliance with respect to specific GDPR consent aspects (cf. Table 1). In these cases, the compliance ratio is recalculated based on the requirements associated with each aspect, as detailed in Table 2. This analysis evaluates whether the influence of website origin, category, or the presence of differences is consistent across all consent aspects or varies by aspect.

Logistic regression was performed for Model 1, while quasi-binomial logistic regression was used for Models 2 and 3. Factors with regression coefficients showing a p-value below 0.05 were considered statistically significant. We tested the models for RQ2 and RQ3 using two datasets: one comprising all websites in the corpus and another restricted

Table 7: Summary of analyzed websites per country, including the presence of privacy interfaces and the number of sites violating at least one requirement.

		# sites analyzed				Differ	Privacy interface present				At least one violation			
		EU	UK	CA	Cali		EU	UK	Canada	California	EU	UK	Canada	California
Tot		535	535	535	315	138 (25.8%)	361 (67.5%)	368 (68.8%)	302 (56.5%)	87 (27.6%)	523 (97.8%)	525 (98.1%)	473 (88.4%)	312 (99.1%)
Origin	EU	215	215	215	127	23 (10.7%)	189 (87.9%)	188 (87.4%)	184 (85.6%)	2 (1.6%)	215 (100%)	213 (99.1%)	180 (83.7%)	127 (100%)
	UK	94	94	94	58	31 (33.0%)	89 (94.7%)	92 (97.9%)	69 (73.4%)	25 (43.1%)	94 (100%)	94 (100%)	79 (84.0%)	58 (100%)
	US	122	122	122	67	55 (45.1%)	46 (37.7%)	47 (38.5%)	21 (17.2%)	56 (83.6%)	115 (94.3%)	116 (95.1%)	117 (95.9%)	64 (95.5%)
	CA	104	104	104	63	29 (27.9%)	37 (35.6%)	41 (39.4%)	28 (26.9%)	4 (6.4%)	99 (95.2%)	102 (98.1%)	97 (93.3%)	63 (100%)
Category	News	180	180	180	152	78 (43.3%)	163 (90.6%)	165 (91.7%)	109 (60.6%)	50 (32.9%)	180 (100%)	180 (100%)	177 (98.3%)	150 (98.7%)
	E-comm	169	169	169	156	46 (27.2%)	123 (72.8%)	128 (75.7%)	120 (71.0%)	36 (23.1%)	161 (95.3%)	164 (97.0%)	155 (91.7%)	155 (99.4%)
	Govt	186	186	186	7	14 (7.5%)	75 (40.3%)	75 (40.3%)	73 (39.3%)	1 (14.3%)	182 (97.9%)	181 (97.3%)	141 (75.8%)	7 (100%)

to websites for which all requirements are applicable. This allows us to examine whether websites bound by the complete set of requirements exhibit distinct compliance patterns compared to the entire dataset.

4 Results

Table 7 summarizes the presence of relevant privacy interfaces across countries, showing how many websites display these interfaces based on user location. It also reports the number of sites analyzed for compliance in each country and those violating at least one requirement in that country. Note that the number of websites assessed for California is lower due to the applicability of the CCPA (see Section 3.3).

We can observe that approximately 70% of websites display a consent notice in the EU, 71% in the UK, and 61% in Canada. In California, 28% of websites provide a "Do Not Sell" link, which may also include a "Limit the Use of My Sensitive Personal Information" or "Your Privacy Choices" link. Around 26% of websites exhibit differences in privacy interfaces based on user location. Notably, almost all websites analyzed violate at least one legal requirement, revealing substantial compliance gaps. In the EU, UK, and California, over 90% of websites fail to meet at least one applicable requirement. In Canada, approximately 88% of the websites exhibit at least one violation; this trend is consistent across all website categories and countries of origin, with at least 75% of websites in every category failing to comply with at least one requirement.

Table 8 analyzes compliance with GDPR consent requirements when websites are accessed from the EU and UK. The results show that full compliance with consent aspects is notably rare. For most consent aspects, at least 69% of websites fail to meet at least one requirement. An exception is the 'specific' consent aspect, where compliance may be higher due to the limited number of applicable requirements (only two). These findings highlight widespread violations of GDPR requirements.

4.1 RQ1: Differences in Privacy Interfaces

Presence of privacy interfaces: Fig. 3 presents the results of the regression analysis examining the presence of privacy interfaces based on website origin and category; coefficients are reported in [60]. The McFadden pseudo R-squared values, ranging from 0.33 to 0.55, indicate that the models account for approximately 33-55% of the variance

Table 8: Number of sites violating at least one requirement per consent aspect, reported separately for access from the EU and the UK.

