

Navigating Cookie Consent Violations Across the Globe

Brian Tang, Duc Bui, Kang Shin

Tracking Cookies

- Cookies still used for tracking browsing behavior
- Placed on websites for ad personalization, marketing, analytics, etc.

Third-party cookie retargeting



Source:

<https://www.cookieyes.com/third-party-cookies>

CookieYes

f t in /CookieYesHQ

GDPR and EU Regulations




ePrivacy Directive



IAB TCF v2.2.



 | stay on the safe side

You can't scale privacy without AI

Govern well. Move fast. AI makes both possible.

Learn more



Your Opt Out Preference Signal is Honored

Why do we use cookies and other tracking technologies?

Our site enables script (e.g. cookies) that is able to read, store, and write information on your browser and in your device. The information processed by this script includes data relating to you which may include personal identifiers (e.g. IP address and session details) and browsing activity. We use this information for various purposes - e.g. to deliver content, maintain security, enable user choice, improve our sites, and for marketing purposes. You can reject all non-essential processing by choosing to accept only necessary cookies. [Cookie Notice](#)

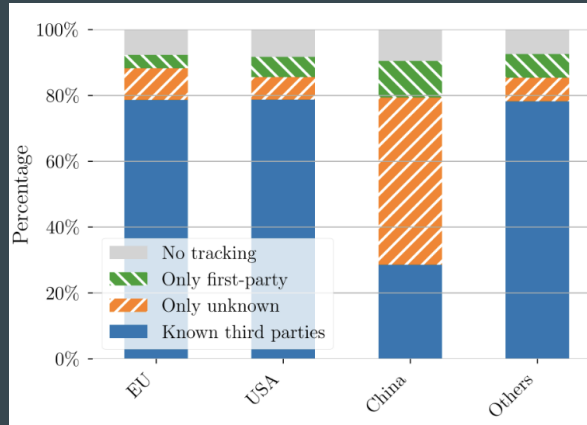
Accept opt-in

Stay opted-out

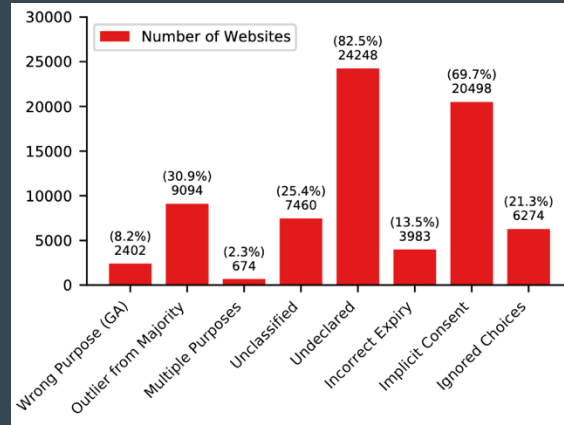
Customize Settings

Loyalty Program Breach

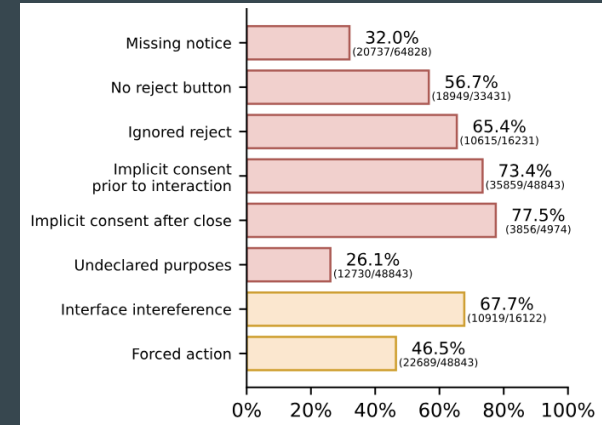
Prior Work on Cookie Consent



Sanchez-Rola et al. 2019



Bollinger et al. 2022



Bouhoula et al. 2024

And many more (Matte'20, Van Eijk'21, Rasaii'23, Liu'23, Kancherla'24, etc...)

What about cookie consent outside of the GDPR?





Canada (PIPEDA)

PIPEDA's global extra-territorial jurisdiction and right to be forgotten: A.T. v. Globe24h.com

FEBRUARY 1, 2017 · BARRY SOOKMAN

The Federal Court of Canada released a landmark decision finding that the court has the jurisdiction to make an extra-territorial order with world-wide effects against a foreign resident requiring the foreign person to remove documents containing personal information about a Canadian citizen that violates the person's rights under Canada's privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA). In *A.T. v. Globe24h.com*, 2017 FC 114 the Honourable Mr Justice Mosely ordered the individual operator of the website Globe24h.com to remove all Canadian tribunal and court decisions posted on the site that contain personal information and to take all necessary steps to remove the decisions from search engines caches.

PIPEDA and User Choice

PIPEDA requires an individual's knowledge and consent for the collection, use of information. ¹ PIPEDA also requires that the purposes for which an individual's information is collected, used or disclosed be explained in a clear and transparent manner. It recognizes that the form of consent can vary: for example, express consent (for sensitive information, and implied consent (opt-out) when the information is not sensitive. It is to note that the sensitivity of information depends on the nature of the information which it is being collected, used or disclosed. Certain types of information are sensitive because of the specific risks to individuals when said information is disclosed. This would include information such as health and financial data, ethnic and racial origins, genetic and biometric data, an individual's sex life or sexual orientation, and philosophical beliefs.

While obtaining consent in the online environment is not without its challenges, it is possible. Opt-out consent for online behavioural advertising could be considered reasonable providing that:

- Individuals are made aware of the purposes for the practice in a manner that is clear and understandable – the purposes must be made obvious and cannot be buried in a privacy policy. Organizations should be transparent about their practices and consider how to effectively inform individuals of their online behavioural advertising practices, by using a variety of communication methods, such as online banners, layered approaches, and interactive tools;
- Individuals are informed of these purposes at or before the time of collection and provided with information about the various parties involved in online behavioural advertising;
- Individuals are able to easily opt-out of the practice - ideally at or before the time the information is collected;
- The opt-out takes effect immediately and is persistent;
- The information collected and used is limited, to the extent practicable, to non-sensitive information (avoiding information that is generally considered sensitive such as medical or health information, financial data, ethnic and racial origins, political opinions, genetic and biometric data, an individual's sex life or sexual orientation, and religious/philosophical beliefs); and
- Information collected and used is destroyed as soon as possible or effectively de-identified.



California (CCPA)

3. What is considered personal information and sensitive personal information under the CCPA?

4. What is not considered personal information under the CCPA?

5. What businesses does the CCPA apply to?

The CCPA applies to for-profit businesses that do business in California and meet any of the following:

- Have a gross annual revenue of over \$25 million;
- Buy, sell, or share the personal information of 100,000 or more California residents or households; or
- Derive 50% or more of their annual revenue from selling California residents' personal information.

