troutman pepper locke

PRIVACY + CYBER PRACTICE

2024 Privacy, AI & Cybersecurity Year in Review

Table of **contents**

Introduction

Traditional and Emerging Legal Frameworks Converge in the New Data Economy

2024 was a pivotal year in the regulation of data practices, with increased scrutiny of artificial intelligence (AI), data brokers, and the ecosystem of commercial data, and the continued proliferation of comprehensive United States (US) state privacy laws with bespoke twists such as expanded protections for teen data. While new laws created headlines, existing laws and consumer protection frameworks proved equally important in shaping the regulatory landscape, especially in the U.S. This convergence, in conjunction with uncertainty around the priorities of key federal agencies such as the Federal Trade Commission (FTC), presents challenges and opportunities for organizations, particularly those that depend on the data broker ecosystem or data broker services.

TROUTMAN PEPPER LOCKE

Contributors

Ronald I. Raether, Jr.

Partner

ron.raether@troutman.com

949.622.2722

James Koenig

Partner

jim.koenig@troutman.com

610.246.4426

Theodore P. Augustinos

Partner

ted.augustinos@troutman.com

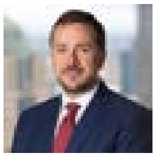
860.541.7710

Tambry Lynette Bradford

Partner

tambry.bradford@troutman.com

213.928.9805



Joshua D. Davey

Partner

joshua.davey@troutman.com

704.916.1503

Laura Hamady

Counsel

laura.hamady@troutman.com

312.759.8880

Brent T. Hoard

Partner

brent.hoard@troutman.com

470.832.5573

Joel M. Lutz

Counsel

joel.lutz@troutman.com

404.832.6007

Sadia Mirza

Partner

sadia.mirza@troutman.com

949.622.2786

Kim Phan

Partner

kim.phan@troutman.com

202.274.2992

James Shreve

Partner

james.shreve@troutman.com

312.443.0656

Julie Hoffmeister Smith

Partner

julie.hoffmeister@troutman.com

804.697.1448

Molly McGinnis Stine

Counsel

molly.mcginnisstine@troutman.com

312.443.0327

Angelo A. Stio III

Partner

angelo.stio@troutman.com

609.951.4125

Kenneth K. Suh

Counsel

kenneth.suh@troutman.com

312.443.0640

Tara L. Trifon

Counsel

tara.trifon@troutman.com

860.541.7740

Peter T. Wakiyama

Partner

peter.wakiyama@troutman.com

215.981.4538

Trends to Watch in 2025

Looking in the 2024 Rearview Mirror to Develop a Key Action Item Roadmap for 2025

Trend One – AI Meets Everything

As consumers, businesses, and the markets began to navigate a world newly imbued with AI, the regulatory landscape underwent a seismic shift in early 2024 with the adoption of the European Union's AI Act (EU AI Act), establishing the first comprehensive framework for AI governance globally. This watershed moment, combined with the enactment of the Colorado AI Act at the U.S. state level, evolving U.S. federal activity on AI, including three executive orders (EOs) under the Biden administration,[1] the AI Training Act, and the National AI Initiative, as well as the newly issued and still-forthcoming Trump EOs, created a complex compliance environment that has led many companies to seek an integrated and consolidated approach to compliance.

- **Regulatory Convergence.** The EU AI Act's risk-based approach to AI system categorization has emerged as a de facto global standard and has forced organizations to reassess their privacy frameworks and governance structures. This risk-based regulatory framework requires organizations to demonstrate robust governance of AI systems while maintaining stringent privacy protections. In response, companies are transforming how they approach their privacy documentation, risk assessment processes, and governance structures.
- **Reshaping Privacy Documentation for the AI Era.** Traditional privacy policies and terms of service must evolve to address the unique challenges posed by AI systems. Organizations are updating their privacy policies and terms of service to clearly articulate how AI processes personal data, explain

[1] In 2024, President Biden issued three executive orders related to AI: (1) Maintaining American Leadership in Artificial Intelligence, (2) Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government, and (3) The Safe, Secure, and Trustworthy Development and Use of AI.

automated decision-making mechanisms, delineate user rights regarding AI-driven processes, allocate AI-related risks, and address emerging IP ownership issues, among other topics. This transparency extends beyond mere compliance – it builds trust with stakeholders and establishes clear expectations for AI system deployment. Organizations must carefully balance innovation with risk management, establishing clear boundaries for AI system use while maintaining operational flexibility – for example, when updating their terms of service agreements to address novel concerns around AI-generated content, liability frameworks, and dispute resolution mechanisms.

