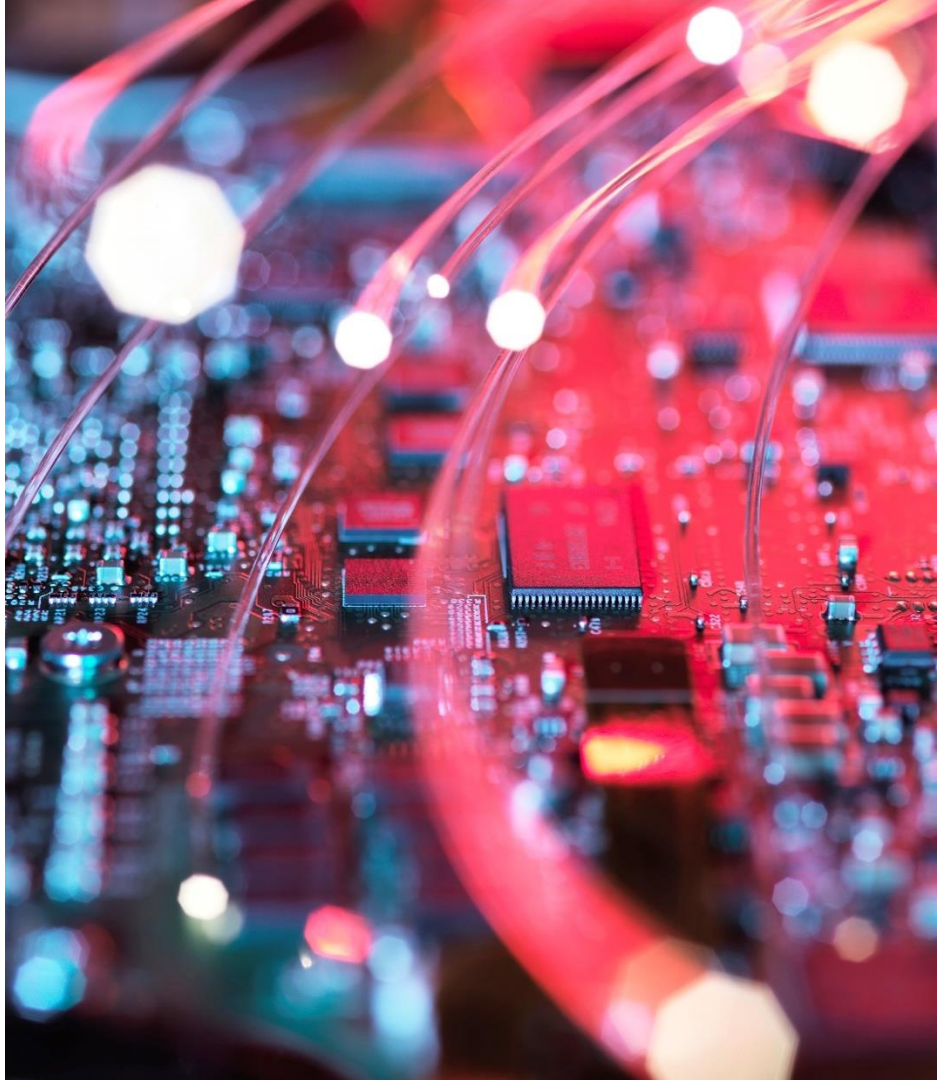
NORTON ROSE FULBRIGHT

ACC Association of Corporate Counsel
SOUTHERN CALIFORNIA

Navigating the Frontier: Trends and Tactics in Cybersecurity and Privacy Litigation

