

Cookies, VPPA and Other AdTech and Tracking Practices that Can Get You in Trouble

*Privacy and Security Forum
May 11, 2023*



Moderator: James Koenig
jim.Koenig@troutman.com

Panelists:

Brent T. Hoard
brent.hoard@troutman.com

Nitish Jayan
nitish.jayan@inmobi.com

Joel M. Lutz –
joel.lutz@troutman.com

Angelo A. Stio III
angelo.stio@troutman.com

Agenda

1. Cases Being Pursued
2. Technologies and How They Are Used
3. Pixels
4. Legal Theories Being Pursued
5. How to Reduce Risks

Cases Being Pursued

AdTech in the headlines

Video Streamer FloSports Sued Over Data Sharing with Facebook

New Wave of “Live Chat” and “Key Stroke” Wiretapping Class Actions Hits California Courts

Is the Video Privacy Protection Act a New Litigation Weapon for Consumers?

NFL Is Latest Target in Lawsuits Over Data-Sharing With Meta

Boston Globe Class Action Claims Newspaper Shares Subscriber Data With Facebook Without Consent

Privacy Law Trends to Watch: Wiretapping Class Actions Focused on Session Replay

18 hospitals, health systems facing lawsuits for healthcare data-sharing

Netflix Settles Privacy-Violations Lawsuit for \$9 Million

**SPORTS TV NEWS
ESPN Accused Of Data Sharing Without Consent In Class Action Lawsuit**

Sephora to pay \$1.2m to settle Cali privacy law claims

Louisiana systems hit with lawsuits for allegedly sharing patient data with Facebook

NBA Sued For Providing Digital Data To Meta Without Consent

Tracking Technologies and How They are Used

Types of Technologies, How They Work, What They Track

- Pixels
- Cookies
- Session Replays
- Chat Box
- Google Analytics



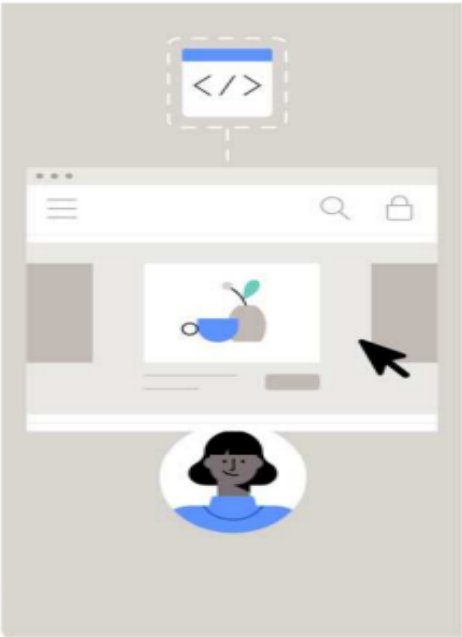
Pixels

The Meta Pixel

- The Meta Pixel is a free and publicly available piece of code that Meta allows third-party website developers to install on their websites.
- The Pixel is customizable: website developers choose which types of user action to measure, and program the Pixel accordingly.
- Website developers in a range of industries use the Pixel.
- The Meta Pixel allows website developers to learn: (1) if and when website users take certain actions on a website, and (2) generalized information about website users, which can be used for targeting advertising.


The Meta Pixel


Connect Website Activity Using Facebook Pixel




[Give feedback](#)

How it works

-  **Pixel is used to track actions customers take on your website.**

Pixel is a way to capture what customers do on your website, so you can use this information to build audiences and run more effective ads.
-  **Customer actions are captured through an event.**

This can be a user going to your website and clicking on 'Add to Cart'. An event will track this action.
-  **Event parameters capture the details of an event.**

If a user clicks 'Add to Cart', parameters capture key details of that action such as identifying the price and currency of the item that was added.