- **Building an Integrated Governance Framework.** Successful AI governance requires a coordinated approach that bridges technical, legal, and operational considerations. To build governance for AI, many companies are establishing a cross-functional AI governance body that includes privacy, legal, security, IT, and business unit leadership. Such a governance body can serve as the central nervous system for AI-related decision-making, ensuring consistent risk assessment and rapid response to regulatory changes by overseeing and coordinating data governance in a comprehensive and strategic way to account for AI's unique characteristics to ensure that tasks that are owned by distinct functions work together. Three key examples of the types of activities that, when coordinated, allow many companies to achieve outsized compliance impact with minimal business interruption are risk assessments, data governance activities, and incident management.
    - **Example One:** Expanding traditional privacy impact assessments (PIAs or DPIAs) that are required under most comprehensive privacy laws to encompass AI-specific considerations.[2] Organizations need to evaluate algorithmic bias, transparency of decision-making processes, usage rights, and training requirements for data sources, particularly those sourced from data brokers, and potential unintended consequences of AI deployment. This enhanced risk assessment protocol should be integrated into existing privacy frameworks to create a unified approach to risk management.
    - **Example Two:** Conducting data protective activities to strategically maintain privacy and security throughout the AI lifecycle while enabling innovation and operational efficiency. Activities that can be overseen by an AI governance body include maintaining dynamic data maps and system inventories, establishing model training controls, and implementing robust monitoring systems.
    - **Example Three:** Considering AI systems in all aspects of the incident response planning process. Organizations must prepare for novel scenarios involving AI-related security events and privacy incidents, establishing clear escalation procedures and communication protocols. This preparation ensures rapid response to incidents while maintaining stakeholder trust.

Trend Two – State Privacy Laws Continue to Grow in Number, Complexity

The U.S. state privacy law landscape expanded significantly in 2024, growing to a total of 19 states with statutes, and eight states with enforceable laws, in some cases with broad applicability and compliance obligations.[3] For example, Oregon and Texas joined the ranks of U.S. states with both comprehensive privacy legislation and data broker regulations. The expansion will continue for the foreseeable future, and the impact will continue to grow. For example, already in 2025, five state privacy statutes previously passed have come into effect, with three additional laws coming into force by the end of the year.

[2] This will also meet certain AI laws' requirements, such as those of the CO AI Act.

[3] Most U.S. state privacy laws only apply if an organization meets a specific revenue threshold, data processing threshold, and/or is not a small business. However, the types of exemptions and the thresholds to meet those exemptions differ depending on each state. For example, the Oregon Consumer Privacy Act applies only to businesses that process 100,000 or more consumers' personal data or process 25,000 or more consumers' data and that derive 25% or more of their annual gross revenue from the sale of that data. Or. Rev. Stat. § 646A.572(1). Further, the Oregon Consumer Privacy Act and the Texas Data Privacy and Security Act have exemptions for protected health information processed under the Health Insurance Portability and Accountability Act, data processed solely for employment purposes, activities involving collecting or using information in relation to a consumer's credit, and information collected and disclosed in accordance with certain federal laws. Or. Rev. Stat. § 646A.572(2), TX BUS & COM § 541.003.

- **The Dawn of Teen Privacy.** The Children's Online Privacy Protection Act (COPPA), a federal law protecting the online privacy of minors under the age of 13 in the U.S., has been the singular law protecting children's privacy in commercial contexts. Until the California Consumer Privacy Act (CCPA) provisions extending new protections to minors between the ages of 13 and 16, most organizations that did not have child-directed sites or services did not feel the need to dedicate compliance resources specifically focused on children's privacy. Today, the majority of the 19 states with comprehensive privacy laws require specialized treatment of personal data collected from minors between the ages of 13 and 18 – depending on the state. To further complicate the compliance landscape, the FTC recently finalized its first amendments to the COPPA Rule, expanding requirements for verifiable parental consent, including for targeted advertising; placing limits on data retention; and enhancing disclosure obligations.

