AN A.S. PRATT PUBLICATION
JANUARY 2026
VOL. 12 NO. 1

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Data Privacy Litigation Trends Against Insurers and Financial Services Companies

By Kara Baysinger, Debra Bogo-Ernst, Laura Leigh Geist, Susan Rohol, Amy Orlov and Tahirih Khademi*

In this article, the authors discuss the new wave of data privacy litigation against insurers and other financial services companies.

Data privacy litigation has rapidly expanded in recent years and is now targeting insurers and other financial services companies that may share customer information with third parties via technologies on their websites and apps. In this new wave of litigation, plaintiffs' firms are filing class-action lawsuits against insurers and financial services companies that use data tracking technologies, such as pixels and cookies on their websites, software development kits (SDKs) in their apps, as well as session-replay tools and chat widgets.

PLAINTIFFS' FIRMS SHOEHORN MODERN DATA TRACKING TECHNOLOGY INTO OLD WIRETAPPING LAWS

In these lawsuits, plaintiffs are bringing claims under antiquated federal and state wiretapping laws that prohibit third parties from eavesdropping on and "intercepting" communications without the consent of one or both parties to the communication. Although these laws were passed in the 1960s and 1980s and were historically used to protect face-to-face and telephone conversations from being recorded, they are now being applied to modern digital contexts. Plaintiffs originally targeted technology companies in these lawsuits, but now, plaintiffs are using wiretapping laws to pursue claims against insurance and financial services companies for disclosure of consumers' personal information via analytics tools, as well as social media, marketing, and advertising cookies or pixels. Plaintiffs also commonly sue over session replay tools and third-party chatbots, alleging similar wiretapping theories.[1]

On the federal level, the Electronic Communications Privacy Act of 1986 (ECPA) establishes liability for any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[2] ECPA is a one-party consent statute, meaning that there

* The authors, attorneys with Willkie Farr & Gallagher LLP, may be contacted at kbaysinger@willkie.com, dernst@willkie.com, lgeist@willkie.com, srohol@willkie.com, aorlov@willkie.com and tkhademi@willkie.com, respectively.

[1] See, e.g., Javier v. Assurance IQ, LLC, 649 F. Supp. 3d 891 (N.D. Cal. 2023); Shah v. Cap. One Fin. Corp., 768 F. Supp. 3d 1033 (N.D. Cal. 2025); Adair v. Cigna Corps. Servs. Inc., LLC, No. 2:25-cv-02384 (E.D. Pa. filed May 9, 2025).

[2] 18 U.S.C. § 2511(1)(a).

is no violation when one of the parties to the communication has consented to a third-party "intercepting" the communication.[3] Under this rule, in the context of data privacy litigation, a plaintiff cannot bring suit against a company when that company consented to the plaintiff's information being collected by third parties.

However, plaintiffs' firms attempt to circumvent the one-party consent by relying on an exception for instances in which a communication is "intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State," also known as the "crime-tort" exception.[4] Under this exception, ECPA still imposes liability when a communication has been intercepted for the purpose of committing a separate crime or tort.[5] In essence, a plaintiff may bring a claim against a defendant who allowed for the interception of a communication if the plaintiff can show that the defendant allowed the interception for the purpose of committing a separate crime or tort. In order to meet the requirements of the crime-tort exception, plaintiffs' firms commonly allege that insurers and other financial services companies intend to violate either the Gramm-Leach-Bliley Act (GLBA) or the Health Insurance Portability and Accountability Act (HIPAA) by allowing third parties to intercept personal information.

- *GLBA*: Plaintiffs argue that financial services companies breach the GLBA by disclosing information via the data tracking technologies.[6] Under the GLBA, personally identifiable financial information – such as information provided by a consumer to obtain a financial product or service, or information showing that an individual has obtained a financial product or service – is confidential.[7] Plaintiffs frame GLBA violations as the "crime" required to satisfy the crime-tort exception, alleging that financial services companies have intentionally allowed third parties to intercept this information without consumers' consent.

- *HIPAA*: Plaintiffs also now rely on HIPAA – specifically, the HIPAA Privacy Rule – as the basis for framing alleged violations against HIPAA-covered entities, e.g., health plans, as "crimes" under the crime-tort exception.[8] HIPAA requires prior authorization to reveal personal health information, such as "unique health identifiers" relating to an individual's physical or mental health and/or payment for healthcare, which can be used to identify the individual.[9] Under this framework, plaintiffs have attempted

---

[3] 18 U.S.C. § 2511(2)(d) (no liability "where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception").

