LOKKER
POWERING PRIVACY

ONLINE DATA PRIVACY REPORT

Website Privacy and Compliance Challenges

Quantifying Website Privacy Risks

March 2024

TABLE OF CONTENTS

Continuing Challenges with Web Tracker Privacy and Compliance

The recent surge in public and private legal actions against companies for online privacy violations signifies a broader development in state and federal regulation and enforcement. They highlight the increased urgency for companies to gain control over the unauthorized data collected and shared from their websites. The problems investigated in this report indicate technical deficiencies in managing online privacy inherent in modern web architecture.

According to HTTP Archive's latest "Annual State of the Web Report" (Sep. 2022), 94% of sites use at least one third-party, and the top 1,000 websites use 53 third-party scripts, on average. This prevalence aligns with the contemporary approach to website development, which heavily relies on cloud software and third-party integrations to enable website functionalities such as forms, video players, content delivery, analytics, payment processing, shopping carts, and e-commerce features. These tools have revolutionized website construction, simplifying the process and enhancing user experience beyond basic HTML frameworks. Furthermore, websites utilize various advertising technology (ad tech) and analytics tools to draw specific traffic from platforms such as Google, Meta (including Facebook and Instagram), and other social media platforms. These tools heavily depend on third-party services to guarantee the efficiency and accurate tracking of online advertisements and campaign performance

While these integrations offer essential business tools, facilitating enhanced functionality and traffic generation, they come with a notable tradeoff: sharing visitor data among interconnected tools. Introducing all this activity into millions of browser sessions has become chaotic and impossible to monitor and manage for unauthorized data collection, theft, and exploitation. Thus, each customer's web browser now represents a new vector for cyber risk, exposing visitors to dozens (or hundreds) of third parties. While many of these third parties are reasonably well-intentioned, many are not, and the underlying architecture lends itself to exploitation. As a result, the companies hosting the website are often left holding the bag for unauthorized data collection and privacy violations.

It's worth noting that we have seen advancements in privacy technology, which is encouraging. This includes deprecating third-party cookies and more sophisticated solutions like Privacy Sandbox and private browsing options. However, companies cannot solely rely on consumers adopting the right browser with the appropriate settings enabled. The responsibility to safeguard customers' privacy ultimately rests with the companies themselves. The ad tech industry represents a market of immense value, estimated at half a trillion dollars, and it will undoubtedly continue to evolve and adapt. Unfortunately, alongside these advancements, entities will be willing to exploit technology and violate privacy regulations. Much like cybersecurity, a corresponding challenge or threat exists for every progressive step forward. These threats are the focus of our research.

Our Research

With increased attention on data protection and privacy rights, there's momentum for innovation in privacy-enhancing technologies to address new regulations. This surge of interest fosters opportunities for individuals and organizations to take more control over their online data and digital identities, ultimately shaping a more secure and private online environment.

By publishing this report, we aim to inform website owners about privacy concerns, potential repercussions, and mitigation strategies. We also strive to underscore the necessity for increased governance within companies and tools beyond typical consent management to ensure a safer and more transparent online experience for users.

Methodology

This report offers a comprehensive analysis of web privacy risks across 3,419 websites in four main sectors: healthcare, technology, financial services, and retail, along with all sites listed in the S&P 500 index.

The report establishes a benchmark of statistics to track trends and facilitate comparisons over time in the following areas:

1. Unauthorized data collection via third-party trackers, tags, and pixels, highlighting their role in data proliferation and the expansion of the data broker ecosystem, which is often underestimated in its pervasiveness.

2. Assessment of the efficacy of existing online privacy tools and their effectiveness in terms of overall privacy and compliance with emerging laws. For example, consent platforms frequently overlook cookies and tags firing on websites, or load before consent has been granted by users.

3. Additional context on the scope and scale of web privacy risks, violations, fines, and lawsuits companies face based on their current web privacy practices; like VPPA, wiretapping and HIPPA violations.