> In the meantime, companies should continue focusing on understanding their automatic online data collection and governing their data risks through good data governance practices, including by conducting DPIAs and actively managing inventories of online trackers.

- **Automated Decision-Making and Profiling Practices.** A key theme emerging across U.S. state privacy frameworks is the increasing focus on automated decision-making and profiling practices. States have adopted varying approaches to what constitutes automated decision-making requiring special handling, ranging from decisions affecting financial or housing opportunities to those impacting employment or education.[4] These differences in scope and threshold requirements create challenges for organizations operating across multiple jurisdictions. With several states now requiring documented evaluation of algorithmic impacts before deployment, companies are watching as the trend toward mandatory assessments for automated systems gains momentum and increasingly aligns in important ways with the increased focus and regulation on AI – even without the adoption of AI-specific laws.[5] As with the implementation of AI, these automated decision practices are encouraging companies to revise and enhance the scope of their risk assessments and increase their baseline monitoring practices to detect bias and other unintended impacts on individuals.

- **Online Advertising and Tracking Technologies.** Online advertising and the use of online tracking and analytic technologies to potentially target and profile consumers naturally faced heightened scrutiny under these new frameworks. States continue to focus on providing consumer choice when it comes to cross-context behavioral advertising, with most mandating clear opt-out mechanisms. The implementation of universal opt-out signals has gained traction, though technical specifications and compliance requirements vary

[4] For example, Colorado's law addresses automated processing that produces "similarly significant effects" for consumers, while Virginia focuses on decisions that "produce legal or similarly significant effects concerning the consumer." 4 Colo. Code Regs. § 904-3 Rule 6.03, Va. Code Ann. § 59.1-575. Maryland also limits consumers' rights to opt out of profiling that are "solely automated decisions that produce legal or similarly significant effects concerning the consumer." Md. Code, Com. Law § 14-4705(b)(7)(iii).

[5] For example, comprehensive state privacy laws in Colorado and Nevada regulate automated decision-making by regulating "profiling," which encompasses various automated decision-making processes. The Colorado Privacy Act rules require companies to conduct data protection assessments before profiling that presents a reasonably foreseeable risk of disparate impact, financial, or physical injury; privacy violations, or any other substantial injury to consumers. 4 Colo. Code Regs. § 904-3 Rule 9.06. The Nevada Data Privacy Act includes a reasonably foreseeable risk of reputational injury as a factor that triggers a duty to conduct data protection assessments in addition to all the factors included in the Colorado rules. Neb. Rev. Stat. § 87-1102(25), Neb. Rev. Stat. § 87-1116(c).

by jurisdiction. These developments have particular significance for organizations engaged in targeted advertising or operating adtech platforms.[6] Companies that haven't done so before are now developing inventories of their online trackers and implementing governance for the use of new trackers.

- **Litigation Involving Collection and Use of Data Continues.** In 2024, we saw the continued filing of lawsuits alleging the collection and use of information without consent. Plaintiffs have focused their attention on the use of tracking technologies, including cookies, pixels, SDKs and other trackers, to claim that their personal data was collected and using information without consent, allegedly in violation of Wiretap Act statutes. While these cases continue to work their way through the courts, two recent decisions from the Massachusetts Supreme Court and the California Superior Court are helpful for companies that face such claims. In *Vita v. New England Baptist Hosp.*, 494 Mass. 824, 826 (2024), the Supreme Court of Massachusetts found a criminal Wiretap Act cannot form the basis of a suit against a website owner for claims related to unlawful collection and use of date. That court held: "We cannot conclude that the wiretap act unambiguously prohibits and, indeed, criminalizes the interception of web browsing activity, because there appears to be a difference in kind and not degree between interactions on a website available to the public and private conversations in your house or on your telephone." *Id*. The Los Angeles Superior Court, in *Licea v. Hickory Farms LLC*, 2024 WL 1698147, at *4 (Cal. Super., Los Angeles County Mar. 13, 2024), reached a similar conclusion, finding a claim under the California Invasion of Privacy Act (a state surveillance act statute) was not cognizable because "[s]uch a broad based interpretation [of the law] would potentially disrupt a large swath of internet commerce without further refinement as the precise basis of liability, which the court declines to consider." *Id*. We expect more cases to be decided in 2025, which should provide both clarity and guidance on the risks associated with the use of tracking technologies.

