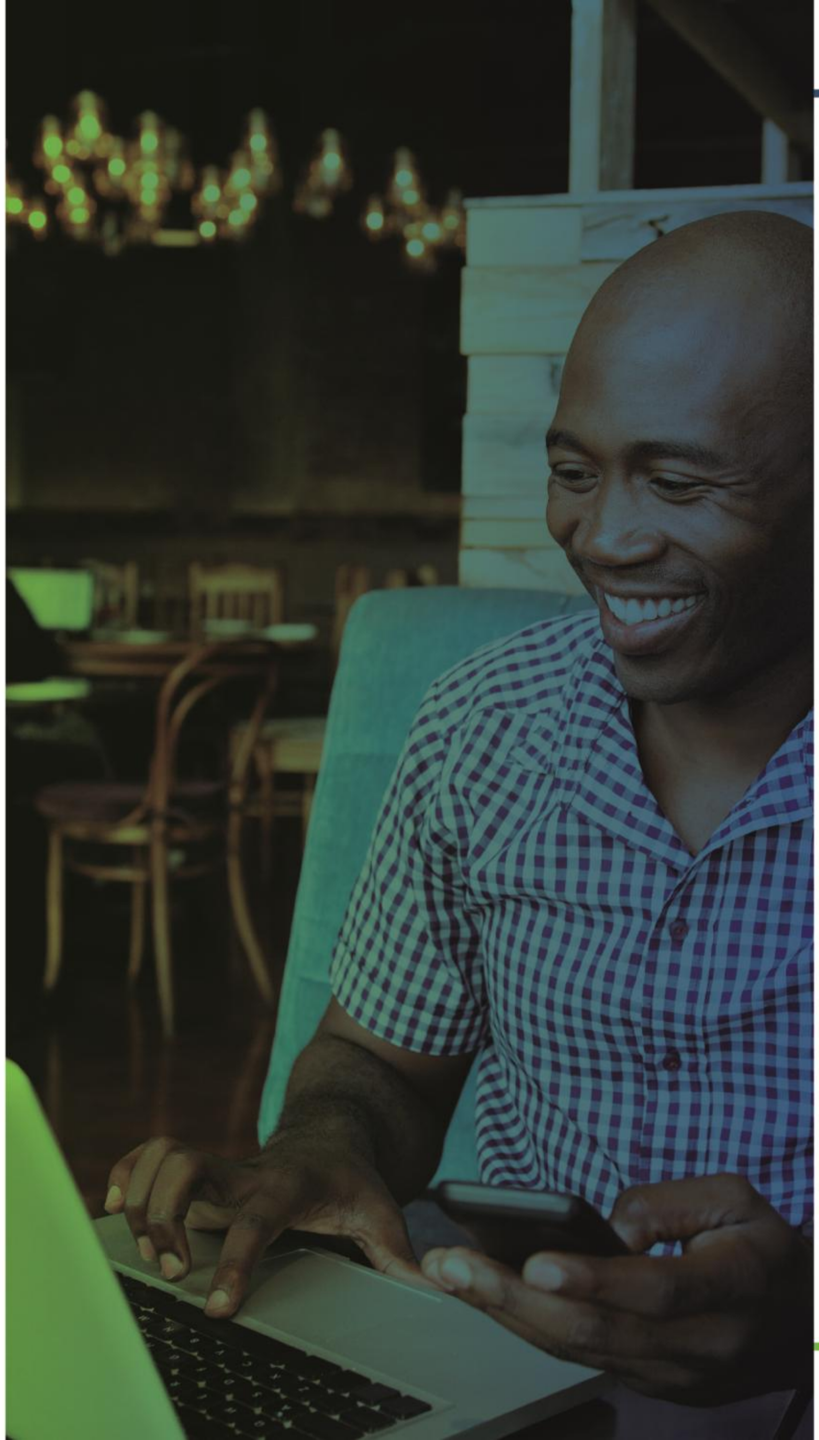


iapp

Avoiding privacy lawsuits in 2026: Lessons from real claims and settlements

Wednesday, 4 March
08:00–09:00 PST
11:00–12:00 EST
17:00–18:00 CET

Welcome & Introductions

Alex Proctor
AIGP, CIPP/E, CIPP/US, CIPM, CIPT, FIP
Chief Trust & Privacy Officer
Captain Compliance

alex@captaincompliance.com

Website Privacy Litigation Overview

Important Laws, Litigation Tactics, & Case References

Private Litigation: A Major Risk Vector

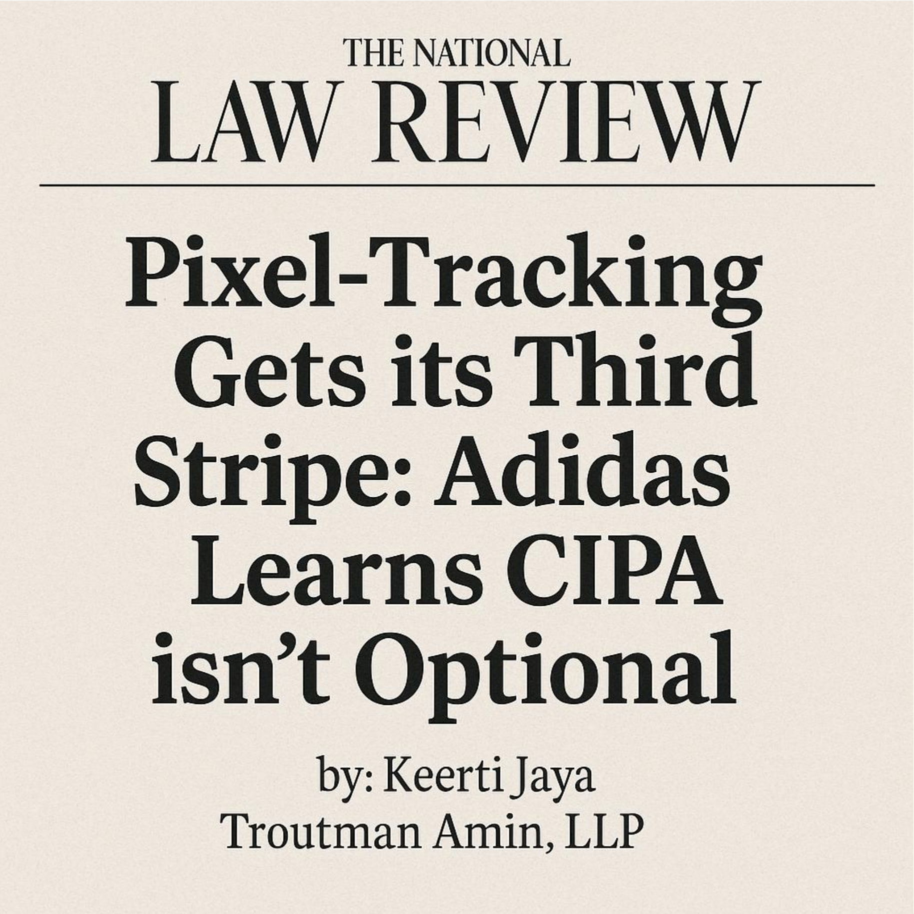
- **Litigation risks** stemming from tracking technologies, consent failures, and misrepresented privacy practices are amongst the most significant privacy risks.

- Opportunistic plaintiff's attorneys are targeting organizations at an unprecedented pace, targeting businesses across a wide variety of industries.

- Privacy lawsuits are leading to **multimillion-dollar settlements**, reputational damage, and significant operational disruptions - even when settled early.

- Businesses of all sizes face litigation risks - unlike the modern privacy laws, there are no revenue or processing thresholds to limit exposure.

- Privacy litigation risk cannot be completely eliminated, but it can be **greatly reduced** through the proactive management of simple privacy practices and controls.



THE NATIONAL
LAW REVIEW

Pixel-Tracking Gets its Third Stripe: Adidas Learns CIPA isn't Optional

by: Keerti Jaya
Troutman Amin, LLP

Reference: https://natlawreview.com/article/pixel-tracking-gets-its-third-stripe-adidas-learns-cipa-isnt-optional

Compliance Risk v. Litigation Risk

Consideration	U.S. Privacy Regulation	U.S. Privacy Litigation
Scope of Applicability	**Narrower:** State-level privacy laws apply to businesses meeting specific revenue or data processing thresholds, often with exemptions for certain industries.	**Broader:** Plaintiffs can generally target any organization handling consumer data - regardless of size or industry - if there is a perceived violation of privacy rights.
Enforcement Likelihood	**Lower:** Enforcement is increasing, with state agencies actively pursuing violations. However, enforcement is less frequent than litigation and some states allow cure periods.	**Higher:** Privacy-related class lawsuits are common and filed frequently, often in response to improper data sharing. Certain litigators have a strong financial incentive.
Financial Impact	**Lower:** Fines for non-compliance can be substantial (often $7,500 per violation). However, the largest penalties to-date are much lower than that of largest litigation settlements.	**Higher:** Class action settlements can be extremely costly, with some settlements costing tens of millions of dollars in high-profile data cases. Legal fees add to the burden.
Reputational Impact	**High:** Regulatory enforcement actions can damage an organization's reputation, especially when high-profile misuse allegations are highly publicized by state regulators.	**High:** Lawsuits can damage an organization's reputation, especially with high-profile data misuse allegations. Litigation can also lead to sustained public backlash.
Overall Risk	**Lower:** The risk of regulatory action is growing as more states enact privacy laws, but enforcement is still inconsistent, and smaller organizations may avoid scrutiny.	**Higher:** Privacy lawsuits are both common and expensive. Most organizations are viable targets, and many have website privacy gaps that can be exploited by litigators.

iapp

Old Wiretapping Laws? But...Why?

- **Wiretapping laws** (like California's CIPA) are at the center of hundreds of website-related lawsuits targeting tools like pixels, chatbots, and analytics.

- Ironically, these decades-old laws are being applied to modern tracking technologies despite being written long before the Internet existed.

- Plaintiffs' attorneys favor wiretapping statutes because they include a private right of action, which most of the modern privacy laws do not include.

- With limited enforcement options under modern laws, wiretapping claims have become a key legal pathway for **challenging website practices**.

- There has been a surge in wiretapping lawsuits against websites, and the long-term viability of these claims remains uncertain as courts issue conflicting rulings.

iapp

CIPA: Californian Wiretapping Law

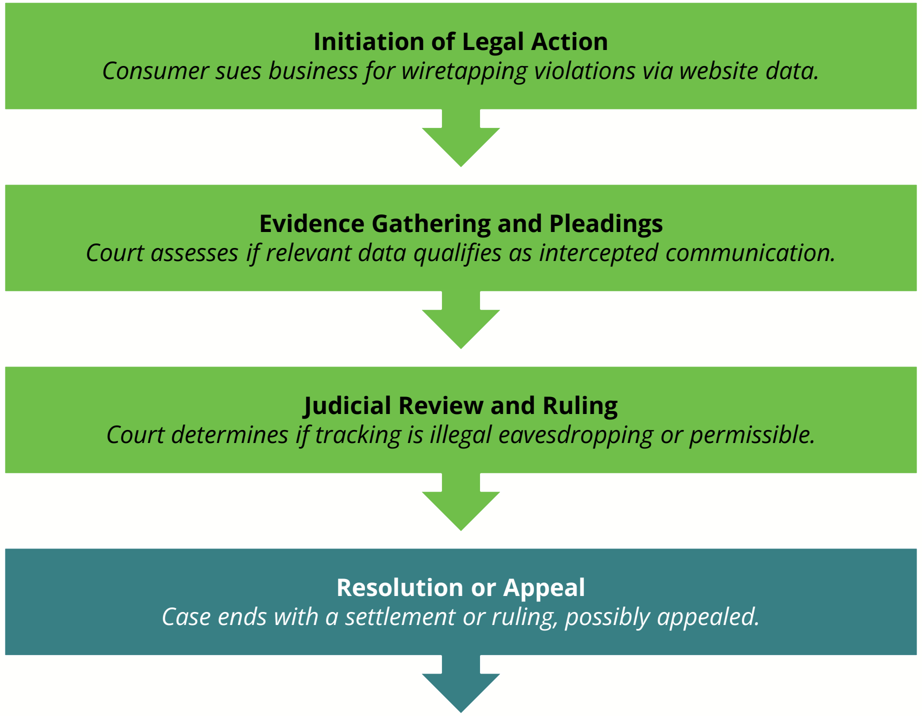
- The **California Invasion of Privacy Act** (CIPA) is a 1960’s wiretapping law at the epicenter of modern website privacy litigation, with over a thousand lawsuits filed since 2022.

- CIPA prohibits the unauthorized interception of communications, and courts have allowed claims that third-party tracking tools function as digital wiretaps when not properly disclosed.

- The law provides statutory damages of **$5,000 per violation**, which can escalate quickly in class actions if each website visit is treated as a separate offense.

- Courts are divided on how CIPA applies to website tracking, with inconsistent rulings on whether session data, clickstream events, or metadata count as intercepted communications.

CIPA & Wiretapping Litigation Sequence



Initiation of Legal Action
Consumer sues business for wiretapping violations via website data.

Evidence Gathering and Pleadings
Court assesses if relevant data qualifies as intercepted communication.

Judicial Review and Ruling
Court determines if tracking is illegal eavesdropping or permissible.

Resolution or Appeal
Case ends with a settlement or ruling, possibly appealed.

Frequently-Cited Sections from CIPA:

CIPA Section	CIPA Section Summary	Modern Considerations
631(a)(i)	Prohibits intentional tapping of any telegraph, telephone wire, line, cable, or (...) communication system instrument.	1. Using session replay tools may be seen as illegal wiretapping if not disclosed. 2. Clearly inform users about tracking tools and offer an opt-out to reduce risk.
631(a)(ii)	Prohibits unauthorized interception and reading of any message, report, or communication contents while in transit.	1. Tracking real-time user data (mouse movements, etc.) may be seen as an interception. 2. Some courts may allow tracking of metadata, like IP addresses and timestamps.
631(a)(iii)	Prohibits use of intercepted communication contents without authorization.	1. Using data from trackers without user consent can lead to liability. 2. If the data is only used to benefit the business, CIPA may not apply.
631(a)(iv)	Prevents a party to the communication from aiding or abetting a third party in committing the above prohibited acts.	1. You may be liable if your tools help others intercept user data without consent. 2. Limit what third parties can do with user data to avoid aiding illegal tracking.
632(a)	Requires consent from all parties before recording any confidential communications	1. Not getting consent before recording interactions (e.g., via chatbots) can violate CIPA. 2. Use opt-in tools to reduce legal risk and improve compliance.
638.51(a)	Prohibits use of a pen register without a court order or the user's prior consent.	1. Tracking IP addresses or device fingerprints may count as using a pen register. 2. Courts might dismiss if the data isn't personal or the plaintiff lacks standing.

