POLSINELLI | What a law firm *should* be.™

Technology Transactions & Data Privacy

2026 REPORT

As we enter 2026, the changes of the last several years are no longer abstract. Technology decisions are now examined closely by regulators, courts and counterparties, often long after those decisions were made. At the same time, organizations remain under pressure to move quickly, adopt new tools and modernize infrastructure. Managing the balance between innovation and accountability has become a central challenge for legal and business leaders.

This year's **Technology Transactions & Data Privacy Report** reflects that reality. The articles focus on the issues we see most often in practice, including how organizations govern technology in real-world environments; how contracts allocate risk, once systems are deployed; and how privacy and security programs perform when tested by regulators or litigation.

Artificial intelligence is featured prominently throughout this report, but the discussion has shifted. For many organizations, the question is no longer whether to use AI, but how to control it responsibly. Tools that act autonomously, interact with enterprise systems or make decisions without constant human input raise difficult questions about oversight and liability. Litigation and enforcement activity are beginning to reflect these concerns, particularly where AI tools collect data, listen to communications or are deployed in sensitive contexts such as hiring.

Privacy compliance continues to evolve in a similar direction. Regulators and plaintiffs are increasingly focused on whether privacy programs operate as described, especially with respect to online tracking, consent and third-party technologies. Cross-border data transfers remain an area of sustained attention, requiring alignment of legal, contractual and technical safeguards across jurisdictions.

Data security is also under greater scrutiny. After a breach, regulators are examining not only the incident itself but the design and day-to-day operation of security programs. The cyber insurance market is reinforcing these expectations through tighter underwriting and renewed focus on documentation, vendor management and incident readiness. New state safe harbor statutes and compliance regimes such as CMMC are further shaping how organizations assess risk, particularly in regulated supply chains.

Looking ahead to 2026, investment in AI and data center infrastructure will continue to grow. AI workloads are driving decisions about where data is stored, how systems are secured and which vendors are involved. Those infrastructure choices increasingly influence transaction strategy, regulatory exposure and long-term operational risk. In this report, Polsinelli lawyers share practical insight, drawn from their work with clients navigating these issues every day. We remain committed to helping clients make technology decisions that are forward-looking and defensible in an increasingly complex environment.

Greg M. Kratofil, Jr.
Technology Transactions
& Data Privacy Chair

Contents

CCPA 2025 Enforcement in Review: Ensuring Privacy Programs Work in Practice

Ashleigh Bickford
Associate
Kansas City

Gregory J. Leighton
Privacy & Incident Response Vice Chair
Chicago

KEY TAKEAWAY: California got more aggressive on privacy in 2025. Regulators now expect privacy tools to work in practice — not just on paper — and they're testing opt-outs, vendor contracts and employee notices for real-world performance.

Enforcement of the California Consumer Privacy Act (CCPA) entered a new and more assertive phase in 2025, with regulators focusing on how privacy practices actually function to protect consumers. Both the California Privacy Protection Agency (CalPrivacy) and the California Attorney General (AG) played active roles in this shift. CalPrivacy issued investigations, and its first enforcement orders centered on the technical performance of opt-out mechanisms, consent tools and data subject rights portals. The AG also brought its own enforcement action, also reinforcing that CCPA compliance depends on whether business' privacy controls operate effectively, not just whether they exist on paper. For businesses subject to the CCPA, 2025 enforcement made clear that compliance turns on how privacy practices work in reality — not just how they appear online or on paper.

In this article, we look at a series of 2025 CCPA enforcement actions to show what regulators' "proof-of-performance" focus means for privacy compliance obligations. CalPrivacy's settlement with Tractor Supply Co. highlights increased scrutiny of privacy notices for consumers, employees and job applicants. Settlements with American Honda Motor Co. and Todd Snyder Inc. highlight expectations around CCPA-compliant vendor and adtech contracts, functioning cookie management platforms (CMPs) and opt-out tools, and right-sized identity verification. The AG's settlement with Healthline Media, LLC illustrates the CCPA's purpose-limitation principle in the context of sensitive health data, and

CalPrivacy's recent Delete Act actions against multiple data brokers reinforce registration obligations. Taken together, these developments show that regulators are increasingly focused on whether privacy programs actually work in practice to protect consumers and that they are willing to test those programs for compliance.

Current, Accurate Privacy Notices

The CCPA requires businesses to maintain privacy notices that accurately disclose the categories of personal information collected and shared; the rights available to consumers to exercise over their personal information; and clear instructions on how those rights may be exercised. These notices must reflect current practices and be updated at least annually. The CCPA is unique among state privacy laws in extending the notice requirement to job applicants and employees, meaning that businesses must prepare and maintain notices tailored to employment.

The Tractor Supply enforcement action illustrates CalPrivacy's heightened scrutiny of privacy notice compliance. CalPrivacy imposed a $1.35 million penalty — its largest CCPA fine to date — after finding that Tractor Supply's consumer-facing privacy notice failed to disclose key categories of personal information collected or shared, did not adequately describe consumer rights and did not provide instructions on how to exercise those rights. CalPrivacy also emphasized that Tractor Supply had not updated its privacy notice in four years, despite the requirement for annual review. In addition, even though the Tractor Supply Co. had job applicants and employee notices in place, the notices were found to be non-compliant because they failed to describe CCPA rights or explain how those rights could be exercised.

From a practical standpoint, the Tractor Supply action demonstrates that businesses must ensure they have current, accurate privacy notices in place, conduct annual notice reviews and treat employee and applicant notices as meaningful compliance documents — not afterthoughts.

CCPA Provisions in Vendor and Adtech Contracts

Businesses under the CCPA must also maintain contracts that contain certain CCPA-required data protection terms with service providers, contractors and other third parties that they disclose personal information to and be able to provide those contracts to regulators upon request. Regulators have made clear that businesses cannot rely on assumptions, generic industry frameworks or vendor assurances to satisfy these obligations. Instead, companies must be able to demonstrate, often on short notice during an audit, that each vendor relationship includes executed agreements containing the required provisions. Increasingly, the concern is not simply that the right contractual terms are missing, but that businesses are unable to locate and produce the agreements when regulators ask.

Several 2025 enforcement actions illustrate this trend. In CalPrivacy's investigation into Honda's privacy practices, CalPrivacy found that Honda had disclosed personal information to advertising technology partners and then could not prove that they had entered into contracts that contained the required CCPA provisions. Similarly, in the AG's settlement with Healthline, the AG concluded that Healthline assumed its advertising partners had adopted industry-standard contracts but

had failed to verify that the agreements included the specific terms required by the CCPA. The Tractor Supply action discussed above also involved insufficient contractual provisions with vendors handling personal information. These actions show that businesses must inventory their vendor relationships, ensure that they have these agreements on hand, identify contractual gaps and confirm that updated CCPA-compliant terms are executed and maintained across all data-sharing partnerships.

Functioning CMPs and Opt-Out Mechanisms

Another focus of 2025 CCPA enforcement was that consumer-facing opt-out tools actually function and are easy for consumers to use. CalPrivacy repeatedly stressed that having a cookie banner, consent-management platform (CMP) or "Do Not Sell or Share My Personal Information" link is not enough if the underlying system does not actually honor consumer choices by stopping tracking technologies or triggering a stop on the sale or sharing of information. Regulators also focused on the "symmetry of choice" principle, which requires businesses to make it just as easy to opt-out of data collection and sharing as it is to opt-in. Applied to CMPs, designs that require users to take extra steps, contain less conspicuous opt-out options or otherwise steer consumers toward "accept all" selections may be treated as dark patterns. Even one additional click required to opt out is enough to create a more burdensome choice. In addition, the option to opt out must be just as apparent to consumers and cannot be displayed in a less conspicuous color or font than the option to opt in.