3,419

NUMBER OF WEBSITES WE ANALYZED

HEALTHCARE	TECH
FINANCIAL SERVICES	RETAIL

Key Findings

ISSUE #1 Web trackers and pixels are leading to extensive data proliferation, fueling the data broker ecosystem, and potentially sharing data with foreign nations

12%

Of websites have the TikTok Pixel

- Including 9% of S&P 500, 25% of retail, 7% of technology, 6% of financial services, and 4% of healthcare companies.
- While TikTok may not have the same prominence on websites as Meta and other social media platforms, it often makes headlines due to its data collection practices. Recently, there have been significant federal conversations, including legislation to ban TikTok in the US, focusing on its data-sharing practices and ties to China.

2%

Use web trackers from risky foreign adversaries

- 2% of websites use web trackers situated in China or Russia, potentially exposing users' data to foreign adversaries.
- On February 28th, 2024, President Biden signed Executive Order 14117 to prevent the sharing of sensitive personal data of Americans with foreign nations. While this 2% represents direct data sharing, it's crucial to recognize that the data broker ecosystem also consolidates information from domestically collected tags, trackers, and pixels.

47%

of websites have the Meta Pixel

- 47% of websites have the Meta Pixel (55% of S&P 500, 58% of retail, 42% of financial services, 33% of healthcare, and 42% of technology companies).
- 33% of researched healthcare companies utilize the Meta pixel on their websites. This is despite lawsuits, breaches, fines, FTC warnings, and the March 2024 OCR guidance against improperly using web trackers to collect sensitive health data.
- This marks a 17.5% decrease from the 40% of healthcare companies' websites LOKKER identified in Oct. 2022.

On page 5, you can find more detailed findings about data collection by foreign entities and more about online trackers on page 7.

ISSUE #2 Existing privacy tools must be improved.

67%

of websites have a consent banner

- 67% of websites across all industries featured a consent banner, suggesting an increased desire to protect consumers and give them the ability to affirmatively consent or opt out of the sharing of their data (88% of S&P 500, 67% of retail, 67% of technology, 63% of financial services, and 59% of healthcare companies).

98.5%

of websites deploy cookies upon page load

However, the research reveals that these tools must be improved to function as intended. 98.5% of websites load cookies upon page load, averaging 33 cookies before consent is given through a consent banner. While site-specific, it appears many cookies are non-essential and impermissibly tracked visitors prior to consent.

We identified the following trends in the current consent management process:

- There's no standardized distinction between performance, analytics, and advertising trackers.
- Consent banners frequently misclassify or overlook cookies and trackers.
- Technologies like fingerprinters, which identify and share customer data, are often excluded from consent tools.
- There are areas for improvement in scanning for new web trackers.
- The dynamic nature of the web means tracker changes may go unnoticed by consent tools, resulting in users unwittingly consenting to undesired data collection.

Get more detailed findings about consent tools on page 16.

ISSUE #3 With a patchwork of state and federal laws expanding, compliance becomes increasingly intricate, accompanied by a surge in regulatory actions and lawsuits

5%

of websites are at risk of VPPA lawsuits

- 5% of websites across all industries researched are at risk of VPPA lawsuits, which are those with the meta pixel on pages containing video players (10% of S&P 500, 5% of technology, 4% of retail, 4% of financial services, and 3% of healthcare companies).

Get more detailed findings about compliance with emerging laws on pages 7 and 19.

Foreign Data Collectors

2% of websites have web trackers from China or Russia.

Across all data collection mechanisms on a site (trackers, cookies, pixels, session replay), we evaluated how many operate in a country with elevated privacy risk, like Russia or China.

While 2% may not initially strike as significant, it gains weight when placed in context. According to a Siteefy survey, roughly 133 million websites exist in the US. Calculating 2% of this total, we estimate approximately 2.7 million websites sharing data with owners situated in foreign countries. Moreover, the impact amplifies when we factor in individuals' average daily visits to websites and the fact that some sites could get hundreds of thousands of web visits a day. A single frequently visited website or one with high traffic could entail data collection from hundreds of thousands of users, emphasizing the broader implications of cross-border data-sharing practices.

We dug in deeper and looked at the percentage of sites in each industry sending data to a foreign domain. We found a clear outlier in the tech industry, which has 15x as many foreign trackers as retail sites, which saw the lowest percentage of foreign trackers.

