BakerHostetler

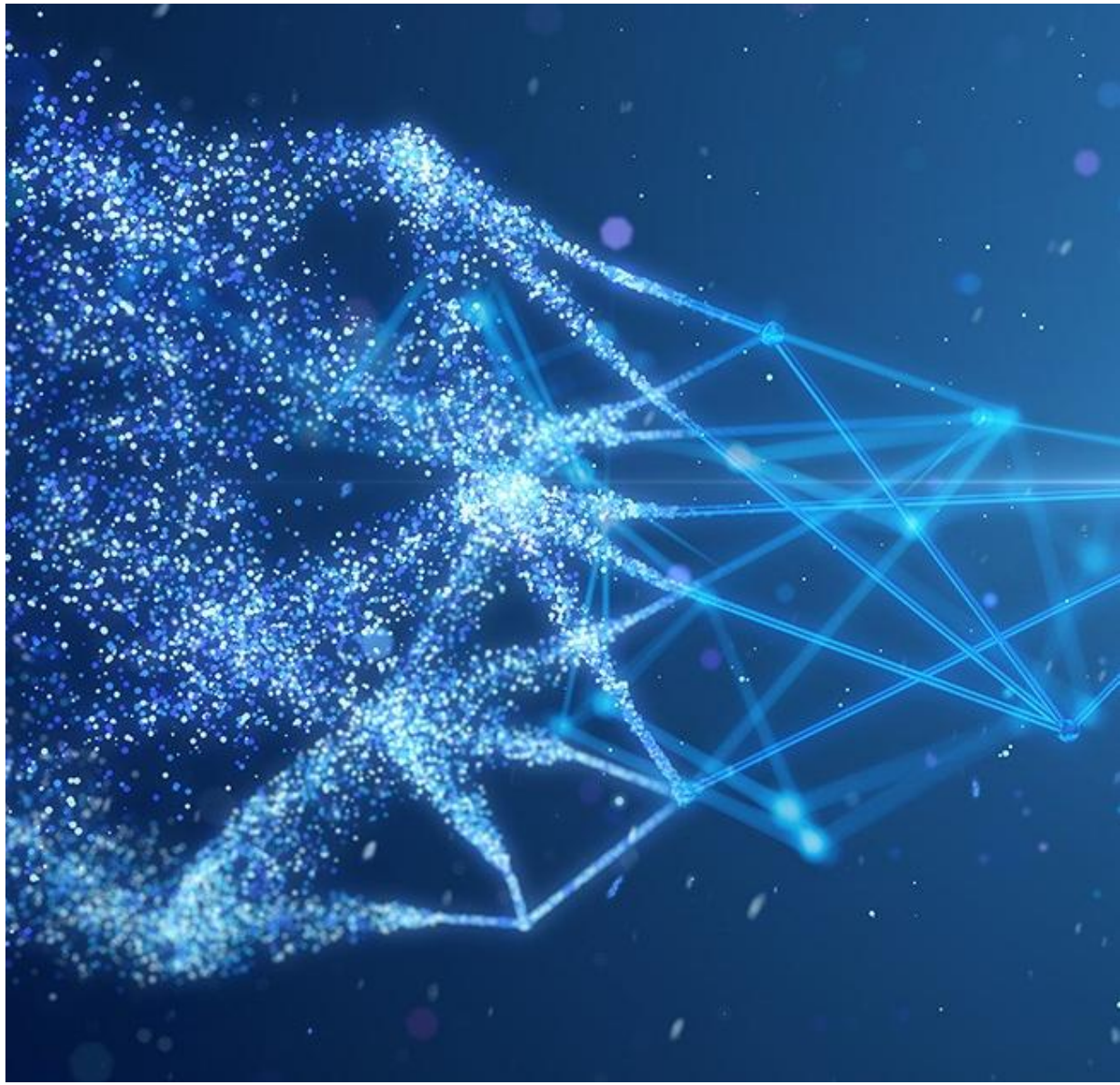
Privacy, Data Litigation, and Cybersecurity Governance