Trend Three – The Rise and Regulation of Third-Party Data

The need for more and more data and the increased regulation of information brokers that make data available to organizations for various commercial purposes, including marketing, analytics, research, and AI model development, led to the continued scrutiny of the data ecosystem and third-party information brokers (data brokers). The established registration frameworks seen first in Vermont and California, and last year in Oregon and Texas, are expanding with new registration and transparency obligations, but the increased regulatory attention on the use of third-party data adds significant new compliance concerns for organizations that rely on third-party data in their operations.

Litigation in this space also increased in 2024. We expect this trend to continue in 2025, including through new laws, enforcement actions, and litigation directly affecting data brokers, and we expect to see downstream effects on organizations that may rely on third-party (brokered) data.

- **Regulatory Focus.** The evolving scrutiny of data brokers has been driven by the growing concerns over privacy and data security. Data brokers (entities that collect and sell personal information about consumers) have become increasingly sophisticated in their operations. However, this sophistication has also attracted the attention of regulatory bodies such as the FTC and state attorneys general (AGs), leading to a series of settlements, enforcement actions, and rulemaking aimed at curbing potentially harmful practices.
- **FTC Settlements and Rulemaking.** In 2024, the FTC made new use of its Section 5 authority by bringing enforcement actions and settling consent orders with several entities from a variety of industries related

[6] For example, comprehensive state privacy laws, such as in Virginia and Nebraska, provide that if a business "sells personal data to third parties or processes personal data for targeted advertising," it must clearly and conspicuously disclose that it sells consumer data and provide consumers an opt-out mechanism. Colorado law has additional requirements for companies to adhere to the requests that come through universal opt-out mechanisms under state law.

[7] *Vita v. New England Baptist Hospital*, SJC-13542, 2024 WL 4558621, (Mass. Oct. 24, 2024)

to the collection and sale of sensitive location data. In settling with these entities, which were broadly labeled data brokers – X-Mode/Outlogic, Gravy Analytics, and Mobilewalla – the FTC highlighted that location data may be considered sensitive when revealing affiliations with places of worship, medical facilities, military installations, private home locations, or other locations that may be protected under the law. This aligns with the states' inclusion of "precise geolocation" as "sensitive personal data" under most new state privacy laws. In conjunction with the FTC's focus on sensitive data, the Commission updated the Health Breach Notification Rule to address technological advancements and direct-to-consumer health products (e.g., fitness trackers), protect consumers from misuse of their health information, and keep pace with the proliferation of digital health records. The updated rule applies to more companies and types of data incidents and requires more information to be included in breach notifications.

- **State Actions.** The FTC was not the only regulator to crack down on data brokers in 2024. Both the California Privacy Protection Agency (CPPA) and the Texas AG announced sweeps of data broker registration. In June, the Texas AG notified over 100 companies of their apparent failure to comply with the Texas data broker law. In October, the CPPA announced an investigative sweep of data broker registration and, two weeks later, announced its first-ever settlement against two data brokers for failing to register in a timely manner. Six days after announcing that settlement, the CPPA again settled with two data brokers for failing to register in a timely manner.
- **New Rulemaking.** While no new states enacted data broker laws in 2024, both the CPPA and the Consumer Financial Protection Bureau (CFPB) engaged in rulemaking regarding data brokers. The CPPA finalized rules requiring data brokers to disclose specific types of personal information during the registration process, including whether the data broker collects the personal information of minors and reproductive health information. The new rules also define data broker for the first time, stating that businesses may be considered data brokers even if they have a direct relationship with the consumer, provided they sell personal information not collected directly from that consumer. The CFPB also made inroads toward regulating data brokers by proposing amendments to Regulation V, which implements the Fair Credit Reporting Act (FCRA). Under the proposed rule, the CFPB aims to address the sale of consumer report information by ensuring data brokers are subject to the same regulations as consumer reporting agencies. The proposed regulations also address many other areas of consumer reporting, such as imposing new requirements and restrictions on the permissible purposes available to end users to obtain consumer reports. The CFPB also finalized a rule to address the reporting of medical debt. While federal regulators made clear steps toward regulating data brokers, this priority will likely change under the Trump administration. For example, leadership at the FTC has been assumed by current Commissioner Andrew Ferguson, who was often critical of the last FTC's priorities and decisions. Further, leadership is expected to change at the CFPB soon, and regulatory actions taken by both agencies in the final weeks of the Biden administration may be stayed pursuant to the Regulatory Freeze issued by President Trump on January 20, 2025.
- **Litigation Continues.** The past year also saw new lawsuits being pursued by private commercial entities that seek to enforce individual privacy rights. These lawsuits have been filed in New Jersey and West Virginia under each state's version of laws that were enacted to protect the privacy of judges, law enforcement officers, and other state officials and their eligible family members. The lawsuits target entities that maintain, disclose, and redisclose personal information (e.g., home address and unpublished phone number) of individuals protected under the statutes, and allege the entities have failed to honor requests to suppress the information. The New Jersey state law has been challenged on the basis that it is unconstitutional. In 2024, the New Jersey Supreme Court granted a petition for certification and will review lower court rulings on Daniel's Law. Oral argument is expected sometime in the spring of 2025. A district court judge in New Jersey also certified his decision on a facial challenge to Daniel's Law to the