Why it's essential to evaluate foreign trackers

There has been a heightened focus on data privacy and security, particularly regarding sharing data with foreign entities. In the past month, the US government has taken two significant actions to safeguard Americans' data privacy from countries of concern.

Percentage of sites with foreign trackers	
Healthcare	.55%
Financial Services	1.07%
Retail	.4%
Tech	6.46%
S&P 500	2.7%

On February 28th, 2024, President Biden signed Executive Order 14117 to prevent the sharing of Americans' sensitive personal data with foreign nations.

This order targets various types of personal information, such as genomic data, biometric data, personal health data, geolocation data, financial data, and specific personally identifiable information. It addresses the risks associated with bad actors exploiting Americans' data for intrusive surveillance, scams, blackmail, and other privacy violations. It's part of a broader initiative to safeguard Americans' personal information and national security interests.

12% of websites across all industries had the TikTok pixel embedded on their platforms

Subsequently, on March 13th, 2024, the US House of Representatives passed a bill requiring ByteDance, TikTok's parent company, to divest the app or face a ban on all US devices. This action reflects legislators' concerns that TikTok's extensive data collection practices could compromise national security, with fears that the Chinese government could access or influence user data due to ByteDance's ownership. It's worth noting that these concerns extend beyond user activities on the platform itself.

When companies integrate the TikTok pixel on their websites, TikTok can collect data on users' online behavior, including shopping preferences, media consumption, and digital footprint. This information reveals sensitive details such as email addresses and phone numbers and potentially revealing factors like political and religious affiliations or medical conditions.

Percentage of sites with TikTok	
Healthcare	4.4%
Financial Services	7.0%
Retail	24.7%
Tech	8.7%
S&P 500	5.5%

Web trackers

Web trackers are central to privacy, compliance, and data proliferation challenges in today's digital landscape. Their extensive use poses significant privacy risks, highlighting the urgent need for transparency, consent, and user control over personal data online. Our research examined the most prevalent trackers today and delved into statistics concerning those frequently discussed in the news or referenced in lawsuits.

The Meta Pixel is on 47% of sites, despite the rise in lawsuits

In 2023 alone, Bloomberg Law reported over 265 lawsuits related to pixel privacy, focusing on web trackers and the meta pixel. What’s interesting is the targeted approach by plaintiffs’ lawyers, who bring pixel-related lawsuits under whichever law they can make fit. The Meta pixel has been cited in numerous lawsuits, including those involving the Video Privacy Protection Act, invasion of privacy laws, wiretapping regulations, unfair and deceptive practices statutes, and even a RICO case.

VPPA Violations Related to the Meta Pixel

According to our research, 5% of websites are susceptible to legal action under the Video Privacy Protection Act (VPPA) due to having the Meta pixel and other social trackers present on pages containing video players.

In 2023, we witnessed a surge in regulatory and legal actions against organizations for unauthorized information collection via website trackers and subsequent data sharing without consent.

Percentage of sites with Meta Pixel	
Healthcare	33%
Financial Services	42%
Retail	58%
Tech	42%
S&P 500	55%

Percentage of sites with VPPA	
Healthcare	4%
Financial Services	3%
Retail	4%
Tech	10%
S&P 500	5%

This encompassed over 80 lawsuits filed under the Video Privacy Protection Act (VPPA), targeting the misuse of Meta Pixel to gather and disseminate video viewing data from websites without user consent, with settlements reaching millions, such as:

- October 2023: Crunchyroll, Sony Pictures Video Privacy, was settled for $16 million in a VPPA Class Action Settlement.
- May 2023: The Boston Globe settled for $5 million for sharing user video data with Facebook under VPPA.

33% of Healthcare Sites Have the Meta Pixel

Despite facing lawsuits, breaches, fines, FTC warnings, and the most recent OCR guidance on web trackers, 33% of healthcare companies persist in deploying the Meta pixel on their websites. The OCR guidance underscores that browsing or searching for symptoms or specific conditions on a webpage can be considered Protected Health Information (PHI), safeguarded for both current and prospective patients. Previously, HIPAA only applied to existing patients. This implies that healthcare, specific retail, and digital health companies must adopt a strict approach toward web trackers to ensure compliance. They should prioritize implementing tools that request explicit consent from individuals. Some notable regulatory actions in this regard include the January 2024 Novant Health settlement of $6.6 Million for a data breach caused by third-party trackers and the March 2023 FTC fine of $7.8 million for sharing sensitive health data for advertising.

