

Mini Summit 47: Pixels and Privacy: Navigating the Litigation and Enforcement Landscape of Website and Mobile App Privacy



October 2023

Presenters

Pixels and Privacy: Navigating the Litigation and Enforcement Landscape of Website and Mobile App Privacy



Christine Moundas, MPH, JD

Partner, Ropes & Gray; Former
Program Analyst, US Department
of Health and Human Services,
Office of Inspector General

New York, NY



Elizabeth Smith, JD

Senior Director, Data Privacy and
Associate General Counsel
Seagen,

Bothell, WA



Katy Van Pelt, JD

Vice President and Head Of Ethics
and Compliance, Data Protection
Officer
Arcus Biosciences

Brisbane, CA



Brian Segobiano

Managing Director & Chief Privacy
Officer,
Epsilon Life Sciences (*Moderator*)

Chicago, IL



Agenda

Pixels and Privacy: Navigating the Litigation and Enforcement Landscape of Website and Mobile App Privacy

1 **Technology Overview**

2 **Current Compliance Landscape: US and Abroad**

3 **Litigation Trends: Laws and Claims Raised**

4 **FTC Enforcement**

Related Items

- Future U.S. State Laws
 - Dark Patterns
 - Use of Artificial Intelligence (AI)
-

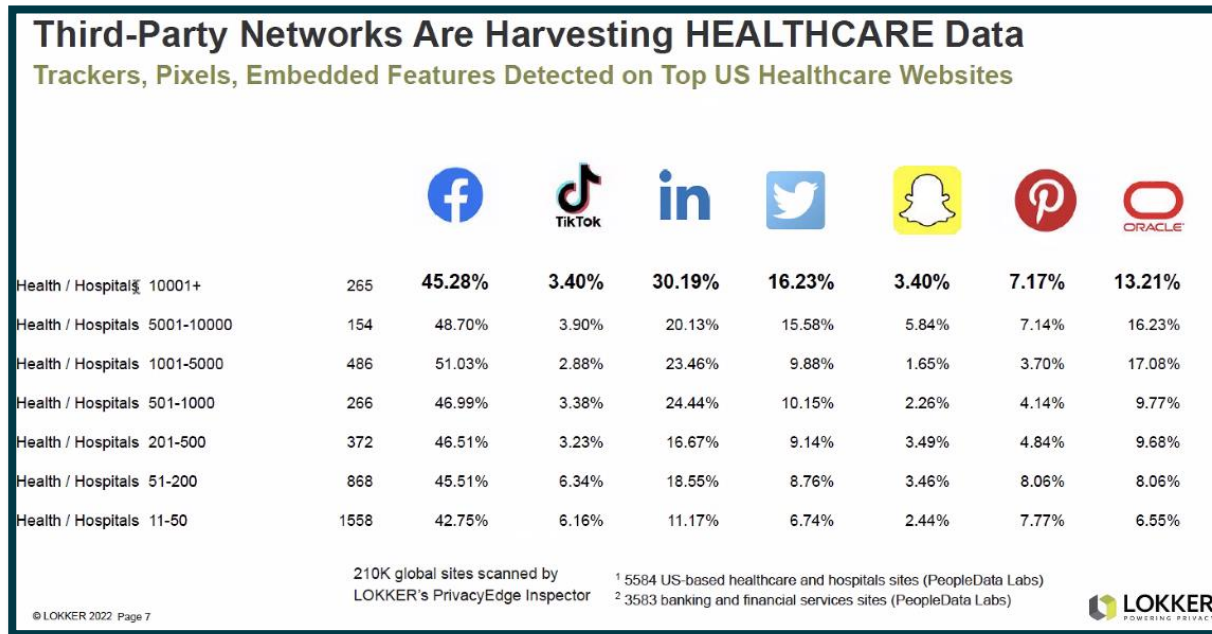
5

6

Contact Info

Website and Mobile App Online Tracking Tools

Pixels and Privacy: Navigating the Litigation and Enforcement Landscape of Website and Mobile App Privacy



Marketing & Analytics

Data lakes of website and app user information to fuel the engine for customer engagement and revenue growth

Management of Risk

Controls to address the new risks associated with these tools, even as they are already in-flight

Technology Overview: Methods of Deployment

Pixels and Privacy: Navigating the Litigation and Enforcement Landscape of Website and Mobile App Privacy



Directly in website source code



Centralized tag management system (e.g., Google Tag Manager)



Third-party widgets and components of websites (e.g., video players, chat bots, etc.)