Ji Won Kim, Partner
Eva Yang, Partner
May 28, 2025



Introduction

Ji Won Kim

Partner, Los Angeles

jiwon.kim@nortonrosefulbright.com

Eva Yang

Partner, Los Angeles

eva.yang@nortonrosefulbright.com

Agenda

01
Emerging trends in cybersecurity litigation

02
Emerging trends in privacy litigation

03
Practical solutions to litigation risks/ takeaways

04
Questions

Backdrop – litigation trends

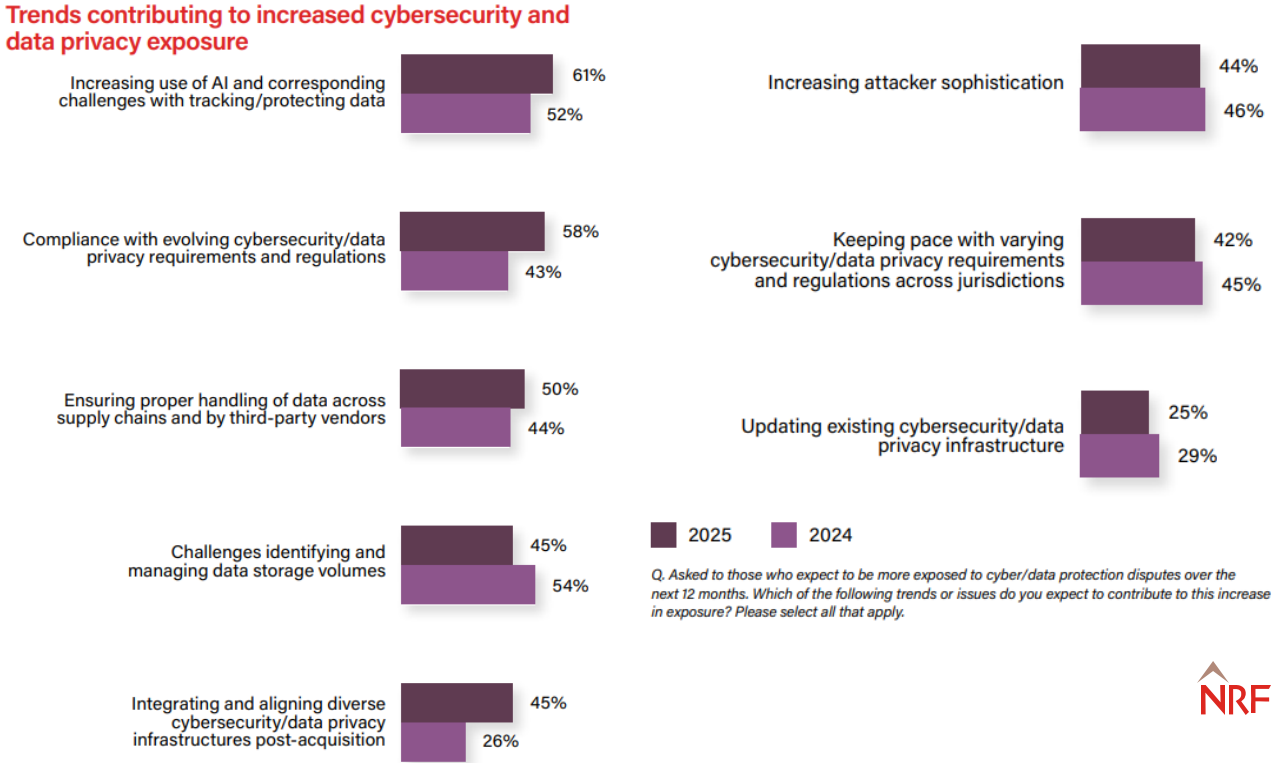
NORTON ROSE FULBRIGHT

20TH ANNIVERSARY

Annual Litigation Trends Survey

PERSPECTIVES FROM CORPORATE COUNSEL

- 36% of respondents with more exposure to cybersecurity and data privacy disputes over the past 12 months
- Majority expect the exposure to stay the same or increase



