Cybersecurity Law Report cslawreport.com

Jan. 17, 2024

Online Advertising

Tracking Technologies: Privacy Regulation, Enforcement and Risk

By Leslie Shanklin, Ryan Blaney and Danielle Brooks, *Proskauer*

Over the past three decades, an expanding set of technologies – cookies, pixels, software development kits and various other types of software – have enabled a vast array of useful and even critical features and functionalities for users online as well as a staggering degree of hyper-personalization of user experiences, content and advertising. The risks, costs and benefits of these tracking technologies have arguably engendered more debate than any other privacy concern and have presented legal, technical and commercial issues of significant complexity.

This first article of a three-part series examines the legal landscape around digital tracking, tracing the journey from the 1990s to the present and looking ahead to where the road may next lead. Part two will take a deep dive into the technology of online tracking and targeting, including a look at how those technologies are evolving to address privacy concerns and compliance requirements. The final installment will review tracking technology governance and offer practical compliance strategies to address the fast-changing rules and ever-increasing risks they present.

See "IAB Unveils Multistate Contract to Satisfy 2023 Laws' Curbs on Targeted Ads" (Feb. 22, 2023).

A Brief History of Digital Tracking Regulation

U.S. Initially Favors a Self-Regulatory Approach

In the early days of website proliferation, Congress acted with relative swiftness in passing the Children's Online Privacy Protection Act (COPPA) in 1998. As concerns started to mount over how cookies were being used to facilitate behavioral tracking and targeting online, the advertising industry stepped in with self-regulation.

In 2000, the Network Advertising Initiative (NAI) published its first Code of Conduct, setting out the core principles of notice and choice that would govern U.S. self-regulation of tracking for ad targeting purposes over the next 20 years. The FTC endorsed the Code and, in 2009, published self-regulatory principles incorporating the Code's fundamental concepts of transparency and choice, a

move that spurred several industry associations to form the Digital Advertising Alliance (DAA) and work together to publish an updated and more comprehensive set of self-regulatory guidelines. The NAI and DAA Codes, along with the consumer behavioral advertising opt-out tools that these organizations developed and administered to address the "choice" principle, continued to evolve along with mobile and tracking tech. While the FTC pursued enforcement actions under its general Section 5 authority to prevent unfair and deceptive trade practices, with the exception of COPPA, self-regulation around tracking and targeting continued to carry the day.

Indicative of the growing risks for businesses around online tracking, the first wave of Video Privacy Protection Act (VPPA) cases filed in the mid-2010s against online streaming services served as a warning of future tracker litigation. In these cases, plaintiffs alleged that incorporating third-party cookies into digital services resulted in an unlawful sharing of consumer PII tied to video viewing information.

See "Federal Courts Offer a Modern Interpretation of the VHS-Era Video Privacy Protection Act" (Oct. 28, 2015).

Europe Takes a Different Stance

In contrast to the U.S.'s self-regulatory path, Europe chose direct regulation in 2009 and amended the ePrivacy Directive to require prior consent for cookies and similar technologies that are not strictly necessary for the core functioning of a website. This so-called "Cookie Directive" led to the proliferation of cookie banners across European websites.

Nine years later, the E.U. GDPR called into question the sufficiency of the "implied-consent" approach to European cookie banners. The GDPR imposed strict requirements for obtaining consent as a legal basis for processing personal data. E.U. legislators did not concurrently update the ePrivacy Directive, and confusion around cookie banner rules remained until guidelines were issued by the U.K. and France data protection regulators and the pivotal Planet 49 decision was issued by the E.U.'s highest court in 2019 – together they made clear that passive consent was not sufficient and that users must take an affirmative, unambiguous action to indicate consent.

Website and app publishers worked to swap out simple cookie banners with consent management platforms (CMPs) in order to meet the increasingly onerous requirements around tracking consents, with many publishers incorporating IAB Europe's evolving Transparency & Consent Framework into their CMPs to address the unique complexities of programmatic advertising. While publishers and adtech companies grappled with the technical challenges of compliance, the French data protection regulator underlined the seriousness with which it was approaching cookie compliance by issuing combined €135 million fines against Google and Amazon in December 2020 for cookie compliance violations.