Reference: https://iapp.org/resources/article/us-litigation-series-website-tracking/

ECPA: Federal Wiretapping Law

- The **Electronic Communications Privacy Act** (ECPA) is a federal law passed in 1986 that protects against unauthorized interception and access to electronic communications such as phone calls, emails, and certain internet activity.

- ECPA is cited less frequently in website tracking lawsuits because it allows one-party consent, making it harder to claim unlawful interception.

- Unlike California's CIPA, which requires all-party consent and provides statutory damages, ECPA offers fewer remedies and may be less optimal for litigators. Still, it is called upon regularly.

- Like CIPA, ECPA's protections were written before the rise of modern web technologies, which has led to growing criticism that the law is outdated and poorly suited to today's digital privacy risks.

CIPA vs. ECPA

Feature	CIPA	ECPA
Relevant Jurisdiction	California Law	Federal Law
Consent Standard	All-Party Consent	One-Party Consent
Web Privacy Litigation	Extremely Prominent	Often Paired with CIPA
Statutory Damages	$5,000/Violation / Actual Damages	$100/Day / Actual Damages (Max $10,000 /Violation)
Private Right Of Action	Yes	Yes

Who is Filing These Lawsuits?

- A relatively small group of law firms and self-representing individuals have seemingly made CIPA litigation a core business, targeting companies using non-essential tracking technologies while lacking effective consent mechanisms and strong disclosures.

- One "privacy advocate" has been bringing extremely extreme volumes of nearly-identical suits involving session replay tools, chat widgets, and pixel tracking.

- These demands may allege typically allege unauthorized interception under CIPA § 631(a) and often seeks large sums in statutory damages.

- These plaintiffs routinely pair CIPA with federal ECPA claims or other theories to increase pressure.

- Complaints rely on broad readings of concepts including "contents," "interception", "pen register," etc.

What Factors Decide These Cases?

- Wiretapping laws apply to real-time interception of communications and generally do not apply to any forms of stored or passively-routed data.

- Wiretapping laws regulate interception of **communication content**, while related pen register provisions govern **routing/addressing metadata**.

- **Consent** can be relied upon to defeat a wiretapping claim, but it *may* need to be obtained before tracking occurs, and privacy notices must be strong.

- There is generally no liability if the defendant or a third party is a direct participant, but courts question whether third parties gain independent benefit or not.

- Courts are divided on whether privacy invasion alone is enough to sue, with many requiring concrete injury.

CIPA Case: Javier v. Assurance IQ

- **Javier v. Assurance IQ** was a pivotal Ninth Circuit case involving session replay technology used throughout the course of an online insurance quote process.

- Session replay tools (in this case, TrustedForm) record user interactions on websites and may violate CIPA if used without prior consent from all parties.

- The court held that **retroactive consent** (in this case, agreeing to privacy terms after filling out an insurance application form) was **not valid** under CIPA, citing that consent must be obtained before recording begins.

- This ruling exposed a **major point of tension** that companies must currently navigate in the United States – the idea that prior consent is required under CIPA conflicts directly with the opt-out models generally allowed by modern state privacy laws.

CIPA Case: Yoon v. Lululemon USA

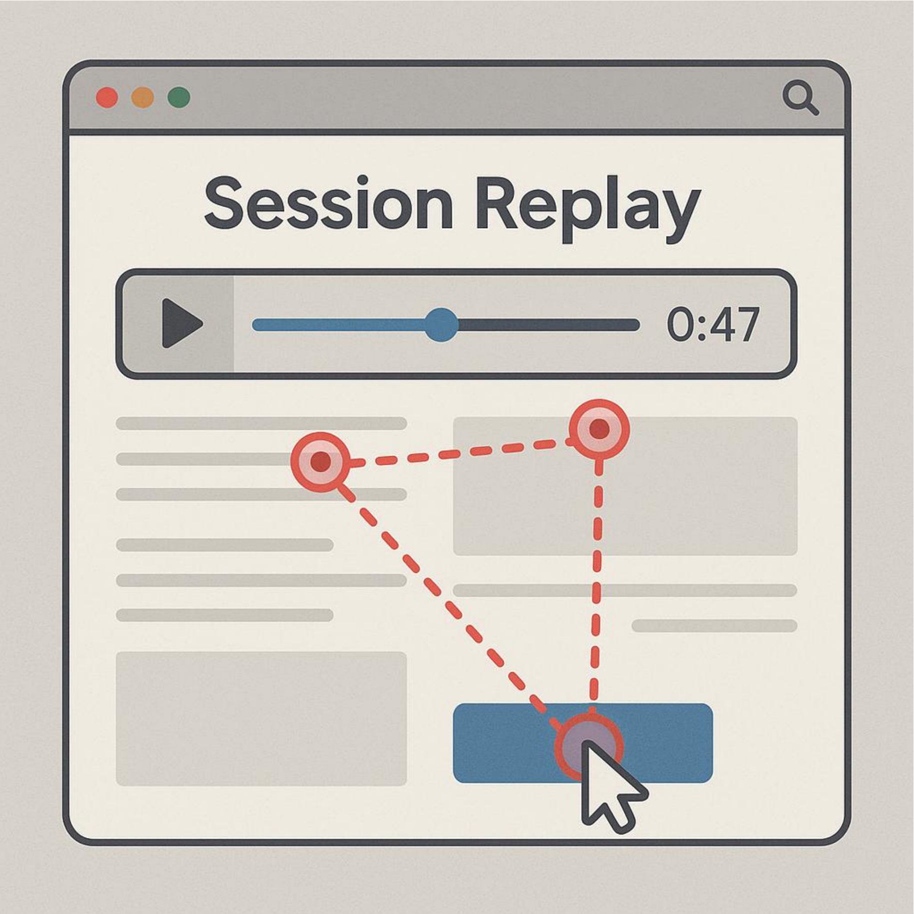
- **Yoon v. Lululemon** involved CIPA claims over Lululemon's use of session replay tech (in this case, Quantum Metric), pointing to weak privacy notices and lack of user consent to the terms of the notice.

- The court questioned if Quantum Metric was a third party or direct participant, noting that embedded tools can still be treated as third parties.

- The court took a narrow view of "content," finding clicks, keystrokes, and billing info to be **metadata**, rather than protected communication content.

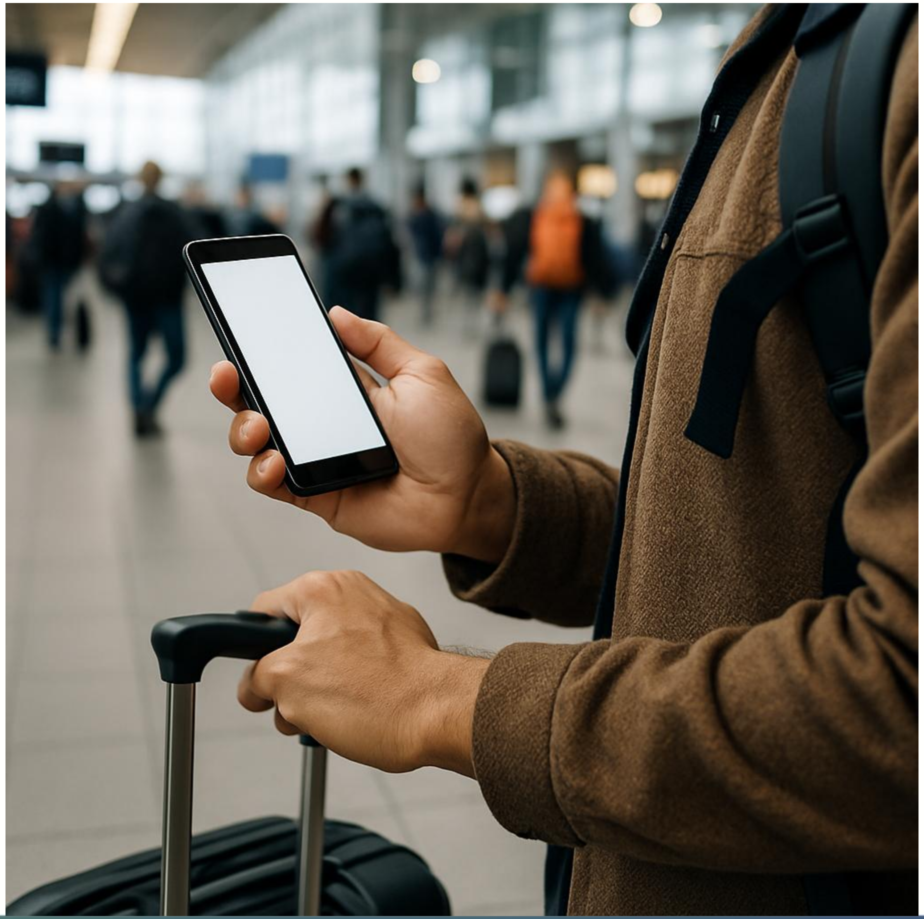
- Claims under CIPA section 631(a)(iv) were allowed to proceed, confirming that businesses may be liable for aiding third-party wiretaps if users aren't aware.

- Vague notices, lack of consent, and unclear data-sharing practices with tools can all lead to liability.



CIPA Case: Greenley v. Kochava

- **Greenley v. Kochava** marked a strategic shift in CIPA litigation, focusing on California's pen register law under Section 638.51 rather than wiretapping claims.
- The case targeted Kochava's mobile SDK, which collects user location and device data across mobile applications, allegedly without valid consent.
- A **pen register** records outgoing routing or signaling info (like phone numbers or device IDs), without capturing content (**trap and trace** devices serve a similar role for incoming connections).
- The court held that Kochava's SDK could qualify as a digital pen register, emphasizing the core function of a pen register over the traditional physical format.
- Claim survived dismissal and opened the door to new lawsuits targeting SDKs, pixels, and embedded tools.



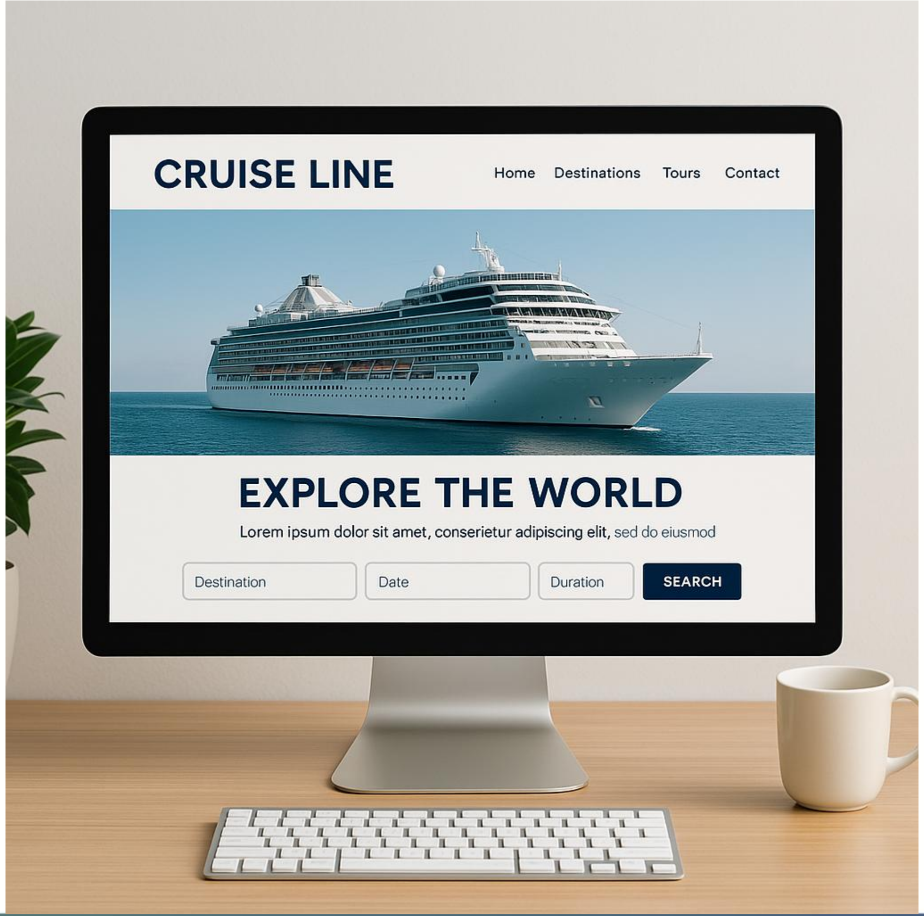
ECPA Case: Price v. Carnival Corporation

- In **Price v. Carnival Corporation**, plaintiffs accused Carnival of unlawfully using **Microsoft Clarity**, a session replay tool, to track and record website user interactions without consent, violating the federal **Electronic Communications Privacy Act (ECPA)**.

- The lawsuit argued that using Microsoft Clarity to intercept user data constituted illegal wiretapping, infringing on users' privacy rights.

- ECPA's one-party consent rule didn't apply because Clarity was considered a separate third party intercepting the data, and users did not consent.

- A federal judge ruled that the wiretap and invasion of privacy claims could proceed, litigation concluded after plaintiffs voluntarily dismissed the action pursuant to a reported settlement.



CIPA Case: Camplisson v. Adidas

- **Camplisson v. Adidas** involved CIPA claims under California's Pen Register statute, section 638.51, based on allegations that Adidas deployed third party pixels that captured users' IP addresses and transmitted them to external partners.

- Plaintiffs argued that the pixel vendor acted as a third party interceptor by collecting routing information, and the court declined to treat the vendor as a direct participant in the communication.

- The court emphasized that pen register provisions focus on the capture of dialing, routing, and addressing information and do not require the interception of communication content.