Recent Lessons and 2026 Expectations

Marcus McCutcheon

Jennifer L. Mitchell

March 5, 2026



Presenters

Jennifer Mitchell

Privacy Governance & Technology Transactions

Team Co-Lead | Partner

Los Angeles

jlmitchell@bakerlaw.com

Marcus McCutcheon

Digital Risk Advisory & Cybersecurity

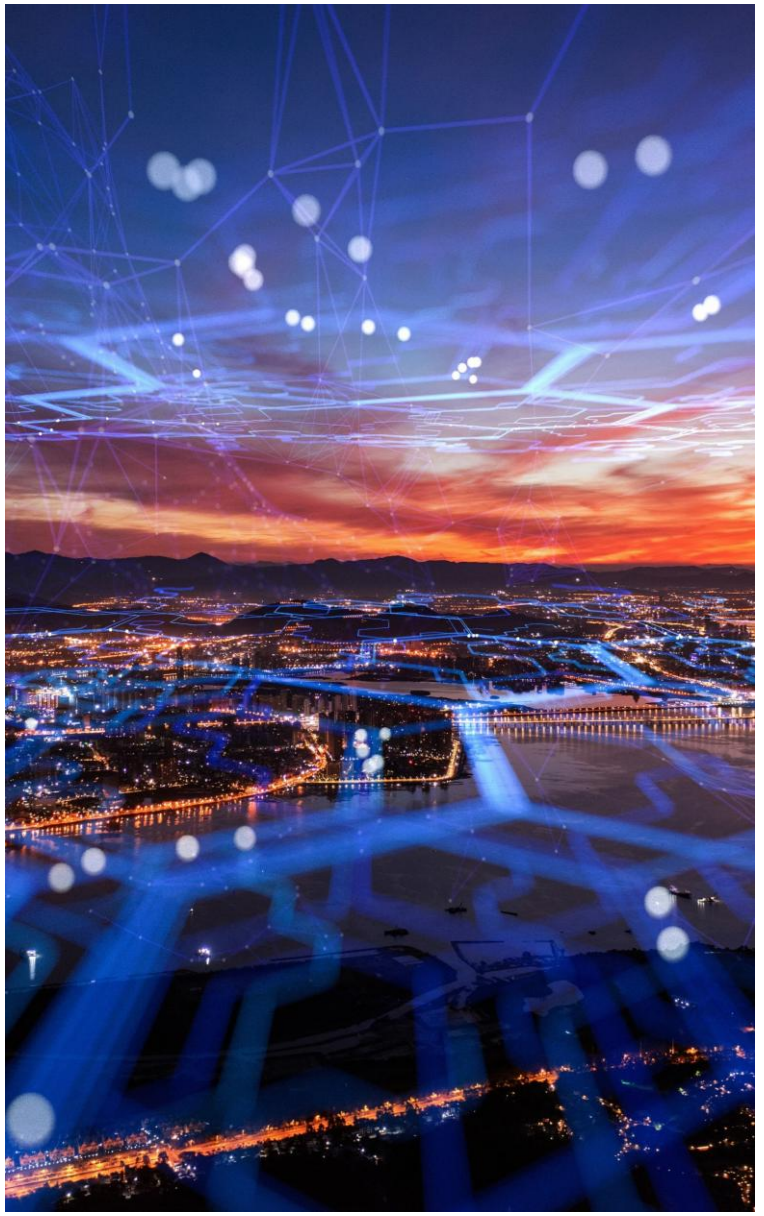
Counsel

Orange County

mmccutcheon@bakerlaw.com

Agenda

- California Privacy Governance & Compliance
- California Data Privacy Litigation Trends
- Cybersecurity Governance
- Incident Response & Incident Response Preparedness

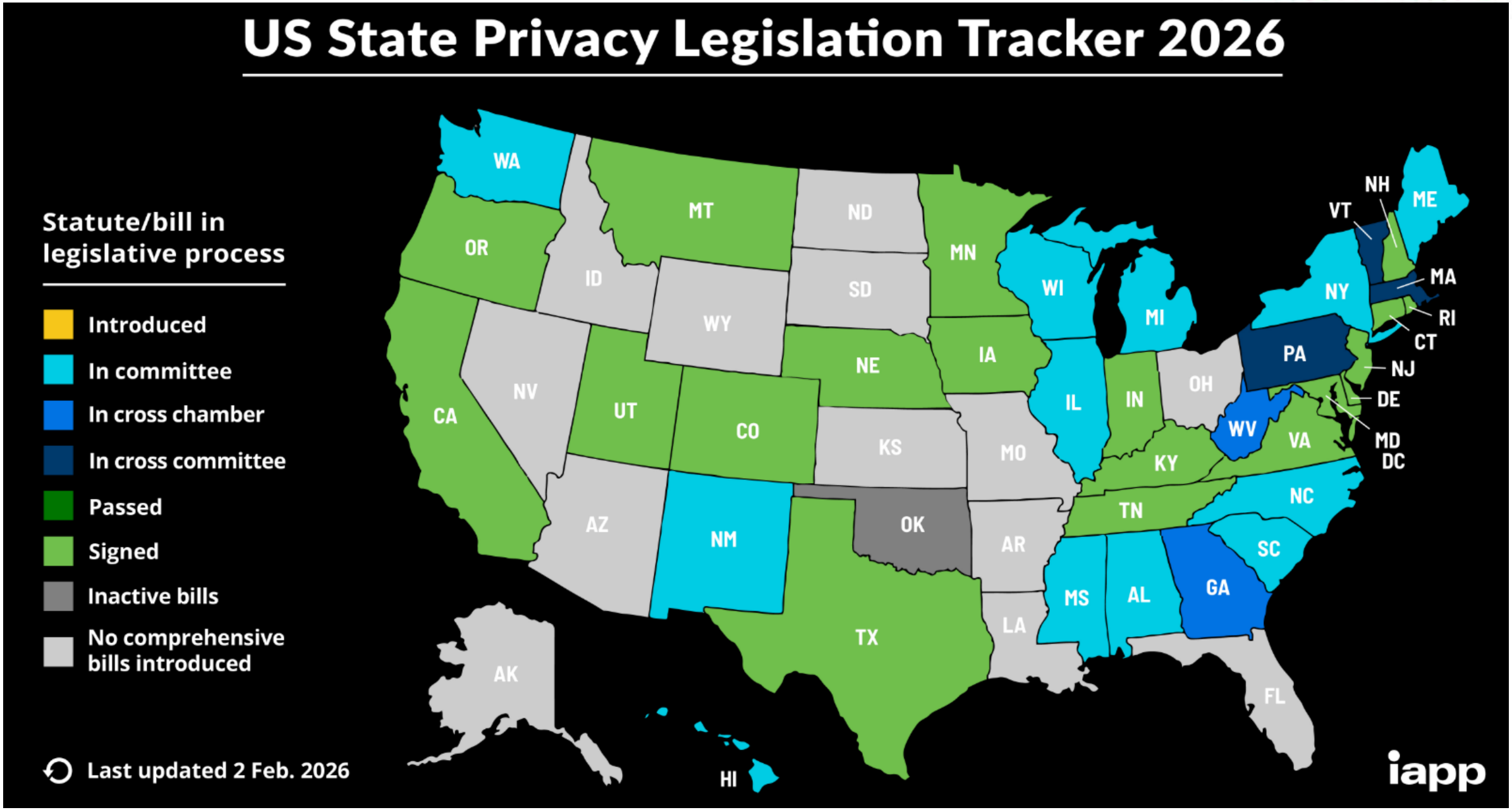


Privacy Governance & Compliance

Expansion of U.S. Privacy Laws

BakerHostetler

- Jan 1, 2020 – California Consumer Privacy Act (CCPA) went into effect; gave California residents data subject rights (Access, Delete, and Do Not Sell My Personal Information) and imposed new privacy obligations on businesses
- Jan 1, 2023 – the CCPA was amended, which increases the number of data subject rights, expands the scope to include all California employees (B2E), vendors and commercial customers (B2B), and imposes more stringent obligations on businesses
- In 2023, 4 more new state privacy laws went into effect in Virginia, Colorado, Connecticut, and Utah
- In 2024, 3 more new state privacy laws went into effect in Oregon, Texas, and Montana
- In 2025, 8 more new state privacy laws went into effect in Delaware, Iowa, Maryland, Minnesota, Nebraska, New Hampshire, New Jersey, and Tennessee
- In 2026, 3 more new state privacy laws went into effect in Indiana, Kentucky, and Rhode Island


