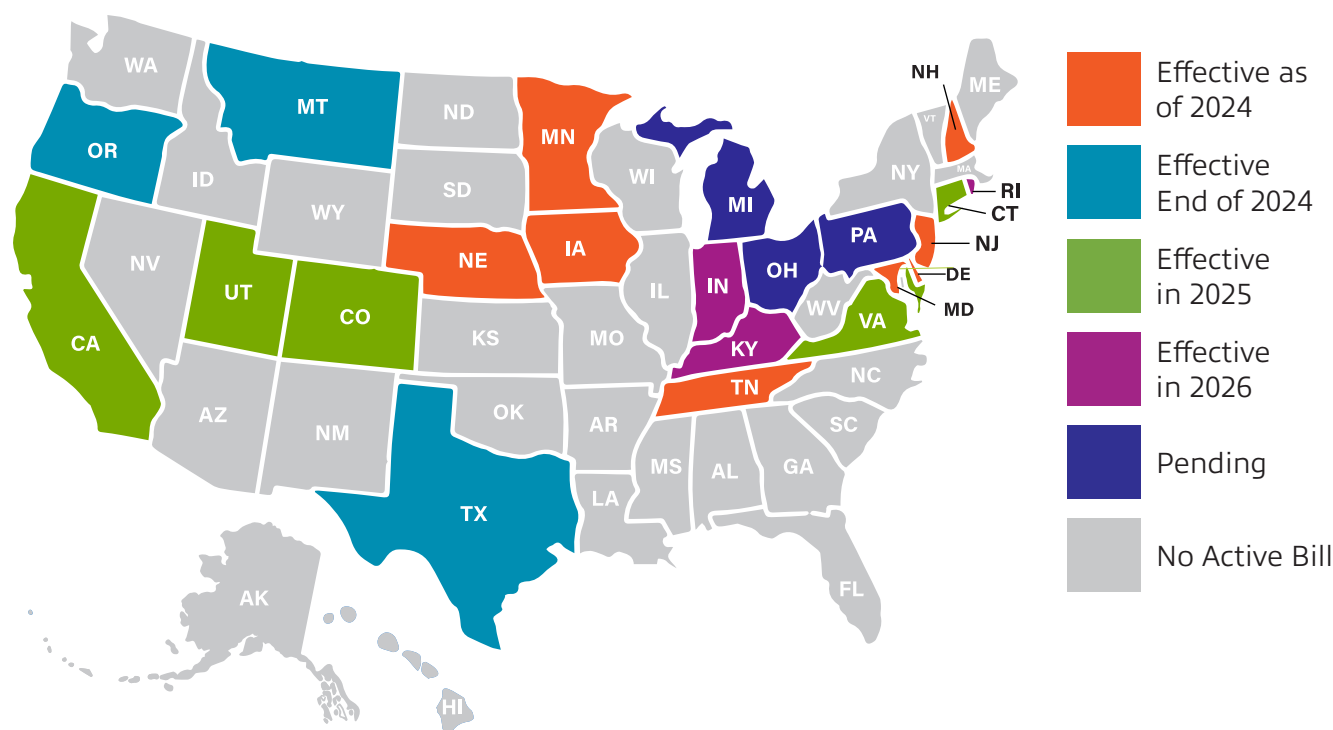


Cybersecurity, Data Privacy & AI Compliance – A Year in Review and What’s Ahead for 2025 & Beyond

As the digital landscape continues to evolve, so does the regulatory environment surrounding cybersecurity, data privacy, and artificial intelligence (AI). In a recent webinar hosted by Brooks Kushman, experts John Rondini, James Bertino, Abha Fadipe, and Muhammad Siwani provided an in-depth review of the current state of these critical areas and a forecast of what to expect in 2025 and beyond.

THE DRUMBEAT OF CHANGE IN U.S. PRIVACY LAWS

The U.S. has seen a surge in state-level privacy legislation since 2020, with 18 states enacting various laws to protect consumer data. By 2024, several states have introduced new regulations, setting thresholds for businesses based on jurisdiction and data collection practices. These laws vary significantly, with some states like New Jersey providing no exemptions for specific data types, highlighting a trend of increasing divergence in privacy legislation across the U.S.