6. Does the CCPA apply to nonprofits or government agencies?

1. What rights do I have under the CCPA?

2. What if I am not a California resident?

3. What is considered personal information and sensitive personal information under the CCPA?

Personal information is information that identifies, relates to, or could reasonably be linked with you or your household. For example, it could include your name, social security number, email address, records of products purchased, internet browsing history, geolocation data, fingerprints, and inferences from other personal information that could create a profile about your preferences and characteristics.

Sensitive personal information is a specific subset of personal information that includes certain government identifiers (such as social security numbers); an account log-in, financial account, debit card, or credit card number with any required security code, password, or credentials allowing access to an account; precise geolocation; contents of mail, email, and text messages; genetic data; biometric information processed to identify a consumer; information concerning a consumer's health, sex life, or sexual orientation; or information about racial or ethnic origin, religious or philosophical beliefs, or union membership. Consumers have the right to also limit a business's use and disclosure of their sensitive personal information.

Personal information does not include publicly available information (including public real estate/property records) and certain types of information.



Singapore (PDPA)

Transfer of personal data outside Singapore

26.—(1) An organisation must not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under this Act to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under this Act.

(2) The Commission may, on the application of any organisation, by written notice exempt the organisation from any requirement prescribed pursuant to subsection (1) in respect of any transfer of personal data by that organisation.

(3) An exemption under subsection (2) —

- (a) may be granted subject to such conditions as the Commission may specify in writing; and
- (b) need not be published in the *Gazette* and may be revoked at any time by the Commission.

(4) The Commission may at any time add to, vary or revoke any condition imposed under this section.

Withdrawal of consent

16.—(1) On giving reasonable notice to the organisation, an individual may at any time withdraw any consent given, or deemed to have been given under this Act, in respect of the collection, use or disclosure by that organisation of personal data about the individual for any purpose.

(2) On receipt of the notice mentioned in subsection (1), the organisation concerned must inform the individual of the likely consequences of withdrawing his or her consent.

(3) An organisation must not prohibit an individual from withdrawing his or her consent to the collection, use or disclosure of personal data about the individual, but this section does not affect any legal consequences arising from such withdrawal.

(4) Subject to section 25, if an individual withdraws consent to the collection, use or disclosure of personal data about the individual by an organisation for any purpose, the organisation must cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing the personal data (as the case may be) unless such collection, use or disclosure (as the case may be) without the individual's consent is required or authorised under this Act or other written law.



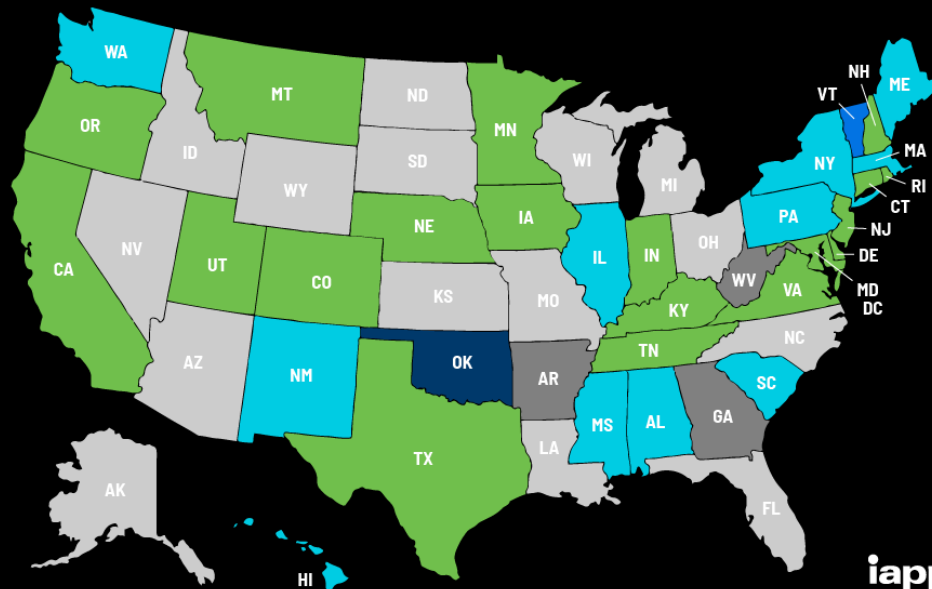
United States of America (Other)

The US is also a market of great interest to advertisers.

US State Privacy Legislation Tracker 2025

Statute/bill in legislative process

- Introduced
- In committee
- In cross chamber
- In cross committee
- Passed
- Signed
- Inactive bills
- No comprehensive bills introduced

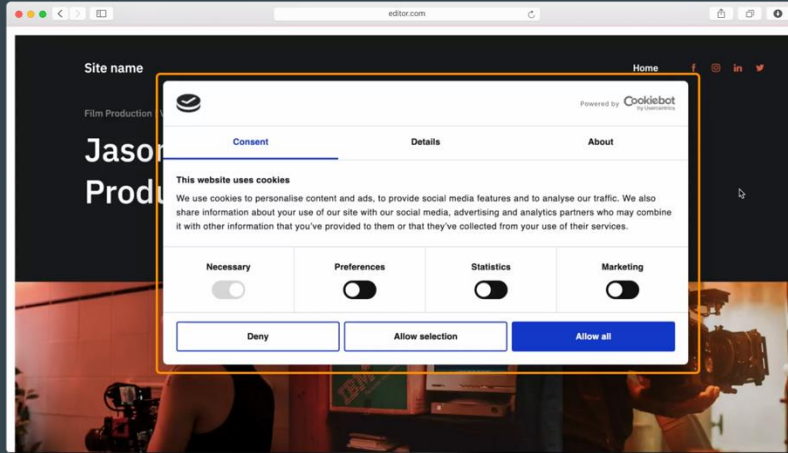


Last updated 21 Apr. 2025

iapp

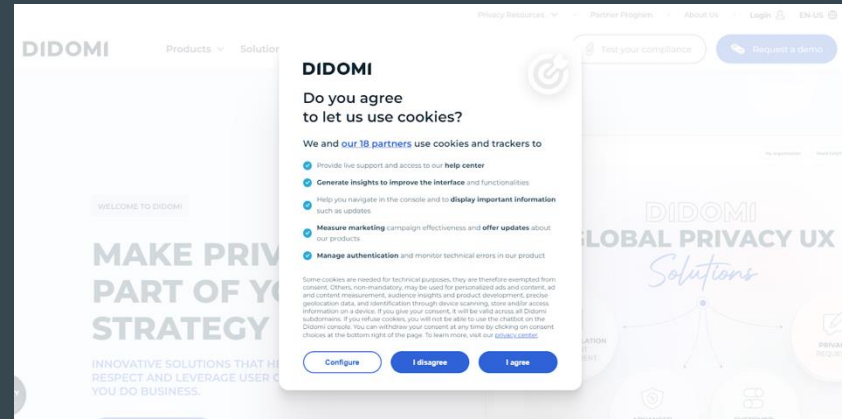
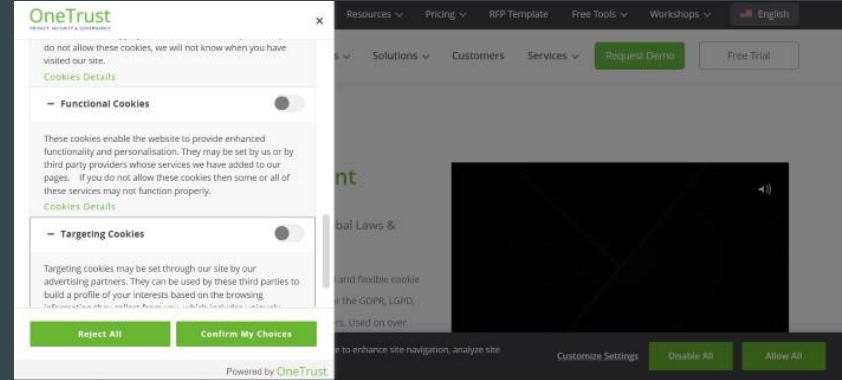
Consent Management Platforms (CMPs)

- OneTrust, Cookiebot, Didomi, etc.