US State Privacy Legislation Tracker 2026
Statute/bill in legislative process
Introduced
In committee
In cross chamber
In cross committee
Passed
Signed
Inactive bills
No comprehensive bills introduced
Last updated 2 Feb. 2026
WA
OR
CA
ID
NV
MT
WY
UT
AZ
CO
NM
ND
SD
NE
KS
OK
TX
MN
IA
MO
AR
LA
WI
IL
MI
IN
KY
TN
MS
AL
OH
WV
GA
FL
SC
NC
VA
PA
NY
VT
NH
ME
MA
RI
CT
NJ
DE
MD
DC
AK
HI
iapp

Mitigating Privacy Litigation & Enforcement Risks

- Website audits
- Privacy Notice Disclosures
- Accurate and adequate
- Tracking Technologies
- Use, disclosure, and opt outs
- Data Protection Agreements
- Service providers and processors
- Enforcement Priorities
- Honda, Healthline, Tractor Supply, Jam City, and Sling TV judgments (CPPA)

Enforcement Sweeps in California

- Opt-outs in mobile app context
- Loyalty programs
- Connected vehicles
- Streaming services
- Employee privacy

Automotive Manufacturer Enforcement Action

- Violations:
  - Required excessive identity verification for opt-out requests
  - Cookie preference center did not have symmetrical privacy choices (two steps to opt out, one step to opt-in)
  - Failure to maintain CCPA compliant contracts with ad tech vendors
- Remedies:
  - $632,500 fine
  - Certify its compliance, train its employees, and consult a user experience (UX) designer to evaluate its methods for submitting privacy requests
  - Change contracting process

Healthline Enforcement Action

- Violations:
  - Faulty “consent banner” that didn’t disable tracking cookies despite representing it would
  - Continued the sale and sharing of consumer PI after receiving opt-out requests
  - Violating the purpose limitation principle by using consumer PI inconsistent with the purposes for the initial collection (“sharing article titles suggesting consumer may have…a medical condition”)
  - Lack of CCPA-compliant third-party agreements
- Settlement terms:
  - $1.55 million settlement
  - Update all disclosures and correctly process opt-out requests
  - Disgorge all SPI collected
  - Prohibiting all sales of PI indicating a consumer viewed a specific article
  - Executing CCPA compliant contracts

Tractor Supply Enforcement Action

- Violations:
  - Failing to maintain privacy policy that notified consumers of their privacy rights
  - Failing to notify California job applicants of their privacy rights and how to exercise them
  - Failing to provide effective mechanism to opt-out (including through GPC)
  - Disclosing personal information to other companies without entering into contracts with privacy protections
- Settlement terms:
  - $1.35 million settlement
  - Scanning digital properties to inventory tracking technologies
  - Annual certification of compliance

Sling TV and Dish Media Supply Enforcement Action

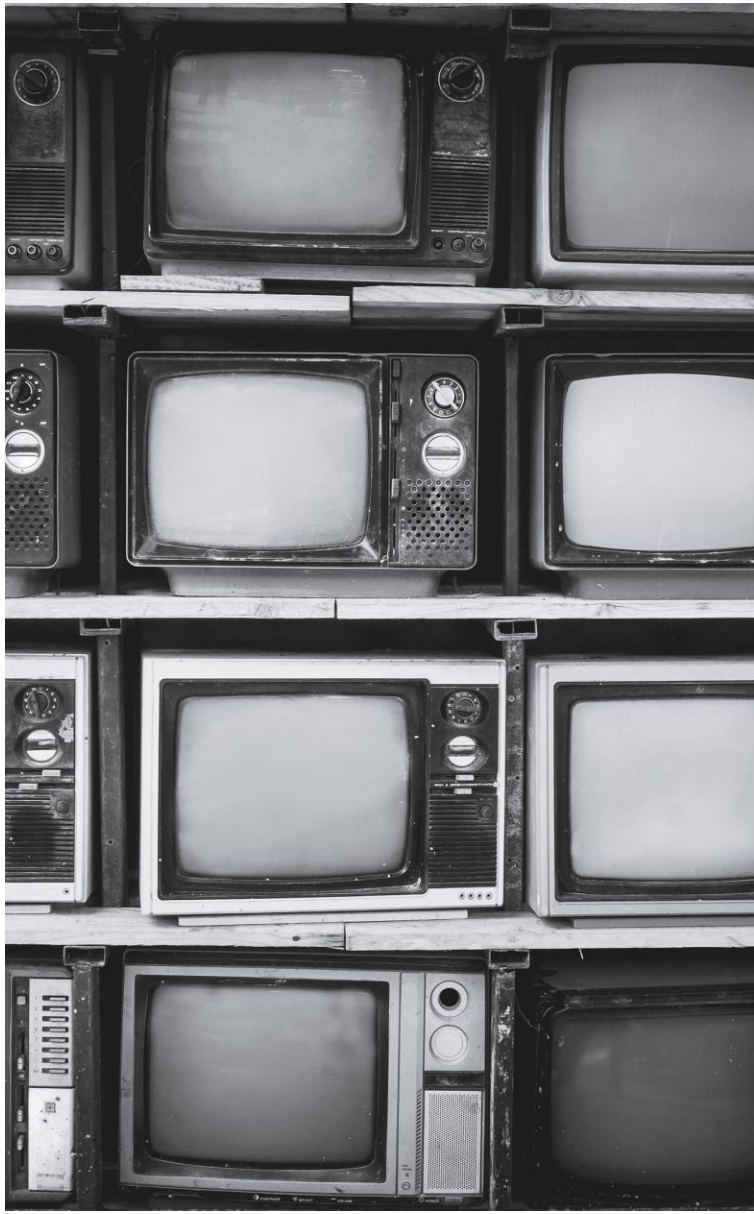
- Violations:
  - Failing to provide effective mechanism to opt-out, especially on its apps
  - Failing to provide sufficient privacy protections to children
  - Combined CCPA opt-out with cookie choices in a confusing way
- Settlement terms:
  - $530,000
  - Maintain an opt-out that's easy to use with minimal steps
  - "Kid's profiles" and other tools to minimize children's data