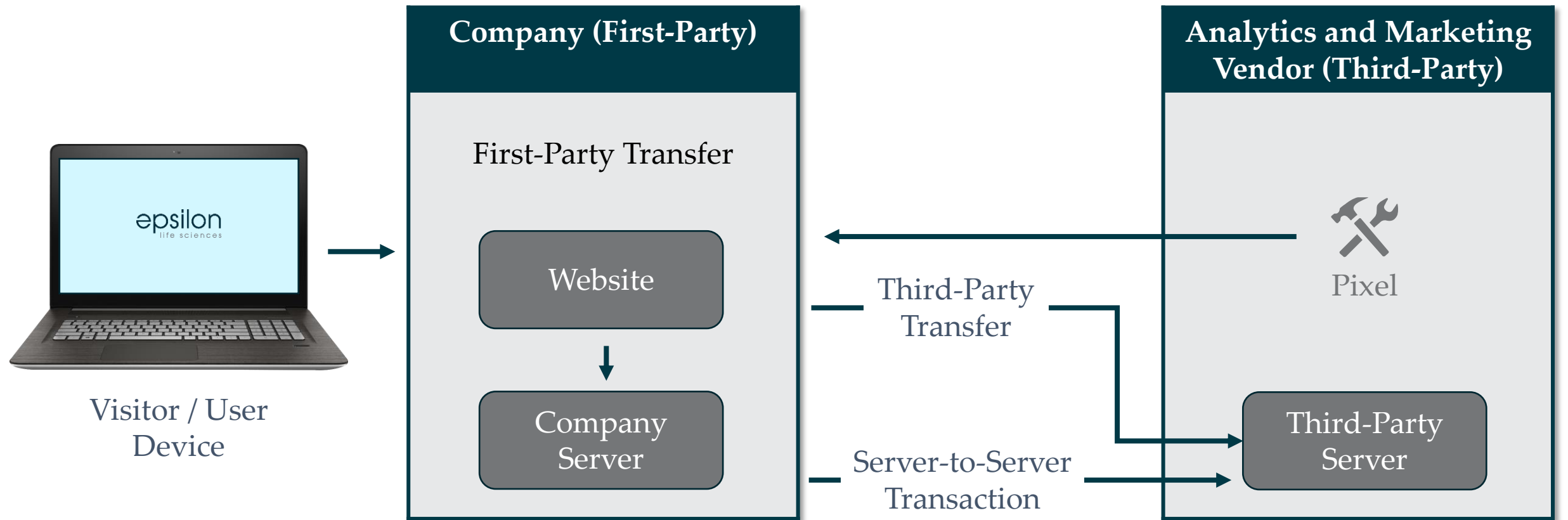


Third-party Platforms (e.g., Facebook CAPI)

Descriptions of Key Technology

Pixels and Privacy: Navigating the Litigation and Enforcement Landscape of Website and Mobile App Privacy

Example of how the information flow could work across a user device, first, and third party



Current Compliance Landscape US and Abroad

Pixels and Privacy: Navigating the Litigation and Enforcement Landscape of Website and Mobile App Privacy

GDPR – this might apply to you if your products/services are directed at EEA residents (or if your website/app is not specifically noted as being intended for another audience, such as U.S. only)

The **European Union's General Data Protection Regulation** (GDPR) imposes requirements and limitations on the use of personal data collected about residents of the EEA, including personal data collected on websites, such as:

- Strict requirements around the transfer of personal data from the EEA to jurisdictions that aren't considered to have adequate protections;
- Requirements around notice (clearly inform users of what will be collected and where it will be used) and consent (opt-out not sufficient)
- Data Protection Authorities in several European countries including Sweden, France, Italy, and Austria have ruled that Google Analytics is impermissible because in tracking user activity, it transfers personal data to the United States without sufficient safeguards. Keep an eye on the EU-US Data Privacy Framework, including whether it withstands expected challenges, because it may provide a legal pathway (Google is certified under the DPF)

Current Compliance Landscape US and Abroad

Pixels and Privacy: Navigating the Litigation and Enforcement Landscape of Website and Mobile App Privacy

A number of countries have similar requirements restricting transfers without consent or prior authorization, and we continue to see rapid development of laws. In addition to the GDPR, a few of the many countries with potentially applicable privacy laws to consider:

- China
- Brazil
- Canada
- Iceland
- India
- South Korea
- Japan
- South Africa
- Switzerland
- UK
- Israel



Current Compliance Landscape US and Abroad

Pixels and Privacy: Navigating the Litigation and Enforcement Landscape of Website and Mobile App Privacy

Plethora of state law developments (see [IAPP tracker](#)) but first question: Does the law apply to your business and to the proposed business activity?

For each law, consider the minimum threshold for applicability to your company (i.e., entity must process data of 100,000 data subjects; derive 50% of revenue from processing; annual revenue exceeding \$25 million)

	Employee Data	B2B Data	Patient (non-HIPAA)/HCP/Consumer Data (marketing)	Clinical Trial Data/HIPAA covered data
California	Yes	Yes	Yes	No
Virginia	No	No	Yes	No
Colorado	No	No	Yes	No
Connecticut	No	No	Yes	No
Utah	No	No	Yes	No
Washington	No	No	Yes (health data only)	No
Others (including proposed)	No	No	Yes	No

Current Compliance Landscape US and Abroad

Pixels and Privacy: Navigating the Litigation and Enforcement Landscape of Website and Mobile App Privacy

Washington My Health My Data Act

- **Scope:**
 - “**Consumer Health Data**” is broadly defined to include any information reasonably linkable to an individual that relates to past, present, or future health status
 - “**Consumer**” includes anyone whose data is collected in Washington (not just residents)
 - Unlike other state laws, there is no minimum number of data subjects or revenue threshold for applicability
- Main requirements:
 - “**Consumer health privacy policy**” prominently displayed on all web pages or apps where personal data is collected that includes:
 - Categories of data collected
 - Categories of sources of that data
 - Categories (or list of?) third-parties/affiliates with whom data is shared
 - Affirmative consent to the specific processing activity – if anything changes from what was in the privacy policy at the time consent was obtained, must re-consent

Current Compliance Landscape US and Abroad

Pixels and Privacy: Navigating the Litigation and Enforcement Landscape of Website and Mobile App Privacy

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.

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.

Threshold question – does HIPAA apply to you and to this business activity?

1. Does it apply to you? Only applies to **covered entities** and their **business associates**
 - A. Covered entities includes applicable to health plans, health care clearinghouses, and health care providers
 - B. Business associates includes entities performing certain functions on behalf of or providing services to covered entities
 - C. Clinical trial sponsors:
 - A. HHS: "Sponsors and their vendors are typically not health care providers or HIPAA covered entities . . . [but] they nevertheless may have privacy obligations to subjects based on common law principles, state privacy laws, and/or promises made to prospective subjects." [HHS](#).

Current Compliance Landscape US and Abroad

Pixels and Privacy: Navigating the Litigation and Enforcement Landscape of Website and Mobile App Privacy

FTC

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.

Note - This is not new – it's been around since 2009, but there is apparently renewed interest.

