



Online Tracking Technologies and the Rise of Class Action Lawsuits

AGENDA

- **Overview of Online Tracking Technologies**
- **Recent Perspective Shifts**
- **Recent Regulatory and Enforcement Developments**
 - **Office for Civil Rights (OCR)**
 - **Federal Trade Commission (FTC)**
- **Class Action Lawsuits and Reported Breaches**
- **AHA Response to OCR Guidance**
- **Key Takeaways**

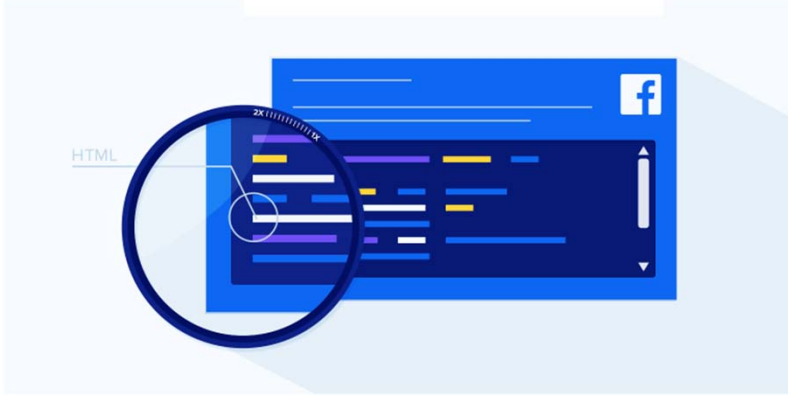
AGENDA

- **Overview of Online Tracking Technologies**
- Recent Perspective Shifts
- Recent Regulatory and Enforcement Developments
 - Office for Civil Rights (OCR)
 - Federal Trade Commission (FTC)
- Class Action Lawsuits and Reported Breaches
- AHA Response to OCR Guidance
- Key Takeaways

Overview of Online Tracking Technologies

- **Tracking technologies** are software that collect information from website/mobile application users such as clicks, geolocation, responses to prompts or surveys, IP addresses, hardware and software specifications, and preferences.
 - Offered by third party vendors, often free-of-charge
 - Typically, snippets of code provided by third-party vendors are embedded by organizations directly in their websites' or applications' code
 - Vendors receive tracking data and, in return, provide useful data to the entity to support web/application development or marketing efforts
 - Entities across industries (health care, IT, financial services) use tracking technologies

Meta Pixel



Google Marketing Platform

Get essential customer insights.

Get a complete understanding of your customers across devices and platforms. Google Analytics gives you the tools, free of charge, to understand the customer journey and improve marketing ROI.

[Get started today](#)

Overview of Online Tracking Technologies

- Tracking technologies include:
 - Cookies: Small files of information that a web server generates and sends to a web browser. Relevant cookies are attached to future requests the user makes of the web server, enabling a personalized user experience
 - Web beacons: Check whether a user has accessed certain content on a website.
 - Tracking Pixel: Tiny snippets of code that allow information to be gathered about website visitors, such as how they browse, what type of ads they click on, etc.
 - Session Replay Scripts: Scripts that record a user's actions while visiting a website. Session replays are often used by vendors to monitor effectiveness of the UI or fix bottlenecks in web design.
 - Fingerprinting: Creates a unique “digital fingerprint” of the website user based on computer hardware, software, preferences, etc.

AGENDA

- Overview of Online Tracking Technologies
- **Recent Perspective Shifts**
- Recent Regulatory and Enforcement Developments
 - Office for Civil Rights (OCR)
 - Federal Trade Commission (FTC)
- Class Action Lawsuits and Reported Breaches
- AHA Response to OCR Guidance
- Key Takeaways

Recent Perspective Shifts

- ***Historical Approach to Online Tracking Technologies***
 - Installation of third-party tracking technologies is widespread across the internet
 - By many estimates, more than 90% of websites use online tracking technology
 - Installation of third-party tracking technologies were historically not considered to involve the use or disclosure of sensitive personal data, in part because entities were not fully aware of the **scope of identifiable information collected** through tracking technologies and **how it was being used**, and because federal agencies had not issued guidance on this topic
 - Many websites believed they covered their bases through broad disclosures in website and mobile application privacy policies, putting website and mobile application users on notice of data collection practices.
 - According to a [recent study from the University of Pennsylvania](#), many Americans don't understand and believe they don't have any control over the data that is tracked in relation to their online behaviors
 - In August 2022, the FTC published an advance notice of proposed rulemaking related to data tracking and security practices

Perspective Shifts in U.S. Began in Healthcare

- ***Mass General Brigham/Dana-Farber Settlement***

- Started with case brought against MGB and Dana-Farber in 2019, where patients alleged that hospitals' use of third-party tracking technology, without patient consent, violated their privacy rights, as well as state consumer protection statutes.
- Settlement in early 2022 for \$18.4 million.

