Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Precautions For New Wave Of Digital Privacy Class Actions

By **Jason Stiehl, Christopher Cole and Gage Javier**
(September 26, 2022, 6:00 PM EDT)

Jason Stiehl

Christopher Cole

Gage Javier

Although many say law drags behind technology, creative class action lawyers are attempting to expand the boundaries of older, existing laws to cover a host of online activities involving new online techniques and software codes, such as Meta Platforms Inc.'s Pixel code, as well as interactive online keystroke and chat functions.

These class actions allege that consumer data, such as keystrokes and user preferences, is captured without notice to the user and then transferred to third parties in violation of statutes such as the Video Privacy Protection Act, or VPPA, and related state laws governing wiretapping.

In the past two months alone, these statutes have accounted for well over two dozen class actions across the country, with two to three filed nearly every day, and undoubtedly the wave has not crested.

Historical Background

Video Privacy

In the 1980s, video stores such as Blockbuster LLC caused one of the first waves of privacy fears and calls to protect personally identifiable information through legislation.

The hullabaloo arose from the judicial branch during the controversial effort to confirm Robert Bork to the U.S. Supreme Court, after the Washington City Paper published Bork's video rental history, which it had obtained from Blockbuster.

The article prompted a backlash and the proposed VPPA to prevent such leaks of personally identifiable information.

As Sen. Patrick Leahy, D-Vt., stated during debate on the statute, "It is nobody's business what Oliver North or Robert Bork or Griffin Bell or Pat Leahy watch on television or read or think about when they are home."

Congress passed the VPPA in 1998,[1] which prohibits videotape service providers from knowingly disclosing users' personally identifiable information without the person having expressly given consent. Numerous states followed by enacting analogs to the VPPA, some of which expanded the web of possible offenders by including not only videotapes but also books or other written materials.[2]

As streaming services grew in the early 2010 time frame, the statute achieved a resurgence, with lawsuits brought against online streaming companies like Paramount Global's Nickelodeon and The Cartoon Network Inc., alleging they were modern-day videotape service providers.

The case In re: Hulu Privacy Litigation[3] cemented in 2015 that these streaming services as covered by the final clause, which addresses "similar audio-visual materials."

Most of the companies, however, avoided liability under the statute, with courts holding that although they may have transmitted a complete record of someone's video history, they did so without connecting that data to a specific individual, and therefore, the information did not constitute personally identifiable information.

Wiretapping

The law against wiretapping evolved separately and earlier than the VPPA. In 1967, the Supreme Court decided Katz v. United States.

In Katz, a New York police officer placed a bug in a telephone booth to collect evidence on a bookie who transmitted betting information by telephone, in violation of federal law.[4]

The court concluded that privacy interests attached to the person, not just the place. Further, it held that a person could have an expectation of privacy regardless of where located.

This prompted Congress to pass the Omnibus Crime Control and Safe Streets Act of 1968, establishing the Wiretap Act, Title I of the Electronic Communications Privacy Act, which prohibits wiretapping and electronic eavesdropping by conferring a civil cause of action on "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter."[5]

Notably, one of the common exceptions to the Wiretap Act is consent by one of the parties to the intercepted communication.[6] The Electronic Communications Privacy Act of 1986 updated the Wiretap Act, which covered interception of conversations using hard telephone lines, to apply to interception of computer and other digital and electronic communications.

In the early 2000s, internet users explored the bounds of the Wiretap Act as it applied to targeted web marketing. DoubleClick Inc., one of the most prevalent advertisement companies at the time, began providing internet ad services in 1995.

In the In re: DoubleClick Inc. Privacy Litigation, the class action plaintiffs alleged that when users visited any DoubleClick-affiliated websites, a cookie was placed on their hard drives to collect and store personal information and GIF tags were used to record users' movements throughout the affiliated website, enabling DoubleClick to learn what information the user sought and viewed.

DoubleClick conceded that its conduct violated Title 18 of the U.S. Code, Section 2511, but it claimed that its actions fell under the consent exception.

With little discussion, the court held in 2001 that the consent given by affiliated websites to DoubleClick to intercept communications was sufficient, and the determinative issue was whether the DoubleClick's actions evinced a criminal or tortious purpose.

It eventually found no criminal or tortious purpose, but rather a purpose to make money by providing a valued service to commercial websites.