Several CalPrivacy enforcement actions last year focused on the functionality of opt-out mechanisms. In the Honda action, Honda's website cookie banner allowed consumers to "Accept All" cookies with one click, but users had to individually toggle off categories of cookies they wanted to opt out of. This extra step was deemed a "dark pattern" and non-compliant with symmetry of choice requirements. The Todd Snyder settlement similarly involved a CMP that was misconfigured for approximately 40 days, during which the banner disappeared before users could interact with it — preventing consumers from submitting opt-out requests altogether. Healthline's enforcement action reinforced this theme: although Healthline implemented multiple opt-out mechanisms, including a "Do Not Sell or Share My Personal Information" link, CMP and Global Privacy Control signal detection, none of the tools functioned correctly, and Healthline continued to disclose personal information to advertisers even after consumers attempted to opt out.

Collectively, these actions signal that businesses must regularly test their CMPs, cookie banners and opt-out tools; review user experience designs for symmetry-of-choice compliance; and monitor vendor-provided tools to ensure they perform as intended.

Purpose Limitation Principle

Regulators also emphasized the CCPA's purpose-limitation principle, which requires that personal information only be used or disclosed for purposes that were disclosed at the time of collecxstion or that consumers can reasonably anticipate. Sensitive personal information, such as data-revealing health conditions, requires special scrutiny because of the heightened risks involved.

The purpose-limitation principle is illustrated by the AG's $1.55 million settlement with Healthline, the Department of Justice's largest CCPA enforcement to date. Healthline allegedly disclosed to advertisers the titles of health-related articles visited by consumers, including content suggesting specific medical diagnoses such as multiple sclerosis or HIV. Although Healthline's privacy policy referenced targeted advertising generally, it did not disclose that sensitive, health condition-revealing browsing data would be shared with third parties for targeted advertising purposes. The AG argued that consumers could not reasonably expect such sensitive information to be used for targeted advertising, and therefore, Healthline violated the purpose-limitation rule. This action underscores the need for businesses to map their data flows, identify whether any sensitive personal information is being used for advertising or analytics and ensure that their privacy notice disclosures clearly and specifically reflect these practices.

Data Subject Requests and Verification

The CCPA differentiates between consumer rights requests that require identity verification and those that do not. Requests to opt-out of the sale or sharing of personal information and requests to limit the use of sensitive personal information do not require verification. For requests to access, delete and correct personal information, the verification process must allow the business to confirm the consumer's identity to a reasonable degree of certainty — typically by matching at least two data points provided by the consumer. Regulators have emphasized that businesses must avoid collecting unnecessary additional personal information for verification purposes when consumers attempt to exercise their data subject rights.

CalPrivacy investigations have found CCPA violations where businesses required consumers to provide more information than necessary to verify their identity, or where they required verification for rights that do not. For example, in the Honda action, a violation was found when they required consumers to submit eight separate data points to verify their identity for access, deletion and even opt-out requests, exceeding what was necessary for identify verification. Similarly, in the Todd Snyder action, CalPrivacy found a violation because the company required consumers to upload a government-issued ID to submit data subject rights requests, even for rights requests that do not require verification.

Together, these actions demonstrate that businesses must calibrate identity-verification procedures to the specific type of request and ensure that their systems for handling data subject requests are not collecting excessive or unnecessary personal information.

Data Broker Enforcement Under the Delete Act

Along with consumer-facing tools, CalPrivacy also kept busy in 2025 enforcing the data broker regulations under the California Delete Act, which applies to any business that collects and sells the personal information of consumers with whom they do not have a direct relationship. The Delete Act requires data brokers to register annually with CalPrivacy and disclose certain information about the information they are collecting and selling, as well as include those same disclosures in their privacy policy. Starting in 2026, data brokers must process statewide deletion requests through CalPrivacy's

centralized Delete Request and Opt-Out Platform (DROP).

In early 2025, CalPrivacy announced multiple enforcement resolutions under the Delete Act, including orders and settlements with Key Marketing Advantage, LLC, National Public Data, Inc., Background Alert, Inc. and other data brokers that failed to register timely. Penalties ranged from $46,000 to $58,500 and included daily fines for late registration, payment of attorneys' fees and costs, and in one case, a requirement that the data broker shut down its operations through 2028 or face a $50,000 penalty.

These actions signal that data broker compliance is an active enforcement priority. For data brokers the message is straightforward: confirm whether you qualify as a data broker, register on time and prepare now for the operational demands of DROP, including the need to honor large volumes of deletion and opt-out requests on a recurring basis.

The Takeaway

Together, these enforcement actions and trends demonstrate that California is moving from a check-the-box model of privacy compliance to a proof-of-performance model. Regulators are increasingly concerned with whether tools are accessible and effective from the consumer's perspective and whether technical implementations match the promises made in privacy notices and user interfaces. To comply, businesses should:

- Regularly test consent tools to confirm that CMPs, cookie banners, GPC recognition and other opt-out mechanisms function technically — not just visually — and that these signals are honored by third-party partners.
- Maintain symmetry of choice by ensuring that opting out is no more burdensome than opting in and by avoiding dark patterns that make opting in easier than opting out.
- Maintain accurate and compliant privacy notices for consumers, job applicants and employees, and update these notices at least annually to reflect current data practices and statutory requirements.
- Ensure data-sharing contracts with vendors include all CCPA-required provisions and that downstream partners are bound to appropriate restrictions on processing and secondary use.
- Implement right-size identity verification for data subject requests to avoid over-verification while still protecting against fraud and unauthorized access.
- Monitor Delete Act obligations for any business that may qualify as a data broker, confirm registration where required, and ensure deletion workflows and request-handling processes meet statutory requirements.

Cross-Border Data Transfers: New Obligations, Stable (For the Moment) Frameworks and Harmonizing Compliance

Alexander S. Altman
Counsel
San Francisco

KEY TAKEAWAY: New U.S. rules restrict outbound transfers of sensitive personal data, while the EU-U.S. framework for inbound transfers remains intact — for now. Companies should map data flows, assess exposure under the Bulk Data Rule and prepare for shifting EU adequacy standards.

2025 saw developments that may either substantially change or stabilize privacy compliance programs for companies engaging in cross-border data transfers, depending largely on the directions of data flows, the types of data to be transferred and existing compliance programs.

For certain categories of personal data leaving the U.S., the Department of Justice (DOJ) finalized the Bulk Data Rule, a new national-security-driven regime that either prohibits or restricts the transfer of U.S. government data and "sensitive U.S. personal data" to "countries of concern."

For data flowing into the U.S. from the European Economic Area, the European General Court's September decision in *Latombe v Commission* has, for now, shored up the EU-U.S. Data Privacy Framework (EU-U.S. DPF) as a lawful mechanism for transatlantic data flows, but uncertainty remains as the case was appealed to the Court of Justice of the European Union (CJEU) at the end of October.

Together, these developments may alternately reshape or stabilize (at least temporarily) the risk calculus for companies operating in complex, global data ecosystems.

The Bulk Data Rule Complicates Transfers of Data Outside the U.S.

