epsilon
life sciences

CLIENT ALERT

# Unveiling the Bittersweet Truth: Cookies, Pixels, and Privacy on the Web

Epsilon Life Sciences has been at the forefront in these matters and will provide an overview of website tracking and advertising technologies for those legal and compliance teams with less technical experience with their deployment and use. We will also cover regulator enforcement and litigation in addition to guidance on what organizations should be doing to manage risk while not destroying their digital engagement strategies.

## Website and Mobile App Marketing and Analytics Tools

Recently, technologies such as cookies, pixels, and similar tools have come under the spotlight for legal and risk teams due to the increasing volume of privacy laws, regulator guidance, investigative journalism, and litigation impacting their usage and deployment. Just a few short years ago, these tools were focused on building organizational data lakes of website and app user information to fuel the engine for customer engagement and revenue growth. However, with the surge in online activity, highlighted during the pandemic, the amount of information being generated, collected, and shared online has reached unprecedented levels. Consequently, organizations are now working to build in controls to address the new risks associated with these tools, even as they are already in-flight. This has caused a certain amount of friction between marketing and risk teams.

## Technology Overview

The following is a brief primer on the key technologies under scrutiny. Cookies, pixels, and other tracking technologies used on websites and online platforms serve many useful (and sweet, if you will) purposes for website owners, enhancing the functionality, and personalizing user experience.

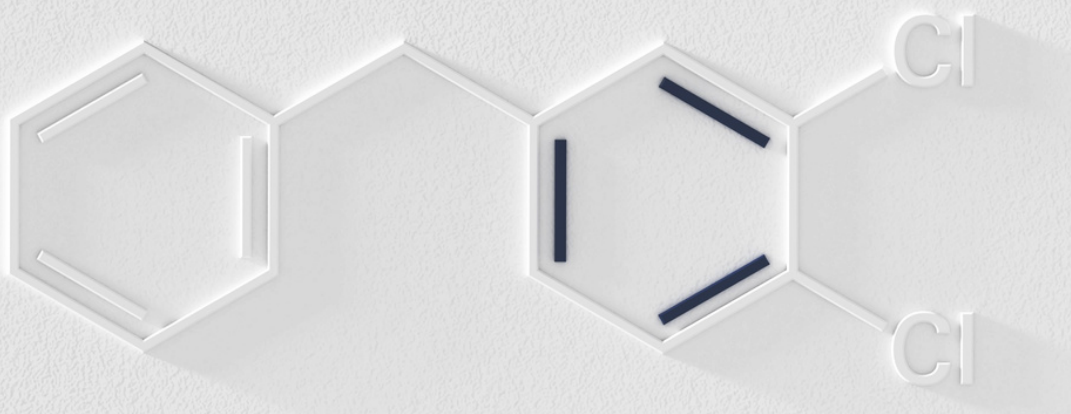
However, they also pose potential risk to user privacy and can lead to bitter litigation or investigations. One of the primary purposes of these technologies is to collect data related to the users' website and search history, preferences, and other interactions to personalize the user experience for subsequent visits. The same technologies may also collect user data to create profiles for analytics and targeted advertising. A few key terms to help understand these tools:

> Cookies: Small text files that store information on a user's browser and can be remembered when revisiting a website. These do not follow users across devices and are primarily used for user experience, as well as marketing.

> Pixels: More specifically a Tracking Pixel, store user information directly to servers and are primarily used for marketing purposes. These are less easily disabled and can track users across devices and websites.

> Parameters: These are attributes in which pixels may instruct cookies to collect or save when certain events occur. They could be general information such as the type of browser and screen resolution, detail the type of event such as a "button click" or "form submission," or they could contain more sensitive details such as a social media user id, email, name, location, etc.