- The court found that IP address collection can qualify as pen register activity when the data is logged and transmitted for use by a third party.

The Hot New Trend: Search Bar Allegations

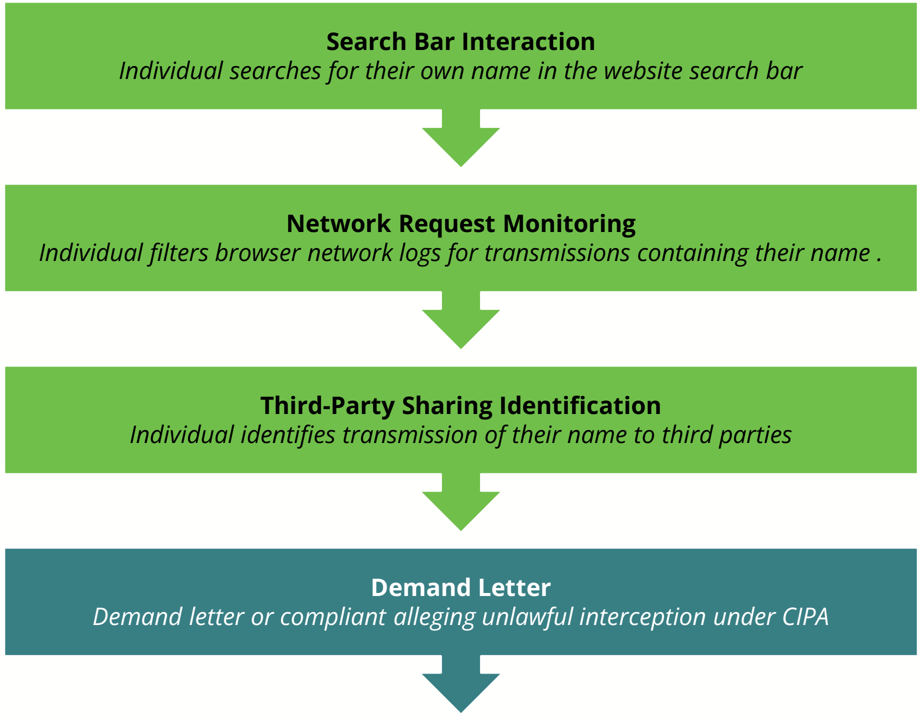
- A recent wiretapping litigation trend targets website search bars. Plaintiffs opt out of tracking (if available) and then **search their <u>own name</u> on the website**.

- If the website <u>builds a URL</u> containing the search term and sends it to third parties (i.e., analytics vendors), plaintiffs can observe this via network monitoring and allege an unauthorized wiretapping “interception”.

- These cases characterize search queries as protected “content” when shared in real time with third parties, <u>even when the alleged harm results from a plaintiff intentionally searching for their own name</u>.

- Risk can be reduced by removing search terms from URLs, limiting transmission of search data, and gating relevant scripts behind consent logic, <u>including for scripts that do not rely on client-side storage (cookies)</u>.

<u>Search Bar Allegation Sequence</u>



Search Bar Interaction
Individual searches for their own name in the website search bar

Network Request Monitoring
Individual filters browser network logs for transmissions containing their name .

Third-Party Sharing Identification
Individual identifies transmission of their name to third parties

Demand Letter
Demand letter or compliant alleging unlawful interception under CIPA

CIPA Case: Heerde v. Learfield

- **Heerde v. Learfield Communications** arose under CIPA section 631(a), after plaintiffs alleged that when users entered search terms into the website's search bar, those queries were transmitted in real time to a third-party service provider through network requests and URL parameters.

- Plaintiffs alleged that the relevant college athletic websites appeared to be run directly by the schools themselves but were in fact operated by an external company that embedded third party tracking tools.

- Plaintiffs argued the operators unlawfully intercepted search bar entries that users reasonably expected to be communicated only to the schools.

- The court allowed the claim to proceed on the theory the embedded vendor could be treated as a third-party interceptor.

Reference: https://www.fisherphillips.com/en/insights/insights/from-search-to-share-court-holds-third-party-interception-of-search-bar-terms-can-support-cipa-claim

VPPA: Video Privacy Protection Act

- The **Video Privacy Protection Act (VPPA)** prohibits video tape service providers from disclosing a consumer's personally identifiable information (PII) - *especially video rental records* - without consent, with only limited exceptions.

- Congress enacted the VPPA in 1988 after a journalist published Robert Bork's video-rental history during his Supreme Court nomination, sparking bipartisan concern over how easily viewing habits were exposed.

- Like the old wiretapping laws, the VPPA has found new life in modern litigation. Plaintiffs argue that websites **offering video content and sharing viewing data with third parties** are violating the VPPA.

- Courts have applied the VPPA to digital video providers and online tracking scenarios, but interpretations vary significantly across jurisdictions.

VPPA Case: Salazar v. NBA

- In **Salazar v. NBA (**October 2024), the Second Circuit ruled on a VPPA case examining whether a website user counts as a "consumer" under the Video Privacy Protection Act (1988).

- Michael Salazar, who signed up for a free NBA newsletter and watched videos on NBA.com, qualified as a "consumer" under the VPPA - even without a video-specific subscription.

- The court held that the NBA might have breached the VPPA by sharing Salazar's video-viewing data with Meta (via **Facebook Pixel**) without consent.

- The NBA petitioned the Supreme Court in March 2025 to review the Second Circuit's findings on standing and VPPA scope, and proceedings remain ongoing.

We'll See You at IAPP GPS 2026!

Richart Ruddie
Founder
Captain Compliance

Sam Seliger
Chief Revenue Officer
Captain Compliance

Alex Proctor
Chief Trust & Privacy Officer
Captain Compliance

Seth Gelblum
Account Executive
Captain Compliance

iapp

Website Privacy Litigation Risk Reduction

Examining a Spectrum of Risk Reduction Options

Privacy Notices and Tracking Disclosures

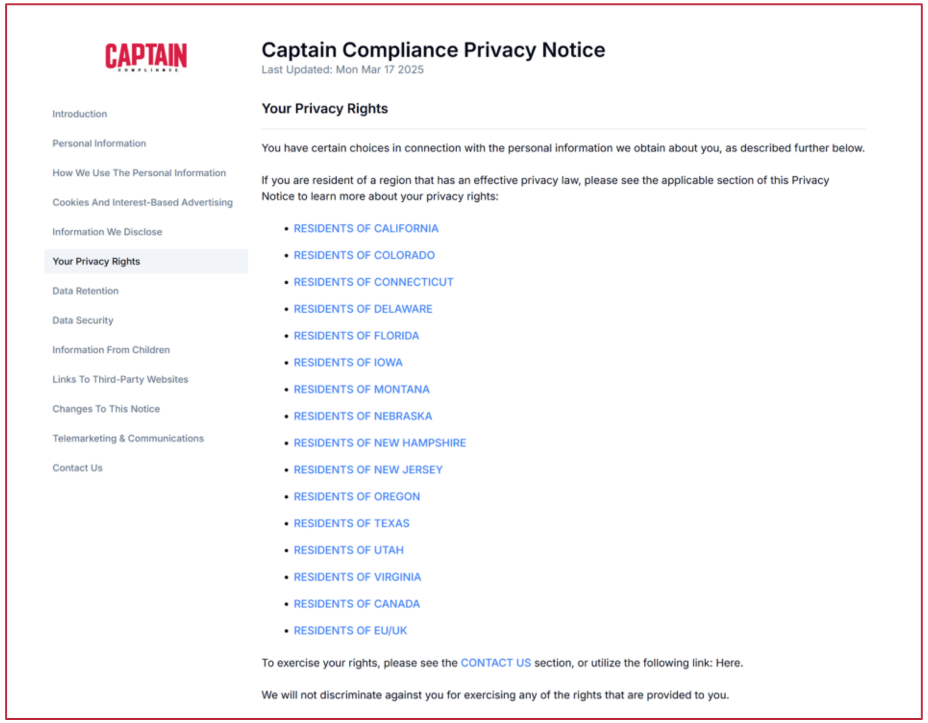
- A **privacy notice** is a publicly-available statement that explains how an organization processes and protects personal data. It should also inform individuals about their rights and how they can execute them.

- One major concern is **deceptive or misleading privacy practices**. If your privacy notice says one thing, but your company actually does something different, you risk legal action.

- Comprehensive privacy laws in the U.S. generally require businesses to provide accessible, clear, and meaningful privacy notices with specific content.

- Privacy notices also play a critical role in reducing litigation risk, as **inconsistent or unclear disclosures are often at the center of privacy lawsuits**.

Privacy Notice Example (Partial)


CAPTAIN
COMPLIANCE
Introduction
Personal Information
How We Use The Personal Information
Cookies And Interest-Based Advertising
Information We Disclose
Your Privacy Rights
Data Retention
Data Security
Information From Children
Links To Third-Party Websites
Changes To This Notice
Telemarketing & Communications
Contact Us

Captain Compliance Privacy Notice

Last Updated: Mon Mar 17 2025

Your Privacy Rights

You have certain choices in connection with the personal information we obtain about you, as described further below.

If you are resident of a region that has an effective privacy law, please see the applicable section of this Privacy Notice to learn more about your privacy rights:

- RESIDENTS OF CALIFORNIA
- RESIDENTS OF COLORADO
- RESIDENTS OF CONNECTICUT
- RESIDENTS OF DELAWARE
- RESIDENTS OF FLORIDA
- RESIDENTS OF IOWA
- RESIDENTS OF MONTANA
- RESIDENTS OF NEBRASKA
- RESIDENTS OF NEW HAMPSHIRE
- RESIDENTS OF NEW JERSEY
- RESIDENTS OF OREGON
- RESIDENTS OF TEXAS
- RESIDENTS OF UTAH
- RESIDENTS OF VIRGINIA
- RESIDENTS OF CANADA
- RESIDENTS OF EU/UK

To exercise your rights, please see the CONTACT US section, or utilize the following link: Here.

We will not discriminate against you for exercising any of the rights that are provided to you.

Consent Management Platforms (CMPs)

- Cookies are **small text files** that are stored on your device by websites that you visit. They are used for a variety of purposes - both essential and non-essential.

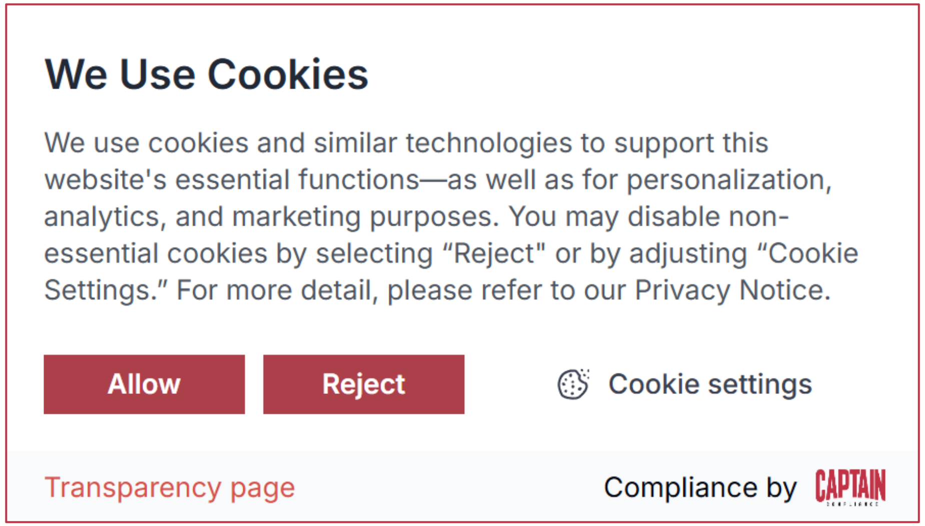
- Cookies have major privacy implications as they are often used to facilitate targeted advertising and can also involve data-sharing with third-party providers.

- Not all web tracking uses cookies, so consent obligations are not exclusive to cookie-based tracking.

- In contrast with the GDPR and some international privacy laws, the existing U.S. state laws *generally allow* for an "opt-out" consent model, so long as clear notice as provided along with relevant opt-out mechanisms.

- **There is a major "grey area" in the U.S. as it relates to wiretapping case law**! (See Javier v. Assurance IQ!)

Consent Management / Cookie Banner Example

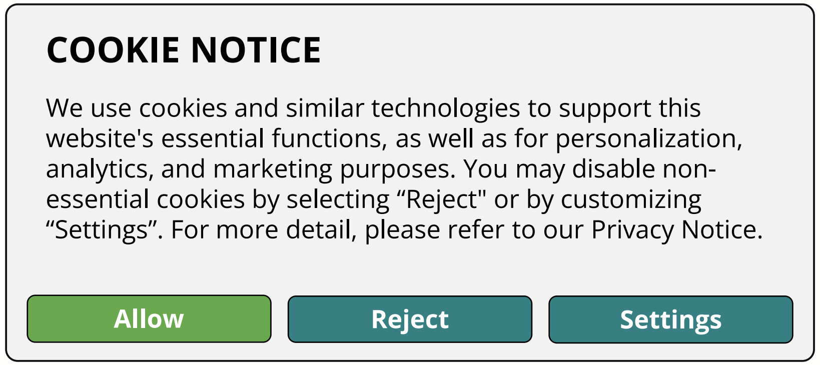


We Use Cookies

We use cookies and similar technologies to support this website's essential functions—as well as for personalization, analytics, and marketing purposes. You may disable non-essential cookies by selecting "Reject" or by adjusting "Cookie Settings." For more detail, please refer to our Privacy Notice.

Which Banner(s) Contain Dark Patterns?