		Freely given		Informed		Specific		Unambiguous	
		EU	UK	EU	UK	EU	UK	EU	UK
Tot		485 (90.7%)	489 (91.4%)	490 (91.6%)	502 (93.8%)	276 (51.6%)	269 (50.3%)	434 (81.1%)	478 (89.4%)
Origin	EU	196 (91.2%)	196 (91.2%)	202 (94.0%)	203 (94.4%)	84 (39.1%)	81 (37.7%)	166 (77.2%)	188 (87.4%)
	UK	81 (86.2%)	80 (85.1%)	90 (95.7%)	92 (97.9%)	27 (28.7%)	14 (14.9%)	73 (77.7%)	84 (89.4%)
	US	113 (92.6%)	114 (93.4%)	103 (84.4%)	109 (89.3%)	88 (72.1%)	93 (76.2%)	104 (85.3%)	110 (90.2%)
	CA	95 (91.4%)	99 (95.2%)	95 (91.4%)	98 (94.2%)	77 (74.0%)	81 (77.9%)	91 (87.5%)	96 (92.3%)
Category	News	178 (98.9%)	177 (98.3%)	177 (98.3%)	179 (99.4%)	51 (28.3%)	61 (33.9%)	168 (93.3%)	177 (98.3%)
	E-comm	160 (94.7%)	163 (96.5%)	156 (92.3%)	158 (93.5%)	80 (47.3%)	67 (39.6%)	137 (81.1%)	157 (92.9%)
	Govt	147 (79.0%)	149 (80.1%)	157 (84.4%)	165 (88.7%)	145 (78.0%)	141 (75.8%)	129 (69.6%)	144 (77.4%)

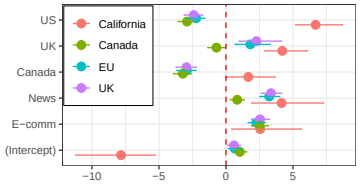

Fig. 3: Regression coefficients indicating the presence likelihood of relevant privacy interfaces observed across countries. Baselines – origin: EU; category – government.

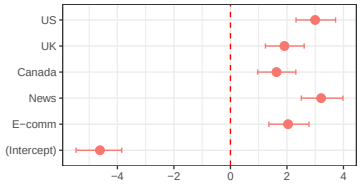

Fig. 4: Regression coefficients indicating the presence of a difference in privacy interfaces among countries. Baselines – origin: EU; category – government.

in the data. The analysis reveals that EU and UK websites are more likely to display consent notices compared to US and Canadian websites. "Do Not Sell" links are most frequently observed on US websites and least likely on EU websites. These results are consistent with companies prioritizing compliance with local laws. Privacy interfaces, regardless of type, are more common on e-commerce and news websites. Government websites, being non-commercial and less reliant on tracking technologies that require consent, are the least likely to display privacy interfaces, including consent notices.

Differences between regions: Fig. 4 illustrates the relationship between differences in privacy interfaces across regions and a website's origin or category; the coefficients are reported in [60]. The McFadden pseudo R-squared value of 0.30 indicates a moderate model fit, accounting for roughly 30% of the variance in the data. The results show that non-EU websites are more likely to exhibit differences in privacy interfaces compared to EU government websites. Similarly, e-commerce and news websites are more likely to have such differences than EU websites. One explanation is that non-EU websites, often written in English, are more likely to target an international audience. In contrast, EU websites, typically written in local languages, tend to focus on domestic users. Internationally oriented websites are incentivized to adjust privacy interfaces based on visitor location to align with regional laws, enabling them to maximize revenue by limiting privacy options in areas with less stringent regulations. The higher prevalence of differences on e-commerce and news websites compared to government websites likely reflects their commercial nature. Government websites, being non-commercial, have less incentive to tailor privacy options based on location, as their primary focus is providing public services to their local audience rather than generating revenue. In

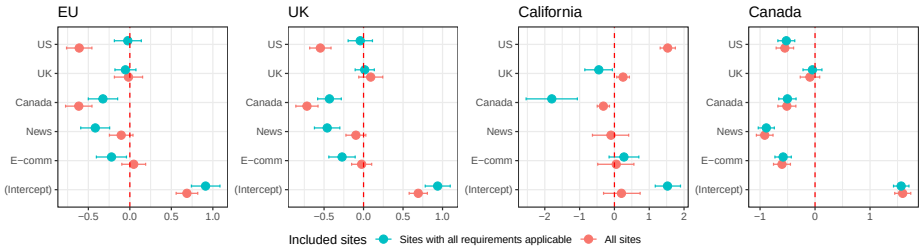

Fig. 5: Regression coefficients of the observed variables w.r.t. the compliance ratio (Model 2). Plot titles indicate the region of visit.

contrast, e-commerce and news websites may strategically adapt privacy interfaces to meet minimum legal requirements by region.