NRF

Backdrop – additional considerations

Compliance complexity coupled with active enforcement

Continued attempts to expand theories of liability

Private right of action under state law

Heightened awareness of cybersecurity and privacy risks

Cybersecurity threat landscape continues to evolve

Cybersecurity Litigation

Cybersecurity enforcement trends

- Increased SEC regulation and enforcement actions
  - **Cybersecurity Disclosure Rules**
  - ***SEC v. Solarwinds*, 1:23-cv-09518-PAE (S.D.N.Y. 2023)**
  - ➢ Alleging that Solarwinds and its CISO defrauded investors by making material misstatements regarding its cybersecurity practices, the description of breach, for not having reasonable internal controls to safeguard the company's crown jewel assets, and for not having reasonable disclosure controls.
  - ➢ Several claims dismissed following Motion to Dismiss; Motion for Summary Judgment currently pending
- FTC and HHS - OCR enforcement actions
- Increased state regulator investigations

Regulator activity trends

Regulators everywhere

Very thorough and highly technical inquiries

Short turnaround time

NRF

Common questions from regulators

Prior work
Organizational structure and board decisions
Policies and procedures
Training
Cybersecurity, privacy, and information governance practices
Third-party risk management
Details regarding cybersecurity attack
Recovery and remediation

Data breach class action

- Sources
- Theories of liability
  - ➢Breach of contract
  - ➢Negligence
  - ➢Consumer protection statutes (e.g., Consumers Legal Remedies Act and Unfair Competition Law)
- Hurdles (e.g., standing)

Securities litigation class actions and shareholder derivative suits

False Claims Act

- Federal and state (e.g., California)

Private right of action

- California Consumer Privacy Act
- Washington My Health My Data Act

NRF

CCPA private right of action developments

- Limited private right of action for certain security-related breaches
  - **Section 1798.150(a)(1):** Provides for a private right of action for consumers if their "nonencrypted and nonredacted personal information" is subject to unauthorized access and exfiltration, theft, or disclosure caused by a business's failure to "implement and maintain security procedures and practices." Cal. Civ. Code. § 1798.150(a)(1).
  - **Cal. Civ. Code. § 1798.150(a)(1)(B) and (C):** Damages available to consumers under this private right of action provision can be as high as $750 per violation. Courts can also provide consumers with injunctive or declaratory relief and "any other relief the court deems proper."
- Recent rulings in N.D. Cal. surviving Motion to Dismiss without allegation of data breach

NRF

Realm of criminal litigation involving cybersecurity

- Federal crime conviction in *United States v. Sullivan*
  - A jury in the Northern District of California found Joseph Sullivan, Uber's former chief security officer guilty of obstruction of justice and misprision of a felony in connection with his role in responding to a 2016 incident (Oct. 2022)
  - Ninth Circuit upheld conviction (Mar. 2025)
  - Simply failing to disclose a breach is not a crime, obstructing a regulatory investigation into a cyber incident and actively concealing an incident from regulators and management becomes a problem
- Corporate victims in cases against cyber criminals

NRF

Takeaways for staying ahead

- Accurate statements about cybersecurity incidents and risks
- Develop processes and controls to help ensure accuracy – Playbooks and tabletop exercises for integration and maturity
- Internal controls for protecting critical assets – Proactive assessments and tracking remediation
- Internal communication protocols
- Build executive and board education and awareness
- Map the regulatory landscape and assess regulatory readiness

Privacy litigation

Tracking technology claims involving pixels

01

A snippet of code embedded on a website, email, or advertisement to track user activity. Meta, TikTok and LinkedIn all have their own pixels

02

Through cookies, the pixel gathers information about a user's website interactions and sends it to Meta, TikTok or LinkedIn

03

The information may be directly linked to the website user's profile depending on the ad tech (e.g., Facebook, LinkedIn or TikTok ID)

04

Primarily used in targeted advertising and allows companies to track conversions, optimize ads and build targeted audiences