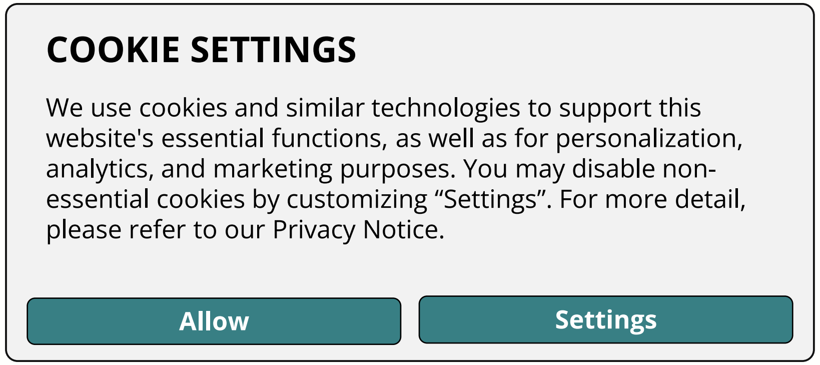
A



COOKIE NOTICE

We use cookies and similar technologies to support this website's essential functions, as well as for personalization, analytics, and marketing purposes. You may disable non-essential cookies by selecting “Reject" or by customizing “Settings”. For more detail, please refer to our Privacy Notice.

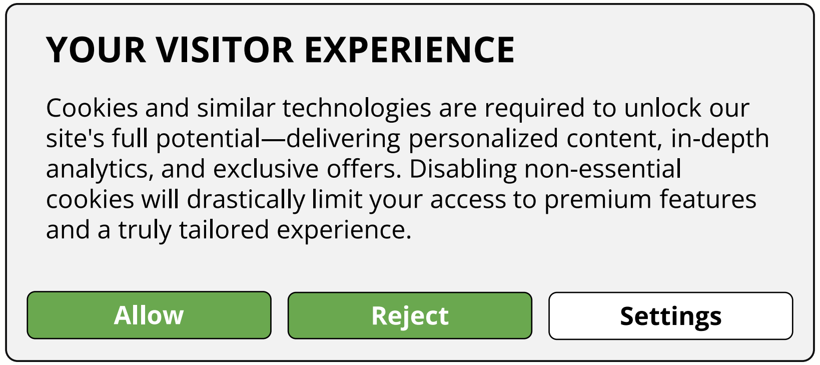
B



COOKIE SETTINGS

We use cookies and similar technologies to support this website's essential functions, as well as for personalization, analytics, and marketing purposes. You may disable non-essential cookies by customizing “Settings”. For more detail, please refer to our Privacy Notice.

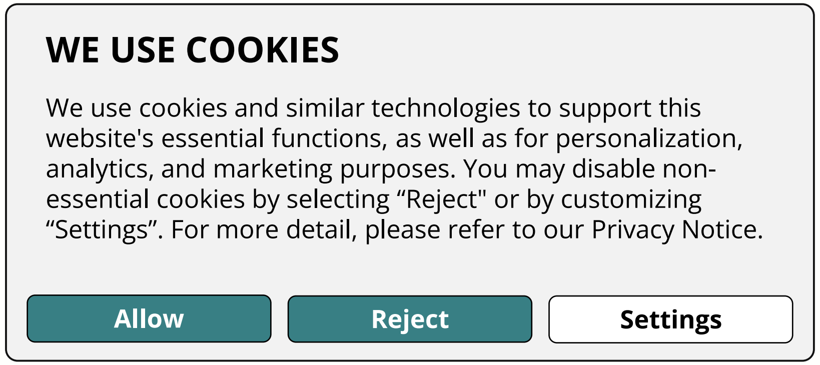
C



YOUR VISITOR EXPERIENCE

Cookies and similar technologies are required to unlock our site's full potential—delivering personalized content, in-depth analytics, and exclusive offers. Disabling non-essential cookies will drastically limit your access to premium features and a truly tailored experience.

D

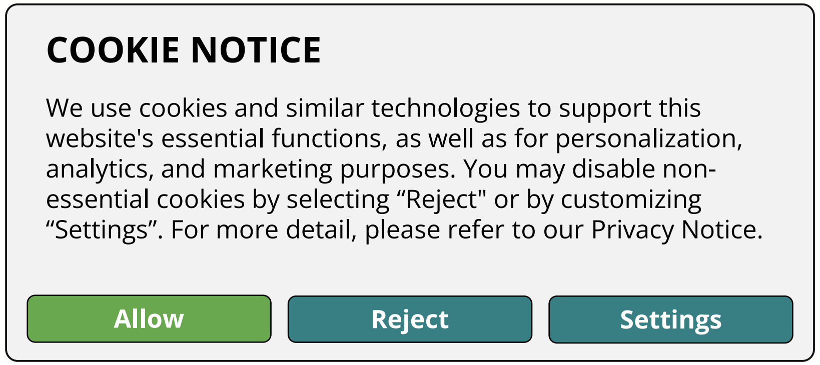


WE USE COOKIES

We use cookies and similar technologies to support this website's essential functions, as well as for personalization, analytics, and marketing purposes. You may disable non-essential cookies by selecting “Reject" or by customizing “Settings”. For more detail, please refer to our Privacy Notice.

Which Banner(s) Contain Dark Patterns?

A

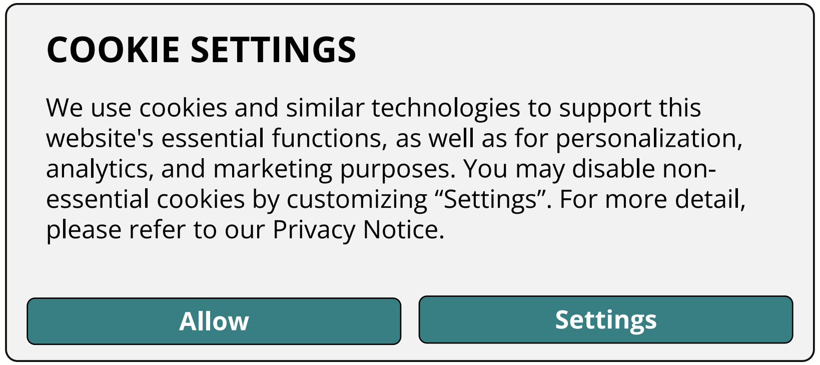


COOKIE NOTICE

We use cookies and similar technologies to support this website's essential functions, as well as for personalization, analytics, and marketing purposes. You may disable non-essential cookies by selecting “Reject" or by customizing “Settings”. For more detail, please refer to our Privacy Notice.

Dark Pattern: “Allow” Button Color

B

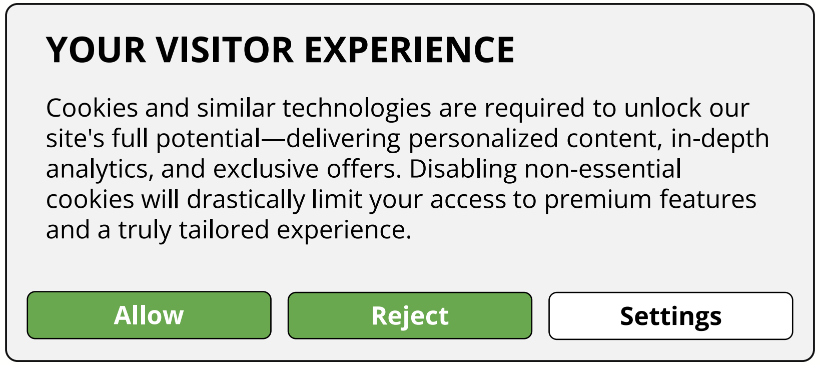


COOKIE SETTINGS

We use cookies and similar technologies to support this website's essential functions, as well as for personalization, analytics, and marketing purposes. You may disable non-essential cookies by customizing “Settings”. For more detail, please refer to our Privacy Notice.

Dark Pattern: Asymmetrical Choices

C

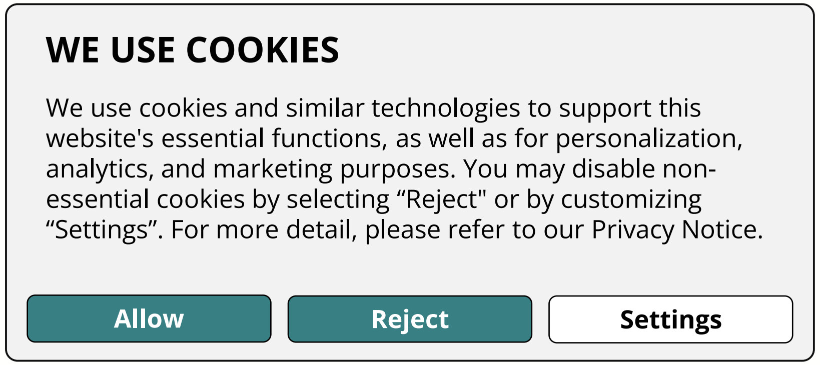


YOUR VISITOR EXPERIENCE

Cookies and similar technologies are required to unlock our site's full potential—delivering personalized content, in-depth analytics, and exclusive offers. Disabling non-essential cookies will drastically limit your access to premium features and a truly tailored experience.

Dark Pattern: Persuasive Language

D



WE USE COOKIES

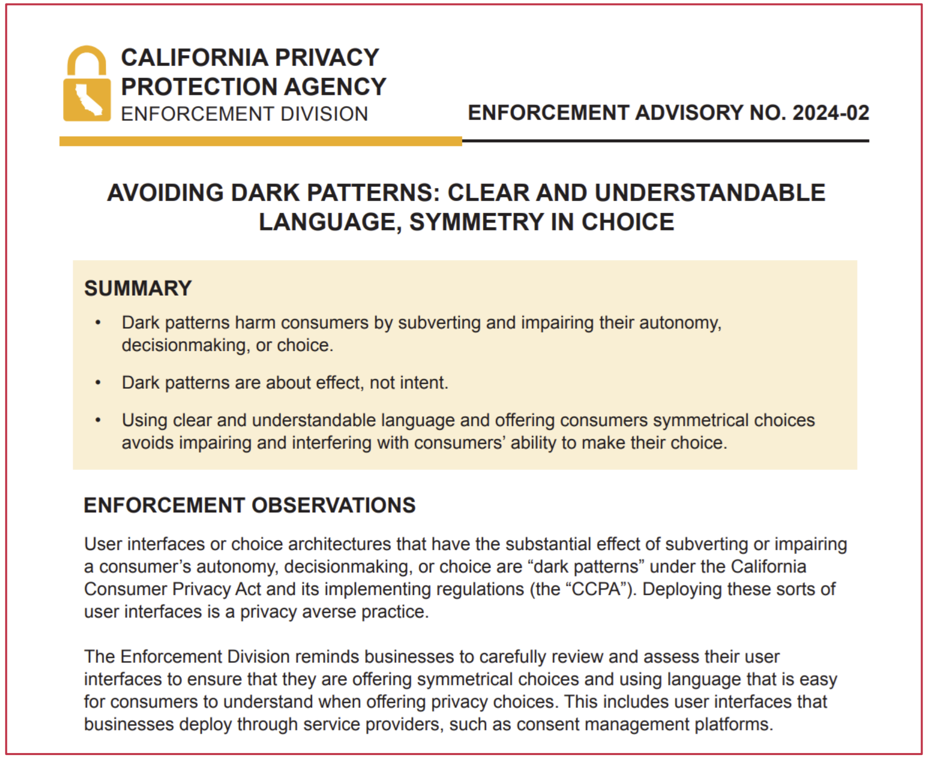
We use cookies and similar technologies to support this website's essential functions, as well as for personalization, analytics, and marketing purposes. You may disable non-essential cookies by selecting “Reject" or by customizing “Settings”. For more detail, please refer to our Privacy Notice.

Dark Pattern: None (Compliant Design)

Dark Patterns & Deceptive Designs

- A **dark pattern** is a user interface design intentionally crafted to subvert or impair consumers' autonomy, decision-making, or ability to choose freely.
- Dark patterns often relate to the following deceptive designs: **complex or confusing language**, **interface elements**, **nagging**, **obstruction**, or **forced action**.
- While EU regulators have been addressing dark patterns for years, US authorities are now increasingly focusing on dark patterns in regulatory actions.
- Businesses are **required** to utilize clear, straightforward language and offer symmetrical, balanced choices, ensuring that no option is made more difficult to select than another.
- Consent obtained using dark patterns may be deemed invalid, highlighting the importance of fair interaces.

CCPA Dark Pattern Advisory: September 2024



CALIFORNIA PRIVACY PROTECTION AGENCY
ENFORCEMENT DIVISION

ENFORCEMENT ADVISORY NO. 2024-02

AVOIDING DARK PATTERNS: CLEAR AND UNDERSTANDABLE LANGUAGE, SYMMETRY IN CHOICE

SUMMARY

- Dark patterns harm consumers by subverting and impairing their autonomy, decisionmaking, or choice.
- Dark patterns are about effect, not intent.
- Using clear and understandable language and offering consumers symmetrical choices avoids impairing and interfering with consumers' ability to make their choice.

ENFORCEMENT OBSERVATIONS

User interfaces or choice architectures that have the substantial effect of subverting or impairing a consumer's autonomy, decisionmaking, or choice are "dark patterns" under the California Consumer Privacy Act and its implementing regulations (the "CCPA"). Deploying these sorts of user interfaces is a privacy averse practice.

The Enforcement Division reminds businesses to carefully review and assess their user interfaces to ensure that they are offering symmetrical choices and using language that is easy for consumers to understand when offering privacy choices. This includes user interfaces that businesses deploy through service providers, such as consent management platforms.

A Key Business Decision: Opt-Out v. Opt-In

- In some regions, CMP configuration decisions tend to be straightforward. For example, the EU requires an **opt-in consent model** for non-essential tracking.

- In the United States, businesses must make a **risk-based business decision** about whether to fire non-essential tracking technologies by default – especially given the previously-mentioned "grey area".

- The opt-in model is the most effective at reducing litigation and regulatory risk, but it carries a signifiant business impact. Because an estimated **95–98% of users do not interact with consent banners**, the (more restrictive) default setting is usually retained.

- As a result, many organizations adopt an **opt-out model** in the U.S., knowingly accepting some residual legal and litigation exposure in exchange for stronger analytics data continuity and marketing performance.