Nationwide Pixel Cases

Pixels and Privacy: Navigating the Litigation and Enforcement Landscape of Website and Mobile App Privacy

Class Actions

- ▶ Hundreds of class actions filed against defendants utilizing pixels or other tracking technology. Many allegations rely on laws that predate the modern internet and have a statutory damage component.

Improper Disclosure of PHI or PII

- ▶ Allegations that defendants improperly disclosed PHI or PII to third parties without authorization

Claims for Damages

- ▶ Claims for damages based on theories of invasion of privacy, identity theft, mitigation efforts, and breach of contract damages

State Wiretapping Statutes: *Common Elements*

Pixels and Privacy: Navigating the Litigation and Enforcement Landscape of Website and Mobile App Privacy



CLASS ACTION

Surge of class action filings in California, Florida, and Pennsylvania as two-party consent states



RECORDED COMMUNICATIONS

Not identical statutes, but generally allow private suits based on allegations that communications were recorded without consent



DAMAGES

Provide statutory damages ranging from \$1,000 to \$5,000 per violation



SESSION REPLAY

Litigation has focused on “session replay” software but has recently shifted to chat software



STANDING?

Standing may present a challenge to would-be plaintiffs

Pixel Litigation: Common Claims

Pixels and Privacy: Navigating the Litigation and Enforcement Landscape of Website and Mobile App Privacy

Invasion of Privacy

Alleges public disclosure of private facts/intrusion upon seclusion

Violation of State Unfair Deceptive Trade Practices Act

State laws prohibit unfair or deceptive practices affecting commerce

Breach of Implied Contract

Claims mutual assent not to disclose PHI/PII based on company data privacy policies

Violation of Electronic Communications Privacy Act (and State Wiretapping Acts)

- Wiretap Act prohibits the unauthorized and intentional interception of wire, oral, or electronic communications
- Stored Communications Act prohibits the divulgence of communications in electronic storage to unauthorized third parties

Breach of Confidence and Fiduciary Duty

Alleges breach of implicit understanding not to share personal information or breach of fiduciary duty

Violation of Video Privacy Protection Act

Prohibits videotape service providers from knowingly disclosing PII

Pixel Litigation: Unique Challenges

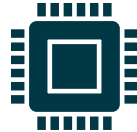
Pixels and Privacy: Navigating the Litigation and Enforcement Landscape of Website and Mobile App Privacy



Need to gather current-state as well as historical data from websites



Many internal and third-party (e.g., ad agency) teams involved



Many non-standard data systems in scope for preservation (e.g.m Google Analytics, FB Business Manager, CRM tools, etc.)



Lack of visibility to full universe of third-parties



Multiple methods for deploying tools via website code and tag managers



Lack of contracts or appropriate clauses with vendors

QUESTION: The FTC made headlines this year with some cases against companies in the healthcare space using pixels. Can you tell us the main issues, results of the cases, and how this kind of enforcement could impact us?

The New York Times

GoodRx Leaked User Health Data to Facebook and Google, F.T.C. Says

The popular drug discount app deceptively shared details on users' illnesses and medicines with ad firms, regulators said in a legal complaint.

The Washington Post

Democracy Dies in Darkness

Fertility app Premom settles with FTC over risky data sharing

The app allegedly shared sensitive user information with China-based companies known for privacy problems



By [Tatum Hunter](#)

May 17, 2023 at 4:26 p.m. EDT

POLITICO

TECHNOLOGY

FTC reaches deal with online therapy company over data misuse claims

The action against BetterHelp is just the latest the agency has taken to protect online health data.

By [JOSH SISCO](#) and [RUTH READER](#)

03/02/2023 11:19 AM EST

Updated: 03/02/2023 12:09 PM EST



The Federal Trade Commission reached a settlement with online therapy company BetterHelp over allegations it shared customers' sensitive health data with third parties for advertising purposes, according to documents from the agency's in-house court filed this morning and reviewed by POLITICO.

