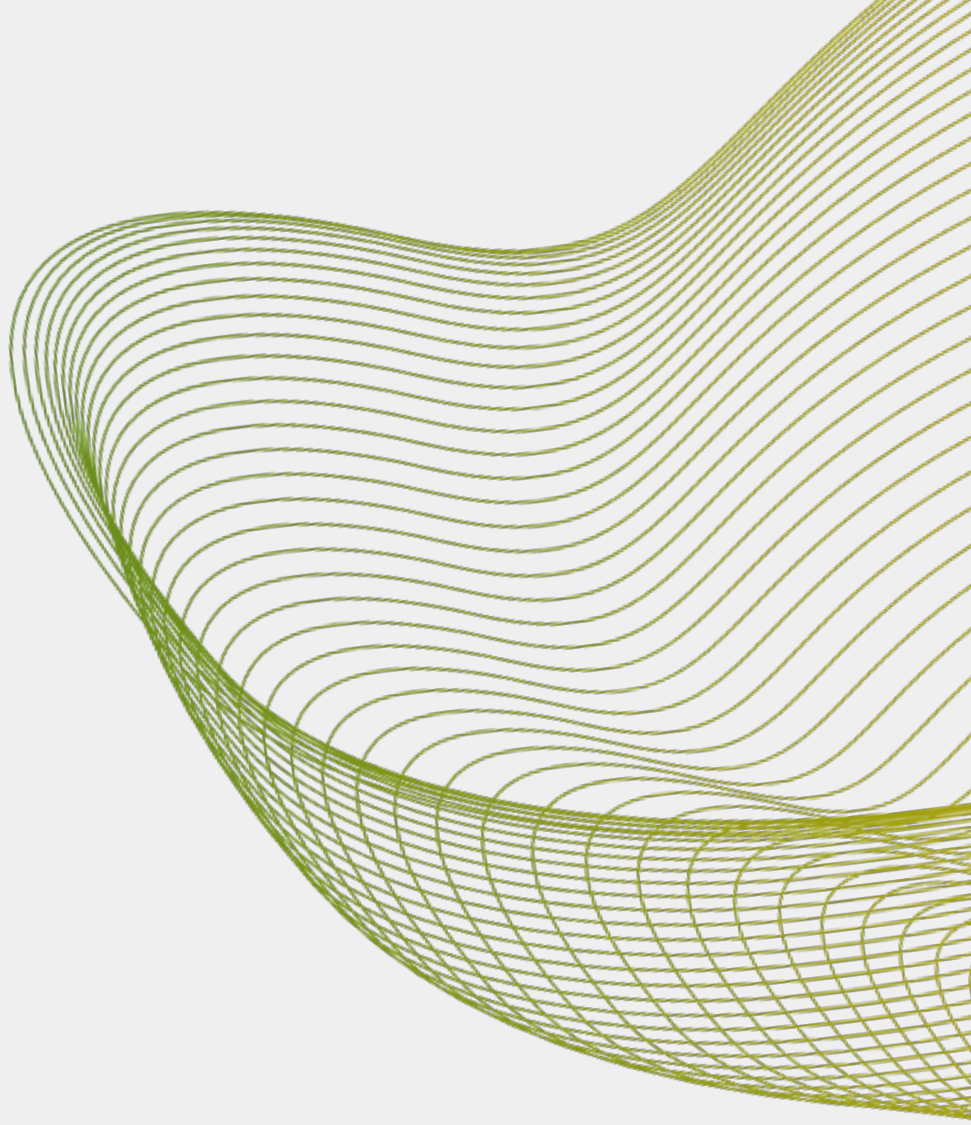
KEKER
VAN NEST
& PETERS



AI and the New Wave of Privacy & Cybersecurity Litigation

March 25, 2026

Presenters



Ben Berkowitz
bberkowitz@keker.com



Melissa Cornell
mcornell@keker.com



Spencer McManus
smcmanus@keker.com



Lauren Kane
lkane@keker.com

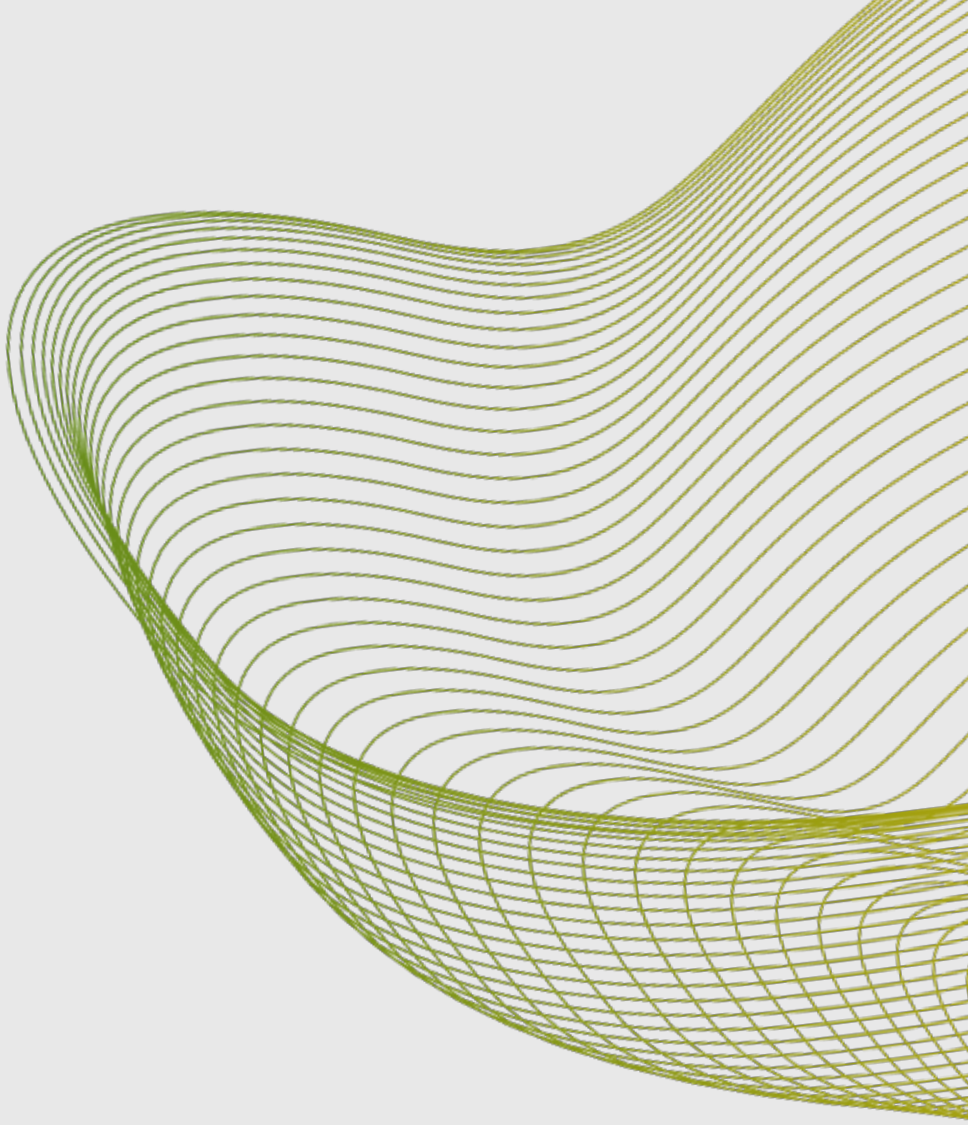
Agenda

- AI Privacy Litigation Landscape
- Eavesdropping & Wiretapping
- Biometrics
- Data Security
- Defense Takeaways
