



U.S. data privacy litigation: Assessing risks and navigating uncertainty

Tuesday, 4 August

07:00-08:00 PDT

10:00-11:00 EDT

16:00-17:00 CEST



Welcomes and Introductions



Kayla Bushey, CIPP/US
Associate Attorney,
McNees Wallace & Nurick



Matt Pearson
Partner, Privacy Counseling and
Class-Action Litigation,
Frankfurt Kurnit Klein & Selz PC

Data Privacy Litigation by the Numbers

The ten largest privacy class action settlements in 2025 totaled approximately **\$802 million**. The ten largest data breach settlements accounted for another **\$516 million**, and major settlements under statutes such as BIPA, the TCPA and the FCRA added roughly **\$280 million** more. Altogether, the 50 largest settlements across five privacy and data security categories exceeded **\$1.5 billion** in 2025.

IAPP research estimates that more than **10,000 privacy-related cases** were filed between 2022 and 2025, including nearly **3,500 in 2025** alone. That upward trajectory is expected to continue through 2026.

User Consent

Consent remains one of the most important concepts in privacy law, serving both as a basis for data processing and, in many circumstances, as a defense against liability. Yet courts continue to scrutinize whether consumers received meaningful notice and whether any purported consent was actually obtained.

California Invasion of Privacy Act

California Code, Penal Code § 631

(a) **Any person who**, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or who **willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state;** or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable . . .

California Code, Penal Code § 638.51

(a) Except as provided in subdivision (b), **a person may not install or use a pen register or a trap and trace device without first obtaining a court order . . .**

Federal Wiretap Act

18 U.S. Code § 2511

(1) Except as otherwise specifically provided in this chapter any person who—

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . .

shall be punished . . .

(2)

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication 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 unless such 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.

California Consumer Privacy Act

California Civil Code Division 3, Part 4, Title 1.81.5

1798.150: Personal Information Security Breaches

(a) (1) **Any consumer** whose **nonencrypted and nonredacted personal information**, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, or whose email address in combination with a password or security question and answer that would permit access to the account **is subject to an unauthorized access and exfiltration, theft, or disclosure** as a result of the business' violation of the duty to implement and maintain **reasonable security procedures and practices** appropriate to the nature of the information to protect the personal information may institute a civil action . . .

Horizon Scanning and Takeaways

Audience Q&A

Web Conference Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here: <https://iappwf.questionpro.com/t/AbBPvZ9LEt>

Thank you in advance!

For more information: www.iapp.org

Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your AIGP, CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration prior to the live webinar will automatically receive credit. After the broadcast date, individuals may submit for credit by completing the continuing education application form here: [submit for CPE credits](#).

Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

**For questions on this or other IAPP Web Conferences
or recordings please contact:**

livewebconteam@iapp.org