Wiretapping claims

- **Beginning in the summer of 2022, plaintiffs began targeting the use of the Meta Pixel tool, which later expanded to other ad tech.**
  - Primarily targeted hospitals in the beginning, later expanded to other businesses
  - Demand letters and arbitration demands not publicly available, the tip of the iceberg
- **Plaintiff's allegations:**
  - Companies are using pixels, which collects information about a user's devices and activities, and sends that information to Meta or other social media platforms without their consent which constitute illegal wiretapping

Wiretapping claims: CIPA

- **California Invasion of Privacy Act (CIPA)**: Enacted in 1967 to address traditional forms of wiretapping, eavesdropping and non-consensual telephone call recording
- Section 631: prohibits intentional wiretapping, wilfully attempting to learn the contents or meaning of a communication in transit, attempting to use or communicate information obtained, and aiding or abetting the aforementioned conduct
- Section 632: prohibits using an amplifying or recording device to eavesdrop or record **confidential communication** intentionally and without consent of all parties
- Section 632.7: prohibits unlawful interception & recordation of communications between "two cellular radio telephones, a cellular radio telephone and a landline telephone, two cordless telephones, a cordless telephone and a landline telephone or a cordless telephone and a cellular radio"
- $5,000 ***per violation***
- Contains a private right of action, no requirement to prove actual damages

Wiretapping claims: ECPA

Electronic Communications Privacy Act (ECPA):

- Prohibits intentional actual or attempted "interception, use, or disclosure" or procurement of another person to intercept or attempt to intercept "any wire, oral, or electronic communication."
  18 U.S.C. § 2511
- "Electronic communication" excludes "any communication from a tracking device."
- Violations may result in five years prison time or up to $250,000 in fines; victims are entitled to civil suits and may recover actual damages, punitive damages and attorney's fees

Exceptions:

- **One party consent** – as long as one party to the communication knows that the communication is being intercepted/recorded, there is no violation
- Note: crime-tort exception
- **Blanket consent** – blanket consent to recording is valid under ECPA

Specific defenses

Consent

- Facebook/TikTok users consent to the use of Meta Pixel or TikTok pixel
- Company's privacy policy (although difficult to establish if browsewrap)

Not a wiretap

- Intercepting a communication or relaying parts of a communication? Is every cookie on the website a potential wiretap?

Party exception

- The Pixel extension of the company or is it using and harvesting the data?

Current pixel litigation

- **Cases allowed to proceed against Meta and health care providers concerning disclosure of personal information or protected health information**
- More significant exposure as PHI or PII is involved
- HIPAA violation
- Companies paying hefty payouts to settle on class action basis

- **Other pixel cases primarily in arbitration or settled quickly**
- Lawyers with business plans
- Low settlement unless threat of mass arbitration, which will be later discussed
- Risk of additional claimants
- Recent cases have been favorable for defense. *See Sonya Valenzuela v. The Kroger Co.* (C.D. Cal. Mar. 13, 2025) 2025 U.S. Dist. LEXIS 52402

Pen register/trap and trace claims

- What is a pen register or trap and trace device?
- Law enforcement officers formerly used “pen registers” or “trap and trace” devices which required physical machines, in investigations to record numbers called or received from a particular telephone
- Plaintiffs are alleging that various software in websites are acting as pen registers that track users' online activity
- Apps that collect information regarding a person’s location and personal information constitute pen registers and thus violate CIPA because it is a device or process that records addressing or signaling information

CIPA: Pen registers/trap and trace

- ***Greenley v. Kochava*** kicked off proliferation of claims
- Common defenses to pen register/trap and trace claims are:
  - Personal jurisdiction
  - Standing
  - Consent from "user" of a device
  - Not a trap and trace device

CIPA: Pen registers/trap and trace

- **Personal Jurisdiction**
  - For specific jurisdiction, a defendant must have “purposefully directed” activities or “purposefully availed” itself the protections of the forum state laws
  - Which contacts are at issue?
  - Website?
  - Sale of products into the forum state?