- Questions

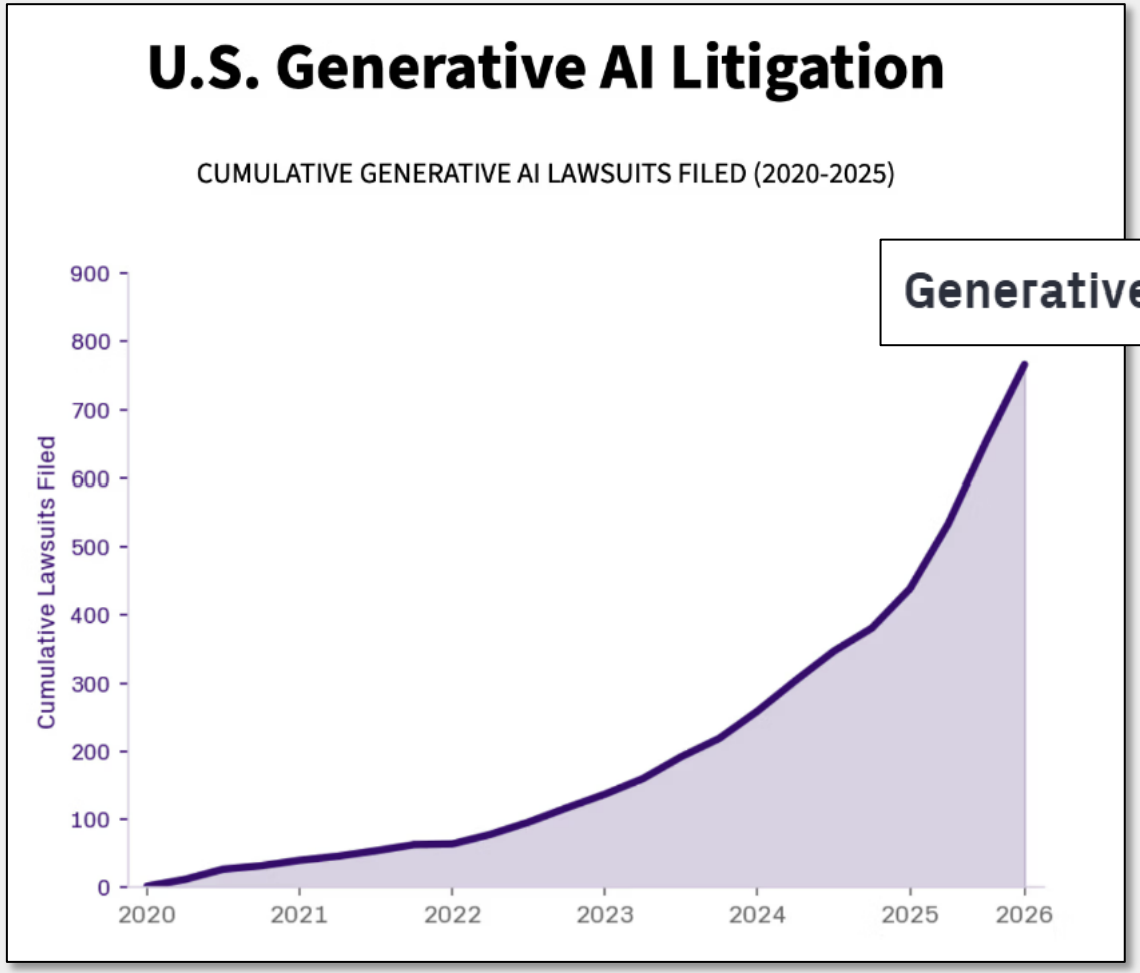


AI Privacy Litigation Landscape

- AI Litigation Increasing Exponentially
- Old Laws, New Tech
- New and Emerging Claims
- Legislative Update
- Exposure and Risk



AI Litigation Is Increasing Exponentially



Generative AI lawsuit filings are up 137% in 2025 and rising

See "The State of Play: Generative AI Litigation Market Overview, 1 January 2026" published by Testudo Global, Inc.