Opt-Out Model v. Opt-In Model

Consent Model	**Opt-Out Model**	**Opt-In Model**
European Union	Not Permissible	Required
United States	**Generally Permissible (Modern Privacy Laws)**	**Potentially Required (SOME CIPA Case Law)**
Default Behavior (Initial Website Load)	Only Essential Trackers Fire	All Trackers Fire
What Happens if the Visitor Does Not Interact with CMP?	Default Behavior Remains In-Place	Default Behavior Remains In-Place
Impact to Analytics Data Collection & Online Marketing	Very Low *(Often 1%-2% Impact)*	Very High *(Often 98-99% Impact)*
Overall Litigation Risk Reduction	**Moderate**	**Very High**

Common Issue: Broken & Faulty CMPs

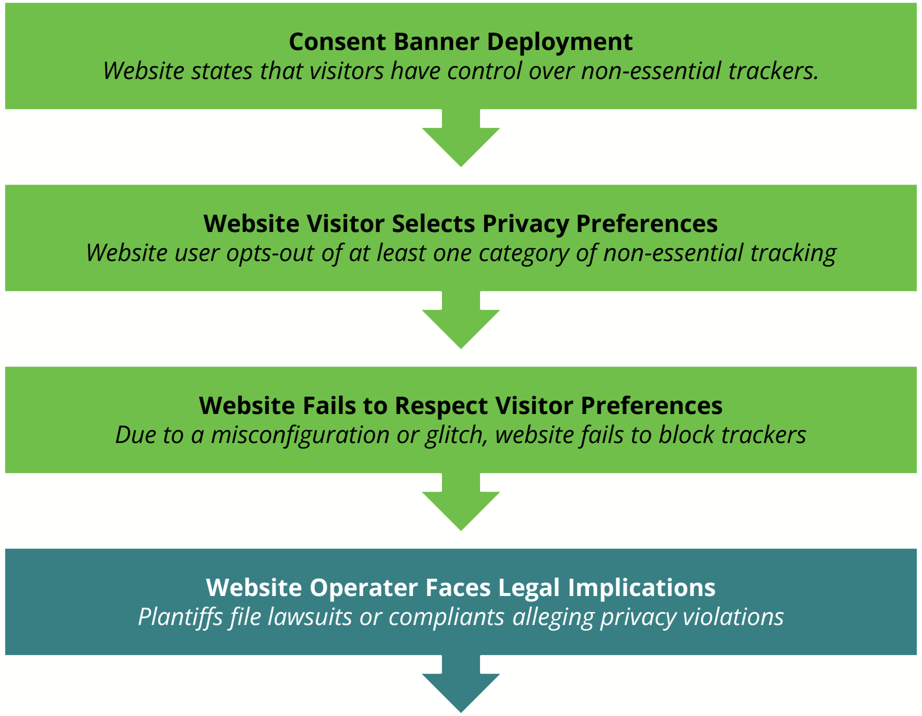
- When a consent banner **fails to block** non-essential cookies or other trackers in response to website visitor opt-outs, it misleads users about their privacy.

- Lawsuits across the country are targeting various industries over these banner failures, alleging misrepresentation of data-collection practices.

- Plaintiffs are pursuing faulty consent banner litigation under various statutes and claims - relating to invasion of privacy, intrusion upon seclusion, wiretapping, misrepresentation, etc.

- Regular testing and monitoring of consent banners is crucial to prevent unnoticed malfunctions and avoid costly litigation - this is especially important after initial deployment, as websites frequently update their design, content, and practices over time.

Problematic Consent Banner Deployment



Consent Banner Deployment
Website states that visitors have control over non-essential trackers.

Website Visitor Selects Privacy Preferences
Website user opts-out of at least one category of non-essential tracking

Website Fails to Respect Visitor Preferences
Due to a misconfiguration or glitch, website fails to block trackers

Website Operater Faces Legal Implications
Plantiffs file lawsuits or compliants alleging privacy violations

Cookie Blocking v. Script Blocking

- There are two primary technical layers through which commercial CMPs operate: **cookie auto-blocking** and **script-level blocking**.

- **Cookie auto-blocking** refers to a CMP's ability to delete, expire, or nullify client-side browser storage.

- **Script blocking** refers to a CMP's ability to "wrap" or conditionally load scripts based on consent logic, including trackers that do not rely on cookies.

- Script blocking is more proactive because it prevents tracking technologies from loading in the first place, (including scripts that do not rely on cookies), while cookie auto-blocking is simpler yet more reactive and cannot address tracking beyond browser storage.

- Mature, defensible deployments typically rely on **both layers** to reduce litigation and regulatory exposure.

Cookie Auto-Blocking v. Script Blocking

Blocking Layer	Cookie Auto-Blocking	Script Blocking
General Concept	Cookies Are Deleted/Nullified When Certain Tracking is Off/Rejected	Scripts/Tags Do Not Load When Certain Tracking is Off/Rejected
General Nature	More Reactive	More Proactive
Configuration Complexity	Lower	Higher *(Script Integration)*
Ideal Consent Model	Opt-Out Model	Either Opt-Out Model OR Opt-In Model
Cookieless Tracking	Unable to Address	Scripts Can be Wrapped
Overall Defensibility	**Moderate**	**Very High**

Network & Search Bar Litigation Risks

- Plaintiffs increasingly allege that **search terms** and related network requests shared with third parties constitute unauthorized interception and form the basis for privacy claims.

- Some courts have held that search terms entered into a website search bar can qualify as "contents of a communication" under statutes such as CIPA.

- Search bar data exposed in outbound network traffic or embedded in URLs can trigger demand letters or litigation, even where no cookies are involved.

- Core issues include search terms passed in URL query strings or referrer headers that are observable by third parties, uncontrolled or inline third-party scripts that execute without consent, and a lack of clear disclosure regarding the collection or sharing of search data.

Search Bar Litigation Risk Remediation Options

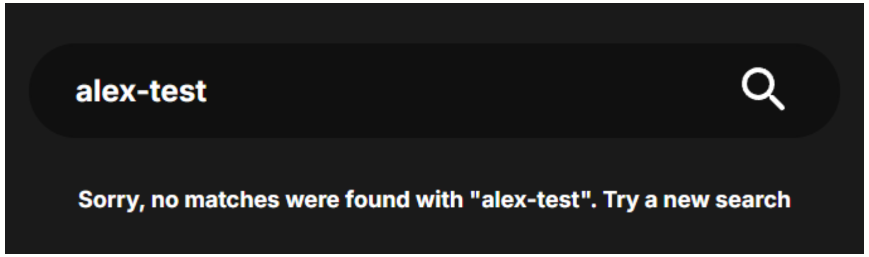
1. **Process search inputs server side where feasible so search terms are not exposed in client-side network traffic.**
2. **Remove search terms from URL query strings and referrer headers so they are not passively visible to third parties.**
3. **Restrict analytics and replay tools from running during search interactions unless consent is obtained.**
4. **Ensure privacy notices clearly explain how search data is collected, used, and shared with third parties.**

Assess Your Search Bar Litigation Risk

1 Use your CMP to **opt-out of non-essential tracking**. Although you may want to restrict search-bar data sharing entirely, the riskiest scenario is one in which you share URL query strings with third parties **after** an opt-out.

Reject All Non-Essential Cookies

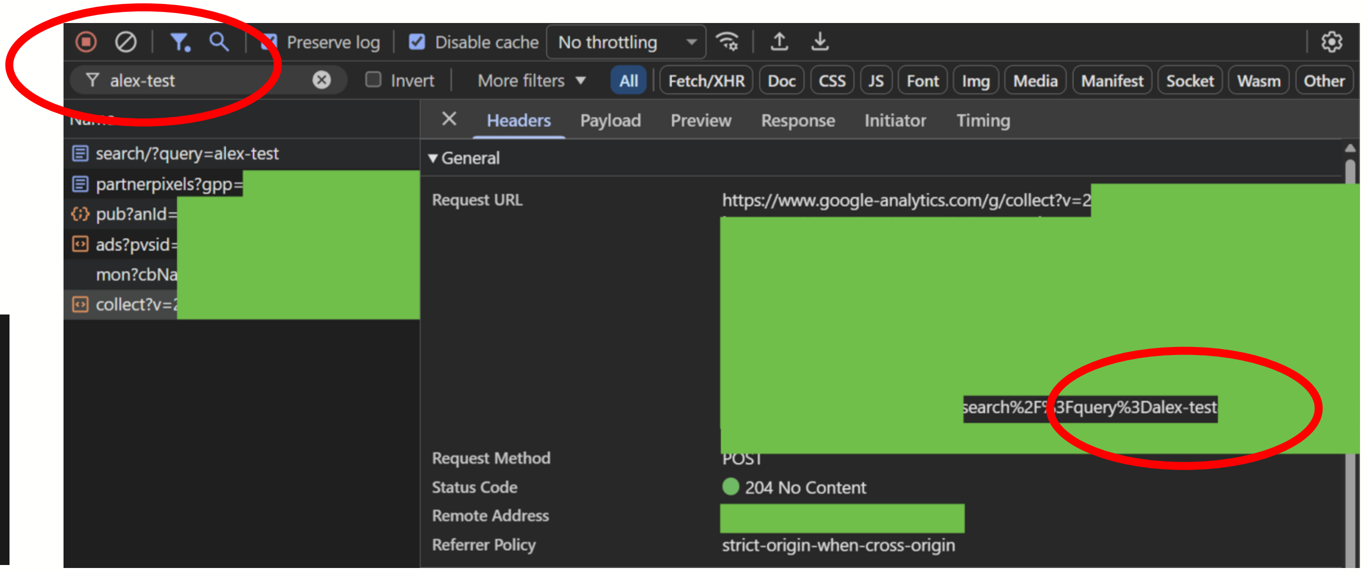
2 Utilize your website's search bar to **conduct a search for a test string**. (Example below uses "*alex-test*"). Usually, plaintiffs will search for their own name to strengthen their claim that any third-party sharing of search queries constitutes a violation.



alex-test

Sorry, no matches were found with "alex-test". Try a new search

3 While conducting your test search, **add a filter for your search term** (*i.e., alex-test*) Then, execute your search and observe the traffic that is logged. Review the logged traffic and look for instances in which your search term is being externally-shared. For example, the screenshot below shows a Google Analytics request with the search term embedded into the externally-shared URL. This is a common issue worth remediating.



Filter: alex-test

search/?query=alex-test
partnerpixels?gpp=[redacted]
pub?anId=[redacted]
ads?pvsid=[redacted]
mon?cbNa[redacted]
collect?v=[redacted]

Request URL https://www.google-analytics.com/g/collect?v=2[redacted] search%2F%3Fquery%3Dalex-test [redacted]

Request Method POST

Status Code 204 No Content

Remote Address [redacted]

Referrer Policy strict-origin-when-cross-origin

Universal Opt-Out Mechanisms (UOOMs)

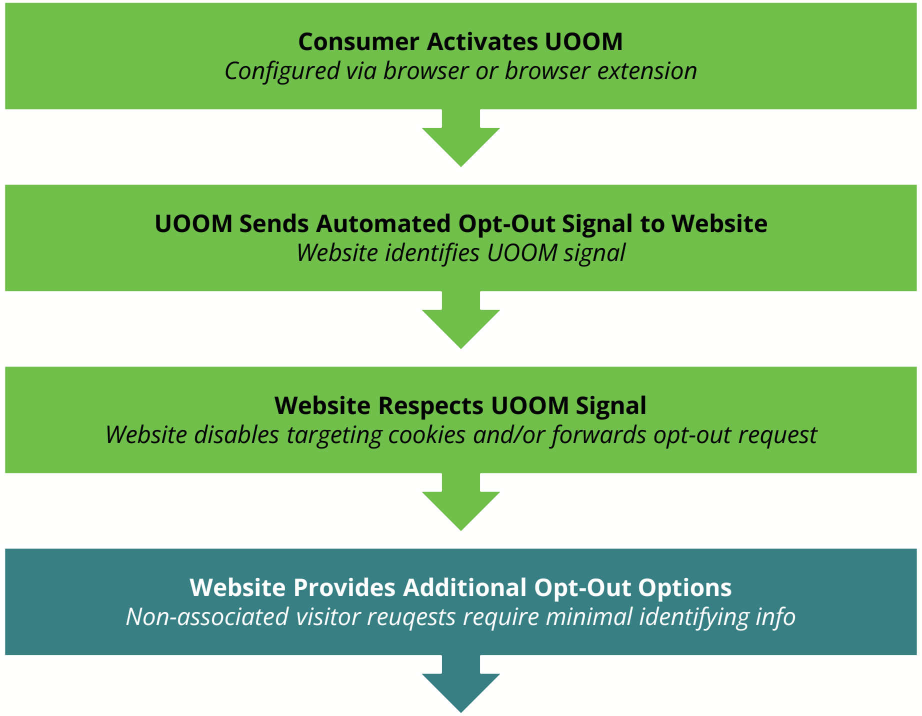
- U.S. state privacy laws require controllers to respect automated opt-out signals delivered from UOOMs, which visitors may automatically send from their browser or browser extensions.

- Over 60% of the other comprehensive state privacy laws require (or will require) UOOM support.

- While UOOMs (like **Global Privacy Control**) aren’t specifically intended for consumers to manage cookie consent preferences, they generally should impact the use of website targeting technologies, potentially alongside additional processing for known visitors.

- UOOM support is more directly relevant to regulatory compliance than private litigation, but it still presents meaningful risk and should be addressed as part of any overarching consent governance strategy.

High-Level UOOM Process Flow



Consumer Activates UOOM
Configured via browser or browser extension

UOOM Sends Automated Opt-Out Signal to Website
Website identifies UOOM signal

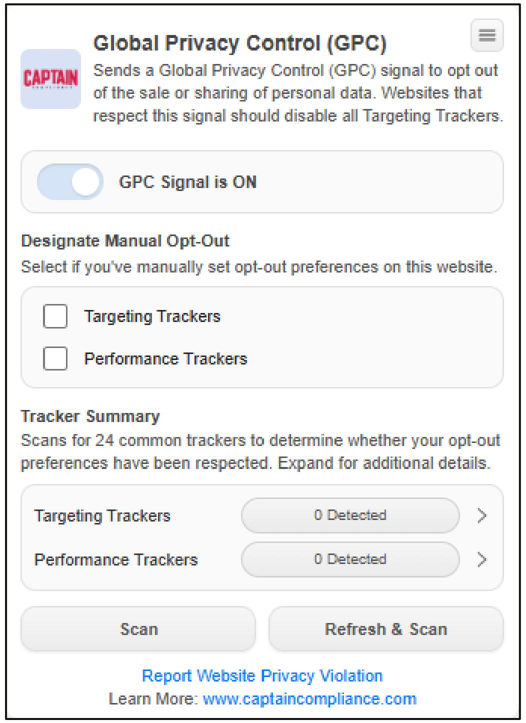
Website Respects UOOM Signal
Website disables targeting cookies and/or forwards opt-out request

Website Provides Additional Opt-Out Options
Non-associated visitor reuqests require minimal identifying info

Global Privacy Control (GPC)

- **Global Privacy Control (GPC)** is the most notable example of a Universal Opt-Out Mechanism (UOOM).
- GPC was developed in 2020 (in response to the CCPA) with the intention of making it easier for individuals to frictionlessly exercise their privacy rights.
- GPC allows users to send a "GPC Signal" (HTTP header and JavaScript variable) to any websites.
- GPC is the only form of UOOM that has been specifically recognized by any U.S state, and it is the standard that should be prioritized by businesses.
- California, Colorado, and Connecticut explicitly require businesses to honor GPC signals, and previously announced a joint enforcement sweep to investigate UOOM/GPC non-compliance.