Jam City Enforcement Action

- Violations:
  - Failing to provide effective mechanism to opt-out in mobile gaming apps (no opt-outs in any of 21 apps)
  - Failing to provide sufficient privacy protections for children
    - Shared or sold data of children between ages 13 to 16 without affirmative consent
- Settlement terms:
  - $1.4 million
  - Provide in-app methods to opt-out of sale or sharing of data
  - No sale or sharing of personal information of consumers between the ages of 13-16 without obtaining affirmative “opt-in” consent

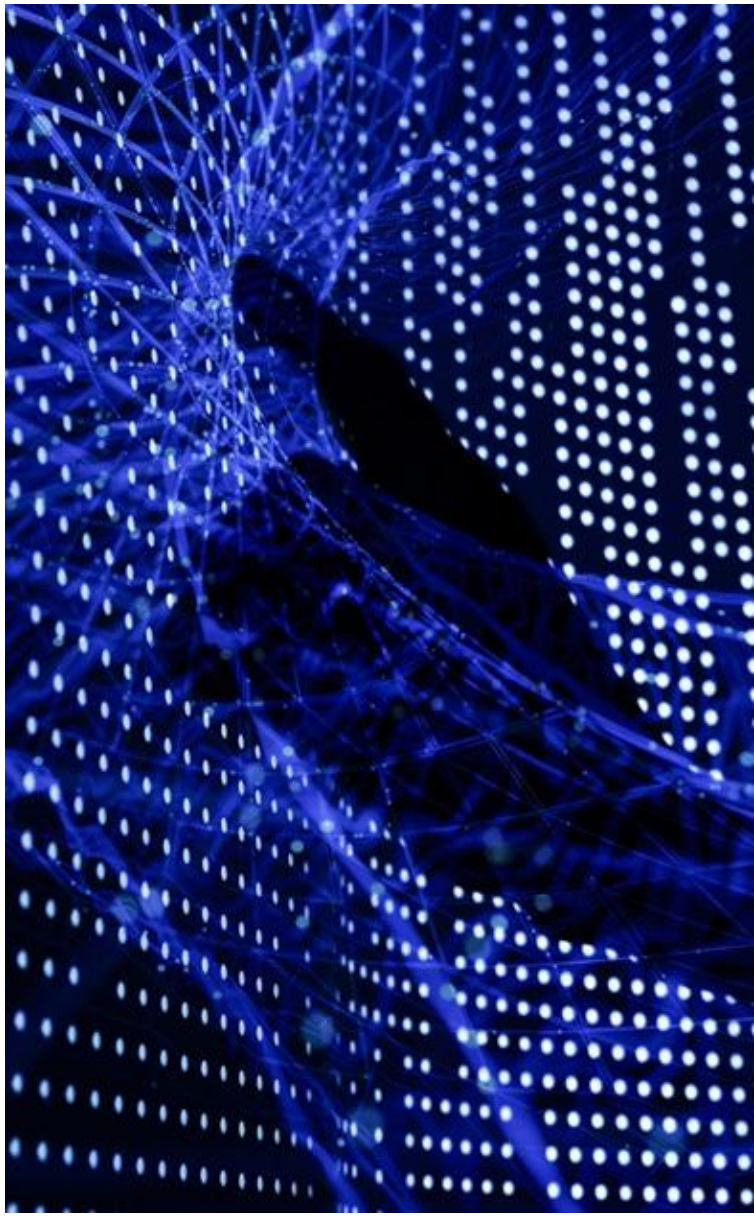
Disney Enforcement Action

- Violations:
  - Failing to provide effective mechanism across devices and services
  - Failing to provide opt out in connected TV streaming apps
- Settlement terms:
  - $2.75 million
  - Provide effective methods to opt-out of sale or sharing of data across devices and services



Regulatory Enforcement – Practical Takeaways

1. Exercising opt-out rights must be easy, symmetrical and effective
2. No identity verification for consumer opt-out requests
3. Ensure that compliant contracts are in place with ad tech vendors
4. Updating notices, keeping them accessible and understandable



Data Privacy Litigation Trends

Data Privacy Litigation Trends

BakerHostetler

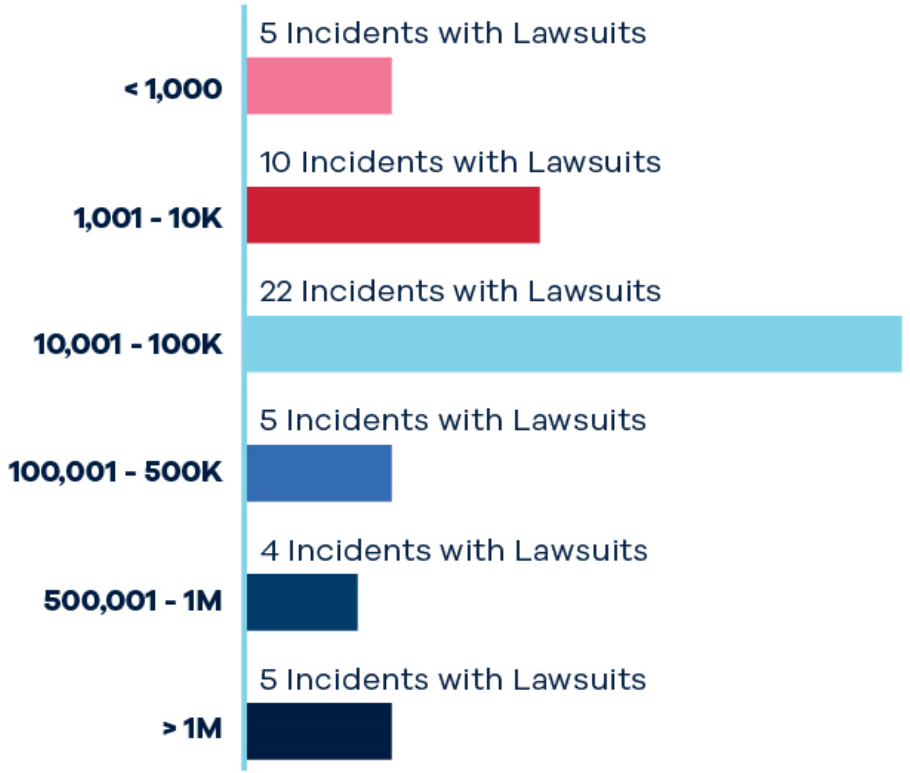
Incident to Litigation Pipeline

1,250+
Incidents Handled in 2024

518
Incidents with Notification

51
Incidents with Lawsuits

Number of Lawsuits by Notice Population Size



Why Privacy Matters…

BakerHostetler

In the past five years:

Defendant	Case	Wrongful Act	Amount Paid
Facebook	In re: Facebook, Inc. Consumer Privacy User Profile Litigation, Case No. 3:18-md-02843-VC (N.D. Cal.).	Data Sharing	$725,000,000
Comcast	Hasson v. Comcast Cable Communications LLC, Case No. 2:23-cv-05039-KMY (E.D. Penn.)	Data Breach	$117,500,000
Google	In re Google Referrer Header Privacy Litigation, Case No. Case No. 5:10-cv-4809-EJD	Data Sharing	$23,000,000
TikTok	In Re: TikTok, Inc., Consumer Privacy Litigation, MDL No. 2948	Data Collection	$92,000,000
Facebook	In re Facebook Biometric Information Privacy Litigation, Case No. 3:15-cv-03747-JD (N.D. Cal.)	Data Collection	$65,000,000

Data Breach Litigation

51
Incidents disclosed in 2024 resulted in one or more lawsuits filed
(compared to 58 in 2023)

- **44** Incidents involved SSNs
- **35** Incidents involved medical/health information
- **27** Incidents involved a healthcare organization
- **7** Incidents involved payment card data
- **32** Incidents involved a network intrusion
  23 of these incidents involved ransomware
- **14** Incidents started with an unpatched vulnerability
- **2** Incidents were vendor related

Maser v. Commonspirit Health (District of Colorado) dismissed because an alleged bank fraud was not fairly traceable to the breach despite allegations that the breach resulted in sensitive information being published on the dark web.

Stern v. Acad. Mortg. Corp. (District of Utah) dismissed despite allegations of a fraudulent loan made using a plaintiff's personal information because the plaintiff failed to show traceability between the data breach and the alleged injury.

McGowan v. Core Cashless (Western District of Pennsylvania) dismissed because the plaintiff did not plausibly allege that misuse of her payment card information was imminent despite allegations that "card numbers [are] for sale on the Dark Web whose common purchase point was [defendant]."

In re Samsung Data Sec. Breach Litig. (District of New Jersey) dismissed because the plaintiff could not establish that the specific information obtained in the data breach could not have been obtained elsewhere, e.g., from sources on the dark web unrelated to the data breach.

Williams v. Bienville Orthopaedic Specialists, LLC (Southern District of Mississippi) dismissed despite allegations of actual fraud and data misuse, reasoning that "[d]ata breaches and other forms of data theft are so prevalent that it is seemingly impossible to trace the misuse of personal information to one particular breach[.]"

Petta v. Christie Business Holding Co., P.C. (Illinois Supreme Court) affirmed dismissal, holding that the alleged harm, an unauthorized loan application, was not fairly traceable to a data breach because the loan application included only publicly available information, such as the plaintiff's name, phone number, and city and state of residence.

Weaponization of Arbitration

BakerHostetler

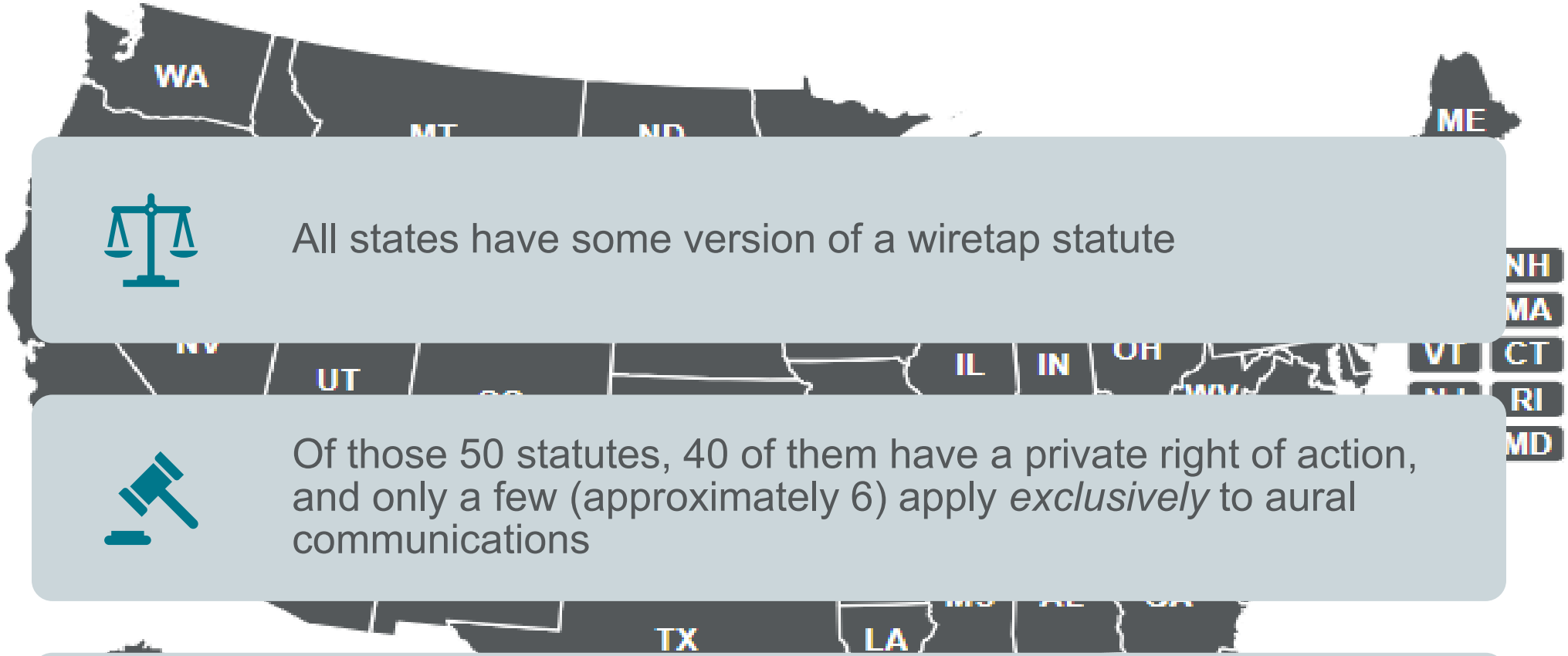
- Intended to manage cost, timing, and publicity of litigation
- Counsel are identifying cases involving:
  - A statutory privacy claim;
  - A company with online terms requring arbitration;
  - Thousands of individuals with data allegedly involved
- Once identified, counsel sends a demand letter threatening to file thousands of individual arbitration demands