Old Laws, New Tech

Plaintiffs are repackaging old laws for use with new facts.



- **Eavesdropping & Wiretapping:** AI transcription and monitoring tools characterized as “third-party listening”
- **Biometrics:** AI-powered facial recognition, voiceprint analysis, and emotion detection
- **Data Security:** AI expanding the breach attack surface and the universe of discoverable artifacts

New and Emerging Claims

- AI chatbots and interception (*Taylor v. ConverseNow Technologies*)
- AI data collection without consent (*Riganian v. LiveRamp*)
- AI systems exploiting “cognitive labor” (*Small v. OpenAI*)



Legislative Update

- One Big Beautiful Bill Act (OBBA) – no moratorium on state regulation of AI
- Trump Administration's National AI Legislative Framework – announced last week
- Recent California AI regulation

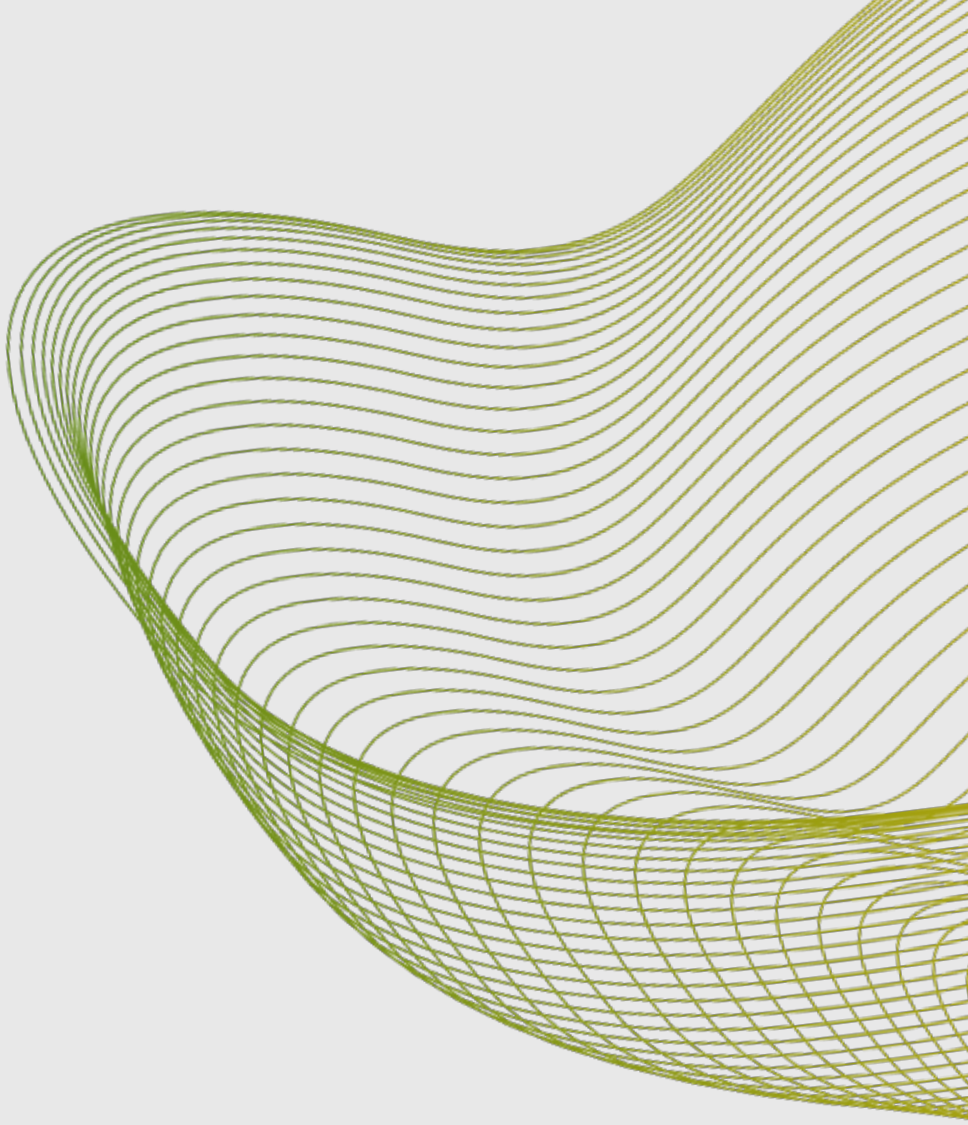


Exposure and Risk



- Statutory penalties - CIPA and BIPA
- Class actions
- Regulatory risk
- Threats of injunctions

Eavesdropping & Wiretapping



- Common Causes of Action
- Case Studies
- Defense Playbook

Common Causes of Action

Statutory Privacy & Wiretapping Claims

- Federal: Wiretap Act, Stored Communications Act, Computer Fraud & Abuse Act
- State: California Invasion of Privacy Act (CIPA), Comprehensive Computer Data Access and Fraud Act (CDAFA)

Consumer Claims

- Unfair Competition Law, Consumer Legal Remedies Act, False Advertising Law
- Breach of contract, common-law fraud, unjust enrichment

Common-Law Privacy Claims

- Intrusion upon seclusion
- Constitutional right to privacy

Claim Spotlight: California Invasion of Privacy Act

CIPA is a criminal statute that provides for civil penalties.