ANSWER TO RQ1. The origin and category of a website significantly influence whether privacy-related interfaces vary based on visitor location. Non-EU websites and commercial sites, such as e-commerce and news, are more likely to adjust their privacy interfaces across regions, whereas EU and government websites tend to present consistent interfaces focused on domestic users. These findings suggest that the adoption of tailored privacy interfaces is often driven by commercial incentives.

4.2 RQ2: Compliance with Requirements

Fig. 5 presents the results of the regression analysis examining the relationship between a website's origin and category and its compliance with requirements from each region. The regression coefficients are reported in [60].[5] For each region, the plot shows the results for all websites and for the ones for which all requirements from that region apply.

The analysis reveals that North American websites are less compliant with EU and UK laws than European websites, which aligns with our expectations. When considering only websites where all requirements apply, we can observe significant shifts in coefficients. News and e-commerce websites appear less compliant, whereas US and Canadian websites show greater compliance. This shift is likely due to the exclusion of US and Canadian government websites, which generally do not display consent notices. As a result, the model increasingly relies on website category rather than origin to explain compliance patterns. Fig. 5 also shows that US websites are more likely to comply with Californian requirements than EU websites. Similarly, UK websites are more likely than EU websites to comply with these requirements, but only when all UK websites are considered. When restricting the analysis to websites for which all Californian requirements apply, UK websites show lower compliance. This discrepancy may stem from differences in geolocation-based requirements, such as US10 and US13, where

[5] The pseudo R-squared values vary across models. For models assessing compliance with EU, UK, and Canadian requirements, values range from 0.12 to 0.23, indicating a moderate explanatory capacity. In contrast, models evaluating compliance with Californian requirements have pseudo R-squared values between 0.50 and 0.55, reflecting a stronger fit.

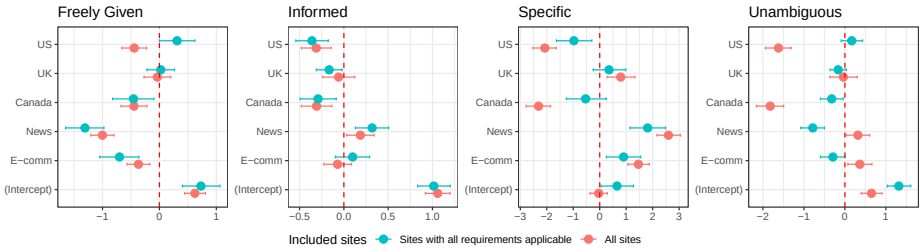

Fig. 6: Regression coefficients of the observed variables w.r.t. the compliance ratio with EU requirements for GDPR consent aspects.

websites requesting geolocation data may fail to display "Do Not Sell" links or other CCPA-mandated information. Canadian websites consistently exhibit lower compliance with Californian requirements than EU websites.

Compliance with Canadian requirements depends more on website category than origin, with government websites being significantly more compliant than news and e-commerce sites. CA01, CA03, and CA04 show near-universal compliance (see [60]), while CA02 and CA05 show most variations. CA02 assesses whether advertising or social media cookies persist after opting out. Government websites, which rarely use ads, have fewer violations, whereas news and e-commerce sites often rely on third-party opt-out mechanisms, which set opt-out cookies that CookieBlock classifies as advertising cookies, leading to violations. CA05 identifies third-party cookies disguised as first-party cookies, often for analytics. Government websites use fewer analytics cookies, leading to higher compliance, while news and e-commerce sites frequently deploy such trackers, making category a strong predictor of CA05 compliance.

To better understand compliance with EU and UK requirements, we analyzed individual GDPR consent aspects. The results are shown in Fig. 6 for the EU; the ones for the UK are similar. Regression coefficients for this analysis are provided in [60].[6] The results highlight differences in compliance with specific consent aspects based on website origin and category. News websites are more likely to violate requirements for freely given consent but perform better in informing users. These patterns remain consistent across datasets, except in models addressing unambiguous consent. This could be explained by the fact that websites cannot request consent ambiguously if they do not request consent at all.