- ***Markup Exposé***

- In June 2022, a tech-focused journalism outlet, The Markup, published an exposé claiming that, of the top 100 Newsweek-ranked U.S. hospitals, 33 had installed the Meta Pixel on appointment scheduling pages, and six had installed Meta Pixel on patient portals, potentially violating patient privacy.



Pixel Hunt

Facebook Is Receiving Sensitive Medical Information from Hospital Websites

Experts say some hospitals' use of an ad tracking tool may violate a federal law protecting health information

Perspective Shifts in U.S. Began in Healthcare

- ***Fallout Post-Markup Article***

- After the Mass General/Dana-Farber settlement and The Markup's exposure of widespread use of tracking technologies in the healthcare industry:
 - Regulators began taking a closer look at whether the use of tracking technologies infringed on applicable privacy rights
 - Entities began considering whether the use of tracking technologies necessitated breach notification under applicable laws and/or amendment to their tracking and data privacy practices
 - Website and mobile application users became aware of potential unauthorized disclosures of their data

Scrutiny Has Extended Beyond Healthcare

■ Additional *Markup* Articles

- In April 2022, it was reported that the Education Department may have shared information about students who applied for student aid online via online trackers in the FAFSA form
- In November 2022, *The Markup*, published another exposé claiming that tax filing websites impermissibly shared tax information; congressional inquiries followed
- Multiple plaintiffs have filed lawsuits against companies alleging privacy harms from the use of online tracking that range from invasion of privacy torts and breach of contract to federal laws like the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and the Video Privacy Protection Act; all statutes and common law theories developed decades before modern tracking

AGENDA

- Overview of Online Tracking Technologies
- Recent Perspective Shifts
- **Recent Regulatory and Enforcement Developments**
 - **Office for Civil Rights (OCR)**
 - Federal Trade Commission (FTC)
- Class Action Lawsuits and Reported Breaches
- AHA Response to OCR Guidance
- Key Takeaways

Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates (December 1, 2022)

- OCR provided guidance for “regulated entities,” e.g., HIPAA Covered Entities and Business Associates
- OCR has taken the position that patient information transmitted to tracking vendors is generally PHI required to be protected under HIPAA, **even if**:
 - The information transmitted does not include health information (e.g., geolocation)
 - The individual does not have an existing relationship with the entity
- OCR states an “impermissible disclosure” leads to a presumption of breach, unless the regulated entity can demonstrate a low probability of compromise.

OCR Guidance

- User-authenticated webpages: User information (e.g., email address, appointment dates, sensitive medical info) is deemed PHI
- Unauthenticated webpages: User information is **not** considered PHI, **except where**:
 - User enters credential information (e.g., patient portal login); OR
 - Notably, the user may be entering information on behalf of someone else
 - The page addresses specific symptoms or health conditions, such as pregnancy or miscarriage; OR
 - Note: likely in response to *Dobbs*, but language is not limited to reproductive health
 - The page allows the user to search for doctors or schedule appointments w/o credentials
- Mobile apps: User information (e.g., fingerprints, device ID, sensitive medical info) is PHI, if the app is offered by a regulated entity
- For any modality, if PHI is received by a vendor, disclosures must be made in accordance w/ HIPAA and BAA must be executed



- In 2009, The FTC issued the Health Breach Notification Rule (“HBNR”), which requires certain entities not subject to HIPAA to notify consumers, the FTC, and, in some cases, the media, following a breach involving unsecured identifiable health information contained in a personal health record that is maintained or offered by the entity or through a product or service provided by the entity.
- Applies to electronic records containing individually identifiable health information (**personal health records**, or **PHRs**), defined as any information that:
 - (A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
 - (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and—
 - (i) identifies the individual; or
 - (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.
- Breach reporting obligations for the following entities:
 - **Vendors of PHRs:** Entities that offer or maintain PHRs (Note: this may include mobile applications used for research)
 - **PHR related entity:** Entities not subject to HIPAA that offer products/services through the website of a vendor of PHRs or HIPAA-covered entity.
 - **Third party service provider:** Entities that offer services to vendors of PHRs.
 - Note: The rule applies to all entities that fall within one of these categories; the HBNR is **not** limited to entities subject to the FTC’s Section 5 jurisdiction (i.e., persons, partnerships, corporations) and **applies to educational institutions, charities, and 501(c)(3)s.**



- ***Scope of HBNR***
 - In September 2021, the FTC released a short policy statement (the “Statement”) on the scope of the HBNR. The Statement:
 - Expanded the definition of “health care providers” to include developers of health apps or connected devices.
 - Clarified that apps that draw information from multiple sources is subject to HBNR, even if the health information only comes from one source.
 - The Statement placed entities on notice of their obligation to disclose breaches to the FTC and signaled the FTC intends to bring actions to enforce the HBNR.