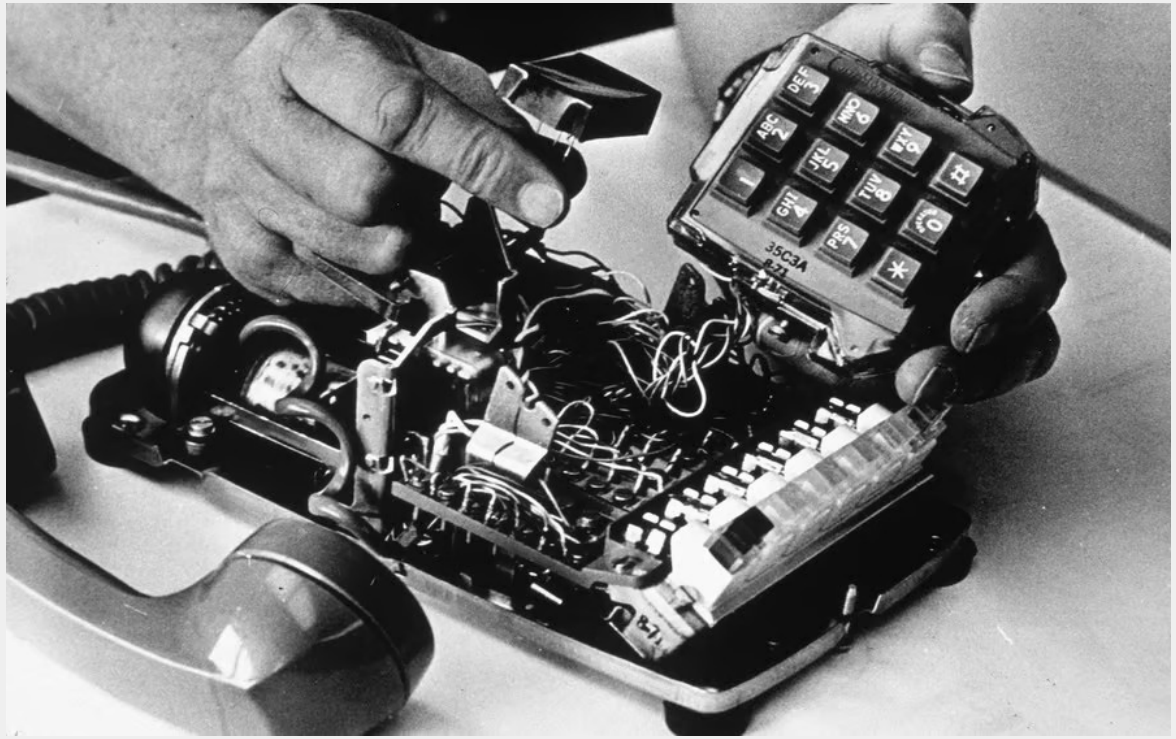
- $5000 statutory damage penalty *per violation*.

CIPA is decades-old and addressed older wiretapping, eavesdropping, and surveillance technologies

- The core provisions were enacted in 1967, with additional provisions added over time.

Plaintiffs have attempted to wield CIPA in privacy litigation addressing new technologies.

- Ad tech (pixels, tags, etc.)
- “Cookie” tracking
- Location information
- AI privacy suits, including chatbots and contact centers



Claim Spotlight: California Invasion of Privacy Act

Modern CIPA law has developed in location tracking and ad tech cases

Hammerling v. Google
(9th Cir. 2024)

What worked on a motion to dismiss → broad privacy policy

- Allegations: Google tracked in-app activity of third-party app usage on Android operating systems
- Claims: CIPA, CA common law, CA consumer statutes (UCL, CLRA)
- Google's privacy policy was a complete defense -> user consent

In re Google Loc. History
(N.D. Cal.)

What worked on a motion to dismiss → precise pleading attack

- Allegations: Google tracked users' locations using their mobile devices
- Dismissed based on statutory req's:
  - Software services ≠ "device"
  - No pleading that "electronic tracking device" was "attached" to "vehicle or movable thing"

Claim Spotlight: California Invasion of Privacy Act

Similar strategies also effective in new AI-related cases

Esparza v. Charter Commc'ns
(C.D. Cal. 2025)

What worked on a motion to dismiss → party exception

- Allegations: Charter used third-party Asapp to embed AI chat bot in customer service site
- Claims: CIPA
- Asapp's AI chatbot was a "participant to the chat conversation" rather than a third-party eavesdropper

Cody v. Ring LLC
(N.D. Cal. 2025)

What worked on a motion to dismiss → precise pleading attack

- Allegations: Ring used third party (Kustomer) to intercept chats, analyze data, train AI models
- Claims: CIPA
- Lack of plausible allegations of "in-transit" interception
- Party exception applied to Kustomer

Case Study: Voice AI Cases

- Plaintiffs attempting to apply CIPA to call centers
- Software used at contact centers to assist businesses in fielding customer service inquiries
- Plaintiffs allege that software providers eavesdropped on their phone calls with the businesses and used artificial intelligence to conduct real-time analysis of the content of those calls



Case Study: Voice AI Cases

Freund v. Dialpad
(Santa Clara Super. Ct. 2025)

What worked on a demurrer
→ telephone company exemption

- Allegations: Dialpad AI call center software eavesdropped on calls
- Claims: CIPA
- Dialpad's AI services were exempt under § 631(b)'s telephone company exemption

Ambriz v. Google
(N.D. Cal. 2024)

