JS|HELD

PERSPECTIVES

Litigation Surge From the Use of Tracking Technology & the Sharing of Healthcare and Personal Data

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

Introduction: Tracking Software in the Healthcare Industry

Privacy-related concerns have become increasingly prominent in recent years, especially with the widespread use of third-party tracking tools such as tracking pixels, cookies, and mobile attribution tied to website-related mobile device applications. These advertising technology (AdTech) tools enable website owners to track user behavior and collect personal data, such as IP addresses, browser type, and device identifiers, in part to help companies ascertain user engagement on their websites and related targeting opportunities. AdTech allows advertisers to reach website audiences and determine the efficiency of their digital advertising efforts. These trackers also raise the potential risk of personal information transfers to third parties if not properly managed, or without due consideration of regulatory compliance.

This is particularly relevant in the healthcare industry, where patient data is highly sensitive and must be protected. The use of third-party tracking tools like Meta Pixel, cookies, and mobile attribution tied to mobile applications have been raising healthcare data privacy-related concerns among customers and users. These tools can collect personal identifiable information (PII) and other sensitive data, such as healthcare-related information that falls under the Health Insurance Portability and Accountability Act (HIPAA) and protected health information (PHI).

Increasingly prevalent usage of this technology has led to an increase in class action lawsuits against companies that fail to adequately protect user data or obtain proper consent for data collection. In many instances, this involved privacy claims based on the use of third-party tools by healthcare providers such as hospitals. Some of these cases base their allegations on violation of federal[1] and state wiretapping laws.

This article focuses on the growing use of these tracking technologies such as pixels, cookies, and more, to collect information about users and the risk to consumer privacy, especially in the healthcare industry. More significantly, it also examines the resulting reputational and financial threats to companies who unintentionally share this personal data with third parties, and what management can do to protect their organizations when utilizing these technologies.

Consider one telehealth startup focused on mental health that inadvertently shared patient data. The company said it had determined "that it had disclosed certain information that may be regulated as protected health information ("PHI") under HIPAA to certain Third-Party Platforms and some Subcontractors without having obtained HIPAA-required assurances."

Several other telehealth companies have come under scrutiny for the sharing of patient information without appropriate consent. Class action lawsuits have been filed by private plaintiffs alleging that platforms used to collect the data, such as Meta, shared consumers' medical information with its parent company Meta Platforms Inc., via its pixel tracking tool.

In one putative class action filed in federal court in Illinois,[2] a female plaintiff alleged that a Chicago-based hospital deceptively embedded third-party source code on its website and its MyChart patient portal without her consent. She also contended that this source code, which cannot be seen to those who use the website and portal, caused transmissions of her personally identifiable patient data to Facebook, Google, and others for advertising purposes.

In fact, the Federal Trade Commission recently took enforcement actions against two digital health platforms for allegedly sharing user health data with third parties for advertising. Both instances involved the use of third-party tracking pixels, which enable these platforms to collect and analyze information about user or patient activity. The companies agreed to an FTC ban on the sharing of health information for any advertising purpose and in one of the cases, a ban on the disclosure of other personal information for re-targeting.

Additionally, the U.S. Department of Health and Human Services (HHS) issued a bulletin[3] late last year that clarifies that entities regulated under HIPAA are not permitted to use tracking technologies in ways that would result in impermissible disclosure of protected health information (PHI) to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant consent. HHS noted

[1] https://www.govinfo.gov/content/pkg/USCODE-2021-title18/pdf/USCODE-2021-title18-partI-chap119-sec2511.pdf
[2] https://scholar.google.com/scholar_case?case=12360149155594673136
[3] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html

that such disclosures "may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI."

Customer and Website Owner Mitigation

Opt-outs are one way users can protect their privacy and data security. By opting out of tracking (either when visiting a website from a computer or mobile device), users can minimize the potential of their data from being collected and used for targeted advertising or other purposes.

However, opt-in and opt-out options can sometimes be unclear, particularly for mobile apps. Certain mobile applications may be monitoring or tracking information surreptitiously or are not as transparent in providing users with opt-in and opt-out options as part of their mobile attribution mechanisms. This can occur during installation of apps or anytime later.

In terms of mobile attribution, software development kits (SDKs) are used to track user behavior in mobile apps. These SDKs can collect a range of data, including device type, app usage, and location. Users can opt-out of data collection by disabling tracking in their device settings or by uninstalling the app to help lessen the potential of sensitive data transfers. However, some companies have been criticized for making it difficult for users to opt-out or failing to inform them about data collection practices.

Along similar lines, there are a number of configuration options that website marketing administrators within an organization can proactively implement to mitigate privacy-related risks. To better prevent these risks that can result in class actions, administrators should consider the help of external privacy and tech consultants, who can employ advanced approaches. These include disabling "Automatic Advanced Matching" within the Meta Pixel dashboard or ensuring that anonymization of IP addresses is turned on (when utilizing Google Tag Manager), among other options.