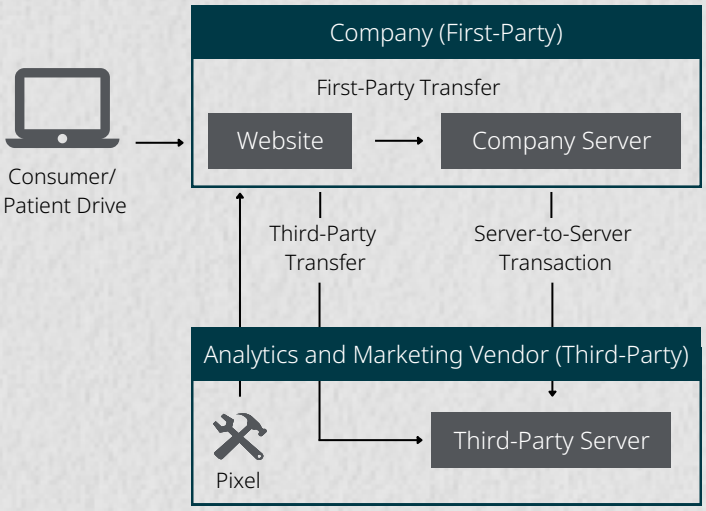
- Events: Tracking technologies can be configured to collect information based on specific actions the visitor takes on the site or app. This could be as simple as a page view or clicking a button. They could also be more bespoke such as when a user begins entering information in an application but then abandons the process.
- Payload: This refers to the data transferred through the parameters as part of the event. Similar to events, this can be relatively simple such as the URL of the page being viewed or it could collect more sensitive details such as a user ID for a social media site, search terms entered in a browser, information from a user profile, appointment information, or buttons the user clicked on a site. Many third-party cookies and pixels will collect more information than organizations realize or intend when they are initially configured. Typical cookie consent management platforms do not have the ability to analyze these payloads to determine the appropriate classification of what is being collected; instead, they rely on generic libraries of the typical ways in which organizations may use the tools.
- First/ Third-Party: Simply put, this means the party that owns the servers that collect the information. A first-party cookie transmits data to the servers managed by the company that owns the website. Third-party cookies are those such as Meta, Google, or other parties that typically provide analytics and advertising services and receive information directly from the user interactions.
- Server-Side Transaction: This is an emerging solution where information is collected by a first-party cookie and is later sent to a third-party through a separate connection to their servers. This can be helpful to allow the website owners to better pseudonymize or de-identify information before sharing it but can also be a blind spot that unknowingly increases the amount of personal information being shared. Server-side Transactions can be harder for plaintiffs or regulators to detect compared to third-party transfers.
- Classification: Cookies are commonly grouped by their purpose such as strictly necessary, functional, performance, analytics, and targeting. Strictly necessary cookies remember core pieces of information that are required for the website to work. Functional cookies remember choices that the user makes such as username, language, shopping carts, or region and uses that information to customize the user experience. Performance cookies collect information about the way that the user uses a website. Analytics cookies collect data related to the users and use of the website to produce key performance metrics related to website use. Lastly, targeting cookies are used to deliver more relevant ads to site visitors based on their interests. Where a tracking pixel is deployed, it is typically for analytics and targeting purposes.



- Lifecycle: Each type of cookie has a predetermined lifecycle. A cookie is described as either a session cookie or a persistent cookie. A session cookie is defined as a cookie that remains on a user's browser until their browser is closed. These cookies may be used on marketplace websites to help the shopping cart function properly, to store login credentials, or pre-populate a form on the website. A persistent cookie will remain on a user's browser once it is launched until a specified expiration date is met. This expiration date is set by the parameters of the cookie when it is created and can last as long as the creator wants.
- Tag Manager: These are tools that enable organizations to add and edit which tools on their website might collect information, determine what data they collect, and specify the events triggering data collection. This is often where tools such as the Meta Pixel or Google Analytics are added. Some organizations use a centralized tool such as Google Tag Manager to manage all website tags, while others may employ multiple tools or embed the technology directly in their website markup code. These are often managed externally by third-party marketing agencies on behalf of the organization which may create a conflict.

While website analytics and marketing technologies are useful tools which can improve user experience and help brands engage with their existing or prospective customers, a lack of understanding about what they collect or non-compliant configuration can lead to enforcement actions or litigation when personal information is transferred to third parties or is not disclosed as required in the privacy notice.

The chart to the right is an example of how the information flow could work across a user device, first, and third party.