We use essential cookies to make our site work. With your consent, we may also use non-essential cookies to improve user experience and analyze website traffic. By clicking "Accept," you agree to our website's cookie use as described in our [Cookie Policy](#). You can change your cookie settings at any time by clicking "[Preferences](#)."

Accept

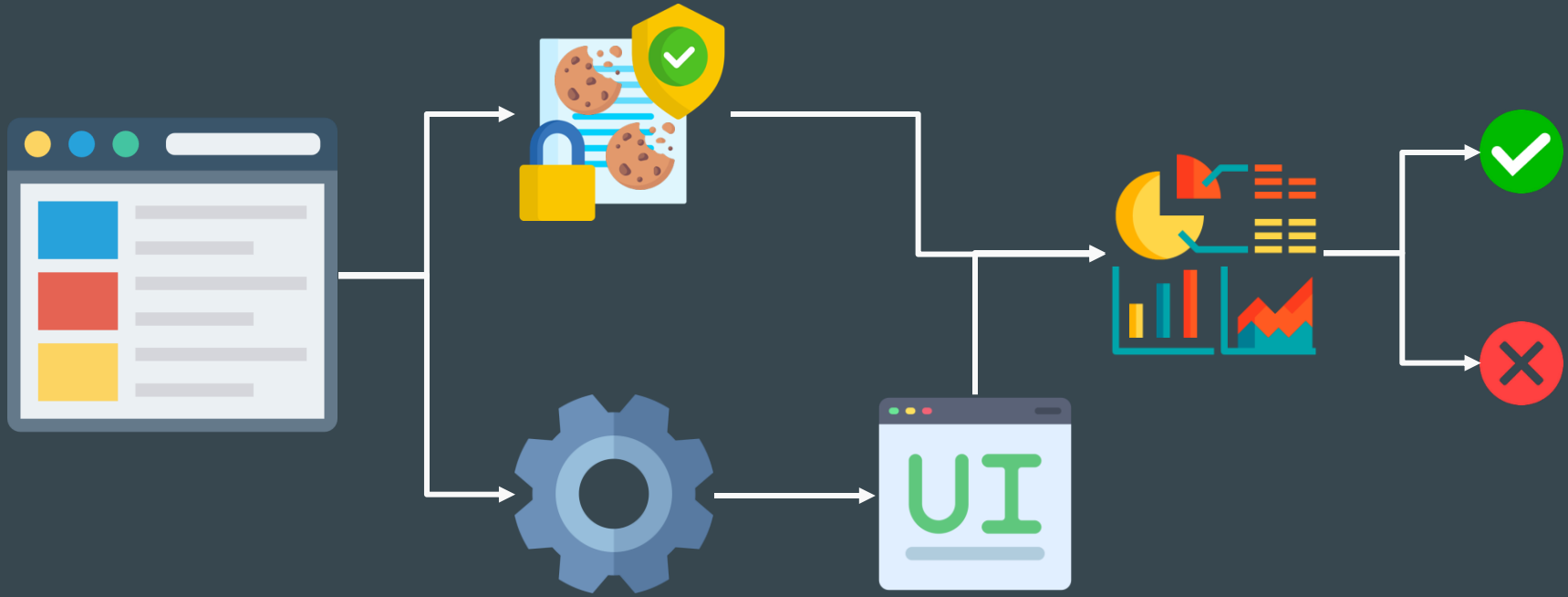


CMPs Provide Interpretations

- Regardless of what actual privacy laws are, CMPs hold the power of interpretation and implementation
- If a regulation is not provided on OneTrust, who will enforce it?
 - Where is PIPEDA, PDPA, APP, POPIA, UK DPA, etc.?

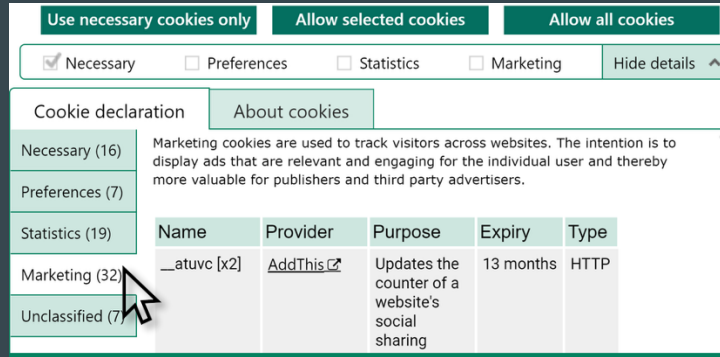
	GDPR General Data Protection Regulation	Europe	<input checked="" type="radio"/>
	TCF 2.2 Transparency & Consent Framework 2.2	 Europe	<input type="radio"/>
	CCPA California Consumer Privacy Act	California	<input type="radio"/>
	CPRA California Privacy Rights Act	California	<input type="radio"/>
	CPA Colorado Privacy Act	Colorado	<input type="radio"/>
	CTDPA Connecticut Data Privacy Act	Connecticut	<input type="radio"/>
	UCPA Utah Consumer Privacy Act	Utah	<input type="radio"/>
	VCDPA Virginia Consumer Data Protection Act	Virginia	<input type="radio"/>

ConsentChk Design



ConsentChk Crawler

- Visits 10 random subpages
- Spoofs user agent
- Uses techniques to simulate human behavior and avoid bot detection



Use necessary cookies only | Allow selected cookies | Allow all cookies

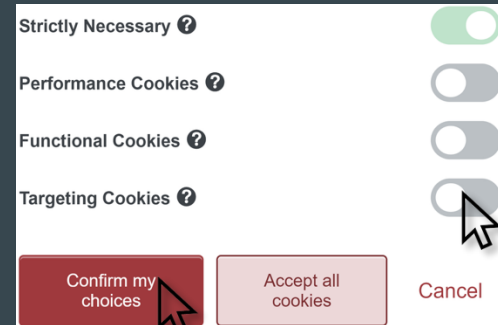
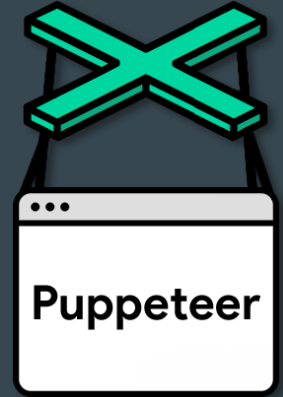
☒ Necessary ☐ Preferences ☐ Statistics ☐ Marketing [Hide details](#)

Cookie declaration | About cookies

Necessary (16) | Preferences (7) | Statistics (19) | Marketing (32) | Unclassified (7)

Marketing cookies are used to track visitors across websites. The intention is to display ads that are relevant and engaging for the individual user and thereby more valuable for publishers and third party advertisers.