The Bulk Data Rule, codified at 28 C.F.R. Part 202, implements the Biden-era Executive Order 14117 "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern." Effective as of April 8, 2025, the Rule prohibits or restricts U.S. entities from engaging in certain "transactions" that would grant access to either "any government-related data" or "bulk U.S. sensitive personal data" to "countries of concern" — specifically, China, Cuba, Iran, North Korea, Russia and Venezuela — and "covered persons," i.e., (a) a foreign entity that is 50% or more owned by one or more countries of concern (or by other covered persons) or that is organized, chartered or has its principal place of business in a country of concern; (b) persons who are "primarily" residents of a country of concern; (c) employees or contractors of a country of concern or other covered person; or (d) any person specified by the U.S. Attorney General (USAG). As of this writing, the USAG has not identified any specific individuals under (d).

"Covered personal identifiers" is extraordinarily broad under the Rule and means, in essence, any combination of two or more pieces of fairly innocuous data points such as internet protocol (IP) addresses, contact information (including email address), cookie data and a number of other identifiers. Thus, even websites with modest traffic that use tracking cookies may find themselves covered by the Rule, provided the data is transferred to a country of concern or covered persons.

Aside from government-related data, the Rule applies only to transfers of "bulk" volumes (measured in the preceding 12 months) of certain categories of "U.S. sensitive personal data," including:

100+
U.S. persons' human genomic data;

1,000+
U.S. persons' biometric data;

1,000+
U.S. devices' precise geolocation data;

10,000+
U.S. persons' personal health data;

10,000+
U.S. persons' personal financial data; and

100,000+
U.S. persons' "covered personal identifiers."

Adding to this breadth, and unlike most data protection laws, data is not exempted or accorded any special treatment by virtue of being encrypted, pseudonymized or anonymized. It is therefore likely that a wide range of U.S. companies may be handling data subject to the Rule. Practically speaking, this only becomes a risk to the extent a company makes such data available to a country of concern or a covered person.

The Rule flatly prohibits transfers in the context of "data brokerage," which is defined as the "sale of data, licensing of access to data, or similar commercial transactions … where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data." Outside of data brokerage, the Rule restricts, but does not prohibit, transfers in the context of vendor agreements, employment agreements and investment agreements. These "restricted transactions" are permitted, subject to the implementation of certain security measures established by the Cybersecurity and Infrastructure Security Agency. There are a number of narrow exemptions to the most restrictive obligations under the Rule. For example, intra-company transfers that are "ordinarily incident to and part of administrative or ancillary business operations" such as for HR and payroll, may be exempt. Certain transfers of de-identified or pseudonymized data "necessary to obtain or maintain" approvals to market drugs, biological products or medical devices outside of the U.S. may be exempt. FDA-regulated clinical investigation and post-marketing surveillance data may also be exempt in certain circumstances. There is also an exemption for transactions that are "ordinarily incident to and part of the provision of" specific financial services. The Rule provides detailed examples of where these exemptions do — and importantly, do not — apply, and careful analysis is required before concluding that a transfer is exempt from certain obligations, as businesses may be subject to detailed recordkeeping requirements even where an exemption applies.

For U.S. companies, the Bulk Data Rule effectively layers a national-security export-control style regime on top of traditional privacy and cybersecurity laws. Cross-border deals involving cloud hosting, analytics, outsourcing, clinical research, ad-tech or data brokering now need to be screened not only

for sanctions and CFIUS risk but also for DOJ bulk-data exposure, particularly where counterparties, infrastructure or subcontractors are linked to China or other countries of concern.

In practice, U.S. companies will want to develop (or supplement existing) detailed data-flow maps and inventories, revisit vendor data processing agreements and align internal data-minimization strategies with the Rule's thresholds. Additionally, sellers in the M&A context will need to perform diligence into buyers to ensure that any deals do not run afoul of the Rule and obtain relevant representations, warranties and covenants.

The EU-U.S. Data Privacy Framework is Safe … For Now

Across the Atlantic, the *Latombe* decision pulls in the opposite direction: toward stabilizing cross-border transfers of personal data, at least for those U.S. companies self-certifying to the EU-U.S. DPF. In essence, the EU-U.S. DPF allows U.S. companies to self-certify with the U.S. Department of Commerce that they will accord certain protections to EEA personal data and abide by specific dispute resolution procedures. U.S. companies may additionally participate in parallel frameworks for transfers from the United Kingdom and Switzerland. On July 17, 2023, the European Commission issued an adequacy decision validating the EU-U.S. DPF as a lawful mechanism for transferring personal data to EU-U.S. DPF participants without the need for additional safeguards such as binding corporate rules or standard contractual clauses (SCCs). In practice, the SCCs are used frequently where the U.S. company importing the personal data is not an EU-U.S. DPF participant, but the CJEU effectively requires EEA data exporters to conduct detailed, and sometimes burdensome, transfer impact assessments to determine whether the personal data will receive essentially equivalent protections under the importing country's laws.

Notably, two previous similar frameworks — the Safe Harbor Framework and EU-U.S. Privacy Shield Framework — were challenged and subsequently invalidated by the CJEU in the Schrems I (2015) and Schrems II (2020) decisions, respectively. The EU-U.S. DPF presents a third bite at the apple, but *Latombe* may upset the apple cart in the long run. In September 2023, Philippe Latombe, a member of the French National Assembly, brought an action before the General Court seeking the annulment of the EC's EU-U.S. DPF adequacy decision, arguing that:

1. The Data Protection Review Court (DPRC) — a key component of the dispute redress mechanism offered to EEA data subjects — is not independent; and
2. U.S. intelligence collection of EEA personal data is not compatible with an adequacy designation because such collection does not require prior authorization from a court or other independent authority.

However, on Sept. 3, 2025, the General Court dismissed the action, holding that, at the time the EU-U.S. DPF was adopted, U.S. law — particularly Executive Order 14086 (Enhancing Safeguards for United States Signals Intelligence Activities) and the creation of the DPRC — ensured a level of protection for EEA personal data "essentially equivalent" to that in the EEA. The General Court found the DPRC sufficiently independent and effective and accepted that U.S. "bulk" signals intelligence collection could be compatible with EU law where subject to necessity, proportionality and *ex post* oversight.

For organizations relying on the DPF or using it as a positive factor in transfer impact assessments for SCCs, this was a major win: it avoids an immediate "*Schrems III*"-style cliff edge. However, legal certainty may be fleeting. The *Latombe* decision has been appealed to the CJEU (Case C-703/25 P) which, as explained above, struck down similar predecessor frameworks after conducting its own assessment of U.S. surveillance law and redress mechanisms in place at the time.

We expect the CJEU, on appeal, to look more critically at issues the General Court treated as sufficiently addressed: the scope and oversight of bulk collection, the real-world independence and transparency of the DPRC and the durability of protections under shifting U.S. executive administrations. The appeal ensures that the DPF — and by extension many EU-U.S. data flows — will remain under judicial scrutiny in 2026 and for the foreseeable future.

Cross-Border Transfers in 2026 and Beyond

Stepping back, the Bulk Data Rule and the EU-U.S. DPF (in light of *Latombe* and the CJEU appeal) are tightly interlinked for cross-border privacy compliance strategy. The EU-U.S. DPF adequacy assessment relies on the robustness of U.S. safeguards around surveillance and government access; at the same time, the U.S. is building a parallel regime that restricts bulk exports of sensitive U.S. data to certain foreign jurisdictions for national-security reasons. From an operational standpoint, companies must now navigate a world in which

1. EU law broadly permits transfers to certified U.S. organizations under the DPF (subject to the outcome of *Latombe* at the CJEU) while
2. U.S. law may restrict outbound data flows in the opposite direction where data could be accessed by countries of concern or their proxies.

