Tracking Technologies & AI: 2023 Privacy Litigation Trends

Confidential/Do Not Distribute

Myriah Jaworski
619.819.2447
mjaworski@clarkhill.com

Chirag Patel
312.360.2127
cpatel@clarkhill.com
Clark Hill. Simply Smarter.

At Clark Hill, our value proposition is simple. We offer our clients an exceptional team, dedicated to the delivery of outstanding service. We recruit and develop talented individuals and empower them to contribute to our rich diversity of legal and industry experience. With locations spanning across the United States, Ireland, and Mexico, we work in agile, collaborative teams, partnering with our clients to help them reach and exceed their business goals.

Our DNA

Clark Hill is built upon a core set of values that guide us in our relationships with our clients, our interactions with each other, and our connection to the communities in which we serve. These values have a real and lasting impact on the way we conduct our business, the way we treat our clients and colleagues, and the way we go about growing our firm. We believe these values come into play in each and every client experience, and are essential to the ultimate success of our lawyers and our firm.

Recent Growth

With a focus on the needs of our clients, Clark Hill has undergone significant, deliberate growth over the last decade. Major recent events include:

- **2023**—The firm was joined by the teams at Conrad O’Brien and Larsson & Scheuritzel, PC, powerhouse east coast firms.
- **2022**—The firm combined with Ryley Carlock & Applewhite, a highly regarded law firm serving the business community in Arizona and the Southwest.
- **2021**—Clark Hill added a Denver office and expanded its Cannabis Industry Group by combining with the Hoban Law Group, a leading cannabis law firm.
- **2019**—The firm announced a combination with Irish firm O’Gradys, expanding the firm’s Dublin office.
- **2018**—The firm combined with Texas-based Strasburger & Price, bringing nearly 200 attorneys to the firm’s ranks in Texas, New York, Washington, DC, and Mexico City.
- **2017**—Clark Hill expanded our footprint to the west coast by joining forces with Morris Polich & Purdy LLP (MPP), a firm with nearly 100 lawyers in California and Nevada.
Pixels, Widgets, Cookies: Oh My

• Growing attention to the capacity of technology to compromise privacy by tracking of activity across sites, apps, platforms etc. harnessed in the interest of targeted advertising/selling.

• Pixel, widgets, cookies: technologies that transmit data to social media platforms and advertisers that are embedded in or “dropped” onto browsers.

• Consumers voluntarily enter information, including personal health information, but are unaware (as may be the businesses/health care entities) that information is being tracked in this manner.

• What happened? 100+ lawsuits filed since 2022
  ▪ June 2022: Pixel Hunt
  ▪ Importance of Dobbs
Pixels, Widgets, Cookies: Other Industries Hit

- Industries
  - Healthcare
  - News Outlets
  - Streaming Services
  - Sports Organizations
  - Financial institutions

- Follow up MarkUp Articles – Tax filing, telehealth etc.

- Insurers and underwriters are aware – and asking questions.

- University Health Care Systems (including Duke University’s Heath System and University of Iowa Hospitals) have been sued for allegedly sharing patient data with Meta
  
  ➢ Earlier this year, a class action lawsuit was filed in California against the UCSF Medical Center, Doe v. Regents of the University of California, alleging a violation of the California Invasion of Privacy Act among other claims for its use of the Meta Pixel on its website and patient portal.
  
  ➢ There has been no ruling on the defendant’s motion to dismiss yet.
The Meta Pixel

- From Plaintiffs’ affidavit in *In re Meta Pixel Healthcare Litigation* (ND Ca. 2022):
  - 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
  - In a nutshell, 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. Id.
  - Plaintiffs allege over 660 healthcare entities use Meta Pixel. They know this from website scans, and Meta user tools (Off Facebook Activity) and access rights
- Primarily used for event tracking and ad measurement, to serve customized/targeted advertising to a particular FID.
What is Being Transmitted via Pixels and Cookies?

• In healthcare context, allegations were that Pixel was dropped upon Log-in to Patient Portal and for “events” in portal:
  ▪ Browsing information about doctors, medical conditions, appointments collected
  ▪ In turn, plaintiffs received health-related advertisements for prescriptions and treatments etc.