See "After Death of the Cookie, New Advertising Strategies Raise Compliance Questions" (Sep. 2, 2020).

CCPA Marks a Watershed Moment in the U.S. for Tracker Regulation

On January 1, 2020, the CCPA ushered in a new era of more comprehensive privacy regulation in the United States. The CCPA took a less strict and more indirect stance on trackers than the European model, requiring users' ability to opt out of "sales" of personal information. This new mandate led to debate as to whether and how that opt-out requirement applied to third-party tracking technologies incorporated into websites and apps for analytics, advertising or other purposes.

Tech giants responded to the CCPA's clarion call in various ways, including Apple's 2020 debut of a collection of new privacy features in iOS and Google's announcement that same year that it would be phasing out third-party cookies in Chrome. Apple's new iOS privacy features included App Tracking Transparency, requiring apps to get prior consent from users for cross-app tracking (linking data collected from one app with data collected from other companies' apps or properties) and preventing publishers from accessing the ad ID for non-consenting users. By going even further than CCPA's opt-out directive and imposing an opt-in requirement for cross-app tracking, Apple's move had immediate impact on ad revenue and well-established models for ad serving and measurement on mobile devices and, together with Google's announcement, further underscored the need for new advertising models that approached consumer data in more privacy-protective ways.

In August 2022, the California AG settled the lingering debate over the CCPA's "sales" definition with its final judgment and $1.2 million fine against the French cosmetic brand Sephora in its first CCPA enforcement action. In its decision, the AG found that the third-party trackers Sephora had incorporated on its website for analytics, ad serving and retargeting purposes constituted a "sale" of personal information and that Sephora's failure to present a "Do Not Sell" link on its site or allow consumers to opt out of the data exchanges facilitated by these trackers therefore constituted a violation of CCPA.

The Sephora decision came as a surprise to many publishers, particularly the AG's inclusion of analytics trackers within the definition of data "sales" and the finding that failing to honor the browser-based Global Privacy Control (GPC) opt-out was a CCPA violation. Publishers quickly got busy ensuring their agreements with tech providers included all the provisions necessary to fit those trackers under the "service provider" exception to data "sales" and, if they had not already done so, incorporating a cookie banner and/or CMP into sites and apps for tracking that that did not meet the "service provider" exception.

See "Lessons From California's First CCPA Enforcement Action" (Sep. 28, 2022).

An Increasingly Complex Regulatory Maze

U.S. Regulation

In a resounding rejection of industry's former hopes of forestalling regulation of trackers and targeted advertising through self-regulation, the U.S. now presents a dizzying and increasingly

complex labyrinth of regulation governing the collection of personal data online. The California Privacy Rights Act (CPRA) amendments to CCPA, which went into effect in 2023, codified and expanded the Sephora enforcement findings around trackers through various means, including: (a) new definitions of data "sharing" and "cross-context behavioral advertising"; (b) heightened contract hurdles to meet the "service provider" exception to selling or sharing; (c) a statutory mandate to honor browser-based opt outs; and (d) provisions making a business responsible for how third parties use, share or sell personal information.

Alongside the upgraded California law, there are now comprehensive privacy laws in effect in four other states (Virginia, Colorado, Connecticut and Utah), a narrow Nevada law providing opt-out rights for online data collection and eight more state comprehensive laws coming online in the next two years (Iowa, Tennessee, Indiana, Montana, Delaware, Oregon and, assuming the governor's signature, New Jersey). As state legislatures around the country debate their own flavor of privacy legislation, we almost certainly will see other state laws get added to the mix as well. While these laws and pending bills have a large degree of overlap with respect to consumer rights around online tracking, there are some differences in scope, definitions and requirements that must be understood.

At a high level, what state laws generally now require with respect tracking technologies (with the exceptions noted below), is an easily-accessible mechanism provided by the website or app allowing a user to opt out of data collection or sharing via trackers that: (a) constitutes a "sale," or (b) enables targeted advertising (called "cross-context behavioral advertising" under CCPA). To underscore a critical point, publishers are on the front lines and directly responsible for all trackers embedded on their services, both their own first-party trackers and those of a third party. Publishers are also required to notify downstream partners of opt-out requests and require those partners to further flow requests downstream, a process that is facilitated by CMP tools and industry frameworks such as the IAB's CCPA Compliance Framework and Multi-State Privacy Agreement but is often quite legally and technically complex.