[4] 18 U.S.C. § 2511(2)(d).

[5] Caro v. Weintraub, 618 F.3d 94, 98-99 (2d Cir. 2010); Planned Parenthood Fed'n of Am., Inc. v. Newman, 51 F.4th 1125, 1135-36 (9th Cir. 2022).

[6] See, e.g., Allen v. Quicken Loans Inc. (D.N.J. Nov. 9, 2018).

[7] 16 C.F.R. § 313.3(o).

[8] See, e.g., Cooper v. Mount Sinai Health Sys., Inc., 742 F. Supp. 3d 369 (S.D.N.Y. 2024); K.L. v. Legacy Health (D. Or. Nov. 14, 2024); Lugo v. Inova Health Care Servs. (E.D. Va. Mar. 25, 2025).

[9] 42 U.S.C. § 1320d-6.

> to argue that, by allowing third parties to collect this information via data tracking technologies, insurers knowingly violate HIPAA.[10]

On the state level, plaintiffs bring a myriad of claims under the California Invasion of Privacy Act (CIPA), which imposes liability on any person who:

(1) Intentionally taps or makes any unauthorized connection with a telegraph or telephone wire;

(2) Reads, attempts to read, or learns the contents of any message while it is in transit;

(3) Uses or attempts to use any information that is so obtained; or

(4) Aids or abets another in carrying out one of the previous acts.[11]

Under CIPA, plaintiffs argue that third-party tracking devices are "instruments" that allow technology companies to eavesdrop on communications with the alleged aid and agreement of insurance and financial services companies.

NEW WIRETAPPING LAWSUITS RELATE TO VIDEO VIEWING AND ALSO TAKE A "KITCHEN SINK" APPROACH

Within the last few years, plaintiffs' firms have also filed claims under the Video Privacy Protection Act of 1988 (VPPA), which was enacted to protect video viewing histories back in the day of Blockbuster video. The VPPA prohibits the knowing disclosure of personally identifiable information concerning any consumer of a video tape service provider, aside from certain exceptions.[12] While the VPPA does not explicitly outline what constitutes "personally identifiable information," many jurisdictions have defined this as information that readily permits an ordinary person to identify a particular individual as having watched certain videos.[13] With VPPA claims, plaintiffs typically allege that defendants fall under the definition of a "video tape service provider" and have wrongfully and knowingly disclosed viewers' personally identifiable information.

When alleging violations of these privacy laws, plaintiffs' firms often take a "kitchen-sink" approach, bringing claims for other unlawful conduct, hoping that at least something will survive early dismissal, including:

---

[10] 42 U.S.C. § 1320d-6.

[11] Cal. Penal Code § 631(a).

[12] 8 U.S.C. § 2710(b).

[13] See, e.g., Eichenberger v. ESPN, Inc., 876 F.3d 979, 985 (9th Cir. 2017); Solomon v. Flipps Media, Inc., 136 F.4th 41, 51 (2d Cir. 2025) (identifying personally identifiable information as including information capable of being used to identify a consumer's video-viewing history); Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 485 (1st Cir. 2016).

- *Breach of Fiduciary Duties*: Plaintiffs frequently bring claims for breaches of fiduciary duties, highlighting the alleged existence of a fiduciary relationship that gives rise to duties of good faith, fairness and honesty, loyalty, and/or protection. Plaintiffs have generally characterized the disclosure of private information as an intentional act by the defendant in direct violation of these fiduciary duties, which directly and proximately causes damage to plaintiffs.

- *Breach of Implied Contract*: Another common claim is breach of implied contract, wherein plaintiffs allege that, by providing private information, a valid contract was formed with the insurance company, and that defendant violated this implied contract by implicitly promising to maintain the security and confidentiality of that individual's personal information.

- *Negligence*: Plaintiffs have also brought negligence claims, alleging that insurance and financial services companies owe plaintiffs a duty to exercise reasonable care in handling their information, including by preventing unauthorized disclosure, and have breached this duty by allowing for the unauthorized disclosure.

- *Invasion of Privacy*: Along with their wiretapping claims, plaintiffs often allege a separate claim for invasion of privacy, asserting that they have a reasonable expectation of privacy in their communications with insurance and financial services companies, which have publicized plaintiffs' information to third parties.

Additional claims brought by plaintiffs under this "kitchen sink" approach include negligence per se, unjust enrichment, breach of implied duty of confidentiality, and violations of state consumer fraud and business practices statutes.