The Teladoc-owned company has agreed to pay \$7.8 million and change a variety of its business practices to resolve allegations that it shared consumer data with third parties despite telling customers it would not, according to the

FTC-HHS joint letter gets to the heart of the risks tracking technologies pose to personal health information

By: [Lesley Fair](#)

July 20, 2023



FTC Enforcement

Pixels and Privacy: Navigating the Litigation and Enforcement Landscape of Website and Mobile App Privacy

GoodRx

Allegations

FTC's Health Breach Notification Rule Violation & unfair and deceptive trade practices – Disclosure of PHI to third parties without the users' authorization, consent, or knowledge

Shared PHI with third party advertising companies (e.g., Facebook, Google, Criteo) – Shared PHI with third parties while promising to never do so

Used PHI for Targeted Advertisements – Used data shared with social media organizations for targeted advertisements on those platforms

Third-Party Use of PHI – Without consent shared data with third parties who used the information for R & D and advertising

Misrepresentation of HIPAA Compliance – Suggested compliance with HIPAA when they allegedly were not

Failure to Implement Policies Protecting PHI – Insufficient written standards related to protecting PHI

Settlement

Financial - \$1.5 million penalty for violating the rule

Sharing health information for advertisements - Prohibited from disclosing health data to third parties for advertising purposes

Consent required prior to sharing health information for purposes other than advertising – Prior to disclosing health data to third parties affirmative express consent must be acquired (manipulative designs are prohibited)

Require deletion of data shared – Must inform third parties that received health data of the FTC enforcement action and require them to delete the health data they had received

Limit Data Retention - Must limit data retention in accordance with a publicly posted data retention schedule

Implementation of a Privacy Program - Must set up a comprehensive privacy program and have **third-party assessor for 20 years**

Information sourced and paraphrased from:

- <https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising>
- <https://www.justice.gov/opa/pr/digital-healthcare-platform-ordered-pay-civil-penalties-and-take-corrective-action>
- https://www.ftc.gov/system/files/ftc_gov/pdf/goodrx_stipulated_order_for_permanent_injunction_civil_penalty_judgment_and_other_relief.pdf

Other Risks

Pixels and Privacy: Navigating the Litigation and Enforcement Landscape of Website and Mobile App Privacy




Future U.S. State Laws

There are several U.S. state privacy legislations currently in committees, in cross-committees, or have been passed. A few states also have inactive bills, while others have not yet introduced comprehensive bills; however, there is a possibility of them introducing bills.



Dark Patterns

Organizations may use deceptive techniques to mislead users or consumers into actions that they may not perform, which could include unknowingly consenting to online tracking.



Use of Artificial Intelligence (AI)

AI raises ethical concerns, particularly regarding data integrity and collection practices. Personally identifiable information (PII) and protected health information (PHI) can be significant issues in the context of online tracking technology.

Contact Info

Pixels and Privacy: Navigating the Litigation and Enforcement Landscape of Website and Mobile App Privacy

Christine Moundas, MPH, JD

*Partner, Ropes & Gray; Former Program Analyst,
US Department of Health and Human Services,
Office of Inspector General*
+1 212.596.9035
Christine.Moundas@ropesgray.com

Elizabeth Smith, JD

*Senior Director, Data Privacy and Associate General
Counsel*

Katy Van Pelt, JD

*Vice President and Head Of Ethics and Compliance,
Data Protection Officer*

Brian Segobiano, CIPP/E

Managing Director and Chief Privacy Officer
+1.312.860.8025 (M)
bsegobiano@epsiloneconomics.com



Descriptions of Key Technology

Pixels and Privacy: Navigating the Litigation and Enforcement Landscape of Website and Mobile App Privacy

Term	Description	Note
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.	<p>They could be:</p> <ul style="list-style-type: none">• General information such as the type of browser and screen resolution• Detail the type of event such as a "button click" or "form submission,"• More sensitive details such as a social media user id, email, name, location, etc.