As another example of diverging policies, each U.S. state privacy law has distinct applicability criteria, typically defined by an entity’s jurisdiction, revenue, data processing volume, and revenue derived from selling personal data. While most states require entities to meet specific personal data processing thresholds—ranging from 35,000 to over 100,000 consumers—Nebraska and Texas stand out by imposing no such thresholds. Instead, companies operating within these states are subject to their privacy laws if they process any consumer personal data.

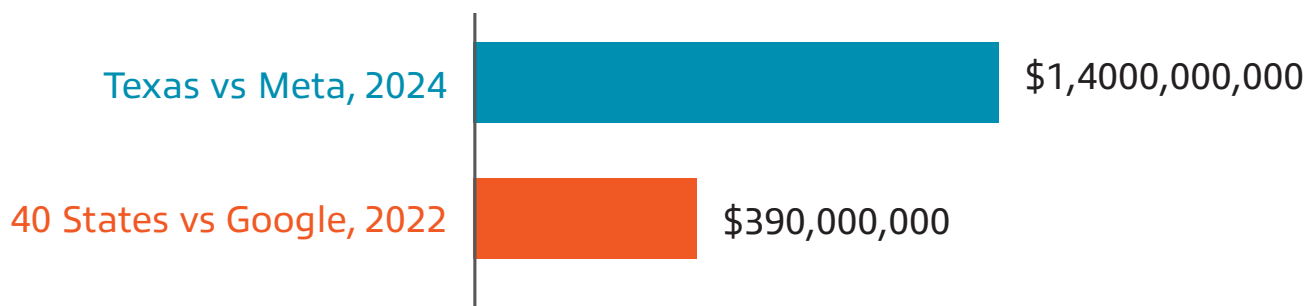
As a result, businesses must navigate a complex landscape of requirements, including providing detailed privacy notices, limiting data collection, and upholding consumer rights.

Rights to Access, Correct, and Delete Data	Opt-Out Options Required in Most States	Private Right of Action
All states: Right to access, correct, and delete personal data. Exceptions: - Iowa & Utah: No right to correct personal data. - Indiana: Can only correct consumer-provided data. - Utah: Can only delete consumer-provided data.	For: - Targeted advertisements - Sale of data - Profiling Exceptions: - Iowa: No opt-out required for targeted ads and profiling. - Utah: No opt-out required for profiling.	- Allowed: California. - Not Allowed: All other states.

ENFORCEMENT AND CONSUMER RIGHTS

State Attorneys General have assumed a vital role in protecting citizens' privacy rights by enforcing both longstanding and newly enacted laws. Leading the charge is Texas, which secured a landmark \$1.4 billion settlement with Meta for the unauthorized collection of biometric data, a violation of the state's Deceptive Trade Practices Act (DTPA). Building on this momentum, Texas has recently initiated investigations into more than a dozen companies for potential breaches of children's privacy and safety regulations. In addition to leveraging established laws like the DTPA, the state is also citing violations of the newly enacted Texas Data Privacy and Security Act.

Largest privacy-related fines brought forward by states, 2022 and 2024



This marks a significant escalation in privacy enforcement, with states increasingly leveraging expanded tools to hold corporations accountable for privacy violations.

CIPA LITIGATION AND ITS IMPACT ON PRIVACY ENFORCEMENT

California has seen a surge in litigation under the California Invasion of Privacy Act (CIPA), driven by claims that businesses' use of tracking technologies such as search bars, cookies, and pixels, violates state wiretapping laws.

of cases filed in 2024 involving tracking technologies from:



398



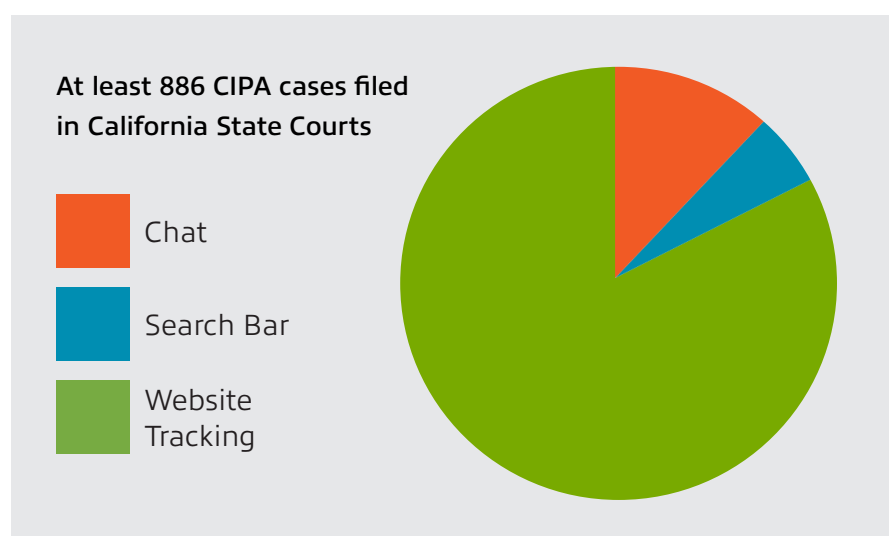
227



227

Plaintiffs argue that these tools intercept electronic communications without proper consent, despite many being widely accepted in online commerce. CIPA litigation is particularly active because California requires all parties to consent to communications being recorded, unlike states that allow recording with only one party's consent. Many CIPA claims conflict with state privacy laws, such as the California Consumer Privacy Act (CCPA), which permits businesses to collect data for targeted advertising as long as consumers are given the right to opt out. Despite these inconsistencies, businesses face increasing

litigation risks due to CIPA's statutory damages, which allow plaintiffs to seek penalties without proving actual harm.



Other states with similar all-party consent wiretapping laws, such as Pennsylvania, Massachusetts, Washington, and Florida, have also seen rising litigation. Given this trend, more states may adopt private rights of action, allowing consumers to sue companies directly.

FEDERAL INITIATIVES: A UNIFIED APPROACH?

The American Privacy Rights Act (APRA) of 2024 proposes a more unified approach to privacy regulation at the federal level. By emphasizing data minimization, privacy by design, and enhanced protections for sensitive data, the act seeks to preempt the fragmented state laws with a cohesive framework, aiming to simplify compliance for businesses while strengthening consumer rights. However, the APRA remains under review by the House Committee on Energy and Commerce, facing obstacles such as concerns over preempting stricter state laws and ongoing debates about its enforcement mechanisms.

THE RISE OF CONSUMER HEALTH DATA LAWS

New consumer health data (CHD) laws in states like Washington and Nevada have broadened the definition of protected health information, exceeding traditional HIPAA guidelines. These laws require explicit consent for non-exempt uses of CHD, impose geofencing prohibitions, and grant private rights of action, signaling a shift towards more robust consumer health data protections.

Scope

- Operating in **Washington** or **Nevada**
- Targeting consumers in these states
- Includes **non-residents' CHD** collected in-state
- **Small Business Grace Period (Washington only):** Until June 30, 2024

Broad CHD Definitions

Includes:

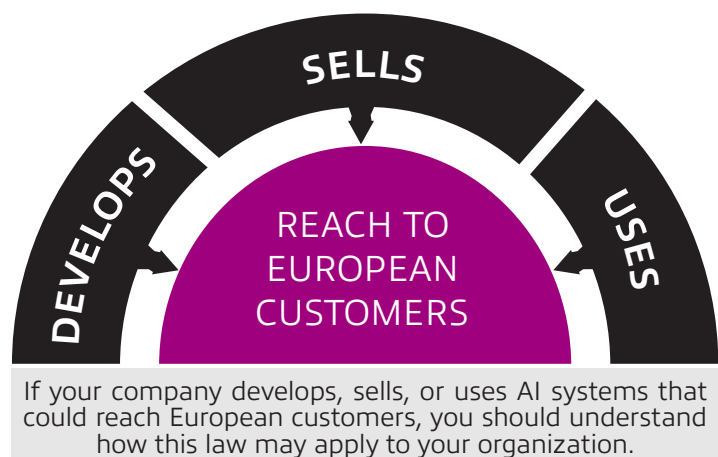
- Health conditions, symptoms, vital signs
- Inferences from non-health data
- Location data linked to health services

Exclusions:

- Deidentified data (but collection for deidentification is regulated)

AI GOVERNANCE AND COMPLIANCE

As AI technologies increasingly integrate into business operations, regulatory frameworks are becoming more stringent. The EU AI Act, which will begin implementation in 2025, classifies AI systems by risk level, imposing strict requirements on high-risk applications. Similarly, South Korea's National Assembly has passed the AI Basic Act, a comprehensive legal framework designed to foster AI development while upholding ethical standards and public trust. This Act is set to take effect in January 2026.