Third Circuit Court of Appeals for review. No decision has been rendered on whether the Third Circuit will accept the petition. Nevertheless, we expect the Supreme Court of New Jersey and the Third Circuit Court of Appeals will weigh in on the New Jersey law.

Litigation against businesses that maintain personal data also is being filed under common law principles relating to an individual's right to publicity, which some states have codified by statute. These lawsuits focus on data brokers – which are defined broadly to include organizations generating revenue from selling information, including personal information that is not directly collected from individuals – that allegedly use an individual's name or likeness in a commercial context without authorization. Specifically, data brokers that offer "people search" directories and use "teaser data" as part of a free preview or free trial to advertise their products and services are being sued for unauthorized commercial use of an individual's name and likeness. No determinations have been made on the merit to the claims being asserted, but members of the industry are watching them closely for guidance.

Trend Four – Cyber Risk Accelerating at the Speed of AI

Throughout 2024, data incidents persisted without interruption, with threat actors increasingly employing more sophisticated techniques in their attacks. Traditional attack vectors, such as business email compromises (BECs) and ransomware, remain the most common types of attacks. As threat actors continue to evolve their tactics and techniques to compromise individuals and exert pressure on their victims, we expect them to utilize all tools at their disposal, potentially including machine learning and AI.

- **BEC scams are on the rise.** In BECs, criminals may send an email that seems to originate from a trusted source making a legitimate request, often to redirect payments to vendors or employees through wire fraud. This scam is frequently carried out by criminals who gain unauthorized access to an organization's email system or an employee's email account, primarily for financial gain. In the past year, we have seen an increase in BECs and the dollar value of losses implicated in such schemes.
- **Phishing Grows Up.** With experience and the availability of AI to assist threat actors engaged in social engineering, phishing emails are becoming more sophisticated and more successful. We expect that it will only become harder for busy workers to recognize fake or "spoofed" email accounts and phishing emails.
- **No Honor Among Thieves.** This year we also saw threat actor groups become increasingly unpredictable, with a growing trend of re-extorting victims after payment of a ransom demand and an increase in "copycat" groups imitating known threat actors. This trend upsets the expectation that at least some established threat actors have a "reputation" to uphold and will stand by their promise not to publish data or re-extort or reattack their victims.

Ten Essential Actions to Immediately Take or Plan to Implement in 2025

Organizations navigating multiple and evolving compliance frameworks and risks can enhance efficiency, reduce risk, and foster innovation and business continuity by aligning internal governance procedures and operational activities.

This can be achieved by focusing on key program integrations, increased use of risk assessments, and regular review and updates of both internal policies and procedures and external data disclosures.

1. **Establish a Cross-Functional AI Governance Body.** Form a governance body that includes representatives from privacy, legal, security, IT, and business units to oversee AI-related decision-making. This body should ensure consistent risk assessment and rapid response to regulatory changes by overseeing and coordinating data governance comprehensively. This approach will help manage the unique risks associated with AI systems, including those related to data sourced from third-party data brokers.