Name	Provider	Purpose	Expiry	Type
__atuvc [x2]	AddThis	Updates the counter of a website's social sharing	13 months	HTTP



Strictly Necessary [?](#) ☒

Performance Cookies [?](#) ☐

Functional Cookies [?](#) ☐

Targeting Cookies [?](#) ☐

[Confirm my choices](#) [Accept all cookies](#) [Cancel](#)

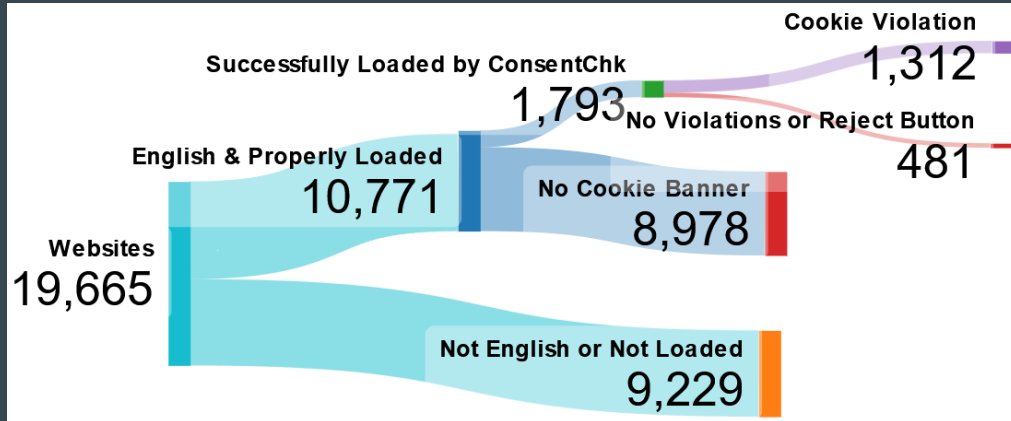
8 Measurement Vantage Points

- English-Speaking
- Privacy Laws
(Except Michigan)
- CA, US, CAN,
UK, EU, ZA, SG,
AU



Crawling Methodology

- 3 CMPs
- Only sites with cookie banner settings
- Only sites which were loaded successfully
- October 4-12 2024



The image shows a cookie consent banner with a toggle switch for 'Targeting Cookies' and a list of cookies. A red dashed box highlights the 'Cookies Details' link, which is labeled (a) Cookie setting. Below the banner, a 'Cookies List' for 'rubiconproject.com' is shown, with a 'View Cookies' link. The list includes details for a cookie named 'ruid'.

Strictly Necessary Cookies	
Performance Cookies	
Functional Cookies	
Targeting Cookies	
Targeting (3rd Party)	

Targeting Cookies

These cookies may be set through our site by our advertising partners. They may be used by those companies to build a profile of your interests and show you relevant adverts on other sites. They do not store directly personal information, but are based on uniquely identifying your browser and internet device. If you do not allow these cookies, you will experience less targeted advertising.

[Cookies Details](#) (a) Cookie setting.

< Cookies List

Search...

rubiconproject.com View Cookies ▶

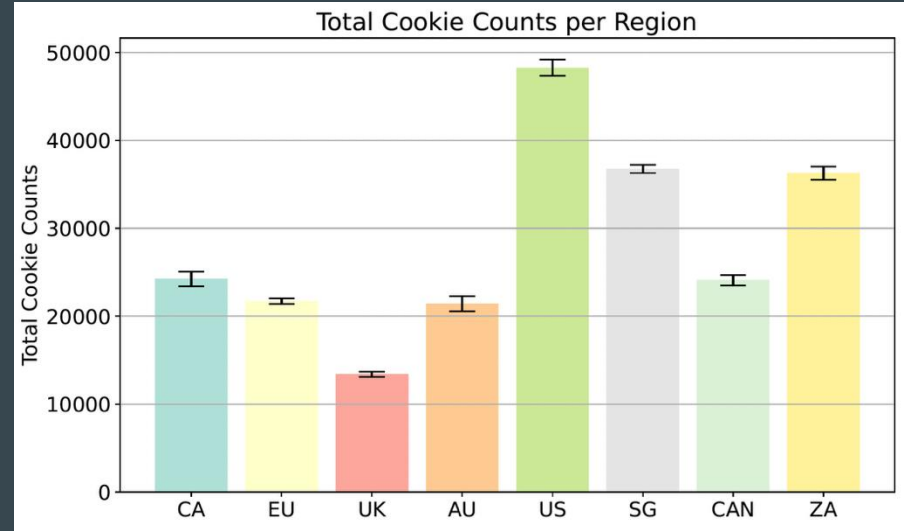
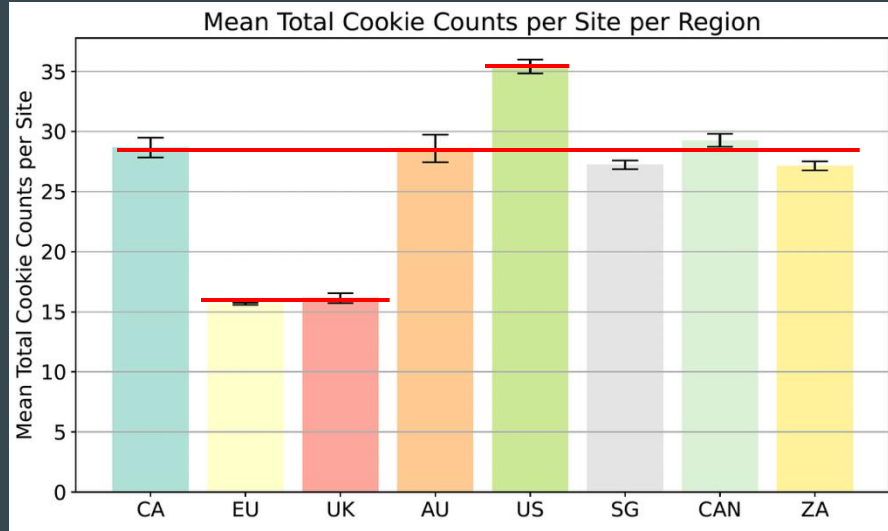
Name	Host	Duration	Type
ruid	rubiconproject.com	a few seconds	Third Party

(b) Cookie declaration.