In the absence of federal legislation, states like Utah, Colorado, and California have introduced laws requiring transparency measures and impact assessments for AI systems, striving to balance technological innovation with ethical accountability. Notably, Utah provides specific regulations targeting both licensed professionals and general business interactions involving Generative AI (GenAI), Colorado focuses on regulating high-risk AI systems—those that significantly impact critical decisions affecting

individuals' lives, and California integrates AI transparency with personal information and intellectual property considerations.

To help companies navigate diverse legal obligations, the National Institute of Standards and Technology (NIST) introduced the AI Management Framework. This framework highlights the importance of AI system trustworthiness and provides key activities and strategies for managing risks effectively.

CHILDREN'S PRIVACY LAWS: EXPANDING PROTECTIONS

Efforts to protect minors online are expanding, with new state laws extending the protections of the Children's Online Privacy Protection Act (COPPA) to include teenagers up to age 17. Some of these regulations mandate stricter default privacy settings for online platforms and provide tools for children and parents to manage personal information, highlighting a growing focus on safeguarding younger users in the digital environment.



The FTC ramped up enforcement against unfair and deceptive digital practices, focusing on sensitive data misuse and dark patterns. A key shift was the agency's increasing use of unfairness claims to combat privacy violations. In February, the FTC fined Avast \$16.5 million for falsely marketing its antivirus software as privacy-protecting while secretly collecting and selling user data, including location data. Later, the agency took action against Gravy Analytics and Venntel, barring them from selling sensitive location data after they unlawfully tracked consumers, including visits to health-related locations and places of worship.

The FTC also cracked down on dark patterns, deceptive design tactics that manipulate users. In 2024, the agency sued Adobe, alleging it misled consumers into annual paid monthly subscriptions by burying a 50% early termination fee (ETF) in fine print. The case follows an ongoing lawsuit against Amazon, set for trial in 2025, over deceptive subscription and cancellation processes. These enforcement actions reflect the FTC's growing focus on privacy violations and consumer manipulation, signaling tougher scrutiny on companies that exploit user trust.

LOOKING AHEAD

As regulatory scrutiny intensifies, 2025 is likely to see stricter enforcement of data minimization and privacy by design. Businesses will face greater obligations to limit data collection, processing, and retention strictly to necessary purposes, reducing excessive data use. Individual rights, including access, correction, deletion, and data portability, will become a central focus, requiring companies to implement more transparent data management practices.

Sensitive data protections, especially for health and financial data and minors under 17, will likely drive heightened FTC and state enforcement actions. Companies handling such data should expect increased compliance burdens and potential liability under federal and state oversight, as well as private rights of action. If federal privacy legislation advances, state law preemption could reshape compliance frameworks, replacing the current patchwork of state regulations with a unified standard. However, with ongoing debates over enforcement authority and exemptions, businesses should prepare for a transition period marked by regulatory uncertainty.

The regulatory landscape for cybersecurity, data privacy, and AI compliance will continue to evolve rapidly. Businesses must stay vigilant, adapting to new laws and enhancing their compliance strategies to navigate this complex environment effectively. The insights from Brooks Kushman's experts underscore the importance of proactive engagement with emerging regulations to mitigate risks and seize opportunities in the digital age.

Panelist Contacts



John Rondini

Co-Chair Cybersecurity,
Data Privacy, and AI
(248) 226-2913

jrondini@brookskushman.com



James Bertino

Shareholder
(248) 226-2895

jbertino@brookskushman.com



Abha Fadipe

Shareholder
(248) 226-2919

afadipe@brookskushman.com



Muhammad Siwani

Associate
248-226-2871

msiwani@brookskushman.com