Pixel Problems in Financial Services

In February 2024, TaxAct Inc., a leading online tax preparation service, reached a significant $23 million settlement to address accusations of sharing confidential taxpayer data with Meta, Google, and other third parties without user consent.

Tracker Troubles in the Retail Industry

The convergence of the retail and healthcare sectors introduces new privacy considerations, especially concerning the application of healthcare-related safeguards to digital health products or stores with healthcare integrations. Consider the case of Costco, which is currently embroiled in a class action lawsuit for purportedly gathering sensitive health information on its pharmacy website.

Beyond the meta pixel, websites have an average of 20 third-party trackers responsible for collecting and sharing data

We analyzed trackers across industries to determine the average and maximum number of trackers per site.

Trackers per industry, average and maximum

Industry	Average Trackers	Max Trackers
Healthcare	16	93
Financial Services	18	111
Retail	24	147
Tech	18	148
S&P 500	26	109

Most frequent trackers across all industries

This table presents the top web trackers identified within five key industries: S&P 500, Technology, Financial Services, Healthcare, and Retail. The trackers are ranked based on their frequency of occurrence, providing insights into the prevalent data collection practices within each sector.

S&P 500	Tech	Financial Services	Healthcare	Retail
googletagmanager.com	googletagmanager.com	googletagmanager.com	googletagmanager.com	googletagmanager.com
doubleclick.net	doubleclick.net	google-analytics.com	doubleclick.net	doubleclick.net
google-analytics.com	google-analytics.com	doubleclick.net	google-analytics.com	google-analytics.com
google.com	google.com	google.com	google.com	google.com
facebook.com	licdn.com	facebook.com	googleapis.com	facebook.net
facebook.net	linkedin.com	facebook.net	youtube.com	facebook.com
linkedin.com	facebook.com	linkedin.com	facebook.com	bing.com
licdn.com	facebook.net	licdn.com	facebook.net	googleapis.com
demdex.net	bing.com	googleapis.com	licdn.com	adnxs.com
bing.com	youtube.com	demdex.net	linkedin.com	rubiconproject.com

Web Trackers and third-party tools undoubtedly offer valuable benefits for website operators. They aid in performance optimization, provide insightful analytics, and enhance advertising effectiveness for targeted audience engagement and increased conversions. However, without proper controls or functioning safeguards (discussed further on page 15), these trackers can covertly collect and share data without user authorization.

Another reason this happens is piggybacking and the nesting of trackers. These are common digital marketing and online advertising tracking techniques to track user behavior and gather analytics data.

Piggybacking involves attaching one tracker to another, such as when a third-party advertiser adds their tracking script to a website's existing analytics tracker without the owner's explicit consent. This allows advertisers to collect data across multiple websites without implementing separate tracking mechanisms.

Nesting trackers entail placing one tracker within another, creating layered tracking mechanisms to gather more detailed user behavior data.

Both piggybacking and nesting trackers raise privacy and data security concerns, as they can lead to extensive data collection without explicit user consent or transparency.

The importance of the web tracker - data broker connection

Web trackers serve as pivotal components in the data broker ecosystem, facilitating extensive data collection on individuals' online activities, preferences, and demographics. This aggregated information is then analyzed and sold to various entities, including marketers, advertisers, researchers, and other organizations keen on understanding consumer behavior and targeting specific demographics.

For context, the US data broker market is projected to experience significant growth, estimated to rise from $280.82 billion in 2023 to $382.16 billion by 2030, with a compound annual growth rate (CAGR) of 4.5%. Notably, the location tracking segment alone represents a $12 billion industry. These expanding sectors are largely driven by the data harvested through pixels and trackers embedded on the websites we visit.

Session Replay Tools

There's an average of one session replay tool on sites scanned.

Session replay scripts are tools website owners or marketers use to record and replay users' interactions on their websites. In real time, these scripts capture user actions such as mouse movements, clicks, scrolling behavior, keystrokes, and form inputs. The recorded sessions are then replayed for analysis or to gain insights into user behavior and website usability.