Violation Types

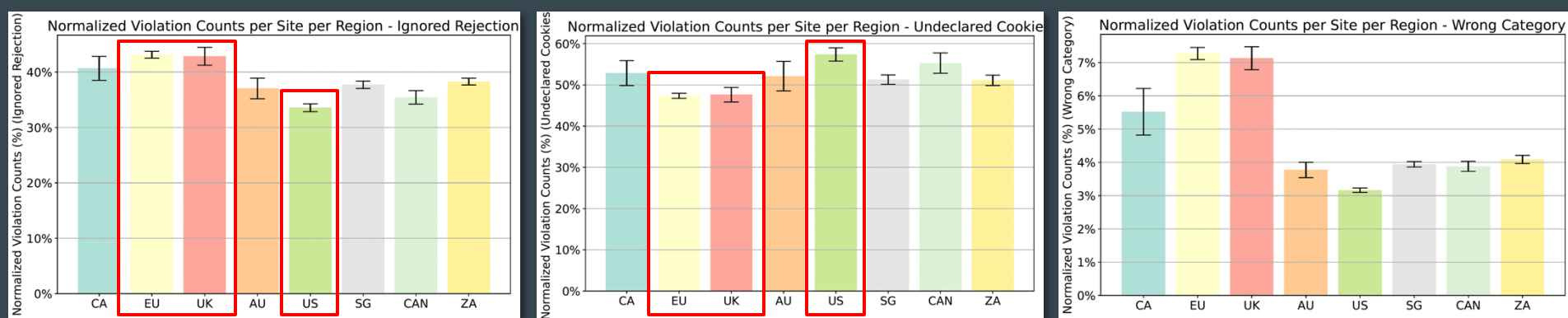
- Ignored Cookie Rejection
 - Click reject button, but cookie still loads
- Undeclared Cookie
 - Cookie not in CMP library and is unable to be rejected or given consent to
- Wrong/Ambiguous Cookie Category
 - Cookie in multiple cookie categories and cannot be rejected

Finding I: Cookie Placement



Regions with stricter privacy regulations have on average 11 fewer cookies per site

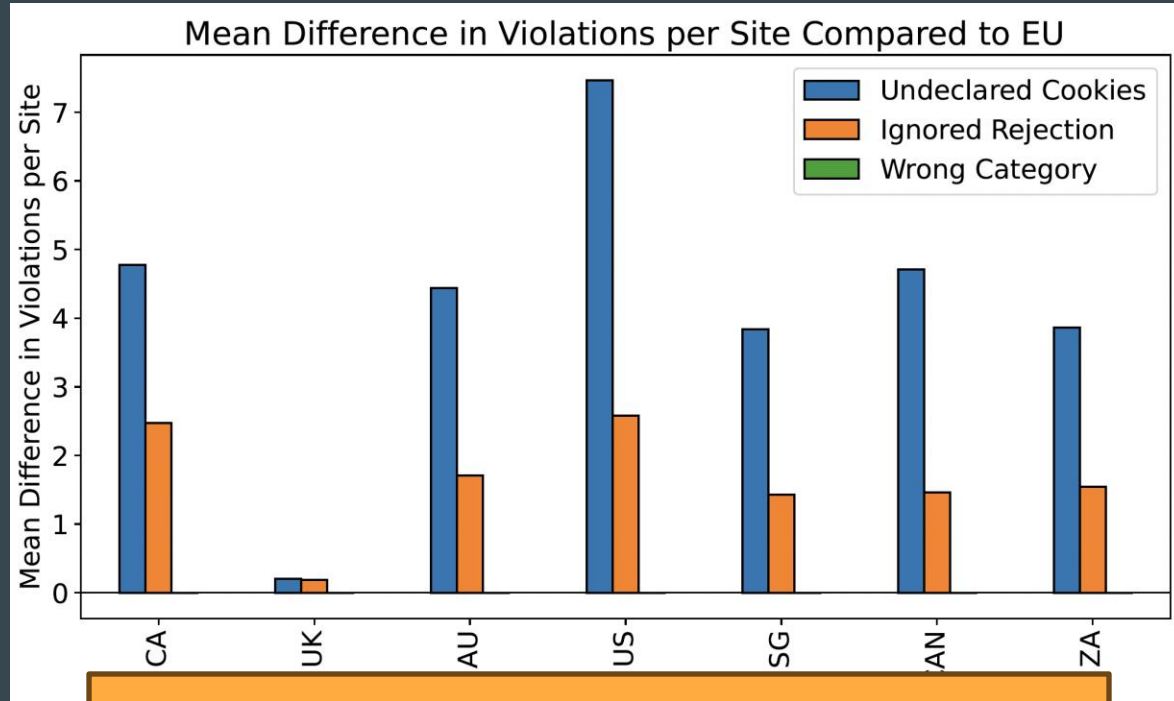
Finding 2: Cookie Consent Violations



Stricter privacy regulations = 4-9% fewer undeclared cookies

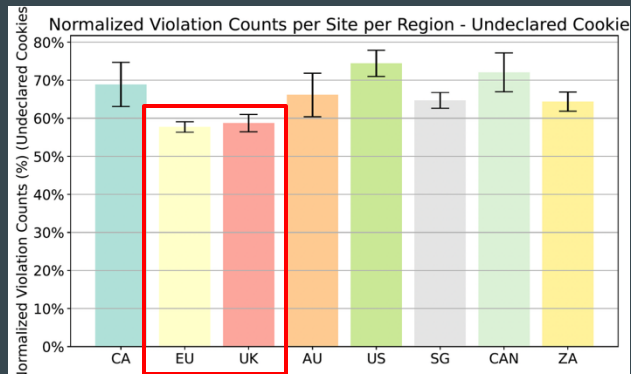
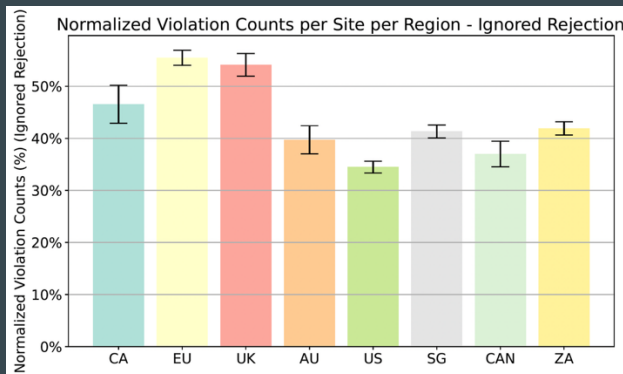
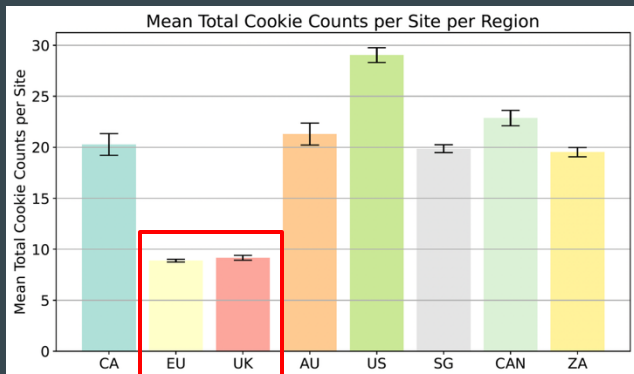
But 4-9% more declared cookies = 3-10% more ignored rejections