For U.S. companies managing cross-border data flows, the practical playbook for 2026 is reasonably clear: treat these developments as complementary constraints rather than isolated issues. On the U.S. side, build a Bulk Data Rule compliance program that inventories bulk-sensitive datasets, identifies any touchpoints with countries of concern (including through vendors and infrastructure) and embeds DOJ screenings into procurement, M&A and collaboration workflows. On the EEA side, continue to make pragmatic use of the EU-U.S. DPF where available, but keep SCCs and other fallback mechanisms in good order, including by conducting transfer impact assessments reflecting current U.S. safeguards while explicitly flagging the pending CJEU appeal. In other words: design data flows that can survive both a more aggressive DOJ enforcement posture and a possible CJEU course-correction — because cross-border privacy law is no longer just about compliance today, but resilience to geopolitical and judicial swings tomorrow.

Beyond the Buzzword: Managing AI Bias Risk in Recruiting After *Mobley v. Workday*

Jennifer Bauer
Counsel
Raleigh

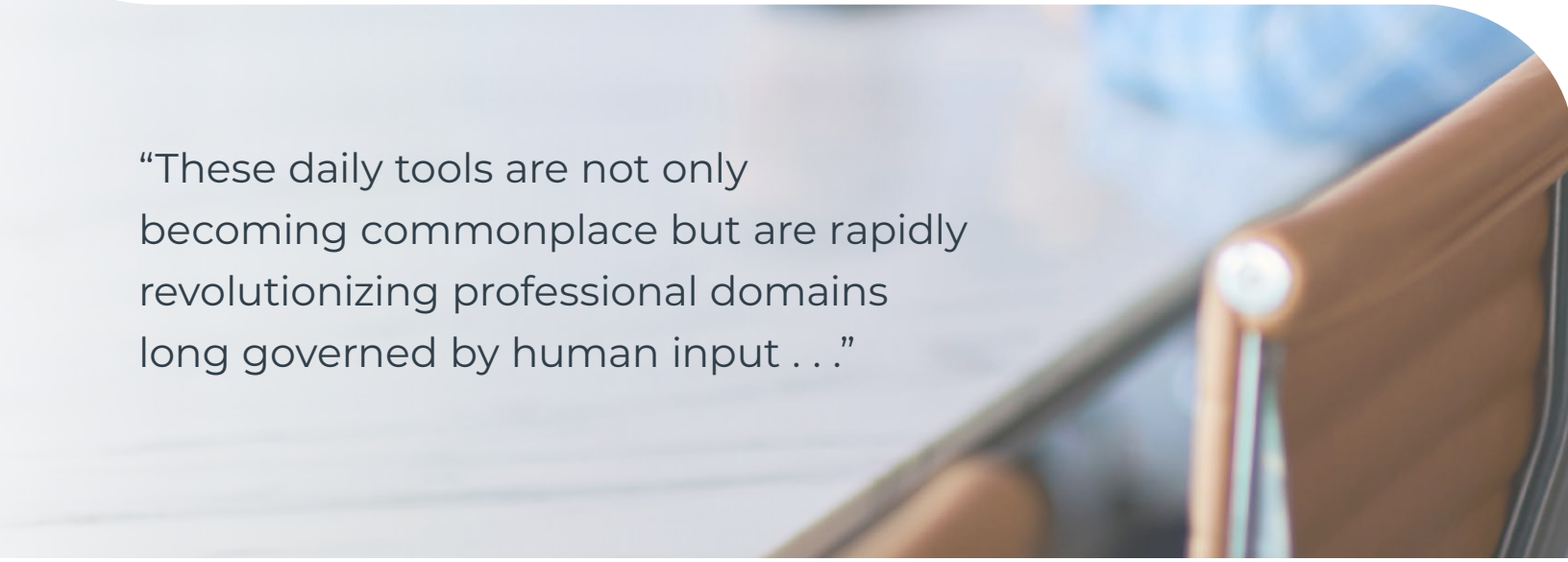
Scott M. Gilbert
Employment Litigation, Arbitration & Dispute Resolution Chair
Chicago

KEY TAKEAWAY: AI in hiring is now a compliance issue. After *Mobley v. Workday* and a wave of state AI laws, legal exposure is growing for both employers and vendors when automated tools shape who gets screened in — or out.

Introduction – AI Is Now a Legal Risk in Recruiting

Artificial intelligence (AI) has quickly moved from a buzzword to a ubiquitous feature deployed across our personal and professional lives. These daily tools are not only becoming commonplace but are rapidly revolutionizing professional domains long governed by human input and decision-making, such as the job application process and human resources (HR) operations.

In the employment context, AI-driven tools can be integrated into applicant tracking systems that are central to the recruiting process and perform functions like sourcing candidates from job boards and social media, automatically parsing resumes, scoring and ranking applications, powering chatbots that answer candidate questions and even conducting online assessments or one-way video interviews. These tools promise speed, efficiency and a more consistent candidate experience. **But when early screening and sorting happens inside opaque models rather than in front of human eyes, the practical effect is that key employment decisions are being made — or at least heavily influenced — by automated systems.**



"These daily tools are not only becoming commonplace but are rapidly revolutionizing professional domains long governed by human input . . ."

That shift is exactly what has attracted the attention of plaintiffs' lawyers, regulators and courts. It has also resulted in two key developments that have moved AI in recruiting from an interesting innovation to a legal risk: (1) high-profile litigation challenging AI-based screening tools and (2) a wave of state and local AI/automated decision-making laws focused on this subject.

High-profile litigation challenging AI-based screening tools

In *Mobley v. Workday, Inc.*, a job applicant alleges that Workday's AI-enabled screening tools unlawfully disadvantaged Black, older and disabled candidates and that the vendor should be treated as a covered entity (i.e., as an "agent" of an employer) under federal anti-discrimination laws because of the control its systems exert over who advances in the hiring process. The litigation is ongoing, but the court's willingness to let key claims proceed past the motion-to-dismiss stage when the vendor would not otherwise qualify as an "employer" signals that judges are prepared to treat AI-driven screening tools as recruitment activities subject to traditional discrimination standards and potentially pull vendors into the liability framework alongside employers.

01

A wave of state and local AI/automated decision-making laws

At the same time, jurisdictions like New York, Colorado, California and Illinois have moved ahead with laws and regulations that explicitly govern automated decision-making in employment. Bias-audit requirements, applicant notice obligations, record-keeping rules and broad "algorithmic discrimination" concepts are quickly turning AI governance from a nice-to-have into a compliance necessity. For multi-state employers using standardized recruiting tools, this emerging patchwork creates both operational complexity and heightened regulatory scrutiny.

02

Together, *Mobley* and these new state and local AI/automated decision-making laws and regulations underscore a simple point: **Using AI in recruiting is not just a technological choice — it is a legal and compliance decision.**

In-house counsel, HR leaders and compliance teams seeking to navigate this rapidly changing space will need to understand ongoing developments to help their organization use technology with their eyes wide open — i.e., understanding where the real legal risks lie, what regulators and courts are signaling and how to build defensible, candidate-respectful processes around these increasingly powerful tools.