What worked on motion to dismiss
→ agent of telephone company

- Allegations: Google Cloud Contact Center AI software eavesdropped on calls made to Verizon
- Google covered by telephone company because (1) Verizon is a telephone company and (2) Google was acting as Verizon's agent

Defense Playbook

Win early . . . before discovery

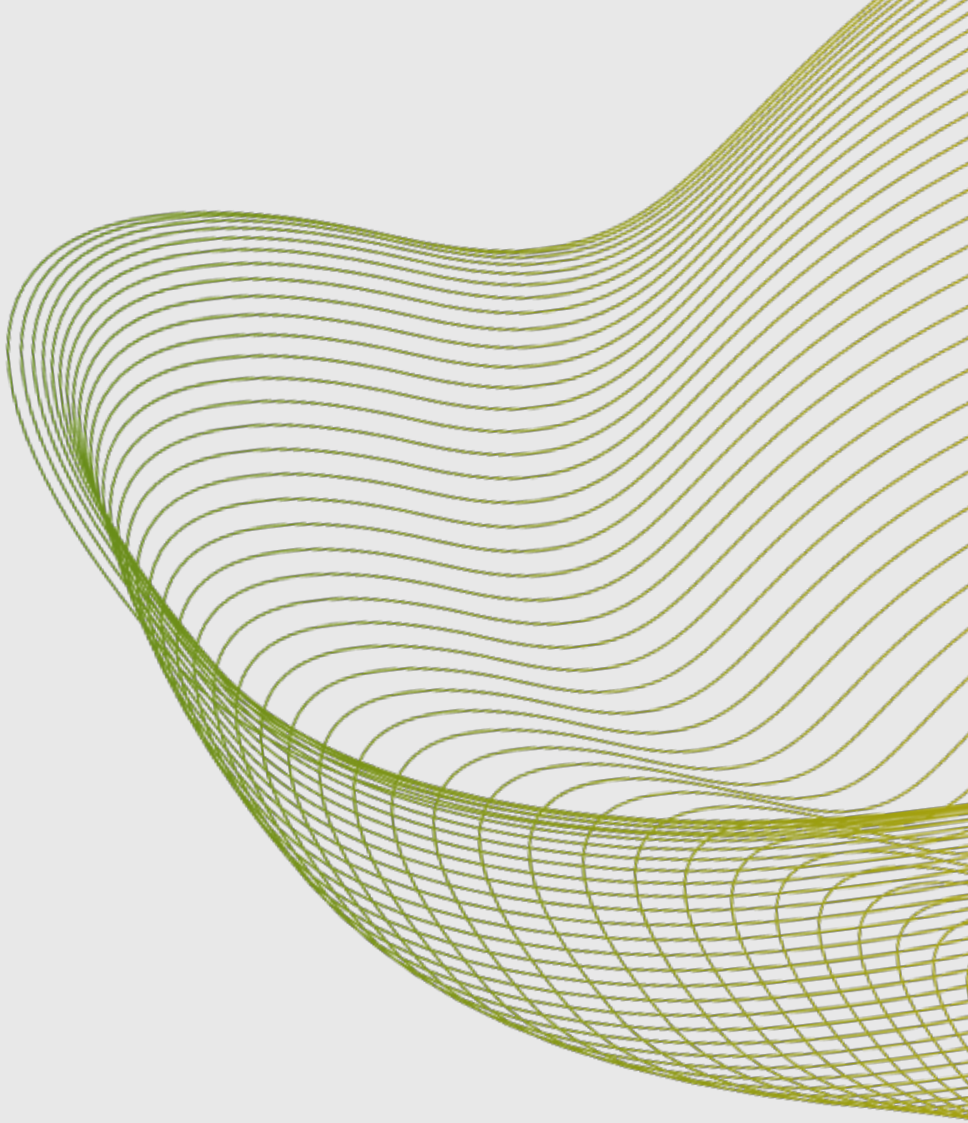
- Motion to dismiss → user consent, jurisdictional defenses, lack of criminal intent, challenge outdated statutory elements
- Motion to compel arbitration → 1st party contract, 3rd party beneficiary, or equitable estoppel

Build an early consent and intent record – submit terms of service, privacy policies, usage restrictions, etc. to (1) bolster consent argument and (2) defeat conclusory allegations of intent

Challenge statutory application – telephone company exemption, party exception, in-transit requirements, device definitions, etc.

Biometrics & AI

- Litigation Trends
- Case Studies
- Defense Strategy



Biometrics & AI: Litigation Trends

Illinois Biometric Information Privacy Act (BIPA)

- 740 ILCS 14/1, *et seq.*
- Establishes standards for how companies handle Illinois consumers' biometric info
- Notice and consent requirement
- Prohibition on selling or otherwise profiting from consumers' biometric information

Covered

Retina / Iris
Fingerprint
Voiceprint
Face geometry

Excluded

Photographs
Written signatures
Demographic data
Physical descriptions

Litigation Trends: Biometrics AI Case Types

- Facial recognition AI
- Voice recognition AI
- Behavioral Analysis & Performance Monitoring AI
- Surveillance and Monitoring AI
- Virtual Try-On AI



Konow v. Brink's, Inc., 721 F. Supp. 3d 752, 754 (N.D. Ill. 2024)

Litigation Trends: BIPA 2024 Amendments

SB 2979 (2024)

- Limits recovery under §15(b) and §15(d) to one recovery per person when collection/disclosure occurs by the same method
- Expands "written release" to include an electronic signature

"BIPA wields the impact of a grenade, but it does not impose liability on everyone who happens to be standing nearby."

— Justice Anderson, *Salinas v. Arthur Schuman Midwest, LLC*, 2026 IL App (3d) 250239 (Il. App. January 30, 2026).