The right outside consultants can help improve company websites in various ways to protect customer privacy and related risks associated with the use of AdTech. They can help identify the best configuration options for companies and develop effective risk management strategies that meet government-mandated privacy compliance standards.

Expert Support

When litigation does ensue and law firms are retained, outside consulting experts can be leveraged to assist, particularly with respect to the defensible identification, collection, analysis, and expert reporting of AdTech-related content (both front-facing to users / customers and also 'back-end' code, related artifacts, logs, and databases). This may include forensic preservation and capture of data sources such as:

- Website page URLs, including underlying HTML and JavaScript code; Configuration settings stored in third-party tracking dashboards,
- Capture of cookie & pixel firings during mock scenario click-throughs (clicking hyperlinks, filling out open fields such as "Request An Appointment," etc.) in defensible, containerized formats that can be later analyzed or provided to other parties (such as opposing counsel),
- Mobile device tracking artifacts and assessment of opt-in / opt-out settings in mobile apps and related browsing sessions,
- Capture of pixel codebase and any changes to codebase, where applicable,
- Capture of related logs such as Internet Information Services (IIS) server logs which may contain identifying user information such as user IPs, browser, and devices utilized, etc.,
- Capture and analysis of SDKs for mobile apps to view opt-in / opt-out settings, and related mechanisms of action,
- Other data sources specific to a given organization.

Once collected, data is typically analyzed and discussed with legal counsel and key stakeholders as part of strategy and related discussions. Findings can be furnished in writing as well, along with expert reporting and testimony, when requested / applicable.

Consulting experts can also offer early stage advice in support of litigation strategy and privacy-related concerns as part of discovery and any potential expert reporting and testimony. Additionally, near or after the conclusion of the litigation, or as part of the remediation steps, experts can work with key stakeholders at the organization and counsel to ensure appropriate privacy-related compliance measures are implemented. These include, but are not limited to, setting up cookie banner settings, configuration or exclusion settings in tracking tool dashboards, or other related remediations. These actions will vary according to an organization's website content and implementation of tracking technology and corresponding compliance programs.

CONCLUSION

Companies must be mindful of privacy concerns when using technology such as third-party tracking tools or leveraging mobile attribution tied to website-related applications. Users and website visitors also need to be aware of the risks associated with these tools. Compliance with HIPAA and other privacy laws is critical to protect sensitive personal information, and obtaining proper consent for data collection is essential.

Once a lawsuit alleging improper disclosure of personal information is filed, retaining outside consultants who can assist in privacy-related class actions by providing defensible and sound advice is required. Expert services related to privacy considerations and overall end-to-end discovery efforts are imperative in such circumstances.

To avoid litigation, regulatory scrutiny, and fines, as well as mitigate overall risk, companies need to take the initiative when it comes to tracking technology on their websites by putting the right compliance programs and safeguards in place.

Acknowledgments

We would like to thank Antonio Rega and Joseph Hoang for providing insight and expertise that greatly assisted this research.

More About J.S. Held's Contributor

Antonio Rega is a Managing Director in J.S. Held's Digital Investigations & Discovery group within the Global Investigations Practice. He has more than 20 years of experience providing consulting, advisory, and subject matter expertise in the areas of digital forensics, data privacy & information governance, digital assets / blockchain technology, and discovery on behalf of global corporations and law firms. Based in New York, Antonio focuses on leading complex investigations and matters involving proactive and reactive discovery and analysis, often conducting in-depth forensic examinations of electronically stored information (ESI) across repositories (cloud-based, localized, or mobile). He regularly assists clients with advice and strategy through all phases of investigations, regulatory compliance, or litigation needs, such as privacy-related regulatory requests, responses to government subpoenas, and related information governance needs, among other areas of specialization.

Prior to joining J.S. Held, Antonio led large-scale investigations and compliance matters involving digital forensics, data privacy, and eDiscovery at several leading consultancies. He has served as a guest lecturer at Fordham University School of Law on the topic of data privacy and related technology. He also contributes material and discussion as a content editor for the American Bar Association (ABA), as well as participating as a member of the Sedona Conference Trade Secrets Working Group 12.

Antonio is a Certified Fraud Examiner (CFE); EnCase Certified Examiner (EnCE); Computer Certified Examiner (CCE); Cryptocurrency Tracing Certified Examiner (CTCE), CipherTrace; Blockchain Council's Certified Cryptocurrency Auditor (CCA); TRM Labs Certified Investigator (TRM-CI); Licensed Private Investigator (PI) for the State of Texas, and Certified Information Privacy Manager (CIPM)-Pending.

Antonio can be reached at antonio.rega@jsheld.com or + 1 551 345 8502.