Mobley v. Workday, Inc. – A Federal Court Looks at AI Bias in Hiring

Mobley v. Workday, Inc. is widely considered a bellwether lawsuit relating to AI bias in hiring and related vendor liability. The court did more than simply accept a novel legal theory — it affirmed that when an AI or algorithm-driven recruiting tool is functionally controlling who advances in the hiring process, the vendor behind it can plausibly be treated as an agent of an employer for purposes of anti-discrimination law. That has major implications not just for the employer using the tool, but also for the vendor providing it.

The *Mobley* plaintiff's ability to survive a motion to dismiss offers meaningful lessons for employers and HR-tech vendors using AI in making employment decisions. The plaintiff alleged that Workday's AI-driven tools systematically rejected older, disabled and minority applicants in violation of Title VII, the ADA and the ADEA and effectively acted as a gatekeeper or "agent" of the employer in the job application process rather than a neutral software platform. The EEOC supported this view in an amicus brief that urged the court to treat AI-enabled vendors as covered entities to prevent employers from outsourcing discriminatory activities via technology. Upon review, the court agreed that Mobley plausibly alleged that Workday functioned as an "agent" of its client-employers by performing core hiring functions like screening, rejecting or recommending applicants and can therefore proceed under a disparate-impact liability theory.

Central to the success of the pleading was that the Workday solutions allegedly operated in a manner that did not just assist employers in their review but operated as a gatekeeper by filtering them, scoring them and even eliminating them without any human interaction. The analysis suggests that:

- **Courts will examine the real-world function of AI hiring tools, in addition to their labels and marketing, to determine whether statutory protections apply.** If a screening tool determines who is screened out or advances to the next stage of the application process — including, e.g., human review — it will be treated like a recruiting decision otherwise governed by anti-discrimination law.
- **Similarly, the use of AI does not shield employers or vendors from liability simply because the decision-making is automatically executed via innovative technology.** Employers cannot blame the algorithm and instead remain liable for the actions taken by their agents, and vendors can be co-liable when their tools play a decisive role in hiring.

In short: *Mobley* makes clear that using AI in recruiting is not a free pass; its use must be evaluated under the same anti-discrimination rules as traditional hiring practices, with the added complexity that vendors may now sit in the hot seat alongside employers.

State and Local AI Employment Rules – A Patchwork Emerging

Across the U.S., localities and states have begun enacting laws and regulations that directly regulate the use of automated decision-making tools in hiring and applicant screening. These laws often impose transparency, auditing, notice and record-keeping obligations on employers and recruiting vendors — layering regulatory requirements on top of existing federal civil-rights liability. See the illustrative examples enclosed below.

New York City Local Law 144 (Effective July 5, 2023)

- Applies to any employer or employment agency that uses an "Automated Employment Decision Tool (AEDT)" to screen or evaluate candidates or employees for hiring, promotion or other employment decisions.
- Employers must obtain an annual bias audit of the AEDT, publicly post a summary of these audit results and provide written notice to candidates advising that an AEDT will be used and describing the job qualifications or characteristics it will assess.

California FEHA Automated-Decision Systems Regulations (Effective Oct. 1, 2025)

- Extends anti-discrimination protections to contexts involving automated-decision systems in employment and defines terms like "agent" and "proxy" to encompass third-party vendors that design or supply these systems.
- Requires covered entities to retain records of automated-decision data for at least four years to support accountability, auditability and potential civil-rights investigations.

Illinois HB 3773 (Effective Jan. 1, 2026)

- Amends the Illinois Human Rights Act to address AI use in recruitment and employment decisions by prohibiting employers from using AI in a manner that has the effect of discriminating against employees or applicants based on protected characteristics.
- Requires employers to give notice to applicants/employees when automated decision tools are used in recruitment or employment decisions and bans the use of certain proxies (like ZIP codes) as substitutes for protected class characteristics.

Colorado Artificial Intelligence Act (CAIA) (Effective June 30, 2026)

- Focuses on "high-risk AI systems" that make or are a substantial factor in making "consequential decisions," which include those around employment opportunities.
- Employers (deployers) of such AI must implement a risk-management program, conduct a risk/impact assessment prior to deployment and take "reasonable care" to prevent "algorithmic discrimination."

California CCPA Automated Decision-Making Technology (ADMT) Regulations (Effective Jan. 1, 2027)

- Applies to businesses using ADMT to make "significant decisions" about California consumers, which expressly includes decisions related to employment, contracting and applicants, since "consumers" under the CCPA include employees and job applicants.
- Illustrative of how many state privacy laws already encompass, or are being expanded to, cover automated decision-making.
- Core compliance obligations include notifying employees/applicants of this use of ADMT, the type of decisions it will inform, key information about how it works and how individuals can exercise their right to opt-out (which means the business must also maintain a manual process alongside any such use of ADMT).

These state and local AI-related laws and regulations are indicative of several emerging trends:

- **Transparency and disclosure are now baseline expectations.**

  Whether under NYC's bias-audit mandate or California's ADMT record-keeping rules, employers must be prepared to document and, in some cases publicly share, how their automated tools operate.

- **Vendor liability is front and center**.

  By defining "agent," "proxy" and automated decision-making explicitly (as in California), these regimes acknowledge that third-party vendors — not just end-user employers — may bear responsibility, paralleling the legal theory in *Mobley v. Workday*.

- **Risk-management and human-review obligations aim to prevent "black-box" auto-rejection at scale.**

  Laws like CAIA specifically require human review/appeal mechanisms or reasonable care processes to prevent adverse employment decisions being based solely on an automated system without sufficient explainability or accountability.

- **Employers operating across multiple jurisdictions face a compliance maze.**

  A single recruiting platform might trigger obligations under multiple laws — for example, bias audits under NYC law, record-keeping under California FEHA and risk-assessment under Colorado CAIA — requiring careful governance and risk management programs, vendor contract negotiations and operational policies.

The rapidly evolving legal and regulatory landscape around this "new" technology means that businesses can no longer assume that AI is unregulated. There might not be consensus or consistency around the specific mechanisms yet, but the growing patchwork of state and local AI-related laws around the subject matter alone mandates a thorough analysis of these requirements before a business implements and scales any AI-enabled HR-related solutions.

Best Practices for Using AI in Recruiting – A Practical Playbook

Businesses seeking to responsibly implement AI in their recruiting processes should consider developing a strategic compliance roadmap that encompasses the following pillars:

- AI inventory, risk assessments and governance
- Vendor diligence, contracting and accountability
- Bias testing, auditing and quality management
- Human oversight, appeals and opt-outs
- Transparency, notice and consent and candidate communication
- Documentation, monitoring and continuous review

For those seeking to initiate this process, there are several interim measures we would recommend addressing the following as part of your immediate compliance strategy to mitigate your AI risk:

- **Assess your risk.** Inventory your AI use cases, evaluate the legal and regulatory risks posed by those use case parameters (e.g., which state and local laws apply?) and ensure your existing governance and compliance programs prevent employees from using AI tools without prior approval.
- **Conduct vendor due diligence.** Review and refresh your current vendor diligence documents and procedures to ensure they address AI-specific risks, ensure your current diligence materials/analysis cover the AI tools currently in-use by employees (e.g., HR) and evaluate whether the corresponding vendor contracts sufficiently address AI or if additional indemnities and/or other contractual provisions are needed.
- **Improve your risk mitigation strategies, including human oversight and documentation.** This may include conducting any bias testing, audits or other risk assessments required for the jurisdictions in which you operate; implementing formal governance policies and procedures to quality management controls like human oversight; or drafting and publishing updated notices regarding your use of automated decision-making technologies and relevant opt-out and/or appeal procedures.

