Westlaw Today
powered by Reuters

Modern adtech regulated under antiquated law: How video killed the internet star

By Katie Staba, Esq., and Corey M. Bieber, Esq., K&L Gates LLP

MARCH 15, 2024

Introduction to adtech technologies

Sometimes described as a 'spaghetti soup' of technologies, adtech, the layered advertising technology ecosystem that facilitates buying, selling and management of online advertising space, operates seamlessly at hyper-speed behind the scenes of digital properties but remains a mystery for many companies.

Certain features have garnered the attention of litigants — chatbots, tracking pixels, session replay, and video tracking technology — asserting that these technologies overstep to invade individual rights.

Certain accessible terms have emerged from this web of technologies — cookie, pixel, beacon, IP addresses — and attached to our general understanding of how an online user is identified, understood, assessed, tracked, or served advertisements on a digital property or device.

In addition to the evolving U.S. state privacy laws that have complicated disclosures, consent and user rights, the use of technologies to enable targeted advertising or better understand users has triggered the reinvigoration of some longstanding laws that predate these current technologies. These laws were largely originally drafted to address an analog landscape, and their application to the digital space has challenged companies to excavate and investigate their own adtech.

Digital activities ripe for scrutiny

Presenting a robust website privacy policy and terms of use is very rarely the sole focus of a company's online compliance efforts. The desire to implement consumer- and experience-focused technologies and tools — coupled with the increasing demand to track and understand its consumers (whether by the company or its adtech vendors) has created a need to bring visibility to *what, when,* and *by whom* those goals are accomplished.

The list of relevant technologies is ever-growing, but certain features have garnered the attention of litigants — chatbots, tracking pixels, session replay, and video tracking technology — asserting that these technologies overstep to invade individual rights. Common among their implementation is the fact that at least three parties are often involved — the consumer (user, website visitor), the company (brand, website owner), and third-party technology or adtech provider(s).

A. ***Website chatbots.*** Web chatbots are artificial intelligence (AI) software applications that simulate human conversation in real-time through text interfaces commonly used to streamline consumer communication channels.

B. ***Tracking pixels.*** Tracking pixels, web beacons, and pixel tags (referred to here generically as tracking pixels) are a small, transparent image or code snippet embedded within a web page or email. Operating surreptitiously, their primary function is to track user interactions and behavior across digital platforms. When a user interacts with a web page or opens an email containing the pixel, it sends HTTP requests to a web server containing data such as the user's IP address, device type, and other relevant information.

C. ***Session replay.*** Session replay technology enables entities to record and playback user sessions in real-time, providing a comprehensive view of how users navigate and engage with their online interfaces. Session replay tools record and timestamp each user event (e.g., click), creating a chronological sequence of actions to view a user session in a narrative-like way.

D. ***Video tracking technology.*** Video tracking technology encompasses a range of tools designed to monitor and analyze user interactions with video content. By embedding such technology within video players or hosting platforms, companies can learn more about the behavior of their users (such as user engagement, viewing habits, and content preferences), and optimize content performance.

New applications of old laws bring expanded liability and leaves questions unanswered

While there is a long list of potential issues relating to use of tracking technologies, we focus below solely on two unexpected

statutes under which new theories of liability and adaption to the digital landscape have captured attention and warrant consideration.

A. California Invasion of Privacy Act (CIPA) provides private litigants avenues of recourse — pen register and wiretapping

CIPA was first enacted in 1967 in response to then-sweeping technological advances (at the time, advances like wiretapping and covert telephone call recording). Today, a similar surge in technological advances has prompted reinvigoration and adaption of the statute.

Web chatbots have become a frequent target for CIPA claims alleging that the software records network routing information or the content of chat conversations without consent.

These obscure terms — ***pen register and trap and trace*** — refer to physical surveillance devices historically used by law enforcement to record outgoing (pen register) and incoming (trap and trace) call numbers from a specific location to produce a call log of phone numbers or IP addresses contacted.