While the U.S. still generally remains an opt-out jurisdiction with respect to data collection through digital trackers, there are three areas of exception that are creating increased regulatory risk and complexity for digital publishers:

1. Sensitive Personal Information

Bucking the general U.S. opt-out approach, many states with comprehensive privacy laws require an express opt in for the collection and processing of "sensitive personal information." Given that the definitions of sensitive information continue to expand, this opt-in requirement presents new hurdles for businesses that must consider whether a consumer's use of their website or app might reveal personal attributes about the user such as their race or ethnic origin, sex life or sexual orientation, or religious beliefs. If so, the business will need to conduct a data protection impact assessment and ensure all cookies, pixels, etc. are technically prevented from collecting data unless and until the user has opted in.

See the Cybersecurity Law Report's two-part series analyzing 2023's new state privacy laws: "The First Six Plus Compliance Measures" (Jun. 28, 2023), and "Oregon and Delaware Join the Strictest Tier" (Jul. 12, 2023).

2. Health Information

Many of the new comprehensive state privacy laws include consumer health information in their definition of sensitive personal information. This has created additional complexity and confusion for entities that may also be regulated by the federal health care privacy law, the Health Insurance Portability and Accountability Act (HIPAA). That complexity is even greater for non-profit health care providers and businesses that may be exempted from complying with most, but not all, comprehensive state privacy laws, as some state privacy laws, including Colorado, Oregon and Delaware, do not exempt non-profits.

The comprehensive state privacy laws are also confusing with respect to health information given that many of states have defined "health data" to include information that is significantly broader in scope than what is covered in HIPAA's definition of protected health information. This expanding concept of "health data" may, therefore, trigger opt-in consent requirements for digital tracking on a wide swath of non-HIPAA regulated sites and apps used to monitor and manage things such as diet, fitness, pregnancy, mental health and sleep quality.

The concerns around consumer health and wellness data being tracked and shared with third parties has engendered amendments to both the Connecticut and Nevada privacy laws as well as Washington's My Health My Data Act, a tailored Washington state law that broadly goes into effect in March 2024. In addition to requiring prior express consent for the collection and sharing of "consumer health data" (broadly defined), the Washington law also requires a signed and dated authorization by the consumer for the sale of such information.

At the federal level, the U.S. Department of Health and Human Services Office for Civil Rights (OCR) published a bulletin in 2023 on the use of online tracking technologies by HIPAA-covered entities and HIPAA business associates. In the bulletin, OCR restricted hospitals' use of certain third-party web technologies that capture IP addresses on web pages related to health conditions or health care providers. The American Hospital Association has filed a lawsuit against the U.S. Department of Health and Human Services alleging that OCR's bulletin on online tracking technologies exceeds its statutory authority under HIPAA.

3. Children's Data

While tracking of kids under 13 online has long been regulated in the U.S. under COPPA, growing cries for further regulation to better protect younger and older kids online has led to legislative activity at both the federal and state level, including proposed updates to COPPA (COPPA 2.0), the proposed bipartisan Kids Online Safety Act and California's Age-Appropriate Design Code Act, which has been signed into law but is currently subject to a district court injunction. Key features

of this legislation include: raising the age of protection to cover children and teens under 18 and shifting away from COPPA's actual knowledge standard to a constructive knowledge standard by applying the provisions to any online service that is "likely to be accessed" by children. In combination, these two critical pivots to how online children's data has been regulated in the U.S. will, if implemented, create even further complexity around tracker compliance. Given that teens, in particular, are known to make use of a vast array of online sites and services for information, entertainment and communication, risk decisions and compliance approaches to tracking technologies are likely to prove challenging for many online brands.

See "Xbox and Alexa COPPA Case Lessons: Negotiating With the FTC Over Algorithms and Remedies" (Jun. 14, 2023).