The concerns with session replay scripts

While session replay can help gain valuable insights about your website visitors, they also raise privacy and security concerns.

Privacy Concerns:
Session replay scripts record and replay user interactions on a website, including keystrokes, mouse movements, and form inputs. If not configured properly, session replay scripts can capture sensitive information such as passwords, credit card numbers, and personal messages, posing a significant privacy risk.

Regulatory Compliance:
Using session replay scripts without proper consent or safeguards may violate privacy regulations and result in legal consequences. In recent years, we've seen many lawsuits challenging website technologies like session replay, with the plaintiff's counsel claiming that these technologies illegally collect user information and violate state wiretapping statutes.

session_replay_domain	% of sites
hotjar.com	13%
hotjar.io	12%
clarity.ms	12%
crazyegg.com	6%
sentry.io	5%
wistia.com	4%
contentsquare.net	4%
litix.io	3%
fullstory.com	3%
quantummetric.com	3%
heapanalytics.com	2%
dynatrace.com	2%
amplitude.com	2%
mouseflow.com	2%
foresee.com	1%

Security Risks:
Session replay scripts may inadvertently capture sensitive information that users enter into forms, exposing it to potential security breaches if the data is not adequately protected.

Tips for Responsible implementation of your session replay script to ensure compliance with state wiretapping laws

Website owners must implement session replay scripts responsibly, ensuring transparency, user consent, and compliance with applicable privacy laws and regulations.

1. Transparency: Disclose to users that session replay is being used on the website.
2. User Consent: Obtain explicit consent from users before recording their sessions
3. Anonymization and Data Minimization: Only record the minimum amount necessary for analysis.
4. Security Measures: Implement robust security measures to protect the recorded session data from unauthorized access, tampering, or breaches.
5. Data Retention Policies: Define clear data retention policies for session replay data. Regularly review and delete old session recordings no longer needed to reduce the risk of unauthorized access or misuse.
6. Opt-Out Mechanism: Provide users with a clear and accessible mechanism to opt out of session replay if they wish to do so.
7. Regular Audits and Compliance Checks: Stay informed about relevant laws and regulations changes and update your practices accordingly to maintain compliance.

Lokker's web privacy platform offers real-time scanning to help users identify if their website is potentially violating wiretapping laws. Additionally, it addresses issues by implementing real-time blocking of unauthorized data collection. For more information about Lokker, refer to page 20.

100+

Pending wiretapping lawsuits related to website session replay, chatbot, and pixel technologies as of January 2024.

Sensitive Data Collection

10% of websites share sensitive form data with a third party

"Sensitive data" refers to specific categories of personal information considered particularly sensitive or private under privacy laws. Sensitive data typically includes personal identifiers, financial information, health, biometrics, genetic data, sexual orientation, and ethnic or racial origins.

The table to the right illustrates the types of data and their occurrences. Notably, the most commonly shared information includes names, email addresses, and phone numbers.

.4% of sites share extremely sensitive information with a third party.

Our analysis across all sites revealed that this fraction transmits data such as credit card information, social security numbers, and banking details through web trackers.

Concerns around sensitive data sharing

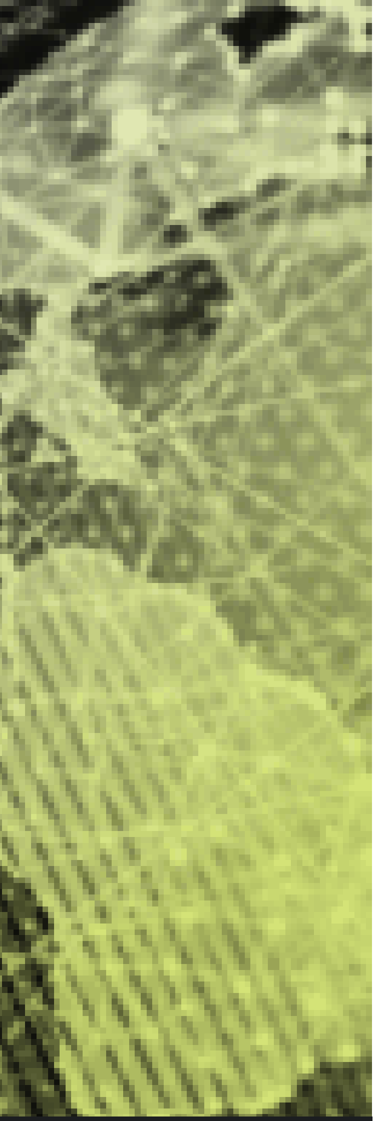
Sensitive data collection from websites raises concerns for both website owners and visitors.