The pen register is effectively the cousin of what we commonly understand as wiretapping, with the critical distinction that it does not capture the *content* of the communications but rather the routing information. While "pen register" originally referred to devices only, the definition was expanded to include devices *and processes* that *recorded dialing, routing, addressing or signaling* information.

CIPA Section 638.51 prohibits the use or installation of a pen register (in device or process form) without a court order, except where the consent of the user has been obtained. The current theory advanced by litigants generally attempts to apply this CIPA provision against any software that tracks website users. This theory — if successful — could effectively envelop the universe of internet-enabled interactions.

CIPA also offers private litigants recourse in the event of unauthorized interceptions of communications, more commonly known as ***wiretapping and eavesdropping***. Under certain clauses of Section 631(a) (wiretapping), unauthorized activities may occur where (1) a non-party to the communication reads, attempts to read, or learns the content of any communication in transit without consent; (2) a non-party *uses* any such information for its own purposes; or (3) an entity directs, aids or abets in completing (1) or (2).

Session replay software, typically deployed on a company website by a third-party session replay provider, is often the subject of allegations under Section 631, alleging unlawful wiretapping, eavesdropping, or recording of confidential communications.

Motion to dismiss decisions have hinged on whether the session replay (1) was alleged to have captured personally identifiable information or otherwise had the figurative fingerprint of the user, (2) whether the provider acted solely as the "tape recorder" of the company defendant (and thus did not constitute a non-party participant) or performed additional functions (analytics, heat mapping), and (3) whether the information was collected instantaneously by the provider (e.g. via Application Programming Interface or API).

Other common marketing technologies have formed the basis of CIPA actions. Web chatbots have become a frequent target for the above CIPA claims alleging that the software records network routing information or the content of chat conversations without consent. Email marketing analytics technologies have become caught in the CIPA crosshairs, under allegations that the analytics software observes and records customer interactions upon receipt of the email (e.g. when the emails are opened and referenced links clicked).

As mentioned above, implementing the technology often involves two entity players — the company (brand, website owner), and third-party technology or adtech provider(s) — resulting in two potential defendants and varying arguments, particularly as to which entity constitutes the "non-party" to the communication.

What is so alluring to litigants is the VPPA's attractive enforcement and damages profile.

CIPA allows for a private right of action for an injunction, as well as statutory damages in the amount of $5,000 for each violation of CIPA or treble damages, whichever is greater. Notably, statutory damages are available without a separate showing of injury aside from a violation of the privacy rights protected by CIPA.

Here we focus on CIPA specifically as an exemplar of similar state invasion-of-privacy statutes outside of California; however, California is not the only state that has an invasion of privacy statute that includes a private right of action. Connecticut, Florida, and Maryland also offer this statutory protection.

B. Video killed the radio star — Video Privacy Protection Act (VPPA) raises questions for inclusion of video content

The VPPA, first enacted in 1988 and later amended, was intended to impose strict prohibitions on videotape service providers (at the time of enactment, brick-and-mortar providers) from knowingly disclosing consumers' personal information or the videos the consumer rented or purchased from third-party service providers.

In recent years, the VPPA has taken on new shape — enabled by creative application of its broad definitions and scope — to capture websites and apps containing recorded videos from which video tracking technologies collect personal information of consumers and further disclose that information to service providers (like

streaming, social media, and analytics providers), without informed written consent.

As currently repurposed, the dragnet of the VPPA is not yet settled. Debates remain as to what constitutes "personally identifiable information" (e.g., device ID, IP addresses), a "video service provider" (whether the business must focus on providing audiovisual content), and a "consumer" (subscribers to the site generally vs. the content specifically), as the pains associated with shoehorning an antiquated statute onto modern facts churn in federal courts and the plaintiffs' bar.

What is so alluring to litigants is the VPPA's attractive enforcement and damages profile. The VPPA provides consumers with a federal private right of action, enabling them to seek redress in the form of actual and punitive damages, reimbursement of legal costs and reasonable attorneys' fees, and the availability of equitable relief.