GPC Extension Example (Free in Chrome Store)



Global Privacy Control (GPC)

Sends a Global Privacy Control (GPC) signal to opt out of the sale or sharing of personal data. Websites that respect this signal should disable all Targeting Trackers.

GPC Signal is ON

Designate Manual Opt-Out

Select if you've manually set opt-out preferences on this website.

□ Targeting Trackers

□ Performance Trackers

Tracker Summary

Scans for 24 common trackers to determine whether your opt-out preferences have been respected. Expand for additional details.

Targeting Trackers	0 Detected
Performance Trackers	0 Detected

Scan | Refresh & Scan

Report Website Privacy Violation

Learn More: www.captaincompliance.com

Reference: https://chromewebstore.google.com/detail/ogjilgkpiolmbhgffpbiioigjmjcaldg?utm_source=item-share-cb

State Laws Requiring UOOM Support

State Regulation	UOOM Requirement Effective Date	Must Facilitate Automated Opt-Out From:			Specifically Recognized UOOMs	
		Personal Data Sale	Targeted Advertising	Certain Profiling	GPC ***	Generic UOOMs
California Privacy Rights Act	07-01-2023	✓	✓	✗	✓	✓
Colorado Privacy Act	07-01-2024	✓	✓	✗	✓	✗
Connecticut Data Privacy Act	01-01-2025	✓	✓	✗	✓	✓
Montana Consumer Data Privacy Act	01-01-2025	✓	✓	✗	✗	✓
Nebraska Data Privacy Act	01-01-2025	✓	✓	✗	✗	✓
New Hampshire Privacy Act	01-01-2025	✓	✓	✓	✗	✓
Texas Data Privacy and Security Act	01-01-2025	✓	✓	✓	✗	✓
New Jersey Data Privacy Act	07-15-2025	✓	✓	✓	✓	✓
Minnesota Consumer Data Privacy Act	07-31-2025	✓	✓	✗	✗	✓
Delaware Personal Data Privacy Act	01-01-2026	✓	✓	✓	✗	✓
Oregon Consumer Privacy Act	01-01-2026	✓	✓	✓	✗	✓
Maryland Online Data Privacy Act	04-01-2026	✓	✓	✓	✗	✓

Reference: https://iapp.org/resources/article/us-litigation-series-website-tracking/

External Integrations “Make or Break” a CMP

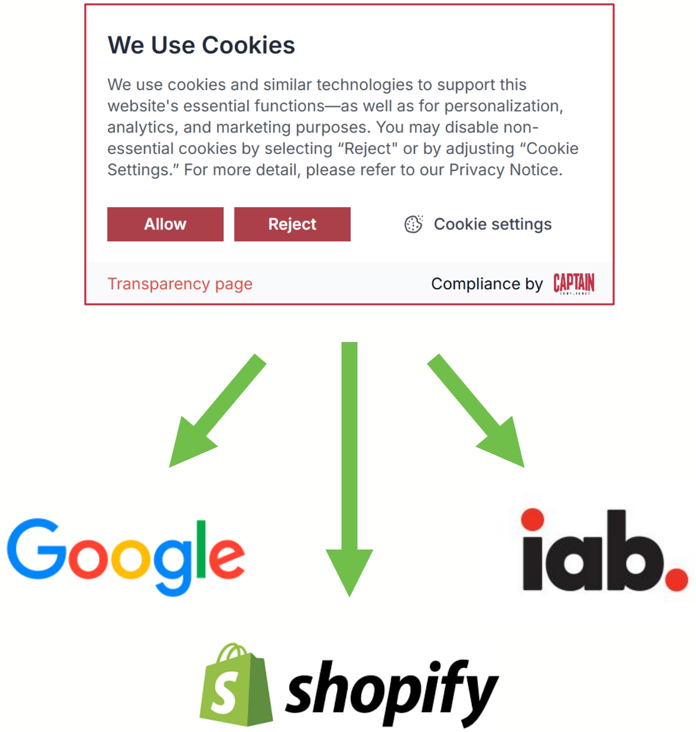
- A consent banner must integrate with the broader tracking ecosystem, including analytics platforms, advertising tools, and embedded technologies, to ensure users can control downstream data collection.

- **Google environments** require active integration with **Google Consent Mode** to set regional defaults and dynamically update GA4, Ads, and related tags when consent changes.

- **Platform-native tracking**, such as within Shopify, often operates in a way that simple script blocking cannot control, and must be API-integrated to properly govern analytics and marketing pixels.

- In the EU, CMPs are expected to interoperate with the **IAB Europe Transparency and Consent Framework** to generate standardized consent strings recognized across the advertising ecosystem.

Consent Management – Integration Examples



We Use Cookies

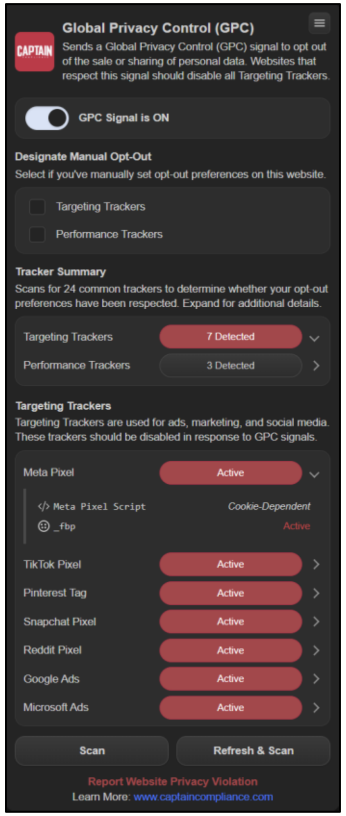
We use cookies and similar technologies to support this website's essential functions—as well as for personalization, analytics, and marketing purposes. You may disable non-essential cookies by selecting "Reject" or by adjusting "Cookie Settings." For more detail, please refer to our Privacy Notice.

Assess Your CMP: Free Extension

Use this toggle to send an automated privacy opt-out to websites that you visit. At a bare minimum, the website *should* disable **targeting trackers** relating to marketing and/or advertising.

This section summarizes key trackers identified on the website. (The extension monitors for 24 targeting and performance trackers). This section can be expanded to provide specific details.

Use these buttons to rescan the webpage. Depending on your testing interests, you may or may not want to refresh the page at the same time that you rescan. Both options are provided.



Global Privacy Control (GPC)

Sends a Global Privacy Control (GPC) signal to opt out of the sale or sharing of personal data. Websites that respect this signal should disable all Targeting Trackers.

GPC Signal is ON

Designate Manual Opt-Out

Select if you've manually set opt-out preferences on this website.

□ Targeting Trackers

□ Performance Trackers

Tracker Summary

Scans for 24 common trackers to determine whether your opt-out preferences have been respected. Expand for additional details.

Targeting Trackers — 7 Detected

Performance Trackers — 3 Detected

Targeting Trackers

Targeting Trackers are used for ads, marketing, and social media. These trackers should be disabled in response to GPC signals.

Meta Pixel — Active

`</> Meta Pixel Script` *Cookie-Dependent*

`_fbp` — Active

TikTok Pixel — Active

Pinterest Tag — Active

Snapchat Pixel — Active

Reddit Pixel — Active

Google Ads — Active

Microsoft Ads — Active

Report Website Privacy Violation

Learn More: www.captaincompliance.com

Use these checkboxes to designate if you've interacted with a consent banner to opt-out of tracking manually. This allows the extension to better identify potential violations of your privacy.

Identified trackers (scripts and cookies) are listed. Their state is contextualized to identify potential violations, which are flagged in red. Each tracker can be expanded to provide specific details.

If you encounter a potential web privacy violation and would like Captain Compliance to offer to help the website owner, you may use this option to report the potential tracking issue for follow-up.

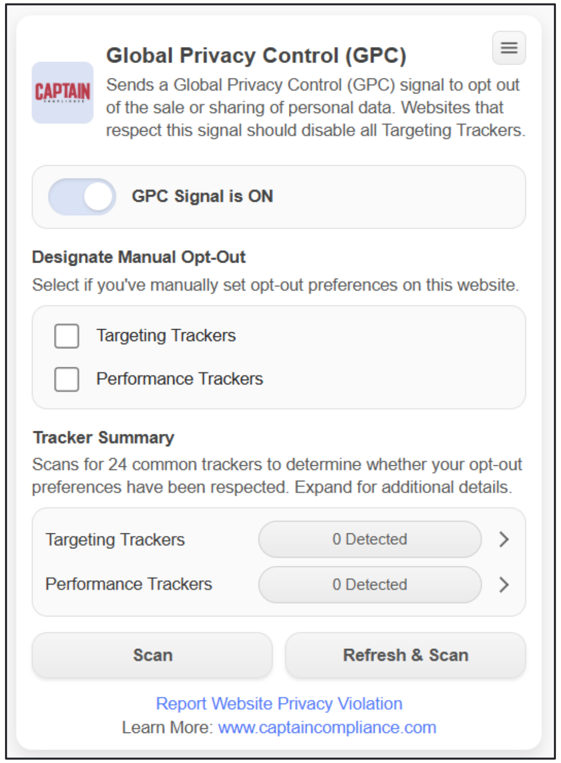
Installing the Free Chrome Extension

Installation:

- **STEP 1:** Visit Chrome Web Store
  - https://chromewebstore.google.com
- **STEP 2:** Search for “Captain Compliance: GPC”
- **STEP 3:** Click “Add to Chrome”

  Chrome will highlight the fact that the extension requires permission for the extension to view cookies. ***Note: All evaluation of tracking behavior occurs on-device.***
- **STEP 5:** Pin Extension to Extensions Bar
  - *Chrome Extensions Icon > Pin Icon*
- **STEP 6:** Open Extension in Side Panel for Easier Testing
  - *Extension Settings > Default to Side Panel*

Captain Compliance: GPC (Free in Chrome Store)



Global Privacy Control (GPC)

Sends a Global Privacy Control (GPC) signal to opt out of the sale or sharing of personal data. Websites that respect this signal should disable all Targeting Trackers.

GPC Signal is ON

Designate Manual Opt-Out

Select if you've manually set opt-out preferences on this website.

☐ Targeting Trackers

☐ Performance Trackers

Tracker Summary

Scans for 24 common trackers to determine whether your opt-out preferences have been respected. Expand for additional details.

Targeting Trackers	0 Detected
Performance Trackers	0 Detected

Report Website Privacy Violation

Learn More: www.captaincompliance.com

Testing with the Free Chrome Extension

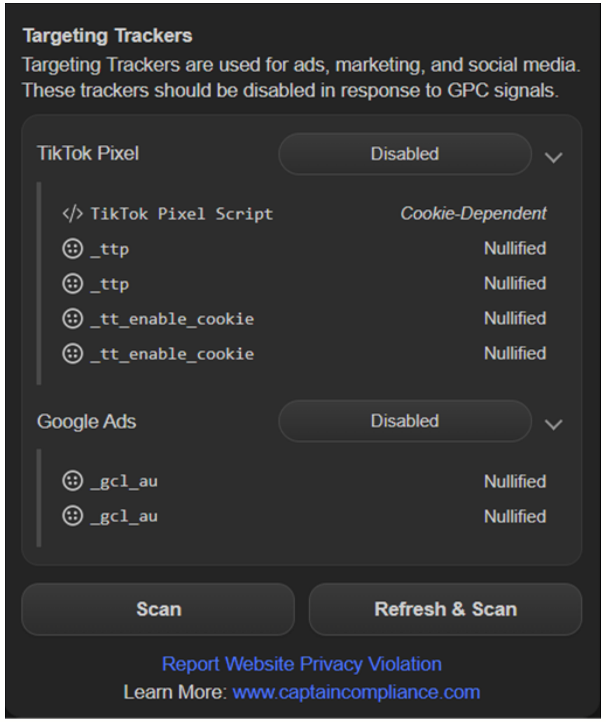
Test if Your Website Respects Privacy Opt-Outs:

- **STEP 1:** Visit your Website and Clear Cookies.
- **STEP 2:** Click “Scan” and Observe Default Trackers
- **STEP 3A:** Reject Tracking via Consent Banner; **AND/OR**
  STEP 3B: Reject Tracking via GPC Signal Delivery
- **STEP 4:** Click “Scan” and Observe Active Trackers
  - *Ideally, non-essential trackers will be removed or nullified (assuming they loaded by default).*

If Active Trackers are Still Detected:

- **STEP 5A:** Manually Delete Cookies; **AND/OR**
  STEP 5B: Click “Refresh & Scan”
  - *While not ideal, some CMPs may block tracker scripts while leaving stale cookies in the browser.*

Example: Successfully-Nullified Trackers



Targeting Trackers

Targeting Trackers are used for ads, marketing, and social media. These trackers should be disabled in response to GPC signals.