International Regulation

Legislatures in many countries were inspired by the GDPR and, to some extent, CCPA, to either upgrade existing legislation or craft entirely new laws to govern consumer privacy, activity that continues in earnest around the world. As these laws take varying approaches to online data collection, market practice regarding use of cookie banners and tracking consent tools outside of the U.S. and Europe is evolving.

Multinational businesses with sites and apps available worldwide are grappling with the pros and cons of taking a consistent worldwide approach to tracker compliance versus crafting solutions for individual countries or regions, decisions that will need to be flexible as global laws continue to evolve.

See "How Do You Put a System of Controls in Place When Your Target Keeps Moving?" (Mar. 31, 2021).

Growing Risk of Litigation and Enforcement Around Trackers

United States

At the federal level, the FTC has long had online tracking firmly in its sights, pursuing enforcement actions against social media platforms and tech giants based on alleged unfair and deceptive trade practices and violations of COPPA relating to tracking and targeting. More recently, the FTC has placed a strong focus on consumer health data tracking with a string of enforcement actions against consumer-focused mental health, prescription and fertility tracking app providers, among other health-related apps, for the use of tracking pixels. The FTC's Office of Technology also issued guidance putting companies on notice that they must monitor the flow of health information to third parties that use tracking technologies integrated into websites and apps, as the unauthorized disclosure of such information may violate the FTC Act and could constitute a breach of security under the FTC's Health Breach Notification Rule.

At the state level, California's enforcement has slowed with its new privacy regulatory agency being put into place and an injunction issued against immediate enforcement of CPRA regulations, but an enforcement focus on compliance with "sale" and "share" opt-outs is likely in 2024 by California and other states as well.

While the risk of a regulatory enforcement action for privacy noncompliance is escalating in the U.S., the more immediate and significant legal risk around tracking technologies has long been, and remains, class action litigation. The plaintiffs' bar has been increasingly creative in dusting off old laws that carry statutory damages to bring class actions based on the use of tracking technologies. The past two years have seen a resurgence in VPPA litigation based on the use of retargeting pixels, with plaintiffs targeting not just video streaming services, but a wide array of businesses that happen to have video content present on websites that use social retargeting pixels. This latest VPPA class action wave appears to be slowing as dismissals of the cases are mounting and, with courts rejecting application of the law to defendants whose businesses do not have video content as a core component, the list of potential defendants is dwindling.

Not slowing are class actions brought under state wiretap statutes such as the California Invasion of Privacy Act (CIPA) and the Pennsylvania Wiretapping and Electronic Surveillance Control Act. In addition to basing claims on chatbot and session replay technologies, plaintiffs have crafted claims asserting that use of retargeting pixels violate state wiretap laws, with a particular focus on hospital websites and mobile apps. Most recently, plaintiffs have shifted focus to tracking tech incorporated in email marketing, asserting causes of action under both CIPA (see *Ramos v. The Gap, Inc.*) and an obscure Arizona law relating to telephone, utility and communication service records (see *Mills v. Saks.com LLC* and *McGee v. Nordstrom Inc.*).

See Cybersecurity Law Report's two-part series on website-tracking lawsuits: "A Guide to New Video Privacy Decisions Starring PBS and People.com" (Mar. 29, 2023), and "Takeaways From New Dismissals of Wiretap Claims" (Apr. 5, 2023).

Europe

As regulatory and litigation risks around tracking technologies continue to mount in the U.S., many companies with a digital presence in Europe are continuing to defend themselves against an avalanche of regulatory enforcement actions stemming from over 700 complaints filed by Max Schrems' privacy activist organization None of Your Business starting in 2021. These complaints assert various alleged deficiencies with the user interfaces and consent experiences presented through data controller "cookie banners" and CMPs.

Data protection authorities across Europe handling these complaints have taken varying stances on the alleged areas of non-compliance, leading the European Data Protection Board to set up a "Cookie Banner Taskforce" in an effort to bring DPAs into greater alignment on how CMP interfaces for tracking consents should be designed and operate. This effort resulted in a report published last year that signaled an effort toward increasing alignment but noted some continuing areas of divergent approaches, leaving digital publishers in the unenviable position of trying to design a consent

approach for pan-European websites that meet the expectations of a multitude of regulatory authorities.