• Outside of healthcare, other industries targeted: media companies and retail organizations.
  ▪ Unique IDs, Advertising IDs, Device IDs, IP addresses, GPS coordinates – oftentimes, not names or data elements we traditionally think of as PII
  ▪ Video viewing, title of video, association of video with User ID

• This information may be associated with or linked to a subscriber (media), patient (healthcare), donor (university, NGO) student (if logged into university account) or Facebook/Social Media user (e.g. existing profile), but not always

• Why is this important?
  ▪ Some success with defensive strategy of drilling down on whether information constitutes PII
Meta Pixel: What Claims are Being Brought?

- **Meta Pixel**
  - Primarily in health care context: breach of contract, intrusion upon seclusion, constitutional right to privacy (CA), CIPA, Unfair Competition
  - VPPA if pixel is used for transmission of video viewing information

- **Video Privacy Protection Act (VPPA):** Generally, for websites deploying videos
  - Video tape service provider: engaged in business of delivery of pre-recorded video materials
  - Recorded videos, not live action (NFL motion to dismiss)
  - Elements:
    - **Knowingly:** allowing or installing the pixel on your website generally is enough, agreement to Meta policies
    - **Discloses:** Installing and maintaining the pixel on the website
    - **Personally identifiable information:**
      - Circuit split on PII: Some circuits (1st) say it is enough if PII can be linked to an anonymous individual, not a particular person
      - The unique identifiers “represent a specific person” and can be enough to state a claim
Pixel Tracking: Old Laws leveraged in New Ways

- Meta Pixel: Creativity of the Plaintiffs’ Bar Continues – could FERPA be next?
  - Recent Cabela’s/Bass Pro filing re: Meta Pixel
    - Irvin v. Cabela’s alleges that the company’s use of the pixel on their websites constitutes illegal wiretapping under the Pennsylvania Wiretapping and Surveillance Control Act ("WESCA");
    - Also alleges it violates the Pennsylvania Uniform Firearms Act ("UFA").
      - Plaintiff purchased firearms through the companies’ websites, both of which incorporate the Meta Pixel
      - Plaintiff alleges that because of the presence of the Meta Pixel on the websites, when he made those purchases (or took other actions on the website) certain event data was transmitted to Meta
      - UFA: has a confidentiality provision requiring gun purchase information to be confidential and not subject to public disclosure
    - What Plaintiffs firms look for: statutory damages and PROA, but PROA not necessary
Rise in “Spyware” Technology & Wiretapping claims

- **Session replay:** technology that records and allows businesses to play-back website browsing sessions, including interactions with the site in recorded or real-time
  - Mouse movements
  - Clicks, taps
  - Scrolling across multiple webpages

- **Chatbots:** Generally, use of AI to respond to consumer inquiries and engage with consumers in written form; most common use case is customer service related

- **Allegations:**
  - The use of “session replay” tools intercepts data communications such as mouse clicks and keystrokes without users’ prior consent
  - Chatbot communications recorded from an online chat feature and stored with a third-party are alleged to be “wiretapping” in the absence of prior consent
Wiretapping Claims

- Tracking technologies:
  - In addition to VPPA and state equivalents, federal and state Wire Tapping Statutes are leveraged
    - Party consent requirements, interception of communications
    - In chatbot context, is vendor intercepting?
    - Type of consent required, implied consent defenses
  - Numerous state laws at play:
    - California Invasion of Privacy Act (CIPA), and state and federal law equivalents
    - Any state or federal law that protects certain information from disclosure
      - E.g. CMIA, PA Firearms etc.
      - FERPA?
Up Next: Leveraging UCL claims for Cookies Compliance

- State Unfair Competition Laws/Acts regulate false and deceptive practices
  - **Auditing cookie management**
    - If I reject all cookies, are they actually rejected?
      - Many third party programs exist to scan websites
    - Does website honor Global Privacy Controls?
    - False promises in PP/TOUs
  - **If not:**
    - State UCL, invasion of privacy
    - Wrongful collection etc. claims.
Mitigate Risks: Questions to Ask Your Marketing Dep’t.