ANSWER TO RQ2. The compliance of websites with privacy laws varies by origin and category, with North American websites less compliant with EU and UK regulations but more aligned with Californian laws. Commercial websites, especially news and e-commerce, show lower compliance, as their reliance on tracking and third-party services often leads to violations. These findings suggest that compliance is

[6] The pseudo R-squared values for these models vary considerably. Models including all websites range from 0.04 to 0.47. When considering only websites for which all requirements apply, values range from 0.12 to 0.23. The lower fit in informed consent models for all websites is likely due to the inclusion of websites without consent notices, which inherently fail to inform users.

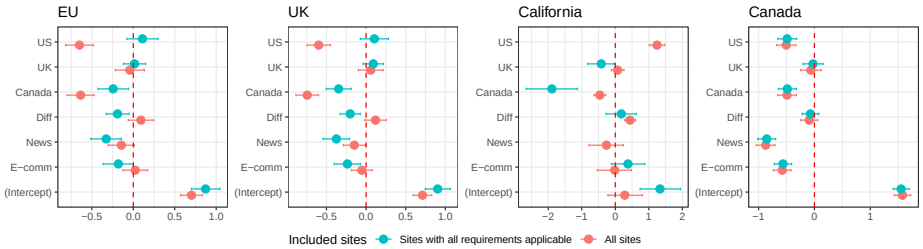

Fig. 7: Regression coefficients of the observed variables w.r.t. the compliance ratio (Model 3). Plot titles indicate the region of visit.

driven by legal risks and business practices rather than uniform standards, highlighting the need for stronger enforcement measures where compliance is low.

4.3 RQ 3: Relation between Differences in Privacy Interfaces and Compliance

Fig. 7 presents the results of the regression analysis examining the relationship between the use of different privacy interfaces when accessing the website from different locations and compliance with requirements; coefficients are reported in [60].[7] For each region, the plot shows the results when considering all websites and when considering only the websites for which all requirements from that region apply.

For EU and UK requirements, we find that websites exhibiting a different consent notice are less likely to comply when analyzing only those where all requirements are applicable. This relationship, however, becomes insignificant when considering all websites, possibly because the broader set includes, for instance, websites inaccessible from certain regions, thus inevitably exhibiting a different behavior when accessed from different regions. To further analyze this correlation, we investigated compliance with EU and UK requirements at the level of individual GDPR consent aspects. Fig. 8 shows the results for the EU; we refer to [60] for the results for the UK and coefficients.[8] The use of different privacy interfaces positively correlates with consent being freely given and specific, but no significant relationship is found for informed consent. Across all websites, we observe a positive relationship. However, when focusing only on sites where all requirements apply, we find that consent requests tend to be more ambiguous. This may be because sites that do not request consent at all cannot do so ambiguously.

For Californian requirements, significant correlations are only observed when considering all websites. This may be because requirements US10 and US13 are inapplicable if geolocation information is not requested. Nonetheless, the positive relationship between differences and compliance when considering all websites suggests that differences may directly influence compliance with Californian law. Higher compliance among websites showing different privacy interfaces may reflect characteristics of websites subject to

[7] The pseudo R^2 values range from 0.15 to 0.23 for EU, UK, and Canadian requirements and from 0.54 to 0.56 for Californian requirements, indicating a stronger relationship for California.

[8] The pseudo R-squared values range from 0.04 to 0.13 for informed consent and from 0.16 to 0.52 for the other consent aspects, suggesting reasonable fits except for informed consent.

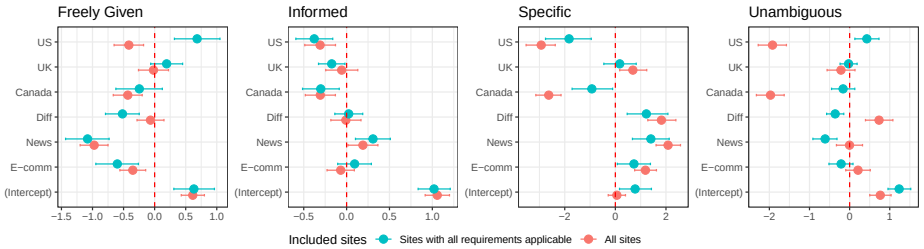

Fig. 8: Regression coefficients of the observed variables w.r.t. the compliance ratio with EU requirements for GDPR consent aspects.

the CCPA. Websites operated by larger organizations, which have stronger incentives to comply with privacy laws, may tailor privacy options based on visitor locations, displaying only region-specific choices.