Some comfort in the form of appropriately framed notice and consent can be found for companies seeking to stay out of the fray of these suits. For example, the statute allows for limited disclosure of consumers' names and addresses to third-party service providers if the consumers are given the *opportunity to opt out* and other retention requirements are met.

The challenge, however, remains for companies to become aware of their use of tracking technologies, even if their sites and apps may only incidentally contain video content.

C. Geographic exclusion from state-specific claims challenging

Some companies and technology providers have relied upon use of IP geolocation and geo-fencing as a strategy to identify the jurisdiction of a user before either deciding to implement tracking technologies or restrict user access. This risk mitigation strategy has been used to exclude users associated with jurisdictions known to have strict and punitive state laws and a litigious affinity.

This practice has become less reliable and prevalent with the rise in use of geographic disguising technologies. There has been a surge in Virtual Private Network (VPN) usage, which has the ability to obscure a user's location and other metadata and present an inaccurate perceived location. The expansion of commercial VPN usage coupled with the integration of VPN functionalities in privacy-oriented browsers and home routers, has made relying on a user's perceived location based solely on their IP address a less attractive approach in some circumstances.

Practice tips and strategies — diligence of your digital properties

Despite the ongoing refinement needed to confirm compliance strategies with or inapplicability of these statutes to certain technologies, companies and technology providers are not without broader insight or direction in approaching and assessing their operations.

A company's regular monitoring of any digital properties' use of tracking technologies will bring to light any unknown, overlooked, (or perhaps forgotten) use of certain tracking technologies, and allow companies to assess the risk of using such technologies against the evolving litigation landscape.

Diligence activities may involve:

- Confirm with marketing departments, information technology departments and third-party agencies the nature and identity of and data collected from known technologies;
- Engage third-party consultants and tools to run complementary assessments;
- Identify any third-party technologies implemented and review relevant contracts for compliance and risk sharing obligations, particularly any limitations on third party technology provider's use of data collected;
- Align on a consistent state-specific (e.g. geofenced), national, or global approach;
- Develop internal procedures to assess technologies prior to implementation; and
- Review results of diligence against existing privacy disclosures and consent mechanisms.

Once the landscape is known, a company may wish to evaluate whether there is value in continued use of tracking technologies, asking:

- Do we need to track users at the level offered through such technology?
- Are we actually using/deriving value from the data we collect through tracking technology?
- Is the value we get from the data worth the cost of compliance or the potential risk?

If tracking technologies are retained, consent review is critical to assess whether (1) existing consent pop-ups are sufficient in content, presentation, optionality of responses, timeliness and recordation; (2) consent is gained *before* any tracking technologies are triggered or chat session begun; and (3) the company retains the ability to unilaterally act (by removing or modifying) in response to any future claims or court decisions.

As we watch the litigation and creative arguments unfold, we can look to the movements of the adtech industry generally for navigation signs. Some would suggest that a consistent sentiment has echoed from across industry associations, brands, technology providers and consumers: An interest in some level of transparency. As has occurred before in this industry, where the law has been slow to provide clarity, industry organizations and standard-setting entities have responded with industry-led initiatives.

About the authors

Katie Staba (L) is a partner in **K&L Gates LLP**'s Chicago office. She focuses her practice on complex global transactions and counseling for consumer brands and technology companies in the areas of digital media planning and buying, advertising and marketing, claim substantiation, software licensing, and intellectual property. Staba brings to her practice years of experience as in-house legal counsel at Publicis Groupe, a French multinational advertising and public relations company, and Amazon Web Services. She currently co-leads the firm's consumer beauty and aesthetics group. She can be reached at katie.staba@klgates.com.

Chicago partner **Corey M. Bieber** (R) concentrates his practice on data protection and legal compliance with regard to emerging technologies, including virtual reality, video games, artificial intelligence, deepfake technology, biometric systems, blockchain, and conventional software and technology systems. He has more than 20 years of experience in the software development and information technology industry, including over a decade as a software developer and solutions architect in the health care industry. He can be contacted at corey.bieber@klgates.com.

This article was first published on Westlaw Today on March 15, 2024.