Govern website interaction or specific transactions

Include provisions to limit mass individual arbitrations

Should include a stand-alone class action waiver

State Wiretap Statutes



All states have some version of a wiretap statute

Of those 50 statutes, 40 of them have a private right of action, and only a few (approximately 6) apply *exclusively* to aural communications

The majority of the statutes provide for either statutory damages (i.e., $5,000 per violation) or liquidated damages (i.e., $100 per day for every day during which the violation occurs)

What is Wiretap Litigation?

The Ninth Circuit gave rise to this litigation (at least in California) when it stated in *Javier v. Assurance IQ, LLC*, No. 21-16351, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) that "[t]hough written in terms of wiretapping, § 631(a) [of the California Invasion of Privacy Act (CIPA)] ***applies to Internet communications***."

Plaintiffs allege that companies violate CIPA (and other state wiretap statutes) through the use of three widely-used internet functionalities:

Chatbot	Session replay	Pixel Technologies

Wiretap Litigation: The Claims

BakerHostetler

California Invasion of Privacy Act (CIPA)

- § 631(a) – aiding and abetting wiretapping

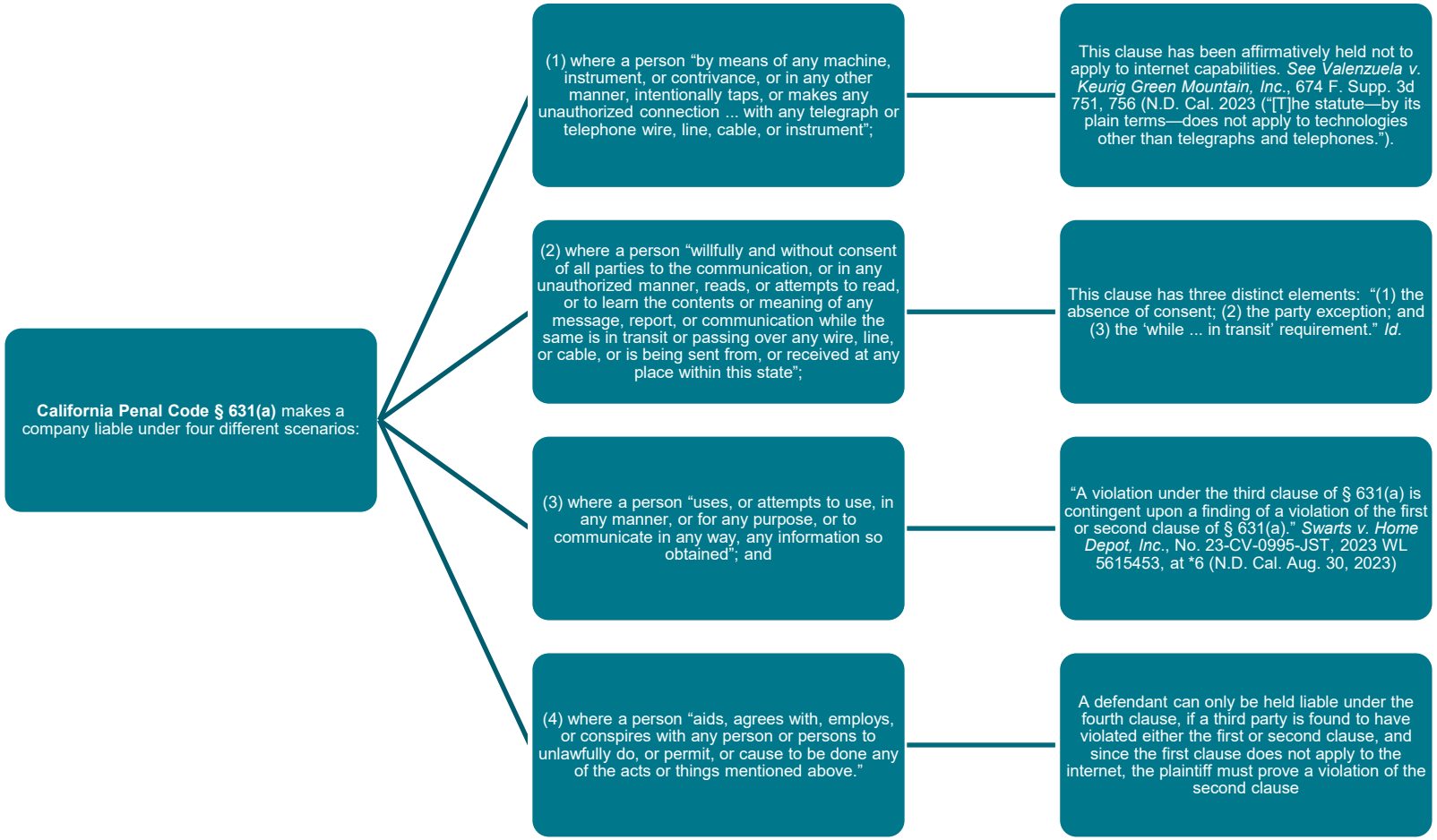
Invasion of Privacy

- Common law and Constitutional

Unfair Competition Law, Bus. & Profs. Code § 17200, *et seq.*

- Unfair, Fraudulent, and Unlawful

Wiretap Litigation: § 631(a) of CIPA



What is Pen-Trap Litigation?