## Legal and Regulatory Risk: Europe, US State Law, HHS, and the FTC

Collecting and storing user information through first or third-party tracking technologies is concerning when websites are not transparent with their users about their use of tracking technologies, or when companies fail to protect their users' data in accordance with data protection and health information privacy laws. The European Union's General Data Protection Regulation (GDPR) and California's Privacy Rights Act (CPRA) impose requirements on websites depending on jurisdiction such as obtaining user consent before deploying tracking technologies that are not necessary for the website functionality, or providing notice to users that tracking technologies are being used and provide an opportunity for users to opt out, limit, or control how their data is being collected and shared. The French Data Protection Authority (CNIL) has been particularly proactive in taking action related to the use of these tools and has issued guidance for organizations on how to make their website analytics tools more compliant[1]. Additionally, the recent Virginia Consumer Data Protection Act (CDPA) also requires organizations to conduct a Data Protection Assessment where they engage in Targeted Advertising[2].

Healthcare providers and payers that are subject to the Health Insurance Portability and Accountability Act (HIPAA), known as covered entities, as well as their business associate vendors, must implement specific safeguards to ensure that they are sharing protected health information (PHI) with online tracking technologies. The U.S. Department of Health and Human Services (HHS) has published a bulletin explaining the HIPAA Privacy, Security, and Breach rules that covered entities must adhere to when sharing PHI with online tracking technologies through websites and mobile applications to avoid OCR enforcement actions[3].

According to HHS, identifiable information, such as IP address or geolocation, collected through covered entities' website tracking tools is still considered PHI even if the user is not an existing patient and if the information does not include treatment or billing details. HHS states that potential health information can be inferred by associating the user with the covered entity's website. The bulletin provides guidance regarding the use of tracking technologies on user-authenticated pages (which are more restricted and likely contain PHI) and unauthenticated pages (where login is not required), but leaves the tricky act of discernment to organizations. HHS highlights potential concerns even on unauthenticated, such as the presence of a "find a doctor" function or search queries related to specific health conditions. For more details and compliance tips, see our recent client alert on the HHS bulletin.

The American Hospital Association (AHA) has expressed concerns about the broad definition of PHI outlined by the OCR in their bulletin. Specifically, the AHA questions the designation of an IP address as a unique identifier and ultimately PHI[4]. According to the AHA, this guidance will deter covered entities from including valuable medical information on their webpages, which hinders the dissemination of reliable health information and access to a large percentage of underserved communities.

The AHA is also concerned about IP addresses being considered PHI because they are often disclosed to third-party tracking technologies for analytics purposes that help broaden the reach of covered entities' websites and its reliable health information to patients in underserved communities, improve translation and provider geolocation services on covered entities' websites, and improve the spread of accurate information via social media.

However due to this new definition of PHI, third-party companies are refusing to sign Business Associate Agreements, and as a result, the covered entities cannot use the third-party tracking technologies for what the AHA believes are important and useful purposes.

Many organizations collect health or medical information that is not directly subject to HIPAA, however, this area is arguably more complex because of the patchwork of jurisdictional and sectoral regulators taking action. The Federal Trade Commission (FTC) has recently demonstrated broad interpretation of the Health Breach Notification Rule and conducted investigations and entered into settlements with organizations related to the health information their websites collect and share with third parties through pixel technologies. They have provided overviews and reinforced their commitment to policing digital health platforms using pixel technologies[5]. The Washington State My Health My Data Act (MHMDA), which is effective in 2024, will have a similarly significant impact on the health information collected by non-HIPAA covered entities operating in or tangential to the healthcare space[6].

It is important to note that the use of these tools to collect health information often violates their terms of service[7]. Reading this documentation in detail can not only help organizations avoid violations, it can help bridge the knowledge gap for compliance professionals.

## Cyber Insurance Impact

Given the increase in litigation and settlements related to these technologies, cyber insurers have started to address the risk in annual renewal processes. Many organizations are being asked by their carriers to address their level of compliance with data protection laws related to their use of pixels and cookies on their websites. It can be a challenge to represent complete compliance and therefore can lead to exclusions in insurance policies. Once in place, they can be very difficult to remove. While a breach of a company servers by a malicious actor might be covered by insurance, it could be the case that a lawsuit related to the information a website collects and shares with big tech firms is not covered, leaving the company fully liable to defend and pay for any alleged or actual damages.