Once data is shared with a third party, visitors and website owners lose control over its usage and distribution. This loss of control makes it challenging to safeguard privacy and prevent unauthorized access to personal information. Depending on your location and the data type shared, legal or regulatory requirements may govern the handling and sharing of personal information. Non-compliant websites or apps could face legal repercussions like lawsuits or fines if they share their visitors' data without consent.

Percentage of sites collecting sensitive data by data type

Data Type	Percentage of sites
first name	9%
last name	9%
email	6%
phone	6%
state	3%
city	3%
full address	1%
middle name	1%
credit_card	.2%
password	.2%
medical term	0.08%

Unauthorized data sharing with third parties also poses risks, such as potential misuse for malicious purposes or unwanted marketing efforts. Moreover, sharing data increases the likelihood of data breaches. If third parties lack proper security measures, visitors' data could be compromised, leading to identity theft or financial loss.



So, what third parties are receiving this data?

The table below displays the most common web trackers identified on websites that collect any type of personally identifiable information (PII).

Top 20 3rd parties receiving any PII from forms	
target_domain	count_source_urls
hsforms.com	1608
fullstory.com	230
segment.io	181
eloqua.com	110
jotform.com	80
pabbly.com	49
leadid.com	47
netnordic.com	47
listrakbi.com	45
tealiumiq.com	40
autoid.com	36
salesforce-sites.com	30
lr-ingest.com	25
leadspace.com	22
callrail.com	22
constantcontact.com	20
geonetric.com	19
botframework.com	18
on-enterprises.com	18
linkedin.com	16

Consent Tools

More Companies are Taking Steps Toward Privacy, But We're Inadvertently Consenting to Much More Than We Realize

As states implement comprehensive privacy laws granting individuals greater control over their personal data, such as the right to opt out of sharing or selling sensitive information and profiling data, websites are increasingly adopting consent management tools.

67% of US websites display a consent banner, suggesting an increased commitment to protecting users.

While companies strive to uphold privacy standards by investing in privacy tools, the tools often fall short, with the individuals implementing these tools frequently lacking crucial insights into how the tools operate. Our research uncovers a prevalent issue: these tools frequently malfunction, as evidenced by:

98.5% of sites drop cookies as soon as the page loads

Our research unveiled a striking statistic: across all industries, 98.5% of websites deploy cookies upon page load, often before any consent can be granted.

On average, we discovered that 33 cookies load before users can consent, encompassing non-essential trackers and leaving users unable to reject cookies before loading, including, on average, 15 first-party cookies and 18 third-party cookies.

Sites with Consent Banners Present

Industry	Percentage of Sites
Financial Services	63%
Healthcare	59%
Retail	67%
S&P 500	88%
Tech	67%

Average % of Cookies Deployed on Page Load

Industry	Percentage
Financial Services	98%
Healthcare	99%
Retail	99%
S&P 500	100%
Tech	97%

Additional Concerns with Website Banners

Our study shows that consent banners often get it wrong with cookies and tags. We see the following issues repeatedly:

Missing: We frequently find that the consent banner is missing from certain website pages. Nothing prevents "unnecessary" tags from being dropped on these pages. As a result, users are exposed to tracking even though they haven't given their consent.

Malfunctioning: Even after selecting "reject all," marketing tags and cookies classified as “analytics,” “tracking,” and “performance” still show up.

Unclassified: Cookies, tags, and trackers were detected but not sorted into categories, so they weren't instructed to be blocked.

Pixels missing: Current consent tools focus on calling out cookies. They don't call out other tracking pixels or beacons that might not use cookies.

Dropping Cookies Before Consent: Many cookies are dropped before consent, which was previously acceptable under CCPA’s Opt Out. This is changing, particularly with new laws around sensitive data requiring an Opt-in. Companies now need the option to block all but strictly necessary third parties before consent is given on certain sites.