Finding 3: Cookie Violations Same-Site Comparison



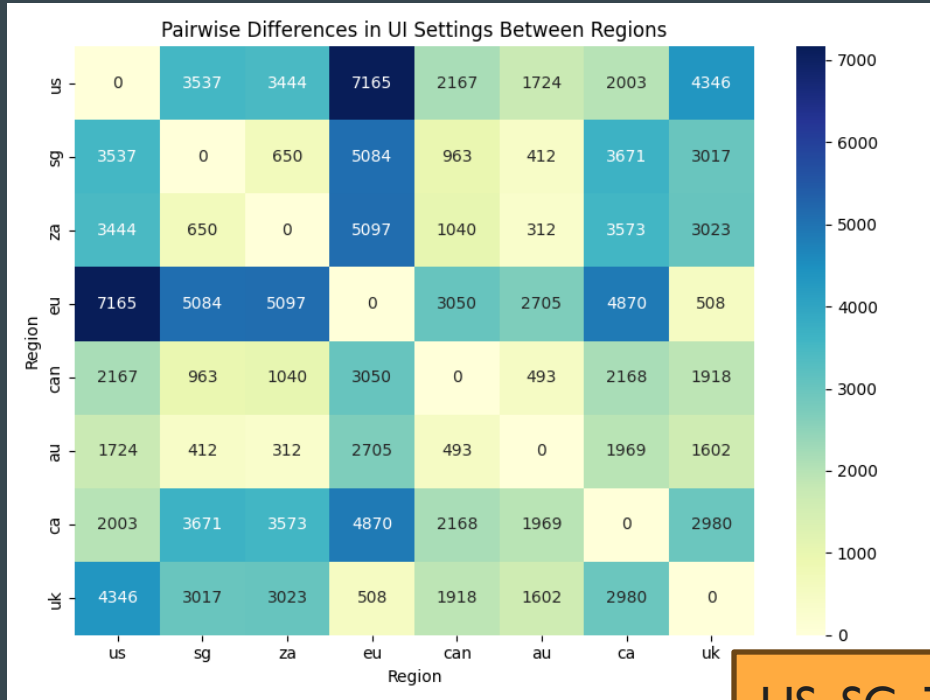
Sites visited from regions with stricter privacy regulations have ~10 more cookie violations.

Finding 4: 3rd Party Cookie Consent Violations



Previous trends are exacerbated by an extra ~6%
for 3rd party cookies

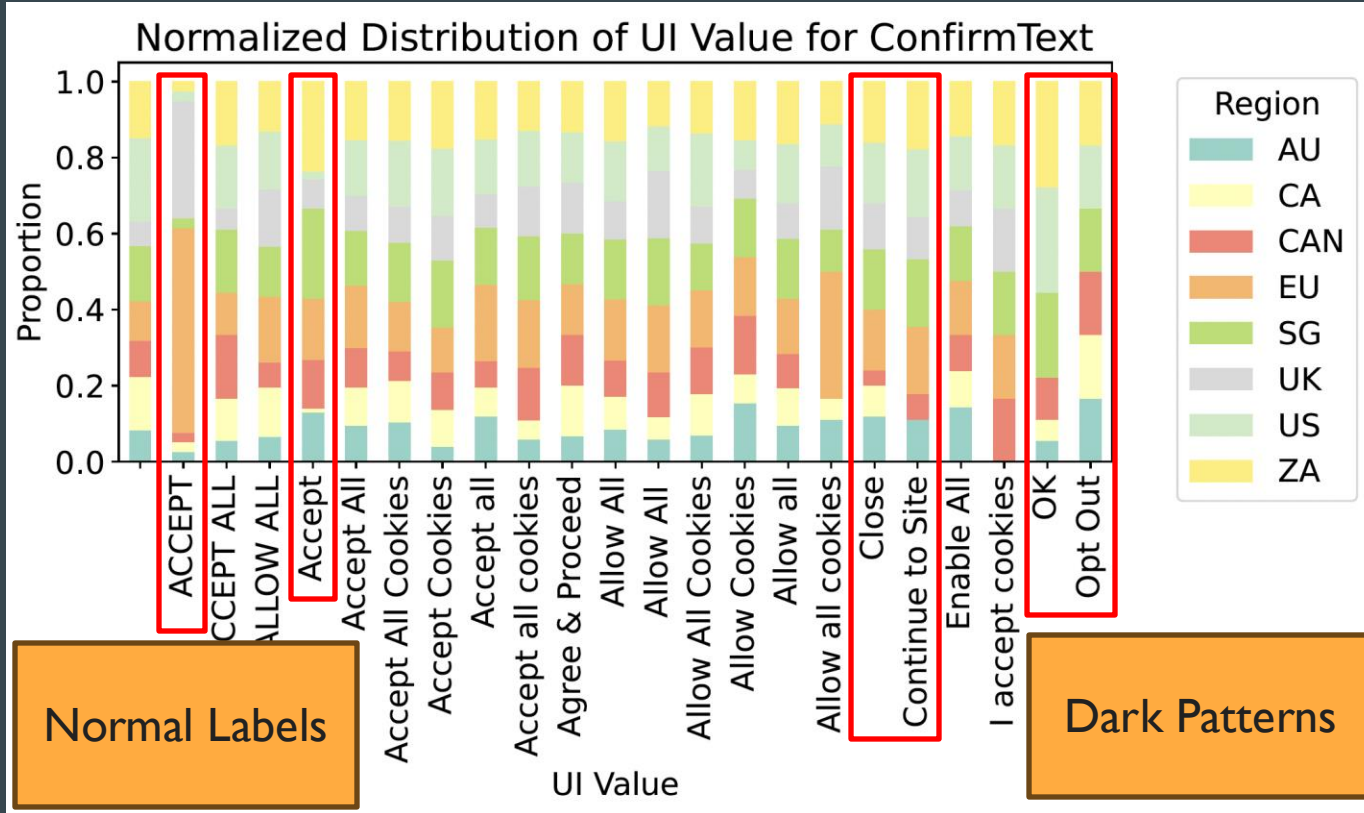
Finding 5: Cookie Banner UI and Behavior Disparities