States now have various laws relating to monitoring or recording communications. The Electronic Communications Privacy Act and many states' laws provide what are known as one-party laws; that is, monitoring or recording of certain communications is permitted, so long as at least one party to the communication consents to such monitoring or recording.

On the other hand, California and 12 other states are all-party states, meaning that all parties to the communication must consent to the communication being monitored or recorded.

The California Invasion of Privacy Act,[7] or CIPA, was enacted to protect the right of privacy of California residents.

Section 632 prohibits eavesdropping upon or recording of any confidential communication, including those occurring among the parties in the presence of one another or by means of a telephone, telegraph or other device, through the use of an electronic amplifying or recording device without the consent of all parties to the communication.

In 2019, CIPA gave rise to claims against personal voice assistants' recordings — e.g., Google Home, Siri and Alexa. The U.S. Court of Appeals for the Ninth Circuit, in In re: Facebook Inc. Internet Tracking Litigation, held in 2020 that Facebook was not an exempt party to these communications, and thus the plaintiffs plausibly alleged federal wiretap and CIPA claims.

Additionally, the Ninth Circuit's ruling found a number of the named plaintiffs had sufficiently alleged economic harm to survive dismissal. This opened a new wave of lawsuits, many of which are based on the alleged monitoring of consumers' internet activity.

In the recent Javier v. Assurance IQ LLC case, the Ninth Circuit read Section 631 to apply to recording information regarding events taking place on websites because "[Section 631] makes liable anyone who 'reads, or attempts to read, or to learn the contents' of a communication 'without the consent of all parties to the communication."

In Javier, the court addressed whether consent under CIPA could occur after a website user had begun interacting with a website. The plaintiff in Javier allegedly visited an insurance-quoting website that utilized third-party software to record a video of a user's interactions with the site.

After completing the insurance quote form on the website, the plaintiff "viewed a screen that stated that clicking the 'View My Quote' button would constitute agreement to Assurance's Privacy Policy." If the user clicked the button, the website would construe this as acceptance of the privacy policy.

The Ninth Circuit disagreed with the U.S. District Court for the Northern District of California and concluded that the California Supreme Court would likely find that — since the plaintiff alleged that because the defendants did not request consent before he filled out the insurance questionnaire

online — his communications were recorded for purposes of CIPA, without his valid consent.

The Wave of New VPPA and Wiretapping Lawsuits

Over the past two months, consumer plaintiffs lawyers across the country, but most notably in California and Illinois, have targeted companies that use source code-based tools to evaluate and interact with visitors to their sites.

Specifically, in Illinois, over a dozen companies have been sued thus far, including WebMD Health Network's WebMD.com, Dotdash Meredith's People.com, CNET Networks and Paramount, for allegedly using the Meta Pixel code to analyze consumers' website usage.

The complaints allege that Meta, through the use of markers such as a user ID marker, an encrypted Facebook ID and browser identifier, and an unencrypted value that identifies the browser, installs a tracking code on webpages.

The complaints allege that once installed, Meta uses these cookies to link the individual to their Facebook ID and corresponding Facebook profile, which may contain personally identifiable information and tracks people as they visit and interact with content on that webpage.

Finally, the complaints allege that Pixel digests this information, including searching for form field and other sources on the website that contain information such as first name, last name and email, to allow the companies to better target their advertisements.

What makes this recent wave worth sounding an alarm is that each violation of the VPPA can result in a $2,500 fine, as well as punitive damages, attorney fees and equitable relief. Moreover, there is a continued expansion of what constitutes similar audiovisual materials, in addition to some of the state-related statutes that cover additional materials.

In a similar wave in California, plaintiffs counsel have focused on companies' use of data analytics and chat functions, alleging that the implementation of such tools violates California Penal Code 632 — the wiretap law.

Thus, in these cases, plaintiffs lawyers are trying to hold companies accountable by applying the federal and state wiretapping laws to the quickly evolving technological landscapes.

For example, in Kauffman v. Zillow Group Inc.,[8] the plaintiff filed a putative class action on Sept. 15 against Zillow for damages and injunctive relief related to alleged violations of CIPA.

According to the plaintiff, the defendant:
Utilized "session replay" spyware to intercept Plaintiff's and the Class Members' electronic computer-to-computer data communications, including how Plaintiff and Class Members interacted with the website, mouse movements and clicks, keystrokes, search items, information inputted into the website, and pages and content viewed while visiting the website.