For Canadian requirements, the presence of a difference in the displayed privacy interface does not significantly impact compliance rates. This aligns with earlier findings: news and e-commerce websites are more likely to have differences (Section 4.1), while government websites are more likely to comply with Canadian requirements (Section 4.2). This suggests that differences may act as a confounding variable for website categories rather than directly determining compliance. Additionally, the limited number of Canadian requirements could contribute to the weak relationship, as discussed in Section 4.2.

ANSWER TO RQ3. Websites presenting different privacy interfaces to visitors from different regions are not necessarily more likely to comply with privacy regulations. While differences are linked to higher compliance with Californian requirements, they are associated with lower compliance in the EU and UK and show no significant impact in Canada. These findings suggest that organizations should focus on meeting legal requirements directly rather than relying on region-specific consent interfaces, as their adoption alone does not necessarily imply compliance.

5 Discussion

Extraterritoriality of privacy laws: Regulations such as the GDPR and CCPA apply extraterritorially, based on the data subject's location rather than that of the data controller or processor. However, websites generally comply more with regulations from their country of origin (cf. Section 4.2). One reason could be that organizations prioritize laws that can be enforced against them. If a company has no offices, employees, or assets in a jurisdiction, enforcement may be difficult, reducing the incentive to comply. Another factor is uncertainty about extraterritorial laws, as organizations may wrongly assume these do not apply to them. Clearer regulatory guidance is needed to address these challenges, particularly for businesses operating across jurisdictions. Regulators could provide more accessible interpretations of privacy laws, while researchers could identify ambiguities in their application. At the same time, regulators need automated detection to help streamline compliance monitoring, allowing them to identify violations more efficiently and expand monitoring efforts beyond manual investigations.

CMP vendor	Number of websites
Didomi	31
Google Funding Choices	21
InMobi	27
OneTrust	72
Sourcepoint	32

Table 9: Results of a preliminary analysis of the CMP vendors used on websites. The analysis does not account for websites that use multiple CMPs simultaneously.

Websites' perception of privacy: Although EU privacy regulations are often 'exported' to other countries [57], a phenomenon known as the Brussels effect [7], our findings show that organizations tailor privacy options to visitors' locations instead of applying the strictest standards globally. This suggests the Brussels effect may be weaker than previously thought and that many organizations treat privacy primarily as a compliance requirement rather than a user right. This lack of incentive is further supported by [30], which found that most websites notified about potential GDPR non-compliance in their cookie banners neither responded nor updated their interfaces, reflecting limited willingness to improve their privacy practices. Future work could explore this further to identify incentives that encourage organizations to offer stronger privacy protections.

Standardization of privacy information & options: Our investigation suggests that privacy laws with detailed requirements such as the CCPA promote the consistent adoption of a standardized interface, whereas general regulations such as the GDPR lead to significant variation in interfaces, potentially hindering users' decision-making and complicating compliance. European regulators should consider stricter guidelines on presenting privacy information and options. Standardized icons (as explored by e.g. [31, 29], or as currently mandated by CCPA [63, § 7015(b)]) or machine-readable privacy information could improve user understanding and better align privacy practices with GDPR's intent.

Compliance frameworks: During data collection, we observed that many websites create their privacy interfaces using consent management platforms (CMPs) from a small group of vendors (Table 9). The choice of CMP often dictates aspects of the privacy interface, including button placement, text, and font size. Since these elements affect compliance, CMPs can significantly influence a website's compliance ratio. Future work could examine how CMP vendors affect compliance rates; additionally, analyzing the effect on compliance of CMP configuration options could help vendors refine their tools and guide organizations in configuring CMPs to better align with privacy requirements. This discussion is particularly relevant in the context of the IAB Europe Transparency & Consent Framework (TCF) industry standard. While the TCF specifies required privacy information [33], it allows flexibility in presentation. Greater standardization by industry organizations could enhance the accessibility and usability of privacy interfaces.

5.1 Threats to Validity

Construct validity. Our interpretation of laws such as the GDPR and CCPA may introduce biases in defining compliance requirements. For example, while the CCPA mandates disclosure using predefined categories, we accepted similar descriptions, which may have been too lenient. Conversely, our strict interpretation of GDPR rules on legitimate interests for commercial purposes may be overly rigid in light of recent court rulings [11]. While these factors could affect specific assessments, most requirements

were derived from literature, ensuring overall robustness. Another limitation is the use of a compliance ratio that weighs all requirements equally, regardless of their significance or frequency of violation. Future research should explore more nuanced compliance metrics to enhance result reliability.