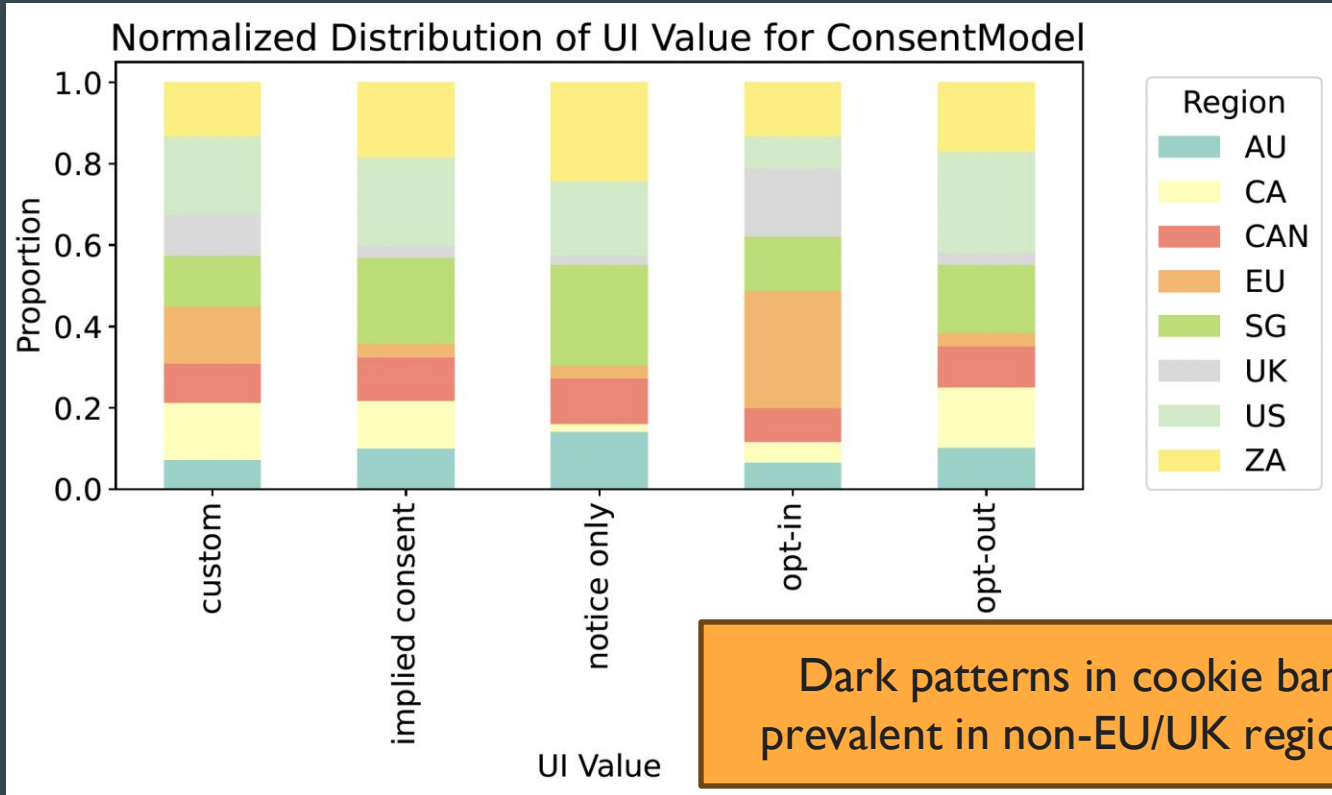
- Metric here is each cookie banner parameter that is different between regions.
 - E.g., button text, colors, position, consent mode, button layout, banner display

US, SG, ZA, CA have most disparities with the EU
SG, ZA, AU, CAN few disparities with each other

Cookie Banner UI Disparities



Cookie Banner Behavior Disparities



Dark patterns in cookie banners are more prevalent in non-EU/UK regions, especially US

Root Causes of Violations: Geolocation Rulesets and Behaviors

usercentrics

Configurations

Geolocation Rulesets

User Management

Company Details

Setup

Legal Specifications

CMP Settings

General Data Protection Regulation (GDPR)

Below you can adjust your settings regarding the General Data Protection Regulation (GDPR).

Regional Settings ⓘ

Display CMP only to EU and EEA users

☐ Reshow GDPR CMP

This resurfaces the CMP and refreshes the users consent choice after the selected time period in months.

☐ Category Consent

Users will be able to consent on category level only. The granular toggles for more detailed co- decisions on Data Processing Service level will not be shown anymore if this feature is enabled

☐ Close CMP without accepting

Users are enabled to close the First Layer of the CMP order to be compliant with regional recommendations. This action is treated in the same way as clicking on Deny All.

Geolocation Rulesets

Create and manage Geolocation Rulesets for an international CMP setup. Learn more in our [documentation](#).

Add Ruleset

GeoRules

...

Rules

Implementation

Rule Name	Regions	Configuration
Default (Global)	All (Global)	Global Config [dKjBORjGMyuXtL]
California	California	US - California [MnxSKo8V8W5tCP]
Europe	Germany, Spain, Italy, France, Denmark, Netherla	Europe & UK [61-0x0ZY6f2IBm]

Geolocation rulesets on CMPs allow for region/regulation specific banners

25

(Website Responsibility)

Why Do Ignored Cookie Rejections Happen?

- Have to place in the <head> before other scripts
- Must update all tracking scripts
 - <script data-usercentrics="Name of Data Processing Service">
- Any scripts loaded afterwards mean cookies will be loaded and not deleted!

Script Tag

Copy the script tag below and paste it into the <head> section of your website. Make sure it is placed before any third-party script that requires user consent.

Auto Blocking



Manual Blocking



```
<script src="https://web.cmp.usercentrics.eu/modules/autoblocker.js">
</script>
<script id="usercentrics-cmp" src="https://web.cmp.usercentrics.eu/ui/loader.js" data-settings-id="xCGkkymMS-0o7V" async></script>
```

How to place the script correctly? ▾

<html>

<head>

```
<script src="https://web.cmp.usercentrics.eu/modules/autoblocker.js"></script>
<script id="usercentrics-cmp" src="https://web.cmp.usercentrics.eu/ui/loader.js" data-settings-id="xCGkkymMS-0o7V" async></script>
```

</head>

<body>

...

</body>

(Website Responsibility)

Why Do Undeclared Cookies Happen?

Developers must label and categorize all cookies that are detected by the crawler but not known to the cookie database.

Status	Service	Category	Domain	Source	Date	Actions
Done	JSDelivr	Essential	https://cdn.jsdelivr.net	https://www.bja...	15.05.2025, 17:22	View Service
Done	Google Maps	Functional	https://www.google.com/maps	https://www.bja...	15.05.2025, 17:22	View Service
Done	gstatic.com	Essential	https://www.gstatic.com	https://www.bja...	15.05.2025, 17:22	View Service
Done	Google Fonts	Functional	https://fonts.googleapis.com	https://www.bja...	15.05.2025, 17:22	View Service
Done	G- Google Calendar	Functional	https://docs.google.com	https://www.bja...	15.05.2025, 17:22	View Service
Done	Google Calendar	Functional	https://calendar.google.com	https://www.bja...	15.05.2025, 17:22	View Service
Done	Google Hosted Libra...	Functional	https://apis.google.com	https://www.bja...	15.05.2025, 17:22	View Service
Done	YouTube Video	Functional	https://www.youtube.com	https://www.bja...	15.05.2025, 17:22	View Service

(Website Responsibility) Dark Patterns

- Developers can set arbitrary labels for your cookie banner buttons
- For example:
 - Button: Accept can be “Close” or “Reject” or “Whatever”

First Layer	Second Layer	Labels
Labels		
Below you can edit all labels used within the Consent Management Platform and translate them for all used languages.		
Label	Current Wording	
Button: Accept (GDPR First Layer)	Accept All	Edit
Button: Accept (GDPR Second Layer)	Accept All	Edit
Button: Deny (GDPR First Layer)	Deny	Edit
Button: Deny (GDPR Second Layer)	Deny	Edit
Button: Save (GDPR)	Save Settings	Edit
Button / Link: More (GDPR)	More Information	Edit
Tab: Categories	Categories	Edit

(CMP Responsibility)

Why Do Cookie Violations Happen?