The complaint alleges that Zillow:
Intentionally tapped and made unauthorized connection to Plaintiff and Class Members' electronic communications to read and understand movement on the website, as well as everything Plaintiff and

Class Members did on those pages, e.g., what Plaintiff and Class Members searched for, looked at, the information inputted, and clicked on.

A similar wave of lawsuits has been brought against over a dozen separate companies, alleging that their interactive chat functions constitute illegal wiretapping under Penal Code 632.

In just the last month, cases have been filed against high-profile companies such as Michael Kors, Aflac Inc., BJ's Wholesale Club Holdings Inc. and Nationwide Mutual Insurance Co., all based on the same theory that their website chats violate CIPA.

Other Jurisdictions

Digital privacy class actions based on violations of state wiretapping laws have been filed in jurisdictions outside California, including:

- Florida Security of Communications Act violations, which served as the basis for more than 30 lawsuits against well-known organizations such as Adidas AG, Avis Budget Group, Inc., Gap Inc.'s Banana Republic and Old Navy, Costco Wholesale Corporation, The Walt Disney Company, Fandango Media LLC, Frontier Airlines Inc, Fossil Group Inc., GNC Holdings Inc., Intel Corporation, Spirit Airlines Inc., Puma SE, Deutsche Telekom AG's T-Mobile and WebMD LLC; and

- Pennsylvania Wiretapping and Electronic Surveillance Control Act violations against AutoZone Inc., Chewy Inc. and Michaels Stores Inc.

Industry Warnings

Organizations must now also be aware of additional obligations put forth by the advertising industry.

The Digital Advertising Accountability Program issued a compliance warning[9] in June regarding the practice of inferring consent from a consumer's passive use of a product or service before engaging in interest-based advertising.

Specifically, the accountability program does not regard a consumer's mere continued use of a product or service to satisfy the action component of consent as defined by the Digital Advertising Alliance's Self-Regulatory Principles for Online Interest-Based Advertising.

The DAA Principles require both a clear, meaningful and prominent notice from the company and an action in response to that notice on the part of the consumer to obtain consent under the principles. The recommended warning will take effect Jan. 1, 2023.

The DAA's industry-standard recommendation carries weight in the existing cases that consent for purposes of the wiretap laws requires affirmative opt-in.

Practical Considerations

The rapid advancement of technology allows the creative leverage of technical tools facilitate advertising and profiling of a retailer or organization's target audience. However, organizations must ensure that they provide users with transparency as to the collection and use of their information.

Companies that employ the Meta Pixel — or similarly complex data tracking and identifying tools, such as cookies — should be familiar with how it works.

Organizations should ensure they fully understand what these tools do, how they are being employed and what risks exist in order to convey the functionality to online and mobile application users.

Additional issues to consider include how software scripts capture information, what information is captured and the subsequent use of that information.

Companies that engage in the sale or sharing of personal information with third-parties that was collected through the monitoring or recording of user activities should be transparent.

Organizations should ensure that users are notified that their information is being shared with third parties.

This is particularly important when in connection with providing interest-based advertising. Several states, including California, have enacted comprehensive privacy laws that require opt-out mechanisms to prevent the selling and sharing of personal information.

Companies that track website mouse movements and clicks, keystrokes, search items, information inputted into the website, chat functionality, and pages and content viewed — to develop user profiles or leverage for targeted advertising — should check those activities against relevant laws.

Organizations must evaluate whether those activities rise to the level of wiretapping violations based on state and federal wiretapping laws.

Organizations must inform consumers and obtain their consent before recording of user activities take place, particularly when relying on third-party technologies that record or monitor a user's web session.

Jason Stiehl is a partner at Crowell & Moring LLP.

Christopher Cole is a partner at the firm and co-chairs its technology and brand protection group.

Gage Javier is an associate at the firm.

Crowell & Moring associates Tiffany Aguiar and Jacob Canter contributed to this article.

[1] 18 U.S.C. 2710 et seq.

[2] See, e.g., Mich. Comp. Laws Ann. 445.1712 (2013).

[3] 86 F. Supp. 3d 1090.

[4] See Katz v. United States, 389 U.S. 347 (1967).

[5] 18 U.S.C. § 2520(a).

[6] 18 U.S.C. § 2511(2)(c), (d).

[7] Cal. Penal Code §§ 630, et seq.

[8] 3:22-cv-01398 (S.D. Cal).

[9] https://bbbprograms.org/media-center/newsroom/daap-compliance-warning-consent.