[Continue](#)

The Facebook Cookie

- Cookies are “small pieces of text used to store information on web browsers, which “store and receive identifiers and other information on computers, phones and other devices.
- Cookies serve a number of different functions, such as personalizing content, tailoring and measuring ads, and providing a safer experience.
- When a Facebook user signs up for Facebook, a Facebook cookie is installed on a Facebook user’s web browsing device.
- When a Facebook user visits a website that has the Meta Pixel enabled, the Pixel identifies the Facebook Cookie and directs a Facebook user’s web browsing device to send information to Meta about websites or applications the Facebook user visits and certain activities the user engages in on a website.

Information Transmitted

```
METHOD: GET +
URL
+ https://www.facebook.com/tr/?id=11168753150746568ev=PageView0dl
=https%3A%2F%2Fpeople.com%2Fmovies%2Fryan-reynolds-hilariously-tr
olls-wife-blake-lively-on-her-birthday%3Ffort=0IT=falseots=1629973
4831638sw=192065h=10806v=2.9.458I=stable&ec=0&o=30&fbp=fb.1.16299
73483160.479923654&it=16299734827918coo=false&rqm=GET
HEADERS
+ accept: image/avif,image/webp,image/apng,image/svg+xml,
image/*,*/*;q=0.8
+ accept-encoding: gzip, deflate, br
+ accept-language: en-US,en;q=0.9
+ connection: keep-alive
+ cookie: sb=ElInYUVyUi-3fBeXpBV2Sx9z;
datr=ElInYUWmOKDIs UdliVT6j94; dpr=1.25;
c_user=1000[REDACTED];
xs=38%3A00yMSe0nZROjTW%3A2%3A1629966886%3A-
1%3A-1;
fr=1NEDIAp1E56NaLh1A.AWXUks_Y1iHSWfmR3LxgY5Tm
ajM.BhJ1IS.xy.AAA.0.0.BhJ1Im.AWW1mkbs54M;
spin=r.1004311916_b.trunk_t.1629966891_s.1_v.
2_
+ host: www.facebook.com
+ referer: https://people.com/movies/ryan-reynolds-
hilariously-trolls-wife-blake-lively-on-her-
birthday/
```

Legal Theories

Meta Pixel Litigation

In re Meta Pixel Healthcare Litigation, (N.D. Cal.) and *Alistair Stewart v. Advocate Aurora Health Inc., et al.*, (N.D. Ill.).

- Putative class actions alleging millions of patients had their medical privacy violated through use of tracking technologies used to track their actions with regard to patient portals and patient scheduling applications.
- Plaintiffs contend the Meta Pixel shares with Meta certain confidential medical information associated with their activities on patient portals used by medical providers.
- Claims: (a) violations of CIPA; (b) violations of CMIA; (c) Wiretap Act; (d) invasion of privacy; (e) breach of express and implied contract; (f) negligence; and (f) unjust enrichment.
- Defenses: (a) consent; (b) information is deidentified; (c) no intent; (d) medical information is filtered and not shared; (e) lack of ascertainability of class; (d) lack of commonality and typicality making class certification improper.

Video Privacy Protection Act

- The Video Privacy Protection Act (“VPPA”) is a federal statute that has its origin in the 1987 confirmation hearings concerning Judge Robert Bork’s nomination to the United States Supreme Court.
- The VPPA prevents a “video tape service provider” from “knowingly” disclosing “personally identifiable information” about one of its consumers “to any person.”
- The VPPA provides for liquidated damages in the amount of \$2,500 per violation and reasonable attorneys’ fees. 18 U.S.C. §§ 2710(b) and 2710(c)(2).
- Being pursued on a class claims to challenge website providers who offer video content that utilizes pixel and cookie technology
 - Digital
 - Streaming companies
 - Social Media Companies
- States have similar laws precluding sharing of video watching activities of an identifiable individual

State Surveillance Law Claims

- Individuals are asserting claims under various state surveillance laws for the unlawful collection of information through use of tracking technologies.
- Theory - entities are using tracking technologies to intercept, wire or electronic communications, in violation of applicable state surveillance law.
- State laws typically provide for a private right of action to recover liquidated damages, attorneys' fees and costs and injunctive relief.
- Defenses include: actual or implied consent, statute of limitations, lack of commonality and typicality.