- The Southern District of California gave rise to Pen-Trap litigation when it decided *Greenley v. Kochava, Inc.*, No. 22-CV-01327-BAS-AHG, 2023 WL 4833466 (S.D. Cal. July 27, 2023)
  - There, the Court stated that:
    - "Today, pen registers take the form of software."
    - "[T]he Court rejects the contention that a private company's surreptitiously embedded software installed in a telephone cannot constitute a 'pen register.'"

Wiretap vs. Pen-trap

- Wiretap – must show no consent for monitoring and that communications were captured
- Pen-trap – must show that pen register was used without consent or court order

What Is A Pen-Trap?

- A “Pen-Trap” is a term used to describe two different things: a “pen register” and a “trap-and-trace” device
  - **Pen Register:** a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication
  - **Trap-and-Trace Device:** a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication
- California law prohibits a person from “install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order” and arguably, **includes a $5,000 per violation statutory damages penalty**

Pen-Trap Litigation: Defenses

BakerHostetler

No Pen-Trap Device Installed or Used

- Pen-Traps can only be used on “telephonic devices”
- An IP Address cannot qualify as “dialing, routing, addressing, or signaling information”

Consent

- Voluntarily visiting a website necessarily includes the voluntary sharing of an IP Address

Public Policy

- Acceptance of Plaintiffs’ theory would, on the whole, make operating a website unlawful

Extraterritorial Application

- CIPA cannot apply to actions taken outside of California

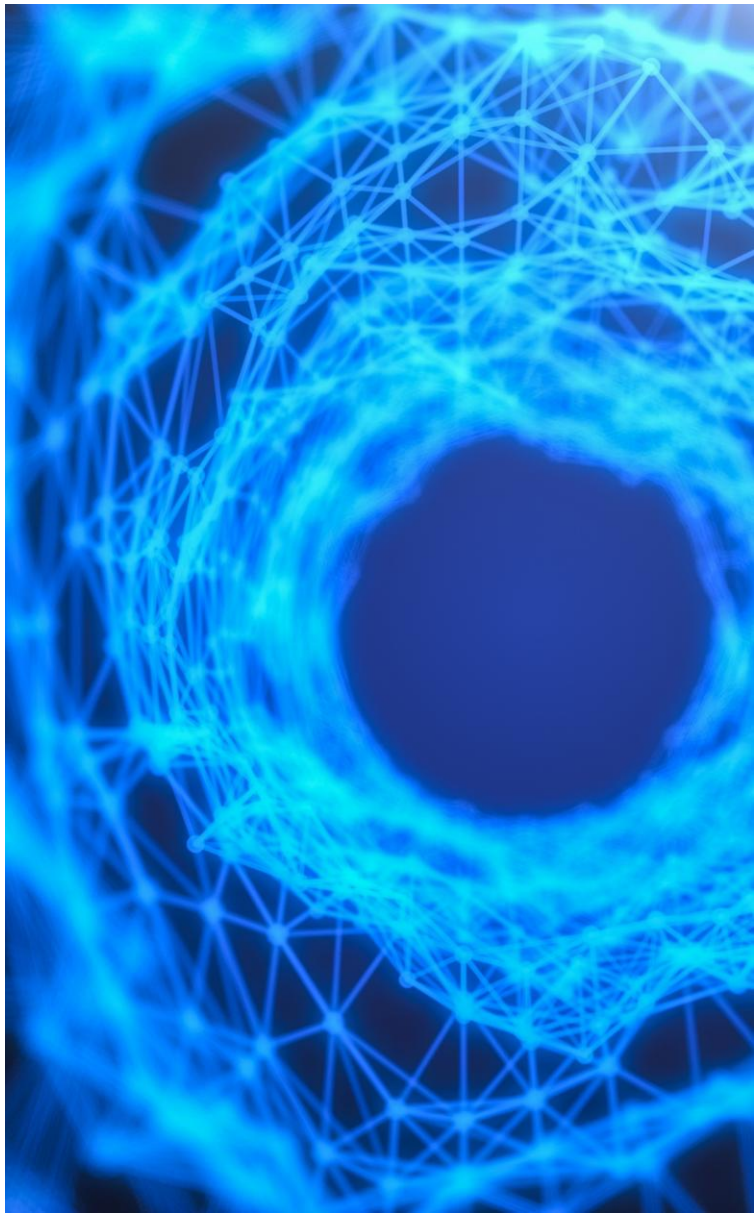
CCPA Cybersecurity Audits

Why This Matters

- Annual cybersecurity audits for certain CCPA-covered business
- CalPrivacy defines “reasonable security” in practice
- Applies where processing presents “significant risk”
- Audits must be thorough and independent

Who is in Scope?

- Driven by business model + data volume
- Applies beyond tech and data-native companies
- The business derives 50% or more of its annual revenues from selling or sharing customer personal information OR
- The business has annual gross revenues exceeding $26,625,000 (w/ periodic adjustments for inflation) AND
  - in the preceding calendar year processed the personal information of 250,000 or more consumers or households OR
  - the sensitive personal information of 50,000 or more consumers



Implementation Timeline – Overview

- Phased rollout from 2027-2029 based on revenue
- Certifications due 2028-2030 depending on tier
- Preparation should begin in 2025-2026
- Build governance muscle memory early

Implementation Timeline – Specifics

- The rule provides a phase implementation predicated on a business's gross revenue:
  - As of January 1, 2027 – businesses with an annual gross revenue over $100mm for CY 2026
    - Must complete an audit covering the 2027 calendar year with certification by April 1, 2028
  - As of January 1, 2028 – businesses with an annual gross revenue between $50mm and $100mm for CY 2027
    - Must complete an audit covering the 2028 calendar year with certification by April 1, 2029
  - As of January 1, 2029 – businesses with an annual gross revenue under $50mm for CY 2028
    - Must complete an audit covering the 2029 year with certification by April 1, 2030
- After the first audit, a business must complete an audit for any year in which it meets the application criteria for the Rule as of January 1 of that year