Biometrics & AI Case Studies

G.T. v. Samsung
(N.D. Ill. 2024)

What worked on a motion to dismiss → precise pleading attack

- No possession of biometric data
- No collection because Samsung took no active step to obtain it
- Facial grouping, without identity, did not qualify as biometric information subject to BIPA

Zellmer v. Meta
(9th Cir. 2024)

What worked on a motion for summary judgment → technical declarations

- Project manager's declaration
- Explained that face signatures are a string of numbers
- Confirmed that face signatures do not reveal any geometric information about the detected face

Beyond BIPA: Other Biometric Statutes

Texas (CUBI)
Notice + consent for capture
Exclusive AG enforcement (civil penalties)

Washington (MHMDA)
Expansive definition of biometric info
AG enforcement + private right of action

NYC (Local Law)
Signage + no sale rule
Private right of action

Biometric Litigation Defense Strategy

A practical sequence for reducing risk and improving defenses:

Arbitration

Enforce arbitration whenever possible to defeat class leverage

Extraterritoriality

Develop facts showing conduct did not occur primarily and substantially in the geographic region

Consent

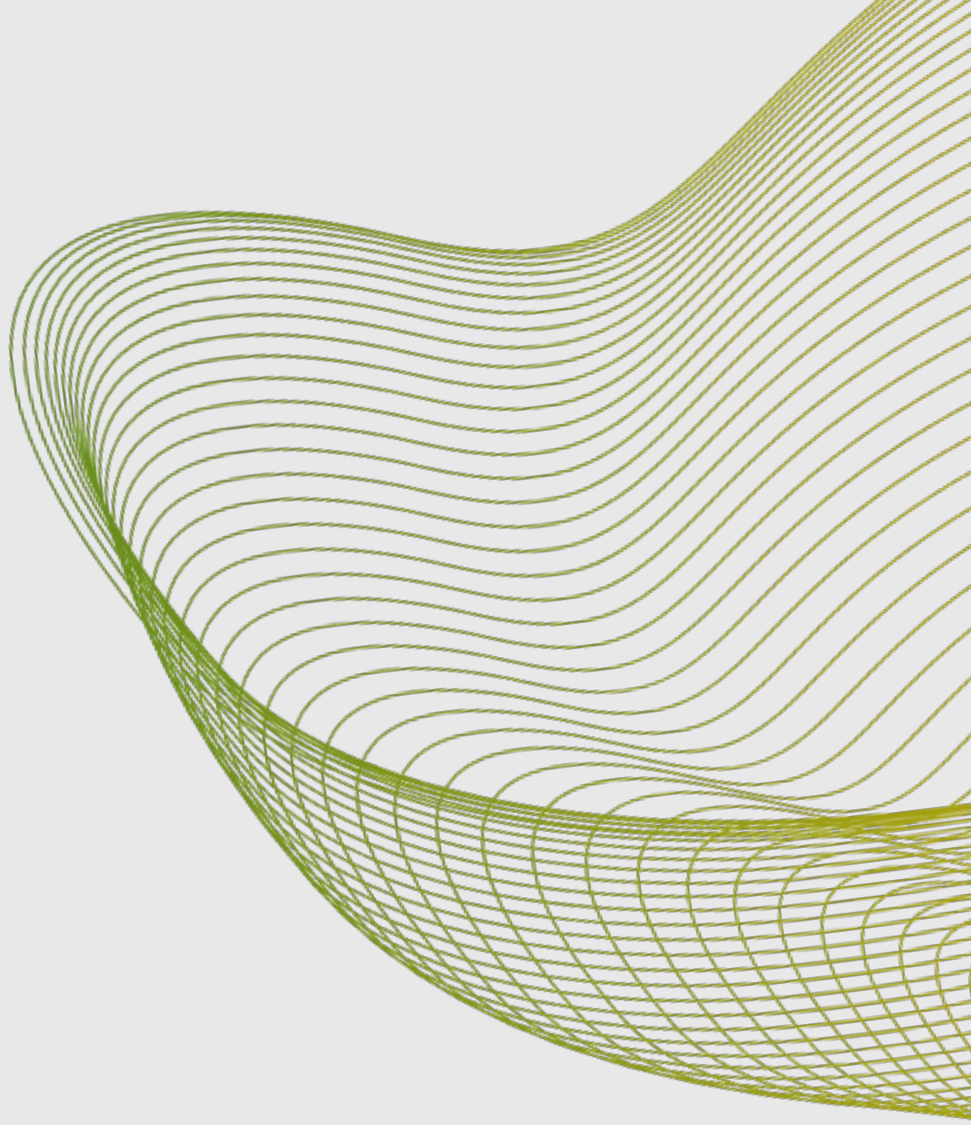
Focus on notice about what was collected, how it would be used, and whether the individual affirmatively agreed

Not biometric information

Defendant did not possess, collect, or capture identifiable biometric data

Data Security

- Litigation risk and trends
- Recent developments involving AI
- Defenses and Mitigation