CIPA: Pen registers/trap and trace

- **Standing**
  - California's standing requirements are similar to federal requirements. *See Limon v. Circle K Stores Inc.* (2022) 84 Cal.App.5th 671
  - Plaintiff must demonstrate a concrete, particularized, actual or imminent injury
    - *Hughes v. Vivint, Inc.*, (C.D.Cal. July 12, 2024) Case No. 2:24-cv-03081-GW-KSx [finding no standing for failure to allege an injury in fact as a result of trap and trace allegations for TikTok software]
    - At least one CA superior court case dismissed a trap and trace claim based on standing. *See Rodriguez v. Fountain 9 Inc.*, LASC Case No. 24STC04504 (July 9, 2024)

CIPA: Pen registers/trap and trace

- **Consent for "User" of that Service**
  - CIPA Section 638.51(b)(5) allows for an exception for the use of pen registers and trap and trace devices "if the consent of the user of that service has been obtained."
  - Under ECPA, courts have found that "User" of that service is the website operator, not visitor
  - Caller ID would otherwise be illegal. *See Sparshott v. Feld Entm't, Inc.* (2002) 311 F.3d 425, 432.
  - Although "persuasive," still denied. See *Moody v. C2 Educ. Sys. Inc.*, 2024 WL 3561367, at *4 (C.D. Cal. July 25, 2024) (finding the website visitor to be the "user" rather than the visitor)
- **Pen registers and trap and trace devices only apply to telephone surveillance and tracking**
  - At least historically, only applied to telephone lines
  - "A law enforcement could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed – a means of establishing communication." (*Smith v. Md.* (1979) 442 U.S. 735, 741.)
  - Reference to "telephone lines" in other parts of CIPA

Relevant decisions

- ***Shah v. Fandom, Inc.***, 2024 WL 4539577 (N.D. Cal. Oct. 21, 2024)
  - Court found that Section 638.51's pen register definition is broad and allegations of the TikTok software can constitute a pen register
  - Sufficiently alleged statutory standing
- ***Moody v. C2 Educ. Sys. Inc.***, 2024 WL 3561367, at *4 (C.D. Cal. July 25, 2024)
  - Plaintiff alleged defendant tutoring program violated CIPA by installing a TikTok Pixel that collected plaintiff's information; Defendant argued that *it* is the user of the website, and *it* gave TikTok consent to install pixel technology

Recent state caselaw

- ***Sanchez v. Cars.com***, 2025 WL 487194 (Cal. Super. Jan. 27, 2025)
  - Plaintiff, a self-described "tester," alleged that Cars.com deployed a tracking beacon on her device that recorded and transmitted her IP address to a third-party service provider
  - The Court dismissed the claim without leave to amend, stating that CIPA was designed to address telephone wiretapping, not routine website tracking
  - The court ruled that website tracking technologies that log a user's IP address do not fall under CIPA's "trap and trace" and "pen register" restrictions, and that website users do not have a reasonable expectation of privacy in their IP addresses
- ***Aviles v. LiveRamp***, 2025 WL 487196 (Cal. Super. Jan. 28, 2025)
  - Plaintiff alleged that LiveRamp deployed a tracking beacon to collect IP addresses and device information.
  - The court found the allegations too vague to move forward, making clear that privacy claims must precisely articulate how a company's data collection practices differ from how the internet normally works
  - For the beacon to be classified as a pen register on a computer, it would need to track outgoing IP addresses – such as those of websites visited by the computer – rather than merely capturing the computer's own IP address

NRF

How to stay ahead of claims?

- Understand the technology being used on your website and how it can be used to assert a privacy claim
- Cookie banner before any cookies are deployed and information transmitted
- Explicit consent to the recording of chat sessions
- Robust disclosure in the privacy policy of information captured when consumers visit a website
- Clickwrap agreements with consent to use of visitor information