See "France's Cookie Enforcement Against TikTok and Microsoft Highlights Common Compliance Missteps" (Jan. 25, 2023).

Looking Ahead: Predictions on the Trajectory of Tracking Tech Regulation and Risk

Digital tracking classically embodies the typical dance between technology and privacy regulation: tracking tech raced ahead, the law endeavored to respond, and business and technology are now working to adapt to an evolving legal playbook. As this article was being written, Google began testing for final phase-out of third-party cookies, and the market is racing to craft new approaches to securing consumer insights, increasing consumer engagement and preserving ad revenue, all activities which have, to date, depended significantly on an array of online tracking technologies.

Unquestionably, regulation will continue to develop in response to tech innovation and shifting market practice, and the dance will go on. It is impossible to predict all the ways the legal and risk landscape will evolve in this complex environment, but we offer a few predictions. In addition to the certainty of additional U.S. state privacy laws being passed and the possibility of a comprehensive federal law at some point, below are some trends to keep in mind.

Litigation Risk

Litigation risks relating to tracking technologies likely will continue to escalate for the foreseeable future. The wave of U.S. state wiretap cases based on tracking tech shows no signs of slowing, and the plaintiffs' bar appears increasingly enthusiastic about leveraging a host of other state laws – unfair competition, computer fraud and abuse, statutory larceny and even more obscure laws – to craft class action claims and see what sticks. Businesses should also keep in mind that Washington's My Health My Data Act, which broadly goes into effect on March 31, 2024, includes a private right of action, and there is little doubt the plaintiffs' bar is waiting for the starter gun to fire on that law. In Europe there is movement toward more U.S. class action-style lawsuits leveraging the "representative actions" remedy available under GDPR, so that is a risk to keep in mind as well, though there are important differences between the U.S. and European procedures that should keep the European litigation in better check.

Shift to Opt-In Model

While the U.S. generally still remains an opt-out jurisdiction for digital tracking, the law is already chipping away at the edges of that approach. Expanded definitions of sensitive data requiring opt-in consent under various state laws and the movement to widen the scope of digital services caught by

children's privacy regulation will increase the number of sites and apps required to seek opt-in consent for online tracking.

In addition, the push by California, Colorado and other states to force websites to honor browser-based consent signals could prove pivotal. In December 2023, the California Privacy Protection Agency Board voted 5-0 to advance a legislative proposal that would require browsers to provide a universal opt-out mechanism such as GPC for consumers to exercise their CCPA opt-out rights at the browser level rather than site-by-site. If passed, this requirement could result in a de facto shift from an opt-out to an opt-in model for many types of digital tracking.

See "How to Approach CCPA's Under-16 Opt-In Consent" (Feb. 12, 2020).

Shift to Paid Subscription Models

With more regulatory and litigation risks, it is quite likely we will see more digital services shift to paid subscription models, as the revenue models that have enabled the provision of free content may prove unsustainable without the ability to track and target at the same scope and scale. The consumer pushback that would likely result from such a shift could lead to yet another wave of regulation and litigation.

See "Benchmarking the Impact of State Privacy Laws on Digital Advertising" (Oct. 11, 2023).

Leslie Shanklin is co-head of Proskauer's global privacy & cybersecurity group, a partner in its corporate department and a member of its technology, media & telecommunications group. Prior to joining the firm, she led global privacy teams for media and entertainment companies for over a decade and most recently served on the privacy leadership team for Warner Bros. Discovery. Her practice focuses on privacy and data security, delivering comprehensive expertise around data-related risk and compliance.

Ryan Blaney is co-head of the global privacy & cybersecurity group and a partner in the health care practice at Proskauer. His practice focuses on regulatory compliance, enforcement, litigation and transactions in the areas of data privacy, cybersecurity, health care and emerging technologies.

Danielle Brooks is an associate in Proskauer's corporate department and a member of the technology, media & telecommunications group.

The authors would like to thank Proskauer associates Caroline Rimmer and Brianna Arscott-Grant for their contributions to this article.