## Brand Damage: Negative News, Litigation, and Settlements

Several hospitals, health systems, and retailers have faced recent lawsuits related to their configurations of the Facebook Tracking Pixel and other tech-giant tracking technologies on their patient or consumer-facing websites. As a result, their impermissible disclosures of personal information to third parties, including Facebook and Google have led to significant disclosure requirements and potential penalties[8]. Advocate Aurora Health, WakeMed Health, Northwestern Memorial Hospital, and University of California San Francisco Medical Center had to notify up to millions of patients, collectively, that their sensitive PHI which was housed on the respective websites' authenticated patient portals, was compromised to third-party tech companies' tracking technologies for advertising purposes. In all three cases, the suits included complaints about inadequate or untimely notice of these practices in the organizations' privacy policies, or inadequate business associate agreements that did not comply with HIPAA.

Facebook's parent company Meta has faced multiple class action lawsuits for these practices of sharing sensitive PHI collected through their Tracking Pixel with other companies to then target patients with advertisements.

Quest Diagnostics is also facing a lawsuit regarding their use of the Facebook Tracking Pixel. The complaint alleges that Quest Diagnostics configured the pixel on their member-facing website and allowed it to collect secure medical communications, tying to a potential of one million members, from the website even though they made a statement declaring that they wouldn't work with third parties to tie together website user data with personally identifiable information[9].

The FTC has announced several recent enforcement actions against organizations for violation of the FTC Act and Health Breach Notification Rule related to their use of pixel technologies. In the first half of 2023, the FTC announced 13 cases of enforcement related to privacy and cybersecurity, which is a 260% increase in this area from all of 2022. Settlements have had significant impact including fines, requirements to retain third-party monitors for 20 years, deletion of marketing and analytics data, and restrictions of certain forms of targeted advertising which can be devastating for marketing teams and budgets.

The Video Privacy Protection Act (VPPA) enacted in 1988 aimed to protect the privacy of consumers' video viewing history by holding companies, which at the time mostly included video rental stores such as Blockbuster, liable for disclosing this history along with personally identifiable information[10]. Recent class action lawsuits have invoked the VPPA against companies that configure tracking technologies on their websites that include videos for consumers to watch related to their products or services. The viewing history of these videos is considered protected by the VPPA according to the complaints.

Non-healthcare companies have also been facing litigation around their use of third-party tracking technologies on their websites for targeted advertising without obtaining consent from users. Chick-Fil-A, the fast-food chain, was sued for violating the VPPA, by configuring the Facebook Tracking Pixel on their website and disclosing information on users' viewing history of videos included on their website[11].

## Common Issues Leading to Litigation or Non-Compliance

Through our extensive engagement in proactive reviews, investigations, and litigation, Epsilon Life Sciences has identified common issues that increase the likelihood or impact of litigation related to website marketing and analytics tools. Understanding these issues is crucial for organizations aiming to mitigate their risk and ensure compliance:

- Unintended Sharing by Default: Many organizations unintentionally collect and share information that is subject to the class action complaints or regulator investigations. Out-of-the-box configurations of analytics and marketing tools often transmit more information than necessary, resulting in unintended sharing of personal information. For example, the occurrence of "Button Clicks" events can trigger a transfer of information to third-parties, including personal, health, or financial related information from forms or questionnaires.
- Server Transactions: Server-to-server transactions involve the transfer of data from one party to another behind closed doors. These transfers can be challenging to trace, potentially leading to unintended sharing of information. Many organizations implemented tools such as the Conversions API to enable these transfers and unintentionally shared information they did not intend to transfer.
- Software Development Kits (SDKs): When developing mobile applications or web apps, many companies use pre-built code snippets to facilitate common activities such as automating an email, providing a chat feature, or other functions. However, many of these SDKs, developed by third parties, may be designed to exfiltrate more information than the organization realizes or intends to share. The use of open-source or no-cost SKDs can further complicate the due diligence required for compliance.
- Hashing is NOT Encryption: Organizations commonly encounter issues when transferring hashed values. Although hashed values seem indecipherable, they can often be easily reidentified by the receiving party if they use the same algorithm to recreate the hashed value. Default hashing algorithms provided by marketing and analytics companies, combined with their extensive datasets, effectively render the information equivalent to plain-text data. Understanding the difference between hashing and encryption is crucial, as proper encryption provides stronger defense for pseudonymization or deidentification.