TikTok Pixel — Disabled

TikTok Pixel Script	*Cookie-Dependent*
_ttp	Nullified
_ttp	Nullified
_tt_enable_cookie	Nullified
_tt_enable_cookie	Nullified

Google Ads — Disabled

_gcl_au	Nullified
_gcl_au	Nullified

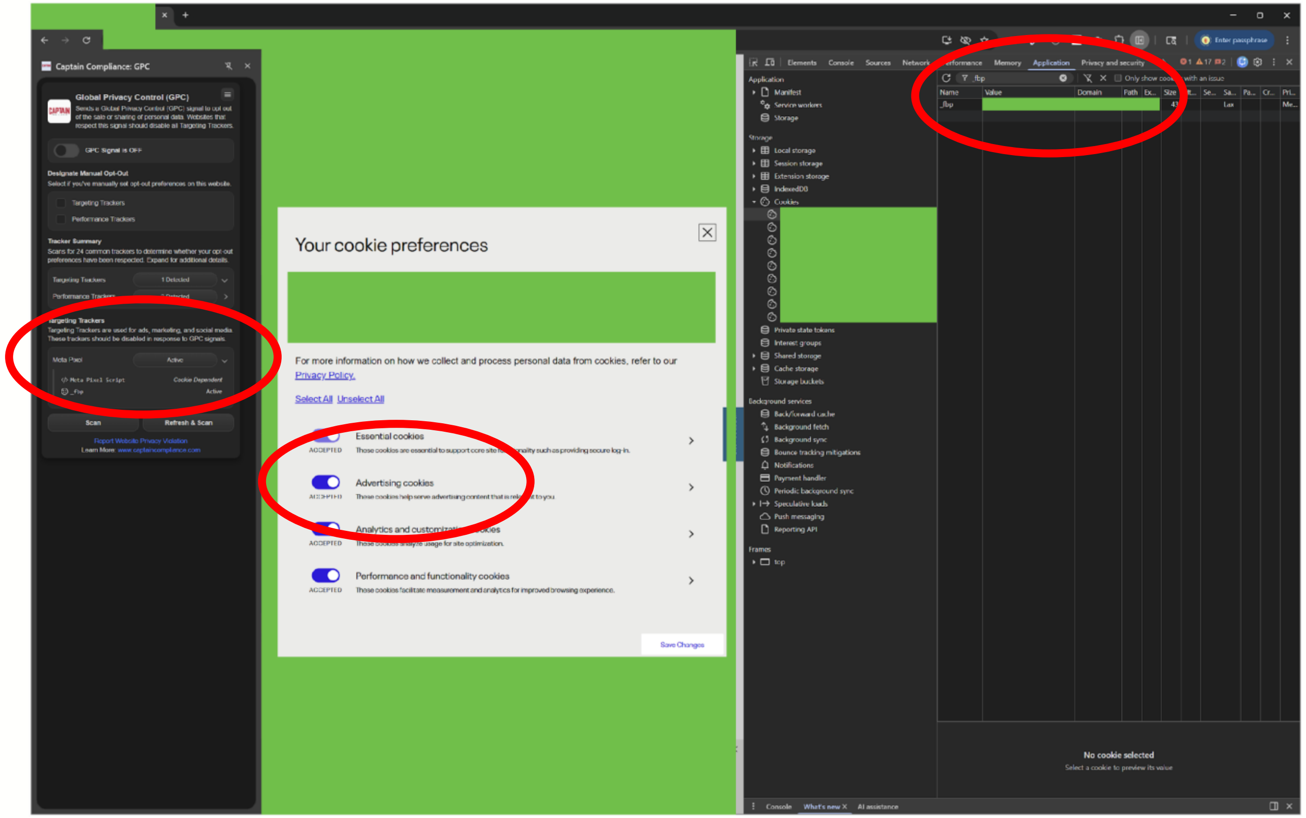
Learn More: www.captaincompliance.com

Test Example: GPC & Meta Pixel (1)

In this example, the Global Privacy Control (GPC) signal is not enabled at the time of initial website load. No preference has been declared.

The Captain Compliance GPC extension identifies multiple website trackers, including the Meta Pixel script and "_fbp" cookie.

A review of the website's default cookie preferences indicates that the "opt-out" consent model is in use. All trackers (including the Meta Pixel) are active by default.



Captain Compliance: GPC

Global Privacy Control (GPC)

Sends a Global Privacy Control (GPC) signal to opt out of the sale or sharing of personal data. Websites that respect this signal should disable all Targeting Trackers.

GPC Signal is OFF

Designate Manual Opt-Out

Select if you've manually set opt-out preferences on this website.

□ Targeting Trackers

□ Performance Trackers

Tracker Summary

Scans for 24 common trackers to determine whether your opt-out preferences have been respected. Expand for additional details.

Targeting Trackers	1 Detected
Performance Trackers	2 Detected

Targeting Trackers

Targeting Trackers are used for ads, marketing, and social media. These trackers should be disabled in response to GPC signals.

Meta Pixel	Active
</> Meta Pixel Script	*Cookie Dependent*
_fbp	Active

Scan | Refresh & Scan

Report Website Privacy Violation

Learn More: www.captaincompliance.com

Your cookie preferences

For more information on how we collect and process personal data from cookies, refer to our Privacy Policy.

Select All Unselect All

ACCEPTED Essential cookies
These cookies are essential to support core site functionality such as providing secure log-in.

ACCEPTED Advertising cookies
These cookies help serve advertising content that is relevant to you.

ACCEPTED Analytics and customization cookies
These cookies analyze usage for site optimization.

ACCEPTED Performance and functionality cookies
These cookies facilitate measurement and analytics for improved browsing experience.

Save Changes

_fbp

☐ Only show cookies with an issue

Name	Value	Domain	Path	Ex...	Size	Ht...	Se...	Sa...	Pa...	Cr...	Pri...
_fbp					43			Lax			Me...

No cookie selected
Select a cookie to preview its value

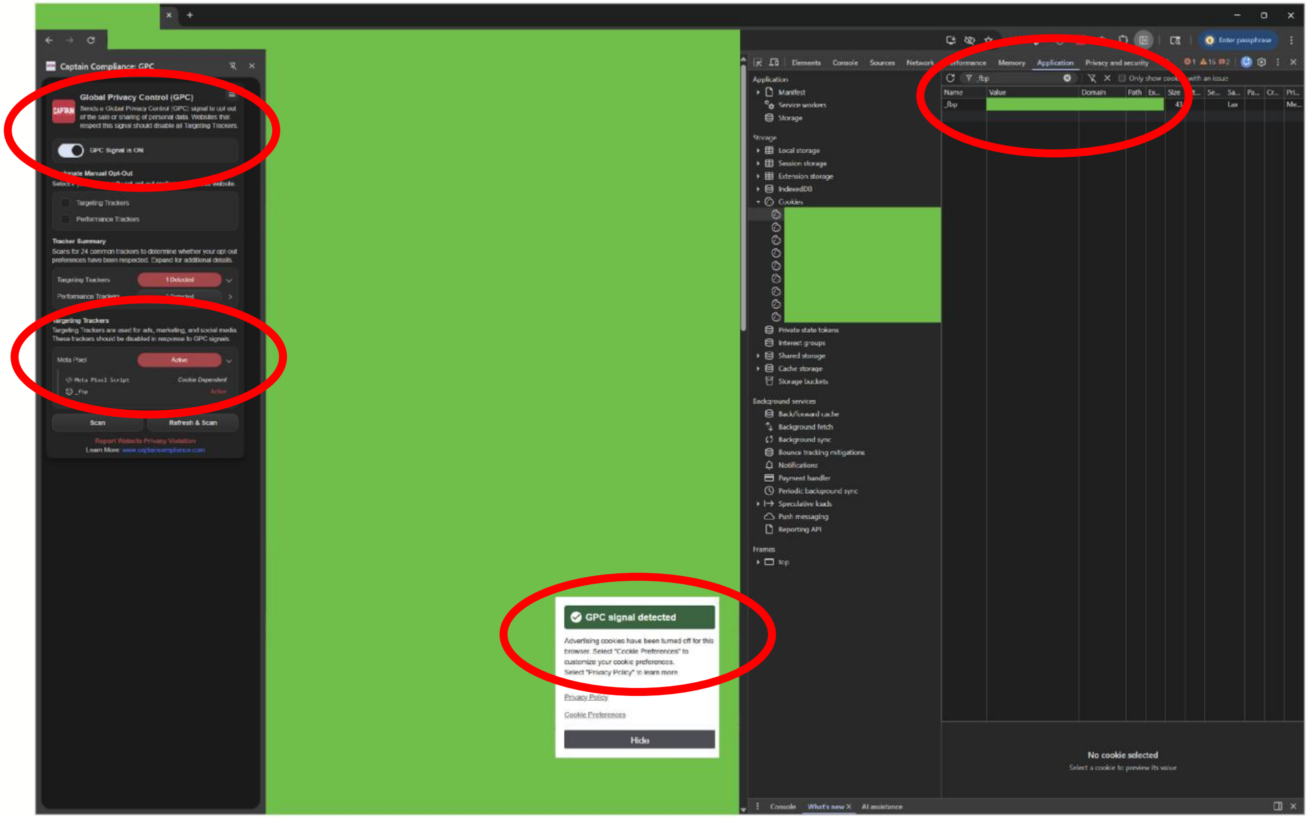
In the browser, the Meta Pixel ("_fbp") is seen loading by default, which is expected and consistent with the opt-out model described by the cookie consent banner.

Test Example: GPC & Meta Pixel (2)

A Global Privacy Control (GPC) signal has now been delivered to the website. This should be interpreted as a “Do Not Sell or Share My Personal Information” opt-out.

At a minimum, targeting trackers should be disabled. Additional processing, unrelated to website trackers, may also be appropriate.

The website delivers a helpful pop-up indicating that a GPC signal has been detected and that advertising cookies have been disabled.



Captain Compliance: GPC

Global Privacy Control (GPC)

Sends a Global Privacy Control (GPC) signal to opt out of the sale or sharing of personal data. Websites that respect this signal should disable all Targeting Trackers.

GPC Signal is ON

...mate Manual Opt-Out

Select ... website.

□ Targeting Trackers

□ Performance Trackers

Tracker Summary

Scans for 24 common trackers to determine whether your opt-out preferences have been respected. Expand for additional details.

Targeting Trackers	1 Detected
Performance Trackers	... Detected

...argeting Trackers

Targeting Trackers are used for ads, marketing, and social media. These trackers should be disabled in response to GPC signals.

Meta Pixel	Active
Meta Pixel Script	Cookie Dependent
_fbp	Active

Scan | Refresh & Scan

Report Website Privacy Violation

Learn More: www.captaincompliance.com

GPC signal detected

Advertising cookies have been turned off for this browser. Select "Cookie Preferences" to customize your cookie preferences. Select "Privacy Policy" to learn more.

Privacy Policy

Cookie Preferences

Hide

Filter: _fbp □ Only show cookies with an issue

Name	Value	Domain	Path	Ex...	Size	...t...	Se...	Sa...	Pa...	Cr...	Pri...
_fbp	[redacted]	[redacted]	[redacted]	[redacted]	43			Lax			Me...

No cookie selected

Select a cookie to preview its value

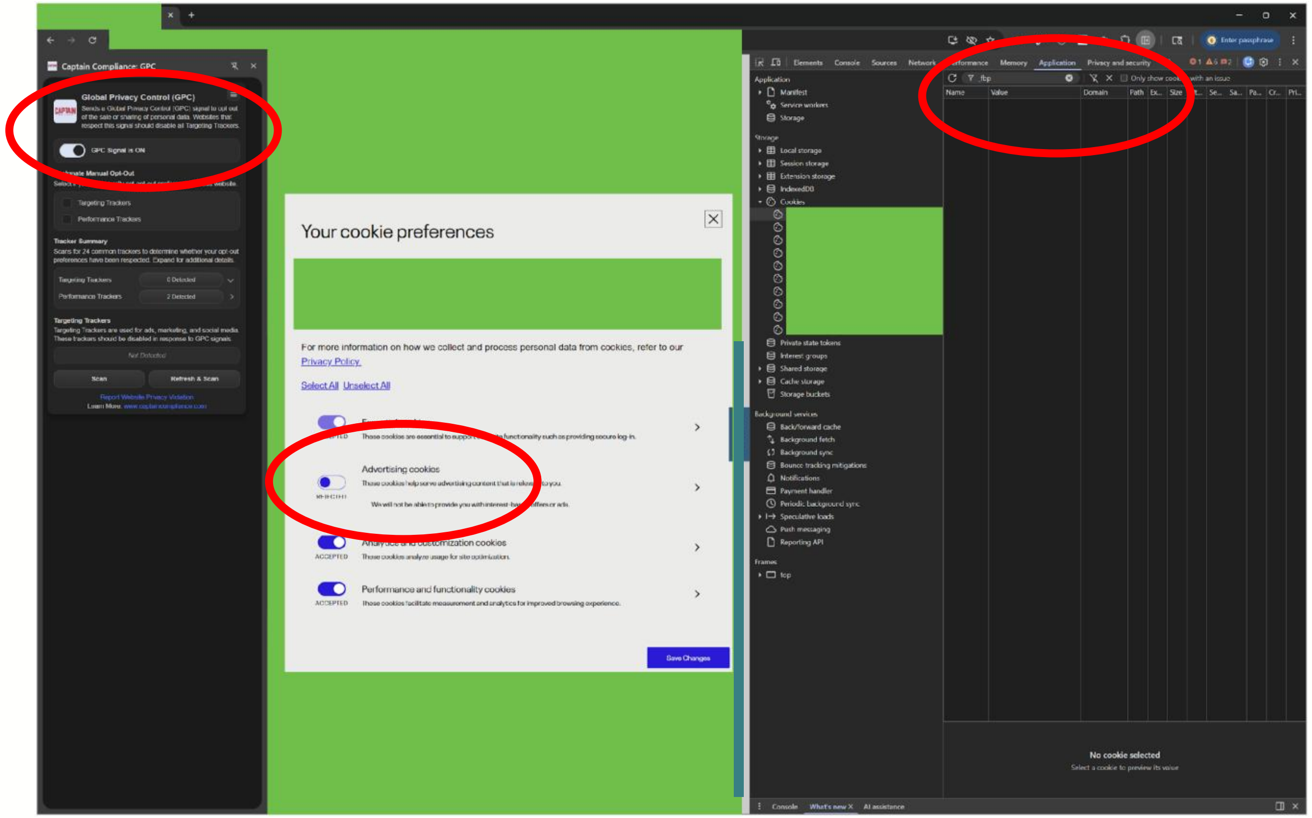
Despite acknowledging the GPC signal, the Meta Pixel appears to remain active. The “_fbp” cookie remains in-place and is not nullified via expiration or value removal.