Confidentiality of Medical Information Act (CMIA)

- Among other things, the CMIA (1) prohibits covered health care providers from disclosing medical information regarding a patient, enrollee, or subscriber without first obtaining authorization, and (2) requires covered health care providers that create, maintain, store or destroy medical information to do so in a manner that preserves the confidentiality of such information.
- Defines “medical information” as any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient’s medical history, mental or physical condition, or treatment. “Individually identifiable” means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient’s name, address, electronic mail address, telephone number, or social security number, or other information that reveals the individual’s identity.
- **Damages**
 - For negligently released confidential information or records, either or both nominal damages of \$1,000 and the amount of actual damages, if any, sustained by the patient. **It shall not be necessary to prove that the plaintiff suffered or was threatened with actual damages to recovery nominal damages.**
 - For knowingly and willfully disclosing or using medical information shall be liable for an administrative fine not to exceed \$2,500 per violation.
- See *also* Minnesota Health Records Act

California Information Privacy Act (CIPA)

- Prohibits recording, monitoring, eavesdropping on a confidential communication.
- Anyone who “reads, or attempts to read, or to learn the contents” of a communication “without the consent of all parties to the communication” is in violation of CIPA.
- Four elements:
 - Intentional act
 - Neither party consented to the act
 - The communication was confidential
 - An electronic device was used during the act
- CIPA provides for a \$5,000 per violation statutory penalty, with no requirement to prove actual damages.



CALIFORNIA REPUBLIC

Tracking Technologies and Health Care (HIPAA)

Key takeaways from the OCR's December 2022 bulletin:

Online tracking technologies may collect protected health information (“PHI”)

Collection or analysis of the data may involve unauthorized disclosures of PHI to third-party vendors

Health information collected on a regulated entity's website/app “generally is PHI”

If using tracking technologies:

- User-authenticated webpages (i.e., login) - must configure to comply with HIPAA
- Unauthenticated webpages (e.g., public homepage) – may need to comply (e.g., collect email/IP)
- Mobile apps – must comply if offered by a regulated entity

Tracking Technologies and Health Care (FTC & State Laws)

Key takeaways from the FTC's BetterHelp and GoodRx enforcements:

Shared personal health information with third party advertisers and advertising platforms

Failure to disclose sharing of personal health information (or indicated that sharing did not occur)

Unauthorized disclosures to third party advertisers under FTC's Health Breach Notification Rule

Key takeaways from Washington's My Health My Data Act:

Consumer personal health data is broadly defined (personal information relating to the past, present, or future physical or mental health of a consumer)

Similar language regarding a "sale" as the CCPA (i.e., monetary or other valuable consideration)

A "sale" of consumer personal health data requires an (onerous) authorization

Private right of action and fertile ground for class actions

How to Reduce Risks

Reducing Risks

- **Privacy Policy – (Surveillance)**
 - Express Consent
 - Implied Consent
- **Express Consent – VPPA**
- **Control and knowing what is on websites**
 - Pop-up banner
 - Inventories
- **Testing of what is collected**
- **Vendor Management**
- **Agreements & terms of use**
 - Indemnity
 - Choice of law
 - Arbitration vs. court
 - Class action waiver
 - Limitation of liability



Tracking Technologies and Health Care (5 Steps)

Five Steps to Address Potential Tracking Technology Issues

1. Prepare an inventory of cookies and tracking technologies
2. Determine internal uses (e.g., speak with marketing, IT, others)
3. Establish the scope of third-party disclosures
4. Amend existing agreements/templates
5. Add a checkpoint in your vendor contracting and PIA processes



Questions?