AGENDA

- Overview of Online Tracking Technologies
- Recent Perspective Shifts
- Recent Regulatory and Enforcement Developments
 - Office for Civil Rights (OCR)
 - Federal Trade Commission (FTC)
- **Class Action Lawsuits and Reported Breaches**
- AHA Response to OCR Guidance
- Key Takeaways

Common Types of Claims in Class Actions

- **Violation of Federal and State Statutes**
 - Electronic Communications Privacy Act (“ECPA”)
 - Computer Fraud and Abuse Act (“CFAA”)
 - State Wiretap Laws (e.g., CIPA)
 - State Unfair Competition Laws
 - State Medical Privacy Laws
- **Common Law Invasion of Privacy – Intrusion Upon Seclusion**
 - Alleges defendants intruded and/or aided, agreed with, employed, and/or conspired with the third party wiretappers to intrude into a private place, conversation, matter; in a manner was highly offensive to a reasonable person
- **Breach of Express Contract**
 - Breach of entity’s terms and conditions and privacy policy
- **Breach of Implied Contract**
 - Based on representation by entity of secure and confidential patient portal
- **Trespass to Chattels**
 - Tracking technologies interfere with plaintiffs’ computing devices

Defenses and Challenges to Class Actions

- **Healthcare facilities are parties to the communication**
- **Healthcare facilities use website analytics as part of standard operations**
- **Lack of tangible harm**
- **No invasion of privacy**
 - Common law consent vitiates tort claims
 - Healthcare systems are not intruding on the privacy of website visitors
- **No clear express or implied contract**
- **Third-party's use of data is proximate cause for harm**
- **Class challenge**
 - Recent ruling in Maryland state court in *Doe v. MedStar Health* denying class certification: “Putative class members who log into their Patient Portal are at a fundamentally greater risk of having confidential health information (i.e., patient status) shared than class members who only use the publicly available websites, regardless of the webpages they ‘visit’ or the searches they conduct on the Defendants’ websites.”
 - Differential impact of browser settings

AGENDA

- Overview of Online Tracking Technologies
- Recent Perspective Shifts
- Recent Regulatory and Enforcement Developments
 - Office for Civil Rights (OCR)
 - Federal Trade Commission (FTC)
- Class Action Lawsuits and Reported Breaches
- **AHA Response to OCR Guidance**
- Key Takeaways

AHA Response to OCR Guidance

- On May 22, 2023, the American Hospital Association wrote a letter urging the OCR to reconsider its December 2022 Online Tracking Guidance asserting that the current Online Tracking Guidance aggravates the risk of health misinformation by treating a mere IP address as a unique identifier under HIPAA
 - *“This guidance ... is too broad and will result in significant adverse consequences for hospitals, patients and the public at large. In particular, by treating a mere IP address as protected health information under HIPAA, the Online Tracking Guidance will reduce public access to credible health information.”*
 - *“Through the use of their websites, apps and other digital platforms, hospitals and health systems are able to reach underserved communities that would not otherwise have access to reliable health information.”*
 - *“Critically, if an IP address, in and of itself, is treated as a unique identifier under HIPAA, hospitals and health systems will be forced to restrict the use of certain technologies that help improve community access to health information.”*

AGENDA

- Overview of Online Tracking Technologies
- Recent Perspective Shifts
- Recent Regulatory and Enforcement Developments
 - Office for Civil Rights (OCR)
 - Federal Trade Commission (FTC)
- Class Action Lawsuits and Reported Breaches
- AHA Response to OCR Guidance
- **Key Takeaways**

Key Takeaways

- Convene a cross-disciplinary team to prioritize understanding organization's use of online tracking technologies on all forms of web assets (websites, portals, mobile apps) with focus on:
 - Full inventory of all web assets (with priority towards understanding higher risk assets)
 - Types of tool (with priority towards understanding higher risk tools)
 - Third parties involved
 - Nature of data disclosures
 - Nature of data uses
- *Consider consulting forensic investigation using third party under privilege*

Key Takeaways (Continued)

- Consider altering or removing existing uses of tracking technologies depending upon risk profile
- Ensure that cookie management tools and preference centers are implemented and properly configured
- Analyze and document which legal regimes apply to a given web asset (e.g., FTC, HIPAA, CCPA/CPRA, GDPR)
- Update external privacy notices and privacy policies
- Implement internal online tracking tool policies and oversight infrastructure
- Consider monthly scans to track changes to online tracking tools

Key Takeaways (Continued)

- Incorporate learnings into contractual language, notices & consents, deal diligence, etc.
- Monitor the third parties with which the organization shares sensitive information, including what information is disclosed and how it is used by the third parties
 - For HIPAA Covered Entities and Business Associates, assess whether the organization has business associate agreements in place with such third parties
- Ensure that the organization is appropriately communicating with consumers about potential uses of their personal and sensitive information
- Stay abreast of rapidly evolving enforcement and litigation landscape