Every AI compliance journey is highly fact-specific, so please let us know if you would like assistance assessing your AI risk, developing a tailored compliance roadmap or drafting requisite policies and notices regarding your AI use.

Conclusion – Recruiting With AI, But with Eyes Wide Open

As AI becomes more deeply embedded in employment decision-making functions, *Mobley* and the first wave of state AI laws make one point unmistakably clear: the use of AI tools now sits squarely inside the existing framework of anti-discrimination and employment-law risk. The era of informal experimentation is ending, replaced by a need for disciplined, auditable governance across HR, legal, compliance and IT. Employers and vendors that proactively assess gaps, update contracts and policies, validate and monitor their tools and build transparent, human-centered workflows will be best positioned to capture the efficiency gains of AI while avoiding the litigation, regulatory and reputational pitfalls that accompany algorithmic hiring.

Agentic AI for General Counsels: What You Need to Know

Bryce H. Bailey
Associate
Dallas

KEY TAKEAWAY: Agentic AI introduces new legal and operational risks, from autonomous decision-making and contract exposure to evolving global regulation. GCs should evaluate these tools early, define their authority clearly and embed oversight into every phase of deployment.

Introduction

In recent years, use of generative and other types of artificial intelligence, machine learning and predictive applications (collectively, AI) has exploded and dominated global conversations. In past editions of our Client Reports, we identified various AI adoption risks and proposed a framework for evaluating AI tools generally.[1] For this year's edition, we are focusing on a particular type of AI tool rising in popularity — Agentic AI.

What is Agentic AI

For several years, businesses have used "predictive AI" to analyze data and forecast outcomes, "generative AI" to create text, images and other original content, and chatbots to interact with customers. Agentic AI goes even further. Agentic AI typically interacts with people or systems, gathers data and completes tasks — like an assistant or service agent — often with no or minimal human input. Certain key features cause it to stand out:

- Goal-driven action, completing multiple tasks or sub-tasks in a self-determined order, or solving bigger issues and coming up with the tasks to do so on its own;
- Accessing information from multiple systems or sources, including potentially other AI agents, enterprise systems or sensors; and
- Autonomous decision-making and execution

1. 2025, 2024 and 2023 Technology Transactions & Data Privacy Reports

Why Agentic AI Deserves Special Attention

In July 2025, MIT's Media Lab reported grim research findings: 95% of corporate AI initiatives show zero return. The issue is often not the product itself, but the insistence on having an "AI initiative" instead of tackling a specific business need. Despite question marks around the return on investment, nearly 40% of organizations reported deploying AI tools — they are already integrated into an entity's tech infrastructure. AI Agents and greater systems are quietly entering operations as a seemingly low-risk, low-cost add-on to existing AI tools for current enterprise systems. But Agentic AI generally requires a constant stream of information, as well as the ability to interact with a world outside its own company systems, to be most effective. It blurs the lines between employee actions, automated processing and decision-making, and accountability. That access, outreach and blurred lines can dramatically ratchet up risk exposure in ways easily overlooked or not yet recognized.

Agentic AI Risk Factors

Agentic AI introduces additional legal exposure because these systems are often designed to act autonomously. Key factors to consider prior to their deployment are described below.

Applicable Comprehensive Laws and Regulations

General Counsel (GCs) must carefully navigate laws and regulations from the international to the state level. Some laws are specific to AI, but others may be indirect (e.g., related to specific data, use cases and industries).

- *In the EU*, the AI Act imposes stringent obligations on high-risk AI systems, including transparency, documentation and human oversight requirements.
- A U.S. federal comprehensive scheme governing AI or data privacy does not exist. Regulatory enforcement, however, has been active. Federal agencies such as the Securities and Exchange Commission (SEC) and the Federal Trade Commission (FTC) continue to signal they will hold AI Agent users accountable through increased scrutiny of AI-related investments, marketing claims and business endeavors.[2] Misleading marketing statements about an AI Agent's capabilities remain a focal point for regulators, as evidenced by recent enforcement trends. The Equal Employment Opportunity Commission (EEOC) launched the Initiative on Artificial Intelligence and Algorithmic Fairness over five years ago. Agentic AI systems may inadvertently violate anti-discrimination rules if their decision-making processes lack transparency or bias controls.
- *At the U.S. state level,* regulations regarding "Agentic AI" by name are nonexistent, but there are laws and regulations on automated decision-making. California, Colorado and Virginia, for example, mandate specific consent and transparency obligations. In early December 2025, the President issued an executive order attempting to ultimately limit state level AI regulations. GCs should monitor and anticipate changes relating to this.

2. FTC Launches Inquiry into AI Chatbots Acting as Companions; FTC Sues to Stop Air AI from Using Deceptive Claims about Business Growth, Earnings Potential, and Refund Guarantees to Bilk Millions from Small Businesses

Liability for Autonomous Decisions

Courts are struggling with questions of how responsibility and liability flow through an AI Agent to the deploying company. Liability has been extended to companies when their AI agent or chatbot makes misleading or inaccurate statements. If this idea of "AI agents as ACTUAL agents" expands, so too will the potential legal complications. Companies might face vicarious liability for actions taken by the Agentic AI (just like an employee or contractor). Agentic AI could also create contractual corporate obligations if third parties are relying on the Agentic AI's output or actions. Negligence claims may arise where organizations fail to implement adequate guardrails or oversight mechanisms.[3] In certain contexts, Agentic AI could also trigger or increase product liability exposure, especially if defects in design, training or warnings lead to foreseeable harm or the Agentic AI relates to the operation, support or maintenance of a tangible good.

Contractual and Operational Risks

Agentic AI that automatically issues refunds, makes representations or enters into transactions may result in unwanted contractual commitments, operational issues or other risks or liability, especially if the Agentic AI does so beyond its intended authority or unexpectedly.

Additionally, Agentic AI's access and use of other software, tools, websites or application program interfaces (APIs) may give rise to a breach of contract. Third-party terms of use may restrict access to certain human users or prohibit automated utilization; an AI Agent accessing, utilizing, modifying or otherwise interacting with that software may be a breach. Similarly, the risk of breach of confidentiality escalates when AI Agents have access to sensitive data and inadvertently expose proprietary or regulated information. These risks underscore the need for robust contractual review and governance.

Security Risks

Agentic AI introduces unique cybersecurity challenges. Attack vectors such as prompt injection or jailbreak exploits can manipulate AI Agents into executing harmful actions. Unauthorized system access or unintended integrations triggered by autonomous decision-making amplify these concerns. Developers can implement sandboxing, permission boundaries and continuous monitoring to mitigate these risks.