Internal validity. A threat to internal validity concerns the collection and classification of cookies. Distinguishing third-party cookies from those originating through external mechanisms (e.g., opt-out tools) is challenging. Additionally, reliance on CookieBlock for categorization introduces a risk of misclassification, potentially leading to incorrect compliance assessments. Another threat arises from using VPN services to simulate visitor locations. Websites may misidentify user locations, though we observed only one such case, suggesting minimal impact. Determining CCPA applicability posed challenges due to inconsistent corporate records and revenue estimates. When official figures were unavailable, we relied on secondary sources, which may be inaccurate. Additionally, using parent company revenues may have led to overestimation, as CCPA aggregation rules apply only to commonly branded entities [64, § 1798.140(d)(2)]. Finally, despite our verification efforts (cf. Sections 3.2 and 3.3), a few misclassifications may have persisted; for instance, some political news websites were misclassified as government websites, affecting compliance assessments, particularly under the CCPA.

External validity. Our dataset of 535 websites may be too small to generalize our findings. Additionally, since we focus on popular websites, our results may not fully represent the broader Internet. Expanding our dataset, potentially through automation, could improve representativeness. Furthermore, some organizations, such as the Canadian federal government and British news publisher Reach plc, have multiple websites in our corpus. Since these sites often share privacy policies, their overrepresentation may skew observed trends, reflecting institutional practices rather than broader industry patterns.

6 Conclusion

This study investigated the differences in privacy interfaces when websites are accessed from different regions and their impact on compliance with privacy laws. To this end, we identified a set of requirements for assessing websites' compliance with privacy laws from the EU, the UK, California, and Canada. We conducted a study evaluating the compliance of 535 websites with these requirements, simulating visits from the countries where the laws were enacted. Our findings revealed that approximately 25% of websites displayed regional differences, which were more common among non-EU websites compared to EU websites. Moreover, nearly all websites violated at least one requirement. Websites with region-specific privacy interfaces were less likely to meet EU and UK requirements but were more likely to comply with Californian regulations, while no significant relationship was observed for Canadian requirements. Additionally, North American websites showed lower compliance with EU and UK requirements but higher compliance with the CCPA compared to EU websites. Future work should focus on expanding the dataset to include more websites, enhancing the scalability and reliability of compliance assessments. Further research could also explore the motivations and incentives that drive privacy compliance, offering insights on how to improve regulatory practices.

References

1. Art. 29 Data Protection Working Party. Op. 04/2012 on Cookie Consent Exemption, 2012.
2. Art. 29 Data Protection Working Party. Guidelines on transparency for Reg. 2016/679, 2018.
3. A. Bekh. Advertising-based revenue model in digital media market. *Econviews: Review of Contemporary Entrepreneurship, Business, and Economic Issues*, 33(2):547–559, 2020.
4. B. M. Berens, H. Dietmann, C. Krisam, O. Kulyk, and M. Volkamer. Cookie Disclaimers: Impact of Design and Users' Attitude. In *ARES*. ACM, 2022.
5. C. Bermejo Fernandez, D. Chatzopoulos, D. Papadopoulos, and P. Hui. This Website Uses Nudging: MTurk Workers' Behaviour on Cookie Consent Notices. In *HCI*. ACM, 2021.
6. D. Bollinger, K. Kubicek, C. Cotrini, and D. Basin. Automating Cookie Consent and GDPR Violation Detection. In *USENIX Security Symposium*, pages 2893–2910, 2022.
7. A. Bradford. The Brussels Effect. *Northwestern University Law Review*, 107(1):1–67, 2012.
8. H. Brignull. Dark Patterns: User Interfaces Designed to Trick People, 2010.
9. H. Brignull. Dark Patterns: Deception vs. Honesty in UI Design, 2011.
10. Canadian Radio-television and Telecommunications Commission. Canada's Anti-Spam Legislation Requirements for Installing Computer Programs, 2020.
11. Court of Justice of the European Union. Koninklijke Nederlandse Lawn Tennisbond v Autoriteit Persoonsgegevens. ECLI:EU:C:2024:857, 2024.
12. A. Dabrowski, G. Merzdovnik, J. Ullrich, G. Sendera, and E. Weippl. Measuring Cookies and Web Privacy in a Post-GDPR World. In *PAM*, pages 258–270. Springer, 2019.
13. EDPB. Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, 2019.
14. EDPB. Guidelines 05/2020 on consent under Regulation 2016/679, 2020.
15. EDPB. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 2020.
16. EDPB. Report of the work undertaken by the Cookie Banner Taskforce, 2023.
17. EDPB (European Data Protection Board). Deceptive design patterns in social media platform interfaces: how to recognise and avoid them, 2023.
18. R. v. Eijk, H. Asghari, P. Winter, and A. Narayanan. The Impact of User Location on Cookie Notices (Inside and Outside of the European Union). In *ConPro*, 2019.
19. European Parliament and Council of the European Union. Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 2002.
20. European Parliament and Council of the European Union. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), 2016.
21. European Parliament and Council of the European Union. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (UK GDPR), 2016.
22. European Parliament and Council of the European Union. Reg. (EU) 2022/2065 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), 2022.
23. European Parliament and Council of the European Union. Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), 2022.
24. C. M. Gray, Y. Kou, B. Battles, J. Hoggatt, and A. L. Toombs. The Dark (Patterns) Side of UX Design. In *Conference on Human Factors in Computing Systems*, page 1–14. ACM, 2018.
25. C. M. Gray, C. Santos, N. Bielova, M. Toth, and D. Clifford. Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective. In *Conference on Human Factors in Computing Systems*. ACM, 2021.