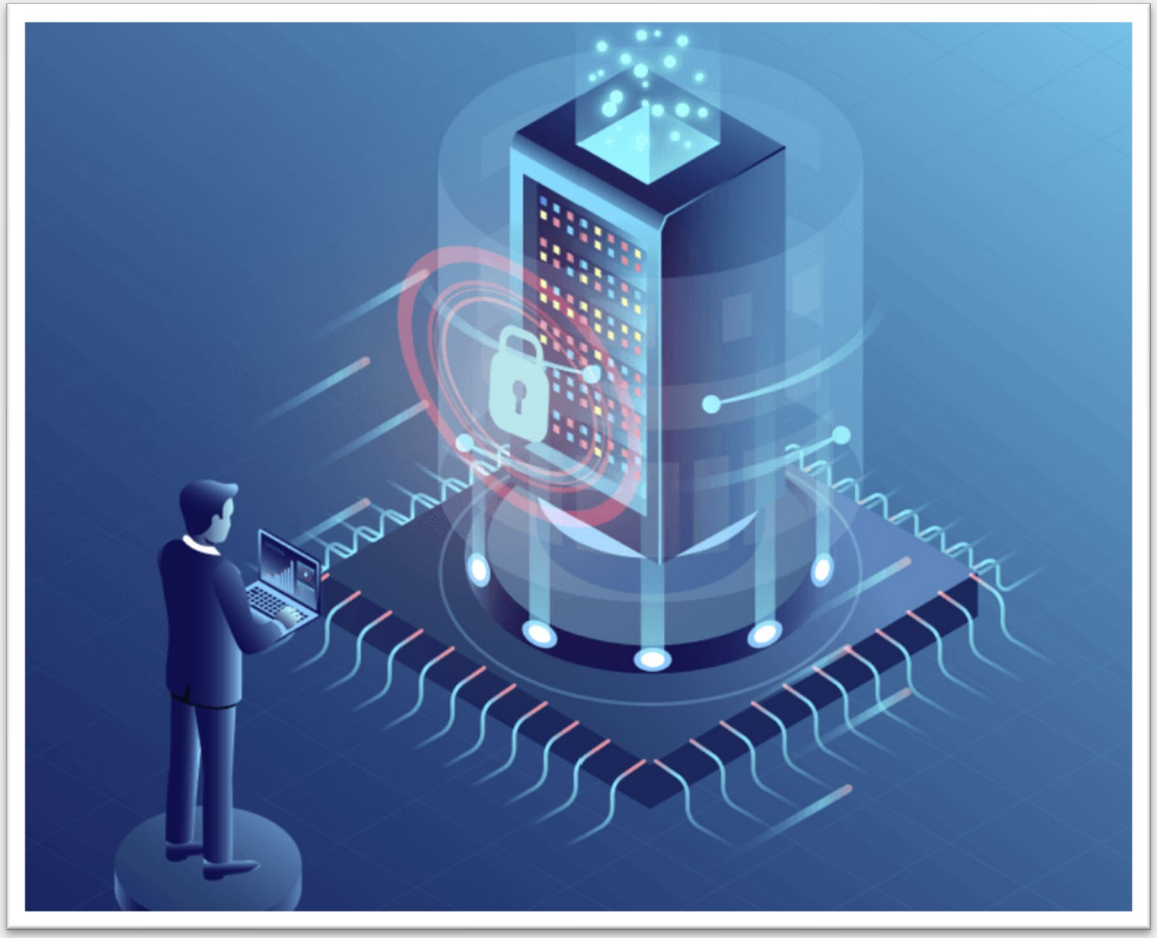
Data Security: Litigation Risk & Trends

Enforcement actions by regulators

- Inside and outside the US
- Within the US, at the federal and state level

Class actions and multi-district litigation (MDL)

Criminal liability at the individual level related to mishandling security obligations



Data Security: AI and Growing Risk

"AI adoption is outpacing oversight."

- Weaponization of AI tools
- New attack vectors
- Misuse or unauthorized use

1 in 6

Number of breaches involving AI-driven attacks

97%

Share of organizations that reported an AI-related breach and lacked proper AI access controls

63%

Share of organizations that lack AI governance policies

See "Cost of a Data Breach Report 2025" published by IBM and Ponemon Institute

Data Security: A Case Study on Standing

Greenstein v. Noblr **(9th Cir. 2024)**

What worked on a motion to dismiss → attacking standing

- Exposure of data not enough to establish harm.
- No allegation of stolen personal information.

"Plaintiffs' standing argument, which is ultimately premised on a "speculative chain of possibilities" about the potential consequences stemming from the manipulation of Noblr's online quote system, does not satisfy their burden of pleading an actual or imminent injury."

Data Security: A Case Study on Privilege

***In re Samsung Customer Data Security Breach Litigation* (D.N.J. 2024)**

What worked in asserting privilege → creating documents for the purpose of providing legal advice

- Not enough that outside counsel directs the work.
- The expert must facilitate legal strategy.

"***[T]he mere delegation of certain business functions to an attorney is insufficient to shield otherwise unprotected factual investigation from discovery.***"

Data Security: An AI Case Study

Wolf v. Serviceaide (N.D. Cal. 2025)