Descriptions of Key Technology

Pixels and Privacy: Navigating the Litigation and Enforcement Landscape of Website and Mobile App Privacy

Term	Description	Note
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.	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

Descriptions of Key Technology

Pixels and Privacy: Navigating the Litigation and Enforcement Landscape of Website and Mobile App Privacy

Term	Description	Note
First / Third-Party	This means the party that owns the servers that collect the information.	<ul style="list-style-type: none">• 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.

Descriptions of Key Technology

Pixels and Privacy: Navigating the Litigation and Enforcement Landscape of Website and Mobile App Privacy

Term

Description

Note

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.
- **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.

Descriptions of Key Technology

Pixels and Privacy: Navigating the Litigation and Enforcement Landscape of Website and Mobile App Privacy

Term	Description	Note
Lifecycle	Each type of cookie has a predetermined lifecycle. A cookie is described as either a session cookie or a persistent cookie.	<ul style="list-style-type: none">• A session cookie is defined as a cookie that remains on a user's browser until their browser is closed.<ul style="list-style-type: none">• 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.<ul style="list-style-type: none">• This expiration date is set by the parameters of the cookie when it is created and can last as long as the creator wants.

Descriptions of Key Technology

Pixels and Privacy: Navigating the Litigation and Enforcement Landscape of Website and Mobile App Privacy

Term	Description	Note
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.	<ul style="list-style-type: none">• 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.

Future U.S. State Laws

Pixels and Privacy: Navigating the Litigation and Enforcement Landscape of Website and Mobile App Privacy

In Committee Statutes/Bills

- Wisconsin
 - Introduced as AB 466, the Wisconsin Privacy Bill had a hearing in the House Committee on Consumer Protection on October 5th. It incorporates provisions like those found in privacy laws of other states.
- Pennsylvania
 - The Consumer Data Privacy Act (House Bill 1201) has been introduced and reviewed by the House Commerce Committee in Pennsylvania. If passed, this act would mandate businesses to offer consumers the option to opt out of data processing and request the deletion of their collected personal data.
- Massachusetts
 - The Massachusetts Data Privacy Protection Act, referred to the House Committee on Advanced Information Technology, Internet, and Cybersecurity, aims to establish a robust state data privacy law. It's designed to shield consumers from unauthorized collection and usage of personal, biometric, and sensitive data.
- North Carolina
 - The Consumer Privacy Act seeks to protect consumers from unauthorized collection of biometric data, protected health information, sensitive data, and specific geological location.

In Cross Committee

- New Hampshire
 - On October 10th, there was a House Judiciary Subcommittee on revising a previously introduced comprehensive privacy bill. Potential points include private right of action and applicable organizations.