- Do you know what is on our website?
- Do you know what data adtech is collecting?
- Why are we sharing visitor, student etc. data?
- Is cookie consent sufficient?
  - Does our data sharing practices match the website TOU and PP
  - Is there easy way to disable tracking? Global Privacy Controls?
- What do 3rd party provider’s terms say about how the information will be used? EdTech?
- Are sites compliant with state privacy laws? Federal? Do we need a BAA?
- Are Marketing, Legal and IT collaborating?
Artificial Intelligence: Lawsuits Are Here

Artificial Intelligence grading your ‘neuroticism’? Welcome to colleges' new frontier

D.C. attorney general introduces bill to ban ‘algorithmic discrimination’

FTC Issues New Guidance, Warning That Bias in Artificial Intelligence Could Create Potential Liability for Enforcement Actions

Ethicist warns universities against using AI in admissions

Algorithms may simply lead to ‘self-fulfilling prophecies’ and do not give reasons for their decisions, Oxford researcher warns
Artificial Intelligence: The New Frontier – Tech E&O, Media, EPL

- Existing federal and state laws prohibit discrimination based on protected class status.
- New lawsuits allege algorithmic bias, disparate impact and discrimination in violation of these laws.
    - Class action alleging insurer used AI/ML technology to automate its claims handling processes for homeowner insurance claims.
    - AI/automated tool allegedly more highly scrutinizes claims of black home owners than white, and denies their insurance claims at greater levels.
    - Violation of federal Fair Housing Act.

Regulators are also paying attention:

- EEOC enforcement action against iTutor Group software platform for its automated rejection of candidates with birthdate above certain year, in violation of age discrimination act.
- EEOC 2023 Strategic Enforcement Plan, FTC AI-Bias guidance
- State insurance: Colorado Algorithmic & Predictive Model regulations
Artificial Intelligence: Emerging Cyber & Privacy Concerns

Wrongful Collection of Data Claims:

- Large Language Model (LLM) AI (e.g., ChatGPT) relies on website scrapping and other mass data collection efforts which may violate TOUs and data consent requirements
- Same employment practices liability (EPL) lawsuits could include wrongful collection/privacy claim if use of PII for purpose is not clearly disclosed
- May violate copyright or other intellectual property laws by relying on protected information

- Confidentiality / Trade Secret Claims: Breach of confidentiality/disclosure of trade secrets by inputting protected data
  - March 2023: OpenAI acknowledges “glitch” that allowed users to access other user chats, but also confidential PII such as names, email addresses, credit card info etc.
  - Recent Samsung incident – employees using ChatGPT lead to disclosure of confidential company data re: product launches, marketing plans, internal strategies
  - Businesses voluntarily uploading IP, proprietary, customer lists or PII

- Other Intellectual Property Issues: Documents or code created with AI assistance may not be protected
Artificial Intelligence: Mitigating Risk

- **Create A Policy Around Acceptable Internal Use:** What is the Use Case? Conduct a risk analysis as to the various ways AI tools could be employed within the organization and form an acceptable use policy based on the organization’s risk tolerance.

- **Track Internal Use:** Require employees to disclose the use of AI tools in any work product, and then maintain an inventory of any work product that utilized AI generated content for easy identification.

- **Disclosure, Consent, and Contract Compliance:** Determine where is it necessary to disclose the employment of AI tools with consumers and contract parties to avoid claims of authorized disclosure or breach of contract; obtain appropriate consents.

- **Audits, Training, and Monitoring:**
  - Continue to monitor the internal use of AI tools for with conformity with acceptable use policy, and other unanticipated and unknown risks - the organizations’ risk profile may change through new and unanticipated uses of AI, or changes in law.
  - Conduct regular training to keep employees informed of the acceptable uses of AI tools, and the risks to the organization of unauthorized uses.
Title IV Alert: Gramm-Leach-Bliley Act ("GLBA") Safeguards Rule


• Requires Title IV schools that administer student financial aid to develop, implement, and maintain a comprehensive, written information security program containing administrative, technical, and physical safeguards. The new rule sets forth nine specific elements that must be included within all Title IV schools’ information security program. These new requirements include, among other things:
  ▪ Risk Assessments;
  ▪ Designing, implementing, and testing safeguards;
  ▪ Preparing a written information security program ("WISP"); and
  ▪ Designating a Qualified Individual for oversight.

• Enforcement:
  ▪ The Department will be responsible for enforcing the amendments to the Safeguards Rule for postsecondary institutions that participate in federal student aid programs. Any finding of noncompliance will be resolved by the FSA as part of its final determination of an institution’s administrative capability.
  ▪ If the FSA’s cybersecurity team determines the institution poses a substantial security threat, it may temporarily or permanently disable the institution’s access to FSA application systems.
Questions? Thank You!

Legal Disclaimer
This document is not intended to give legal advice. It is comprised of general information. Employers facing specific issues should seek the assistance of an attorney.