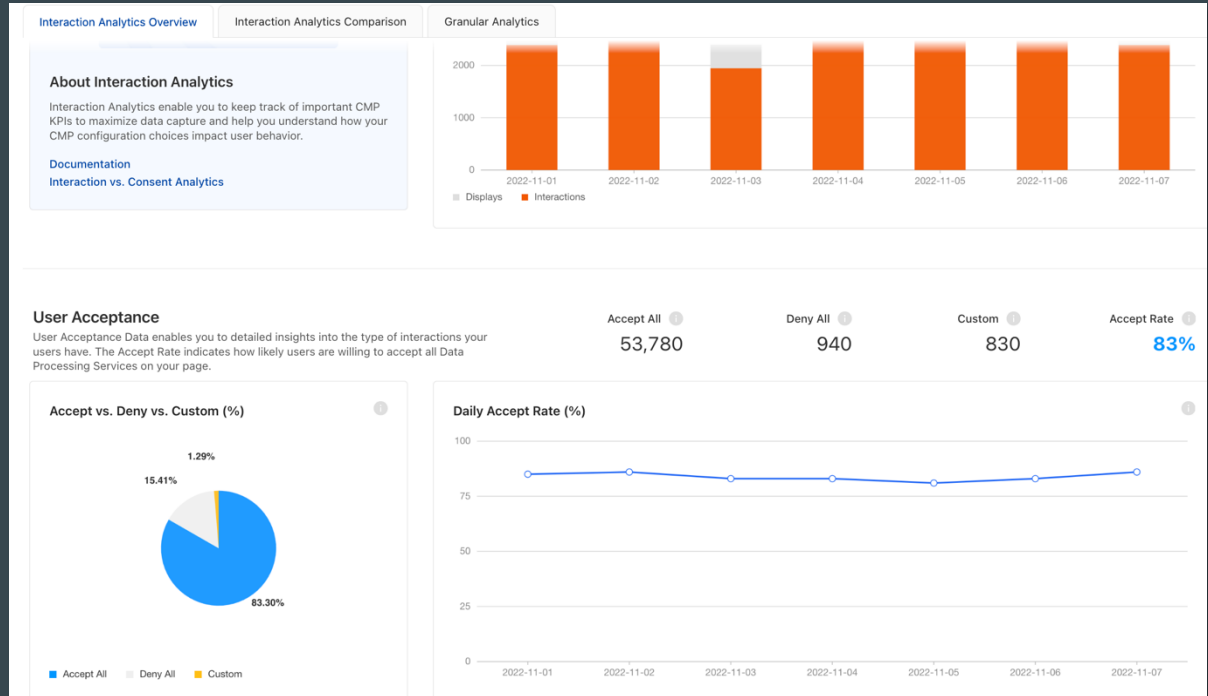
- Ignored Cookie Rejection: Poor documentation on CMP script integrations and script editing.
- Undeclared Cookies: Crawler misses cookies and does not include them in cookie declaration list.



(CMP Responsibility)

Dark Patterns and Dark Incentives

- No guardrails for cookie banner labels
- Analytics that optimize for cookie acceptance rates



4 Years of Measurements

- 2021-2025

Consent Violation Type	UK		US	
	# Cookies	# Websites	# Cookies	# Websites
Rejected Cookie Usage	43,697	82.20% (4,973/6,050)	39,446	81.86% (4,134/5,050)
Consent Choice Omission	52,804	85.02% (5,144/6,050)	70,547	89.05% (4,497/5,050)
Ambiguous Consent	398	4.20% (254/6,050)	345	4.02% (203/5,050)

Inconsistency Type	Ireland (GDPR)		California (CCPA)		Michigan (FTC)		Canada (PIPEDA)	
	# Cookies	% Websites (#)	# Cookies	% Websites (#)	# Cookies	% Websites (#)	# Cookies	% Websites (#)
Rejected Cookie Usage	11,034	82.58% (1,204)	16,417	86.22% (1,201)	15,052	80.76% (1,129)	14,163	80.07% (1,081)
Consent Omission	14,568	88.55% (1,291)	29,725	93.47% (1,302)	36,677	93.13% (1,302)	29,309	92.44% (1,248)
Ambiguous Consent	124	4.53% (66)	101	4.81% (67)	146	5.58% (78)	103	4.89% (66)

Inconsistency Type	South Africa (POPIA)		Singapore (PDPA)		Australia (APP)		UK (DPA)	
	# Cookies	% Websites (#)	# Cookies	% Websites (#)	# Cookies	% Websites (#)	# Cookies	% Websites (#)
Rejected Cookie Usage	12,998	79.32% (1,020)	12,660	77.52% (1,007)	12,993	77.33% (989)	10,662	81.57% (1,164)
Consent Omission	26,637	91.14% (1,172)	23,981	92.07% (1,196)	24,963	92.10% (1,178)	14,920	89.56% (1,278)
Ambiguous Consent	93	5.05% (65)	104	4.93% (64)	94	5.00% (64)	88	4.20% (60)

Violation Type	California (CA)		Ireland (EU)		United Kingdom (UK)		Australia (AU)	
	# Cookies	% Websites	# Cookies	% Websites	# Cookies	% Websites	# Cookies	% Websites
Ignored Cookie Rejection	83,036	88.41%	72,928	86.09%	44,605	84.75%	60,985	80.74%
Undeclared Cookies	115,718	93.61%	87,251	90.19%	54,633	90.04%	99,893	92.86%
Wrong Cookie Category	316	3.03%	365	3.13%	206	2.82%	218	3.20%

Violation Type	Michigan (US)		Singapore (SG)		Canada (CAN)		South Africa (ZA)	
	# Cookies	% Websites	# Cookies	% Websites	# Cookies	% Websites	# Cookies	% Websites
Ignored Cookie Rejection	128,871	84.65%	107,233	82.22%	65,882	81.63%	107,072	81.97%
Undeclared Cookies	250,447	94.15%	167,979	92.90%	117,144	91.20%	165,647	93.56%
Wrong Cookie Category	300	2.50%	395	3.37%	272	3.35%	446	3.69%

Navigating Cookie Consent Violations Across the Globe

Takeaways:

- Cookie consent is still a big part of tracking personal data and privacy
- Privacy laws have a significant impact on cookie consent effectiveness
- CMPs still have a long ways to go for proper implementations of privacy laws
- Websites are inadequate when it comes to managing cookie consent



Resources:

- ❖ Contact: bjaytang@umich.edu | ducui@umich.edu | kgshin@umich.edu
- ❖ Websites: <https://www.bjaytang.com/> | <https://ducui.com/> | <https://web.eecs.umich.edu/~kgshin/>

Paper and Code