2. **Enhance Your Risk Assessment Procedures for the Enterprise and Your Vendors.** Expand traditional DPIAs to address multiple compliance obligations by including AI-specific considerations such as algorithmic bias, transparency of decision-making processes, and potential unintended consequences of AI deployment. This enhanced risk assessment protocol should be integrated into existing privacy frameworks to create a unified approach to risk management. Special attention should be given to third-party risk management practices (for example, utilizing vendor-supplied, AI-forward, or AI-enhanced tools or services) and the origin of data sourced from third parties (including data brokers), to ensure that sources meet necessary diligence and training requirements and can comply with downstream data subject rights requests they must help the company you honor. A unified approach will help manage the complexities of working with multiple regulatory frameworks and minimize the impact on the business.

3. **Perform Adtech Tracker Inventory.** Effective data governance is impossible if companies don't know what they're collecting, and online trackers such as cookies and pixels are often a blind spot. Companies should implement periodic reviews of their digital properties to generate and validate any technologies that automatically collect personal data. The inventory should identify the specific data elements collected, how the data is used, the third parties with whom the data is shared, and the relevant contracts governing this activity.

4. **Adapt to U.S. State and Federal Privacy Laws.** Develop flexible compliance programs that can adapt to the evolving requirements of state privacy laws, particularly those focusing on automated decision-making and profiling practices. Stay updated on data broker registration and transparency obligations to avoid enforcement actions and litigation. Last, but not least – don't forget the children. Review current data collection practices to identify any risks associated with knowingly collecting personal data from children, with new focus on the collection of information of teens.

5. **Update Privacy Policies and Terms of Service.** As part of an annual review of your privacy policies and terms of service, ensure the company has clearly articulated how AI processes personal data, explain automated decision-making mechanisms, and delineate user rights regarding AI-driven processes as appropriate and to the extent that the organization uses AI.

6. **Engage in Proactive Data Governance.** Conduct data protective activities strategically, such as maintaining dynamic data maps, establishing model training controls, and implementing robust monitoring systems to ensure privacy and security throughout the AI life cycle. This includes ensuring that data sourced from third-party data brokers is properly managed and compliant with relevant regulations.

7. **Review Data Minimization and Record Retention and Deletion.** To advance privacy, prepare for AI, and comply with data minimization requirements, review data inventories to ensure that an appropriate data retention period is assigned to categories of personal data, and that processes are in place to delete personal data after the retention period has expired. This not only reduces data compliance risk but also cleans data sources, improving quality and efficiency for strategic uses, such as AI.

8. **Update and Rehearse Your Incident Response Procedures.** Develop and implement clear escalation procedures and communication protocols for security incidents involving AI and ransomware to ensure rapid response to incidents and maintain stakeholder trust. All organizations should also take specific steps to strengthen their vulnerability to common types of exploits, including by implementing multiple verification methods for wire or ACH requests (e.g., requiring a live video call to obtain verbal authorization for the transaction), increasing security training, regularly conducting mock phishing exercises, and routinely testing their incident response plans through tabletop exercises. Publicly traded companies should additionally review their materiality assessment processes and procedures to ensure they account for the Securities and Exchange Commission's cybersecurity disclosure rules and interpretive guidance and align with their incident response plans. Specifically, publicly traded companies must continue to refine their incident response procedures to ensure incidents are evaluated and escalated to an internal disclosure committee early to ensure when filing is appropriate based on the facts of the incident and when reporting may be required.

9. **Conduct Regular Risk Assessments.** Regularly evaluate the risks associated with AI systems, including algorithmic bias and the transparency of decision-making processes, to ensure compliance with regulatory requirements and mitigate potential risks. This should include a thorough assessment of data sourced from third-party data brokers.

10. **Monitor Regulatory Developments.** Keep abreast of new laws, enforcement actions, and litigation trends affecting data brokers and AI systems to proactively adjust compliance strategies and mitigate risks. This includes monitoring developments in the regulation of online advertising and tracking technologies, which are subject to heightened scrutiny under new privacy frameworks.

Next Steps

If you have any questions about the trends or how to apply our recommended 10 steps to your company, please contact one of our authors or any member of our Privacy + Cyber Practice.