Consent banners mainly monitor cookie-setting tags, missing the other ways data is collected and shared. Tags can also send data attached to the URL as part of outbound requests. Or fingerprint data can be shared via request payloads.

As websites evolve daily, so do trackers, but consent tools often struggle to keep up with the daily discovery of new tags.

The opt-out doesn’t work across browsers or different devices, meaning users may inadvertently share data on one browser or device they intended to keep private due to inconsistencies in opt-out settings.

Sometimes, there is no “Reject All” option present. In the US, there isn't always standardized guidance for providing user opt-out; users are often automatically opted in by default. To opt out, users must search for a preference page and manually toggle off individual categories before their consent preferences are applied.

For example, one website we examined listed nine cookies in its consent banner for users to accept or reject. However, in reality, clicking "Accept All" would deploy 74 cookies, 66 of which are third-party.

Significant manual oversight and management are necessary to compensate for shortcomings inherent in consent technology itself.

Much of the cookie and tracker classification process is manual, with some subjectivity regarding what a performance, analytics, or advertising tracker is. Since no standardized rules exist, misclassification is common, potentially resulting in unintended data sharing.

Implementing and maintaining this technology often entails extensive development work, necessitating coordination among various enterprise teams. As a result, progress may be slow, and updates may be overlooked due to the absence of a clear owner or accountable party. Some organizations install a consent banner without proper configuration; even if configured, it can quickly become outdated. Unfortunately, it is often set up once and then forgotten about.

For context, these are the most prominent cookies we found across all sites. They're a mix of analytics, advertising, and performance cookies.

Company	cookie_name	cookie_count
Google Analytics	_ga	126174
Google Analytics	_gid	90970
Google Analytics	_gcl_au	86907
Facebook	_fbp	68640
OneTrust	OptanonConsent	58154
Bing Ads	_uetsid	39315
Bing Ads	_uetvid	39310
Cloudflare	__cf_bm	27817
Adobe Analytics	s_cc	24620
Adobe Target	mbox	19749
Asp.net	ASP.NET_SessionId	18976
Akamai	ak_bmsc	17793
AddThis	at_check	17690
Clicky	_clck	16253
Clicky	_clsk	16178
ThruTalk	_ttp	14252
ThruTalk	_tt_enable_cookie	14252
Pinterest	_pin_unauth	14033
Marketo	_mkto_trk	13801
Rubicon Project	RT	13781
Google Analytics	_gat	13193
Amazon Web Services	AWSALB	12937
Amazon Web Services	AWSALBCORS	12791
Akamai	AKA_A2	12545
Akamai	bm_sz	11867

Regulatory Landscape

Another Layer of Complexity: The Patchwork Regulatory Landscape

Balancing legal requirements, technical solutions, and economic incentives complicates the pursuit of effective web privacy measures. When it comes to privacy laws, there's a myriad of different laws that companies need to follow, with federal laws, emerging state comprehensive laws, and industry-specific laws. We compiled a list of the most prominent laws cited in recent legislation and new laws going into effect that companies should be aware of. We've also noted the statutes with a private right of action, which grants an individual or entity the right to initiate a lawsuit against another party for alleged rights violations. This is significant as over 265 lawsuits filed in 2023 related to web trackers.