26. J. Gunawan, A. Pradeep, D. Choffnes, W. Hartzog, and C. Wilson. A Comparative Study of Dark Patterns Across Web and Mobile Modalities. *ACM Hum.-Comput. Interact.*, 5, 2021.
27. R. Gundelach and D. Herrmann. Cookiescanner: An Automated Tool for Detecting and Evaluating GDPR Consent Notices on Websites. In *ARES*. ACM, 2023.
28. H. Habib, M. Li, E. Young, and L. Cranor. "Okay, whatever": An Evaluation of Cookie Consent Interfaces. In *Conference on Human Factors in Computing Systems*. ACM, 2022.
29. H. Habib, Y. Zou, Y. Yao, A. Acquisti, L. Cranor, J. Reidenberg, N. Sadeh, and F. Schaub. Toggles, Dollar Signs, and Triangles: How to (In)Effectively Convey Privacy Choices with Icons and Link Texts. In *Conference on Human Factors in Computing Systems*. ACM, 2021.
30. A. Hennig, H. Dietmann, F. Lehr, M. Mutter, M. Volkamer, and P. Mayer. Your Cookie Disclaimer is Not in Line with the Ideas of the GDPR. Why? In *Human Aspects of Information Security and Assurance*, pages 218–227. Springer, 2022.
31. L.-E. Holtz, H. Zwingelberg, and M. Hansen. Privacy Policy Icons. In *Privacy and Identity Management for Life*, pages 279–285. Springer, 2011.
32. C. Hutto and E. Gilbert. VADER: A Parsimonious Rule-Based Model for Sentiment Analysis of Social Media Text. *Internat. AAAI Conf. on Web and Social Media*, 8(1):216–225, 2014.
33. IAB Europe. TCF Standardisation Principles.
34. kairi003. Get cookies.txt LOCALLY, 2024.
35. R. Khandelwal, A. Nayak, H. Harkous, and K. Fawaz. Automated Cookie Notice Analysis and Enforcement. In *USENIX Security Symposium*. USENIX Association, 2023.
36. D. Kirkman, K. Vaniea, and D. W. Woods. DarkDialogs: Automated Detection of 10 Dark Patterns on Cookie Dialogs. In *EuroS&P*, pages 847–867. IEEE, 2023.
37. K. Kollnig, R. Binns, M. Van Kleek, U. Lyngs, J. Zhao, C. Tinsman, and N. Shadbolt. Before and After GDPR: Tracking in Mobile Apps. *Internet Policy Review*, 10(4), 2021.
38. K. Kollnig, P. Dewitte, M. V. Kleek, G. Wang, D. Omeiza, H. Webb, and N. Shadbolt. A Fait Accompli? An Empirical Study into the Absence of Consent to Third-Party Tracking in Android Apps. In *SOUP*, pages 181–196. USENIX Association, 2021.
39. C. Matte, N. Bielova, and C. Santos. Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework. In *IEEE Symposium on Security and Privacy*, pages 791–809, 2020.
40. S. Müller, S. Goswami, and H. Krcmar. Monetizing Blogs: Revenue Streams of Individual Blogs. In *European Conf. on Information Systems*, 2011.
41. National Cancer Institute. Simplification of Informed Consent Documents - Recomms., 2006.
42. T. T. Nguyen, M. Backes, N. Marnau, and B. Stock. Share First, Ask Later (or Never?) Studying Violations of GDPR's Explicit Consent in Android Apps. In *USENIX Security Symposium*, pages 3667–3684. USENIX Association, 2021.
43. T. T. Nguyen, M. Backes, and B. Stock. Freely Given Consent? Studying Consent Notice of Third-Party Tracking and Its Violations of GDPR in Android Apps. In *SIGSAC Conference on Computer and Communications Security*, page 2369–2383. ACM, 2022.
44. Office of the Attorney General of the State of California. California Consumer Privacy Act (CCPA), 2023.
45. Office of the Privacy Commissioner of Canada. Policy position on online behavioural advertising, 2021.
46. F. Paci, J. Pizzoli, and N. Zannone. A Comprehensive Study on Third-Party User Tracking in Mobile Applications. In *ARES*. ACM, 2023.
47. E. Papadogiannakis, P. Papadopoulos, N. Kourtellis, and E. P. Markatos. User Tracking in the Post-cookie Era: How Websites Bypass GDPR Consent to Track Users. In *The Web Conference*, page 2130–2141. ACM, 2021.
48. Parliament of Canada. Personal Information Protection and Electronic Documents Act – Exemptions for Organizations in Alberta, British Columbia, and Quebec and for Personal