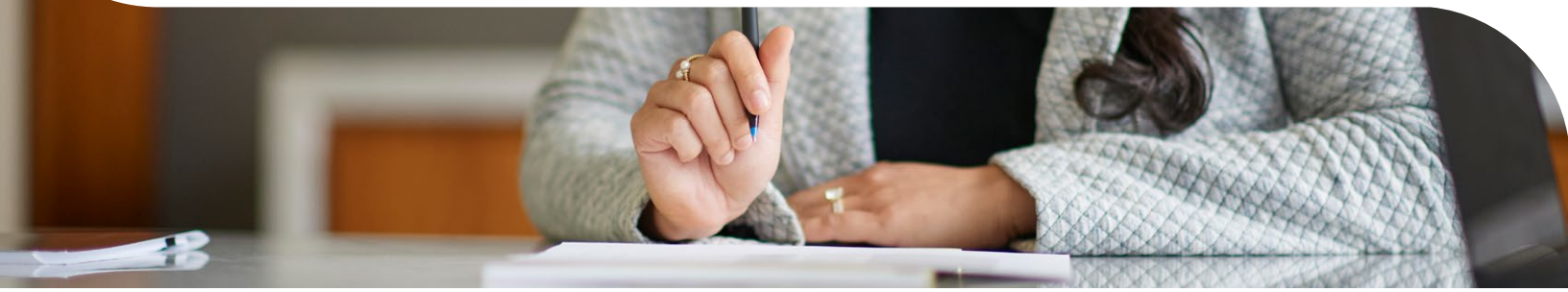
3. *See* also Stephen D. Bittinger, Cat Kozlowski, Melissa M. Yates, Joan Gilhooly, "The Use of Artificial Intelligence in Reimbursement Disputes" 2025 Health Care Reimbursement Newsletter p. 36 (https://polsinelli.gjassets.com/content/uploads/2025/06/2025_HC-Reimburstment-Newsletter_8432803554_v2.pdf)

Evaluating and Mitigating Agentic AI

To evaluate and mitigate Agentic AI risks, begin by asking:

1. **What is the tool?**
   - Is it actually Agentic AI? What models or other tools does it utilize?
   - What are the legal concerns, potential biases or protections baked into the Agentic AI?
2. **What is the use case or issue?**
   - Does this objective benefit from autonomous decision-making?
   - How critical or sensitive is the method by which the objective is achieved?
   - What is the tolerance for error?
3. **What is the data going into it?**
   - Can the AI pull data solely from pre-approved sources?
   - What can be accessed? What is screened off or blocked?
   - What risk does external or public information potentially create?
4. **What are the outputs or actions?**
   - What actions (or inaction) could occur and with what result?
   - What sectors of the business are impacted?
   - Is autonomous decision-making even permissible?
5. **How accurate is it?**
   - How do we measure accuracy (false positives and negatives)?
   - What levels of error (under service level commitments) can we tolerate?
   - Do minor inaccuracies upset the purpose?

Also consider how the Agentic AI's functions were done previously. A lot of tasks being automated by Agentic AI were once outsourced. Manual processes predating Agentic AI likely were not 100% accurate and likely included (i) defined and limited scope and authority by human "agents" based on seniority and role; (ii) escalation or approval paths for certain actions or decisions by supervisors beyond predefined thresholds (e.g., a customer refund or claim over $1,000); (iii) review and oversight for quality control; and (iv) approvals and documentation to audit and justify actions and decisions. Agentic AI may be faster and more accurate and of lower or similar risk, but deploying AI conservatively, alongside supervisory manual processes, will mitigate risks and improve efficiency.



When negotiating agreements for agentic AI tools, we recommend:

- Defining the nature and limitations of the Agentic AI tool's authority
- Allocating risk through warranties, disclaimers and indemnities
- Imposing guardrails and restrictions, such as use of unauthorized systems or data
- Requiring audit trails and rights for traceability
- Mandating transparency to end users, including disclosures that interactions may involve an autonomous agent and options to escalate to a human representative
- Requiring compliance with evolving laws, leading standards and continuous improvements
- Including robust termination and suspension rights in the event of accuracy or safety concerns, regulatory inquiries or material deviations from minimum requirements

These provisions should be calibrated to the specific model and contract. For example, Agentic AI handling low-risk internal administrative tasks does not require the same protections as approving transactions or interacting with customers.

Of course, contractual protections need to be paired with operational and other safeguards — especially for smaller AI vendors with limited financial resources. Accordingly, GCs should ensure that:

- Organizational governance is clearly established, and vendor tools are not solely relied on
- Users receive clear notices and opt-out options
- Agentic AI undergoes rigorous testing before deployment
- "Human-in-the-loop" or "human-on-the-loop" constraints are built into high-impact decisions
- Thresholds and boundaries exist (e.g., cannot execute financial transfers in excess of X)

Conclusion – Summary and Future Legal Trends

Agentic AI offers transformative potential for businesses of all types but introduces risks that demand legal review and consideration during the development phase, deployment phase and regularly thereafter.

Predictions for Future Legal Issues

- Stricter regulatory regimes, including explainability, audit trails and human approvals for high-risk use cases
- Regulatory requirements for sensitive industries (e.g., finance, insurance and health care) and use cases
- Enhanced due diligence standards for AI vendors and tools and ongoing governance and monitoring
- Litigation associated with errors, misrepresentation, discrimination and autonomous output, transactions or decisions

Seven Practical Steps to Data Management: A Guide for Businesses

Kathryn T. Allen
Technology Transactions Vice Chair
Kansas City, Dallas

Kelsey L. Brandes
Associate
Kansas City

Nguyen P. Le
Associate
St. Louis

KEY TAKEAWAY: Good data management is more than storage — it's strategy. From goal-setting and classification to governance, integration and analytics, these seven steps help businesses turn raw data into reliable, scalable insight.

In an era where organizations generate more data than ever before, the ability to manage that data efficiently has become a strategic advantage. Good data management improves decision-making, enhances operational efficiency, reduces risk and opens the door to innovation.

Whether you are a small business considering data management for the first time or a large enterprise optimizing existing products or systems, the following seven practical steps lay the foundation for strong, scalable data management.

1. Identify Your Goals

Every data management initiative should begin with a clear, measurable goal. Determine why you are managing data and what outcomes you want to achieve. Examples include improving reporting accuracy, enabling predictive analytics, ensuring compliance or increasing automation. Or perhaps your goal is simply to save money by removing redundant or outdated data. Defined goals guide technology choices, staffing and long-term planning.

2. Classify Your Data

Organizations often collect and store more data than they realize. Start by inventorying the data you have — customer or vendor data, transactional data, sensor data, financial records, documentation, etc. Then, classify it by sensitivity (public, internal, confidential and regulated) and usage. This aids in assigning the right protections, retention policies and access levels to each classification of data. You will also want to note the different places and systems (including third-party systems) where your data resides.

3. Implement Data Governance Policies

Data governance creates structure and accountability. Define rules for data ownership, quality, security, compliance and usage. Determine time periods for which you will keep each type of classified data and set up deletion protocols to implement when those time periods expire. Decide who can access which types of data and who can delete which types of data. Restrict data to those employees who need to access it. Your policies should reflect the types of data you are managing.

4. Develop Standardized Data Storage Strategies

Data must be stored securely, logically and in a way that supports growth. Choose appropriate storage solutions such as relational databases, cloud data warehouses, data lakes or hybrid environments. Document how and where each data type should be stored. Adopt standardized naming conventions. Establish, maintain and routinely test appropriate backup and recovery procedures, including recovery time objectives (RTO) and recovery point objectives (RPO).

5. Implement Strong Data Security Measures

Seventy-five percent of organizations must adhere to at least two data regulatory regimes relating to security and retention, such as the Health Insurance Portability and Accountability Act (HIPAA) for health care data, Financial Industry Regulatory Authority (FINRA) for financial data, General Data Protection Regulation (GDPR) for European personal information and California Consumer Privacy Act (CCPA) for Californian personal information (or other similar laws in other U.S. states). Many companies are subject to an even greater number of such regulations, and industry compliance standards, such as SOC 2 or PCI DSS. At the same time, fewer than one in three organizations have confidence that their policies could stand up to regulatory scrutiny. Avoid regulatory pitfalls by reinforcing your organization's data security measures.