Inactive and No Comprehensive Bills

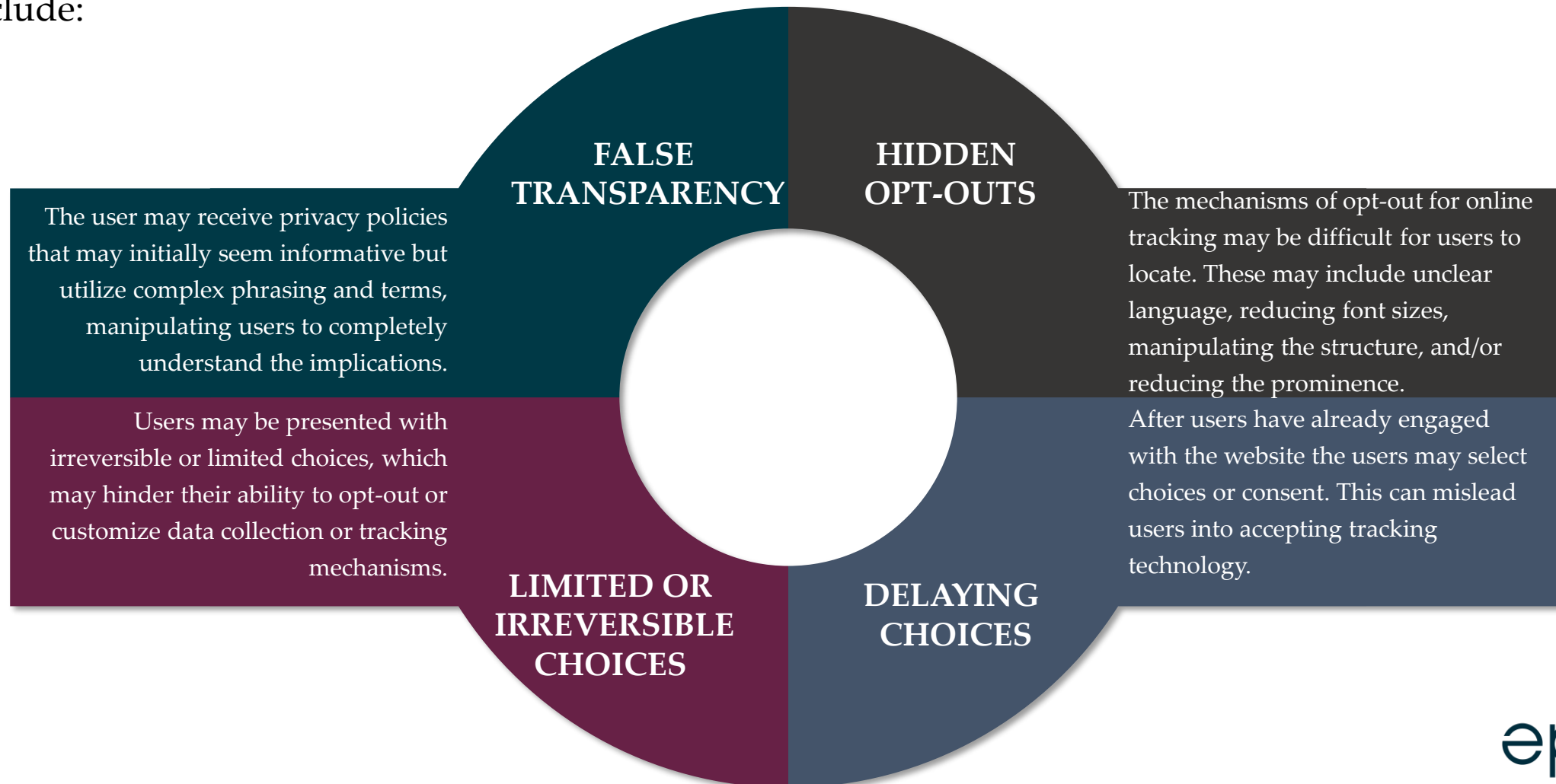
- Inactive
 - Washington, Minnesota, Illinois, Kentucky, West Virginia, Oklahoma, Louisiana, Mississippi, New York, Vermont, Maine, Rhode Island, Maryland, Hawaii
- No Comprehensive Bills
 - Idaho, North Dakota, South Dakota, Nebraska, Wyoming, Nevada, Arizona, New Mexico, Alaska, Arkansas, Kansas, Missouri, Alabama, Georgia, South Carolina, Florida, Ohio, Michigan

Note: These reflect the current legislation as of 10/13/2023.

Dark Patterns

Pixels and Privacy: Navigating the Litigation and Enforcement Landscape of Website and Mobile App Privacy

Dark patterns are deceptive strategies that mislead users into actions that they may not otherwise carry out. These may include:



Use of Artificial Intelligence

Pixels and Privacy: Navigating the Litigation and Enforcement Landscape of Website and Mobile App Privacy

Capture personal information (e.g., browsing habits, location, data, and purchasing history)

Concerns for user consent for tracking and data collection

Algorithmic bias, which could lead to unfair outcomes for content

Ethical considerations about the responsible use of data

Predictive analysis based on historical interactions and patterns

Location tracking and geofencing for targeted messages, promotions, or third-party notifications