Health Information Custodians in New Brunswick, Newfoundland, Labrador, and Nova Scotia. https://laws-lois.justice.gc.ca/eng/acts/P-8.6/, 2000.
49. Parliament of Canada. Personal Information Protection and Electronic Documents Act, 2019.
50. Parliament of Canada. An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, 2023.
51. Parliament of Canada. Privacy Act, 2023.
52. Parliament of the United Kingdom of Great Britain and Northern Ireland. European Union (Withdrawal) Act 2018, 2018.
53. Privacy Community Group. Global Privacy Control - Take Control Of Your Privacy.
54. A. Rasaii, S. Singh, D. Gosain, and O. Gasser. Exploring the Cookieverse: A Multi-Perspective Analysis of Web Cookies. In *PAM*, pages 623–651. Springer, 2023.
55. C. Santos, N. Bielova, and C. Matte. Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners. *Technology and Regulation*, page 91–135, 2020.
56. C. Santos, A. Rossi, L. Sanchez Chamorro, K. Bongard-Blanchy, and R. Abu-Salma. Cookie Banners, What's the Purpose? Analyzing Cookie Banner Text Through a Legal Lens. In *Workshop on Privacy in the Electronic Society*, WPES '21, page 187–194. ACM, 2021.
57. M. Scott and L. Cerulus. Europe's new data protection rules export privacy standards worldwide, 2018.
58. Secretary of State of the United Kingdom of Great Britain and Northern Ireland. The Data Protection, Privacy and Electronic Communications (Amendments, EU Exit) Reg. 2019, 2020.
59. Secretary of State of the United Kingdom of Great Britain and Northern Ireland. The Privacy and Electronic Communications (EC Directive) Regulations 2003, 2020.
60. X. Smeets. Do websites truly value your privacy? An analysis of privacy requirement compliance among websites differing between jurisdictions. Master's thesis, Eindhoven University of Technology, 2024.
61. T. H. Soe, O. E. Nordberg, F. Guribye, and M. Slavkovik. Circumvention by design - dark patterns in cookie consent for online news outlets. In *NordiCHI*. ACM, 2020.
62. Software Freedom Conservancy. Selenium, 2024.
63. State of California. California Code of Regulations - Title 11, Division 6, Chapter 1 - California Consumer Privacy Act Regulations.
64. State of California. California Consumer Privacy Act of 2018, 2018.
65. State of California. California Privacy Rights Act of 2020, 2020.
66. B. Ur, P. G. Leon, L. F. Cranor, R. Shay, and Y. Wang. Smart, useful, scary, creepy: perceptions of online behavioral advertising. In *Symposium on Usable Privacy and Security*. ACM, 2012.
67. C. Utz, M. Degeling, S. Fahl, F. Schaub, and T. Holz. (Un)informed Consent: Studying GDPR Consent Notices in the Field. In *CCS*, page 973–990. ACM, 2019.
68. M. van Nortwick and C. Wilson. Setting the Bar Low: Are Websites Complying With the Minimum Requirements of the CCPA? In *PoPETs Proceedings*, pages 608–628, 2022.
69. K. Walters and M. Hamrell. Consent Forms, Lower Reading Levels, and Using Flesch-Kincaid Readability Software. *Therapeutic Innovation & Regulatory Science*, 42(4):385–394, 2008.
70. A. Yayla, E. Dincelli, and S. Parameswaran. A Mining Town in a Digital Land: Browser-Based Cryptocurrency Mining as an Alternative to Online Advertising. *Information Systems Frontiers*, 2023.
71. G. Zanfir-Fortuna. Planet49 CJEU Judgment brings some 'Cookie Consent' Certainty to Planet Online Tracking, 2019.