## Actions Companies Should Consider

In light of these common issues, organizations, particularly those processing healthcare, financial, or other sensitive data, face the paradoxical challenge of trying to reach as many consumers as possible while simultaneously safeguarding privacy. Companies should consider the following steps to address compliance challenges:

- Conduct a Website Privacy Analysis: Most organizations may have visited their website analytics and marketing technologies several years ago as part of a brand update or when reviewing GDPR compliance.

These technologies change rapidly and can be added or changed based on new strategies or acquisitions. In addition to this, the change in laws and regulator definitions has shifted the bar of personal information to be more inclusive. These analyses, ideally conducted under a legally privileged engagement, provide a comprehensive understanding of the data elements and data flows which are the subject of these issues.

- Bridge the Knowledge Gap: In our experience, there is a knowledge gap that needs to be closed to help mitigate risk while maintaining the ability to engage with and develop new customers. Legal teams need to understand some of the technical aspects of marketing and analytics tools. Similarly, marketing teams need to be aware of the changes in definitions of personal information through new regulations, case law, and regulator guidance. Steep yourself in the foundational concepts of digital tracking (like HTTP requests, network traffic, and third-party domains) and help bridge that gap. Gaining a working knowledge of how digital technology works is crucial to compliance success. When in doubt, ask questions of your organization's IT marketing stakeholders and don't be afraid to say "I don't understand" until you do.
- Establish Clear Goals between Analytics and Targeted Marketing: The risks above should not be interpreted as a wholesale restriction of data collection and sharing. What marketing teams should do is separate the data they need or want by purpose. This could be data required for internal analytics separated from that needed for targeted marketing. Once teams can map the types of information to those goals, then it can be determined what data can be restricted from collection and how privacy notices or consent could be updated to make the residual data collection compliant.
- Build Front-End Controls: Most of the current challenges are magnified because the organization had limited visibility to the full population of information being collected and shared through their websites and were forced to inventory and analyze that data under intense legal or regulatory pressure. Moving forward, having a more defined process for identification, review, approval, and management of these tools across marketing and legal teams will help proactively identify where changes may need to be made to the tools or privacy notices.
- Evaluate Vendors and Architecture: In some cases, the response may be to simply turn off certain website pixels or limit the categories of information they currently collect. For many organizations, that data is crucial for engaging customers, providing information to their market, and their continued growth. In these matters, organizations may need to evaluate whether there are alternative vendors who can provide greater levels of assurance, such as signing a Business Associates Agreement when the information may be considered Protected Health Information. In more extreme cases, organizations with highly sensitive but highly-valued website event information may consider redesigning their analytics and marketing data architecture to have information sent to first-party servers managed by the company instead of third-party domains so they can better manage how the information is shared and used by other parties.

This issue is a moving target based on the expanding privacy laws, interesting approaches by plaintiffs, increasing regulator engagement, and the general growth of digital information. Considering the issues and taking the steps above can help organizations move toward better compliance and mitigate their litigation risks.

**Sources**


1 Google Analytics and data transfers: how to make your analytics tool compliant with the GDPR?
2 Code of Virginia: Consumer Data Protection Act § 59.1-580
3 Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates |HHS.gov
4 AHA Letter to OCR on HIPAA Privacy Rule, Online Tracking Guidance | AHA
5 Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking
6 IAPP: Washington's My Health, My Data Act
7 https://support.google.com/analytics/answer/13297105?hl=en
8 Northwestern Memorial next in line for Meta class action (fiercehealthcare.com)
9 Quest Diagnostics Sued for Use of Facebook Tracking Pixel | Law Street Media
10 New Class Action Alert: VPPA Claims | ArentFox Schiff - JDSupra
11 Chick-Fil-A Sued for Sharing Data through Meta Pixel | Robinson+Cole Data Privacy + Security Insider - JDSupra

**Macie Stratton**
mstratton@epsilonlifesciences.com
702.375.3052

**Mayesha Awal,  MSHM, CBCS, CHW**
mawal@epsilonlifesciences.com
317.652.6429

**Kari Czeszewski, CHC**
kczeszewski@epsilonlifesciences.com
847.226.4042

**Nick Weil, JD, CIPT**
nweil@epsilonlifesciences.com
949.275.4578

**Brian Segobiano, CIPP/E**
bsegobiano@epsilonlifesciences.com
312.860.8025

**Saul B. Helman, MD, MBA, BS**
shelman@epsilonlifesciences.com
317.294.1228