The Captain Compliance GPC extension flags this tracker in red, as a potential compliance violation and litigation risk.

Test Example: GPC & Meta Pixel (3)

A verification of the website's updated cookie preferences indicates that the GPC signal has been appropriately interpreted as a targeting ("advertising") opt-out.

The website may be passing the opt-out signal along for further processing. GPC signals are not exclusively intended to address trackers and cookies. This is only one potential application of signal processing. This may be especially relevant for websites that involve user profiles and login functionality.



Captain Compliance: GPC

Global Privacy Control (GPC)

Sends a Global Privacy Control (GPC) signal to opt out of the sale or sharing of personal data. Websites that respect this signal should disable all Targeting Trackers.

GPC Signal is ON

Alternate Manual Opt-Out

Select ... website.

□ Targeting Trackers

□ Performance Trackers

Tracker Summary

Scans for 24 common trackers to determine whether your opt-out preferences have been respected. Expand for additional details.

Targeting Trackers	0 Detected
Performance Trackers	2 Detected

Targeting Trackers

Targeting Trackers are used for ads, marketing, and social media. These trackers should be disabled in response to GPC signals.

Not Detected

Scan | Refresh & Scan

Report Website Privacy Violation

Learn More: www.captaincompliance.com

Your cookie preferences

For more information on how we collect and process personal data from cookies, refer to our Privacy Policy.

Select All Unselect All

ACCEPTED — These cookies are essential to support ... functionality such as providing secure log-in.

Advertising cookies — REJECTED — These cookies help serve advertising content that is relevant to you. We will not be able to provide you with interest-based offers or ads.

Analytics and customization cookies — ACCEPTED — These cookies analyze usage for site optimization.

Performance and functionality cookies — ACCEPTED — These cookies facilitate measurement and analytics for improved browsing experience.

Save Changes

No cookie selected

Select a cookie to preview its value

After manually deleting the Meta Pixel cookie and refreshing the page, the tracker does not reload.

It is not obvious if the opt-out signal was initially respected or not. It is possible that the Meta Pixel script was disabled while the cookie was left "stale" in the browser, but it is also possible that the tracking was in effect when it should not have been.

Ideally, the "_fbp" cookie would be removed or nullified dynamically (without requiring manual deletion) to eliminate uncertainty and provide maximum defensibility.

Summary: U.S. Litigation Defensibility

Example	Common Example #1 No CMP	Common Example #2 "Free Plugin" CMP	Common Example #3 Broken (Opt-Out) CMP	Common Example #4 QA'd (Opt-Out) CMP	Common Example #5 QA'd (Opt-In) CMP
Privacy Notice	Published	Published	Published	Published	Published
Top-Level Consent Notice	Absent	Clear & Visible	Clear & Visible	Clear & Visible	Clear & Visible
Dark Patterns	N/A	Deceptive UI	None	None	None
Cookie Blocking	N/A	Not Functional	Partially Functional	Functional	Functional
Script Blocking	N/A	N/A	Partially Configured	Mostly Configured	Fully Configured
Default Policy (U.S.)	N/A	Opt-Out Model	Opt-Out Model	Opt-Out Model	Opt-In Model
Global Privacy Control	N/A	Not Respected	Not Respected	Respected	Respected
External Integrations	N/A	Not Addressed	Not Addressed	Addressed	Addressed
Residual Risk	Very High	Very High	High	Medium-Low	Very Low
Litigation Defensibility	**Very Low**	**Very Low**	**Low**	**Medium-High**	**Very High**

Complimentary Privacy Checkup!

- As a special thank-you for attending the IAPP webinar, you're invited to book a **complimentary privacy checkup**!

- We'll assess your website’s privacy risk exposure by reviewing how it uses tracking technologies, how consent mechanisms are configured, and how your privacy notice aligns with best-practices.

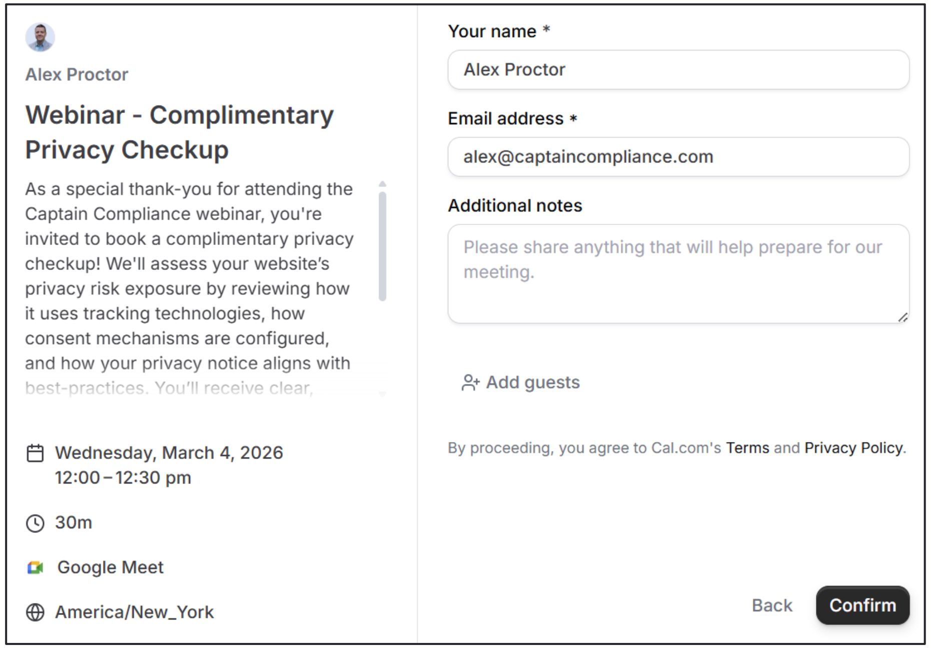
- You’ll receive clear, actionable guidance on what’s working and where improvements may be needed.

- This is a private session. Registration is available through this invite-only link, and spots are limited.

  Sign-up for the complimentary checkup:

  cal.com/alex-captaincompliance/checkup

Schedule Your Complimentary Checkup!



Alex Proctor

Webinar - Complimentary Privacy Checkup

As a special thank-you for attending the Captain Compliance webinar, you're invited to book a complimentary privacy checkup! We'll assess your website’s privacy risk exposure by reviewing how it uses tracking technologies, how consent mechanisms are configured, and how your privacy notice aligns with best-practices. You’ll receive clear,

Wednesday, March 4, 2026
12:00 – 12:30 pm

30m

Google Meet

America/New_York

Your name *

Alex Proctor

Email address *

alex@captaincompliance.com

Additional notes

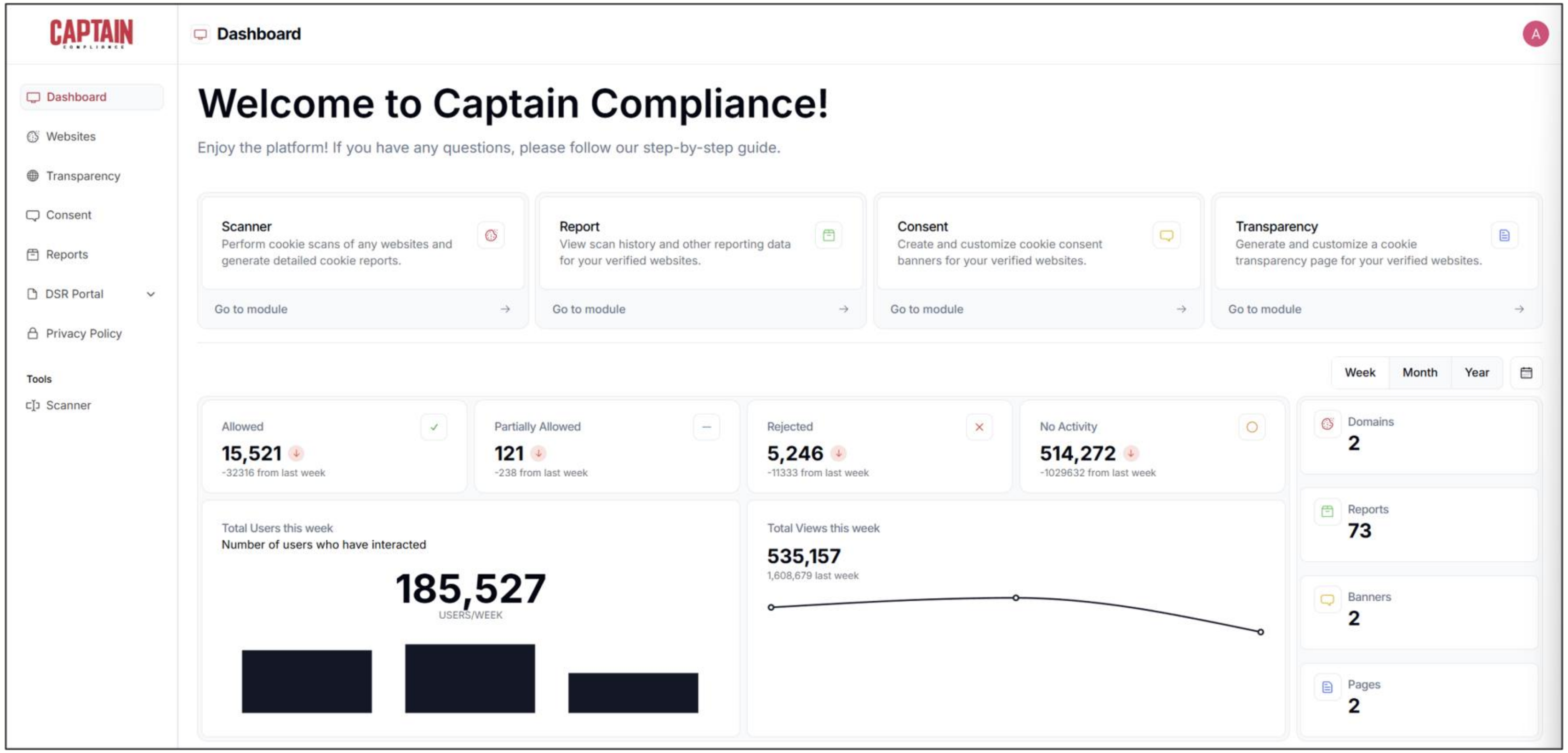
Please share anything that will help prepare for our meeting.

By proceeding, you agree to Cal.com's Terms and Privacy Policy.

Simplify Privacy w/ Captain Compliance!

- **Free Cookie Scanner** analyzes any website and generates a categorized inventory of first-party and third-party cookies—while flagging higher-risk trackers.
- **Cookie Consent Module** delivers regionally-customizable banners and ensures that websites respect visitor tracking preferences in accordance with global privacy laws.
- **Cookie Transparency Page** automatically generates a clear, up-to-date web page describing the cookies and tracking technologies used on websites.
- **Dynamic Privacy Notice** turns a simple questionnaire into a comprehensive privacy disclosure—with dynamic, layered formatting that adjusts based on visitor location.
- **Data Subject Rights (DSR) Portal** provides a customizable and automatable workflow to intake, verify, and fulfill privacy requests from consumers.
- **Privacy-Auditing Browser Extensions** allow insurance providers and similar parties to assess cookie consent functionality, including identifying banner misconfigurations.
- **ComplianceShield** extends beyond technical compliance by providing qualified customers with added legal risk mitigation and defense support in the event of web-tracking litigation.

Captain Compliance Web Platform



Welcome to Captain Compliance!

Enjoy the platform! If you have any questions, please follow our step-by-step guide.

Scanner
Perform cookie scans of any websites and generate detailed cookie reports.

Report
View scan history and other reporting data for your verified websites.

Consent
Create and customize cookie consent banners for your verified websites.

Transparency
Generate and customize a cookie transparency page for your verified websites.

Allowed
15,521 ↓
-32316 from last week

Partially Allowed
121 ↓
-238 from last week

Rejected
5,246 ↓
-11333 from last week

No Activity
514,272 ↓
-1029632 from last week

Domains
2

Reports
73

Banners
2

Pages
2

Total Users this week
Number of users who have interacted
185,527
USERS/WEEK

Total Views this week
535,157
1,608,679 last week

Reduce Website Privacy Litigation Risk

1. **Understand your technology stack.** Audit what is firing on your website, what each technology does, whether it transmits data in real time, and whether it is truly necessary. Remove anything that does not serve a clear purpose.
2. **Make a deliberate decision about default tracking.** Legal requirements vary by region: some jurisdictions mandate opt-in consent, while others, such as much of the United States, require organizations to make a risk-based decision. If your highest priority is privacy and litigation risk reduction, consider an opt-in model. If you adopt an opt-out model to preserve analytics or marketing performance, do so knowingly and acknowledge the residual litigation risk.
3. **Provide meaningful user choice and honor it.** Ensure opt-outs, consent flows, and preference signals (including Global Privacy Control) are technically operational and consistently respected. Avoid dark patterns!
4. **Implement script-level controls where possible.** Wrap tags in consent logic to prevent execution under blocking conditions. This is often easier when using a tag manager such as Google Tag Manager, but scripts can also be wrapped directly within your website code. Ensure that non-cookie tracking technologies are governed as well.
5. **Maintain an accurate and highly visible Privacy Notice.** Your disclosures must reflect your actual data practices, vendors, and tracking technologies, and the notice should be easily accessible to maximize defensibility.
6. **Monitor and audit continuously.** Websites evolve quickly. Configuration drift, vendor updates, or marketing changes can undermine defensibility if controls are not regularly reviewed.

Questions & Answers

Alex Proctor
AIGP, CIPP/E, CIPP/US, CIPM, CIPT, FIP
Chief Trust & Privacy Officer
Captain Compliance

alex@captaincompliance.com

Web Conference
Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here: https://iappwf.questionpro.com/t/AbBPvZ74Gm

Thank you in advance!

For more information: www.iapp.org

Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your AIGP, CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration prior to the live webinar will automatically receive credit. After the broadcast date, individuals may submit for credit by completing the continuing education application form here: submit for CPE credits.

Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

For questions on this or other IAPP Web Conferences or recordings please contact: livewebconteam@iapp.org