Causes of action

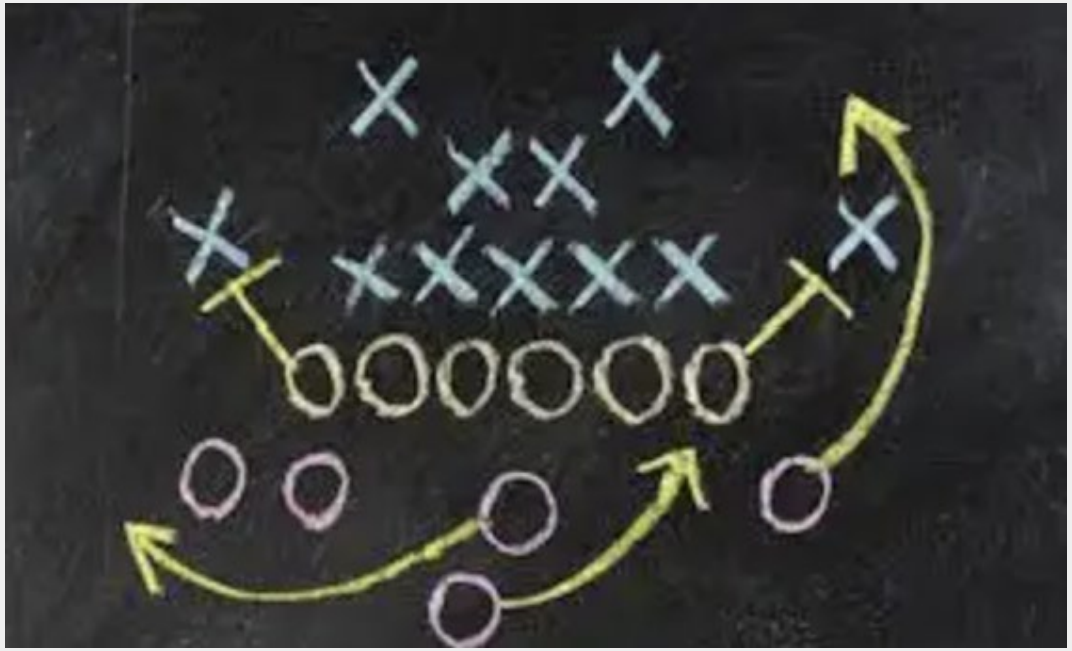
- Negligence
- Breach of implied contract
- Unjust enrichment
- Invasion of privacy
- UCL
- Declaratory judgment

Dismissal arguments

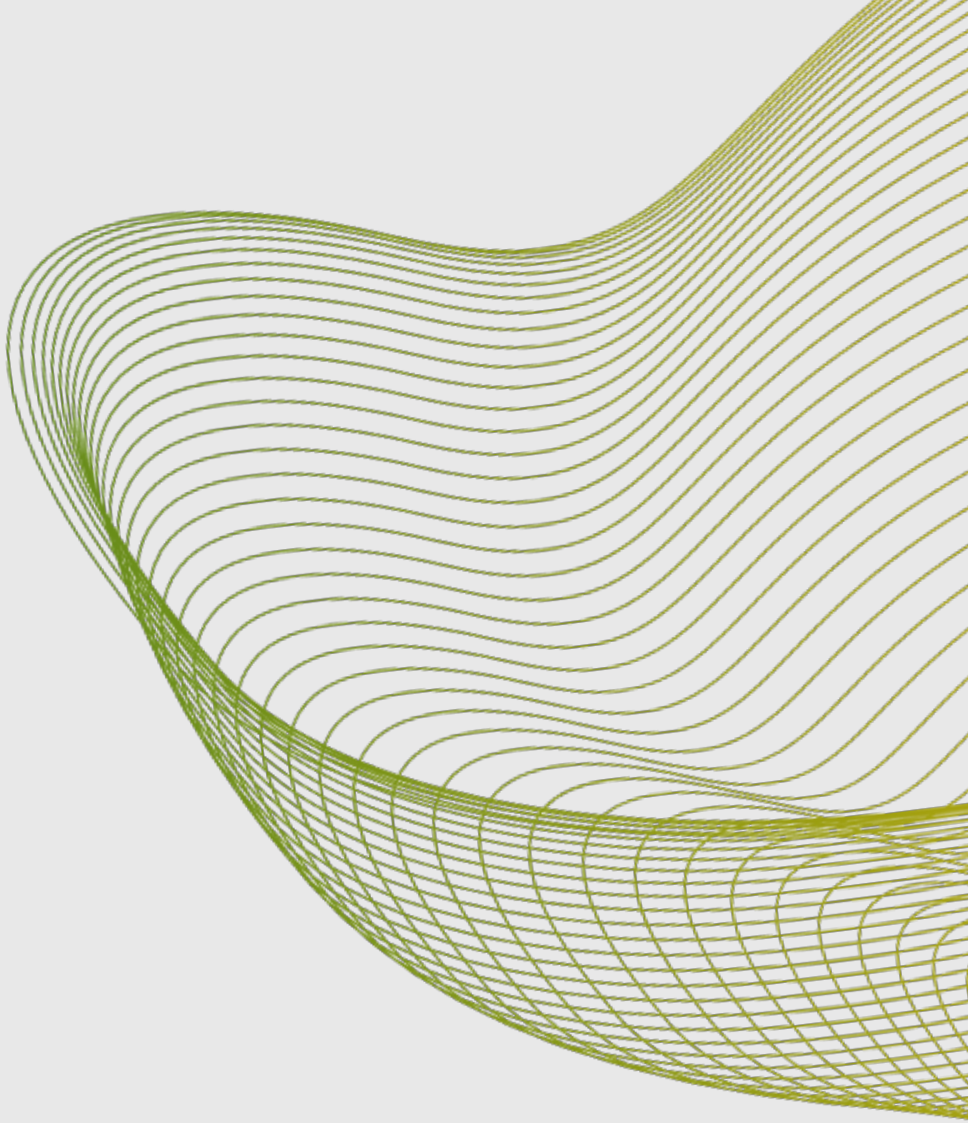
- No standing
- No duty of care
- No causation

Data Security: Defense Playbook

- **Evidence preservation**
- **Using and protecting privilege**
- **Managing multi-district litigation (MDL)**
- **Early motion practice**
  - Challenge injury-in-fact
  - Lack of causation
  - Limitations of liability
  - No duty of care
  - Lack of damages
  - Lack of an intentional violation of privacy rights
- **Defeating class cert**



Defense Strategy Takeaways



Defense Strategy Takeaways

- Educating judges and juries
- Emphasizing key themes
- Early, targeted action

Questions?