Comprehensive state laws signed		
Law	Signed Date	Enacted Date
California Confidentiality of Medical Information Act (CMIA)	Amended in 2022	January 1, 2023
California Privacy Rights Act (CPRA)*	June 28th, 2018	January 1, 2023
Virginia Consumer Data Protection Act (VCDPA)	March 2, 2021	January 1, 2023
Colorado Privacy Act (CPA)	July 7, 2021	July 1, 2023
Utah Consumer Privacy Act (UCPA)	March 24, 2022	December 31, 2023
Washington My Health My Data Act*+	April 27, 2023	March 31, 2024
Nevada Consumer Health Data Privacy Law+	June 5, 2023	March 31, 2024
Connecticut Personal Data Privacy and Online Monitoring Act (CTDPA)	May 10, 2022	July 1, 2024
Oregon Consumer Privacy Act (OCPA)	July 18, 2023	July 1, 2024
Florida Digital Bill of Rights (FDBR)	June 6, 2023	October 1, 2024
Montana Consumer Data Privacy Act (MTCDPA)	May 19, 2023	October 1, 2024
Iowa Consumer Data Protection Act (ICDPA)	March 28, 2023	January 1, 2025
New Hampshire SB 255	March 6, 2024	January 1, 2025
Texas Data Privacy and Security Act (TDPSA)	June 18, 2023	January 1, 2025
Delaware Personal Data Privacy Act (DPDPA)	September 11, 2023	January 1, 2025
New Jersey Data Privacy Act (NJDPA)	January 16, 2024	January 15, 2025
Tennessee Information Protection Act (TIPA)	May 11, 2023	July 1, 2025
Indiana Consumer Data Privacy Act (INCDPA)	May 1, 2023	January 1, 2026

*Private Right of Action. +Health data-specific bill

Federal Laws

We've seen many recent web privacy cases brought under existing federal laws. The following are the most active in terms of enforcement.

- Electronic Communications Privacy Act (ECPA) and Wiretap Act
- Video Privacy Protection Act (VPPA)
- Federal Trade Commission (FTC) Act
- Children's Online Privacy Protection Act (COPPA)
- HIPAA - Health Breach Notification Rule HIPAA Privacy Rule
- Health Information for Economic and Clinical Health Act (HITECH ACT)
- Gramm-Leach-Bliley Act - Privacy of Consumer Financial Information Rule
- Plus, we see a lot of lawsuits citing invasion of privacy laws or unfair and deceptive practices.

Challenges with the patchwork approach

Having a patchwork of privacy laws presents several challenges. Given that the internet doesn't always honor state or even international borders, there are some inherent challenges:

- Compliance Complexity: Different regulations in various regions increase the difficulty and cost of compliance for organizations operating globally.
- Legal Uncertainty: Varying laws create ambiguity, leading to potential compliance breaches and legal risks.
- Data Transfer Restrictions: Inconsistencies hinder the smooth transfer of personal data across borders, requiring additional safeguards.
- Operational Burden: Compliance demands significant resources, especially for smaller businesses, impacting efficiency.
- Conflict of Laws: Conflicting regulations can lead to legal disputes and confusion for organizations.
- Limited Consumer Protection: Legal discrepancies may leave gaps in consumer protection, undermining trust.

Complying with each privacy law is incredibly challenging and time-consuming, especially considering conflicting language in some regulations. Instead of chasing compliance for every law, businesses should address the core problem: preventing unauthorized data collection through these tools for cookie and web tracker compliance. Companies should prioritize blocking any such data collection to ensure compliance and protection of user privacy.

Why Pay Attention to Washington's My Health, My Data Law?

The My Health My Data Act (MHMDA) is notable for its expansive scope. It encompasses any legal entity conducting business in Washington dealing with consumer health data, regardless of revenue or data subject thresholds. MHMDA's "consumer health data" definitions are broad, potentially affecting wellness, fitness, and digital health businesses. Notably, the MHMDA introduces a private right of action for consumers, allowing them to seek damages for violations, increasing the risk of costly class action lawsuits.

Prevent Data Proliferation and Privacy Violations on Your Website with Real-Time Blocking of Unauthorized Data Collection By Lokker

The optimal approach to compliance is addressing the root cause of the issue, which is precisely what LOKKER facilitates. Our software offers an advanced solution for addressing unauthorized data collection across websites, providing comprehensive protection against invasive practices. It meticulously scans for and identifies cookies, trackers, session replay scripts, fingerprinters, and sensitive data collection instances that conventional tools frequently ignore. Additionally, our platform can be configured to instantly block any unauthorized elements, ensuring real-time protection for every user session. This proactive approach guarantees a safer, more secure browsing experience by preventing unauthorized access and data collection.

With LOKKER:

- Identify all website trackers, tags, and pixels.
- Block unauthorized data collection and sharing.
- Prevent privacy violations
- Verify that your consent tools are working

Watch this one-minute video for a quick overview of how the platform works.

Or schedule a demo to see how the Privacy Edge platform can protect your business.