Auditor Independence and Governance

- Auditor must be qualified, objective, and independent
- Permissible to use an internal or external auditor; must have expertise in both cybersecurity and auditing
- Businesses that use an internal audit, such auditor must report to a member of executive management outside cybersecurity leadership
- Business must make available to auditor all information requested by the auditor

Reasonable Security – The Baseline

- Authentication Controls – strong authentication/use of MFA for employees, contractors, and service providers
- Encryption – of personal information both at rest and in transit
- Access control – least privilege access to individuals, accounts, or applications; limit number of privileged accounts/creation of new accounts

Reasonable Security – Data & Vulnerability Management

- Data inventory and data flow mapping – maintaining an inventory of data flows
- Secure configuration
- Patch management
- Vulnerability management – internal and external vulnerability scans, pen testing, and vulnerability disclosure and reporting

Reasonable Security – Monitoring & Containment

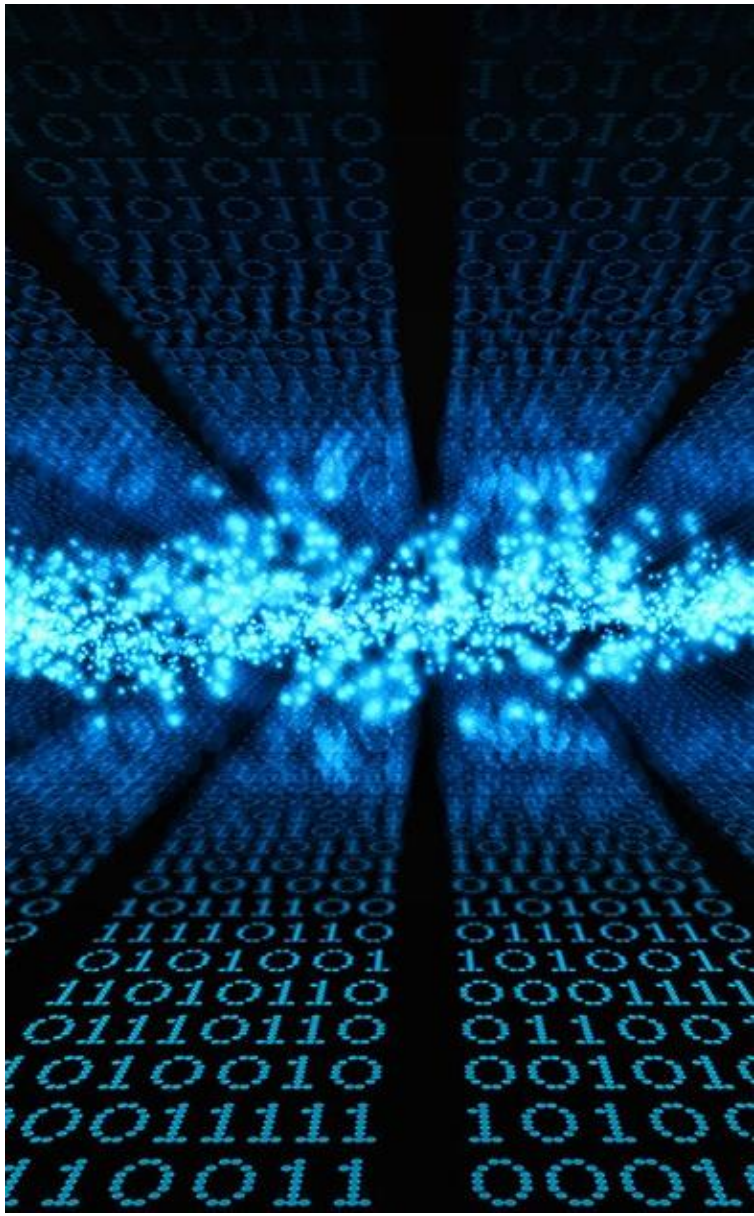
- Logging & Monitoring – centralized logging with meaningful retention
- Deployment of intrusion detection and prevention tools
- Data loss prevention tools
- Malware protection
- Systems Segmentation

Reasonable Security – People & Supply Chain

- Training and awareness – ongoing cybersecurity education and training
- Secure development lifecycle
- Vendor Management – oversight over service providers, contractors, and third parties to ensure compliance with contractual and legal obligations; “third parties are part of the security perimeter”

Reasonable Security – Data Lifecyle & Incident Response

- Information Governance – data retention schedules and secure disposal
- Incident Response – documented incident response plan, regular testing of incident response capabilities
- Regular enterprise-wide testing with executive leadership involvement required



How Will Auditors Judge You?

- Controls – implemented and enforced?
  - Tailored to size, data, and risk profile?
  - Auditor must determine which controls are appropriate
- Gaps – identified and remedied? On what timetable?
- Policies – necessary but not sufficient

Audit Artifacts – "*show your work*"

BakerHostetler

- Audit Report – evidence-based audit report
- Testing, interviews, and documentation
  - Cannot rely on management assertions alone
- Gaps – report must detail identified gaps/weakness and business's plan to remediate
- Auditor Certification – auditor must certify as to impartiality and independence of audit
- Executive Certification – must submit a written certification of completion signed by executive with direct responsibility for cybersecurity audit compliance

Enforcement Reality Check – 23 NYCRR 500 (NYDFS)

- $19M+ in penalties (2025): Eight auto insurers fined for cybersecurity failures and data exposure
- $2M+ penalty (2025): Peer-to-peer payment processor for breach exposing unmasked SSNs
- $2M fine (2025): Fintech company for cybersecurity control failures
- $1M settlement (2023): Title insurance and settlement services company for governance/control breakdowns
- Enforcement is governance-driven – audit and control failures become evidence

BakerHostetler

bakerlaw.com

Atlanta | Austin | Chicago | Cincinnati | Cleveland | Columbus | Dallas

Denver | Houston | Los Angeles | New York | Orange County | Orlando

Philadelphia | San Francisco | Seattle | Washington, D.C. | Wilmington