First, determine the regulations that your organization is subject to and ensure that your organization complies with those. Then, make sure your business is using encryption, role-based access control, multi-factor authentication and network-level protections to secure access to data and networks in general. Once you have strong security measures in place, regularly conduct risk assessments and penetration tests to identify and promptly address security weaknesses. Finally, routinely educate your employees on data security practices and compliance.

6. Create Efficient Data Integration Processes

Data is more useful and valuable when it can flow between systems. Use integration tools such as extract, transform and load (or extract, load and transform) (ETL/ELT) pipelines, application program interfaces (APIs) and middleware to automate integration of data from multiple sources. Seamless automatic integration processes help reduce human errors and ensure data is available in real time or near-real time for analytics and operations.

Data integration processes should also include checks on the quality of the data. Data with more quality controls are more likely to be useful. And poor-quality data can have negative implications on your business. Data quality problems can stem from human error, incompleteness, inaccuracy, inconsistency, duplication or untimely updates.

7. Adopt Scalable Analytics and Reporting Tools

Select and implement analytics tools that meet both current and future needs of your organization. Business intelligence platforms, dashboards, artificial intelligence/machine learning tools and self-service reporting systems empower teams to extract insights independently. Standardize metrics and definitions across tools so that everyone speaks the same "data language" for ease and consistency.

Conclusion

Effective data management requires a balance of strategy, technology and culture. By following these seven practical steps, organizations can transform raw information into a powerful asset that drives innovation, supports better decision-making and ensures long-term resilience. As data ecosystems grow more complex, businesses who invest in disciplined, proactive data management will be better positioned to thrive in a data-driven world.

Seizing the Moment: Leveraging CMMC as an Opportunity to Enhance Cyber Risk Management

Sarah S. Glover
Shareholder
Birmingham

Erin L. Felix
Shareholder
Washington, D.C.
San Diego

Mary Ann H. Quinn
Associate
Washington, D.C.
Atlanta

KEY TAKEAWAY: CMMC raises the stakes for contractors. As formal documentation requirements and heightened security controls become legally binding — inviting increased scrutiny of any gaps — the smart move is folding CMMC into existing governance, not managing it off to the side.

As the Department of Defense[1] (DOD) moves forward with the phased implementation of the Cybersecurity Maturity Model Certification (CMMC), government contractors and their supply chains have an opportunity to rethink how to approach cybersecurity risk management in the context of their ever-increasing compliance requirements. For many organizations, the most difficult aspect of CMMC will not be the technical requirements themselves but positioning the program alongside an existing network of obligations that may include the Health Insurance Portability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Securities and Exchange Commission (SEC) cybersecurity rules, state privacy laws or international frameworks such as the European Union's General Data Protection Regulation (GDPR) or Network and Information Security Directive 2 (NIS2), as well as contractual requirements. There is significant strategic value in approaching CMMC compliance as part of a broader effort to strengthen the organization's compliance architecture and cybersecurity posture as a whole. Taking this coordinated approach will pay dividends beyond CMMC, often simplifying audits for ISO, System and Organizations Controls 2 (SOC2), HIPAA or financial reporting purposes and avoiding the compliance fatigue that organizations have come to feel.

What Makes CMMC Different?

Part of what makes CMMC distinct from other compliance frameworks is that it introduces an expectation of sustained documentation hygiene that may exceed what organizations are accustomed to under other frameworks, particularly those that are more flexible, principle-based or reliant on periodic audits that do not require continuous evidence maintenance. CMMC requires organizations (especially those at Level 2 and above) to produce objective evidence that a control is implemented and operating as designed. **It is not enough to have a particular technical control in place — the organization must be able to regularly show *how* it works, *where* it applies, *what* is responsible for it and when it was last reviewed.**

CMMC documentation may include producing system security plans, detailed network and data flow

1. President Trump signed an Executive Order on September 5, 2025, renaming the Department of Defense to the Department of War. As of the date of this article, CMMC program requirements and the corresponding published regulations continue to reference the Department of Defense, so this article similarly retains this naming convention for consistency.

diagrams, inventories of assets and authorized users, incident-response policies and procedures and a full suite of supporting evidence for each implemented control. While an organization may have a robust patch-management practice, CMMC will require them to maintain written procedures, retain logs that demonstrate scanning and remediation activity and connect those artifacts to broader risk-based decision-making. Similarly, incident response under CMMC is not just about reacting effectively to a cyber event — it is about having documented playbooks, testing those playbooks, capturing lessons learned and mapping the results to ongoing improvements.

CMMC requirements can feel more granular and prescriptive or burdensome than other compliance frameworks and may be challenging for organizations without centralized governance structures or mature cyber risk management processes in place. It is also why companies taking on CMMC compliance for the first time often try to manage it as a siloed or ad hoc effort. But this would be a mistake. By not incorporating CMMC into centralized compliance functions, organizations can end up with fragmented or inconsistent documentation that does not fully reflect their true security posture. Instead, contractors and their supply chains should leverage this moment to fold CMMC compliance into existing governance structures. In many ways, CMMC may act as a forcing mechanism — pushing organizations toward clearer governance, more mature processes and increased operational resilience. Doing so will also enable contractors to adapt more quickly to regulatory change, whether that comes from the DOD, domestic privacy laws, international frameworks or evolving best practices in cybersecurity.

Understanding What's at Stake

The final CMMC rule marks a decisive shift — CMMC is now an enforcement regime, not just a guidance document. By requiring that organizations submit assessments to the Supplier Performance Risk System (SPRS), designate a senior "Affirming Official" to personally attest to accuracy and, in some cases, undergo third-party or government-led assessments, **the program turns cybersecurity compliance into a set of formal representations to the government.** The program's allowance for "conditional" certifications introduces additional expectations. Companies have up to 180 days to close specific gaps, but during that time they must functionally demonstrate steady progress, adhere to eligibility criteria and report failures. This is not punitive; rather, it reflects the government's expectation of ongoing accuracy in submissions tied to contract eligibility. Documentation that is outdated, incomplete or inconsistent can create a disconnect between what a contractor tells the government and what is actually occurring within its environment and program. That disconnect becomes more consequential as agencies, inspectors general and prime contractors increasingly rely on SPRS and CMMC artifacts to evaluate readiness and performance.

If the organization's statements prove inaccurate because a control was not fully implemented or a Plan of Action and Milestones (POA&M) was not properly managed, the issue shifts from a technical shortcoming to a potential misrepresentation and becomes a legal, financial and enterprise risk problem. Inaccurate CMMC-related attestations can expose a contractor to several forms of government action,

including False Claims Act (FCA) investigations, contractual remedies such as withholding of payments or termination for default, and in more severe cases, suspension or debarment. The Department of Justice (DOJ) launched a Civil Cyber-Fraud Initiative in 2021 to "combine the department's expertise in civil fraud enforcement, government procurement and cybersecurity to combat new and emerging cyber threats to the security of sensitive information and critical systems" and has been actively ramping up its enforcement. Early on, the DOJ pursued a cybersecurity-related FCA case against Aerojet Rocketdyne, in which the government alleged that the contractor misrepresented its compliance with DOD cybersecurity requirements, resulting in a multimillion-dollar settlement. The DOJ and Georgia Tech Research Corporation (GTRC) also recently announced a settlement to resolve civil False Claims Act allegations that GTRC misrepresented the nature and extent of its cybersecurity compliance under multiple DOD contracts. But enforcement actions are not limited to the DOJ — other agencies, including the SEC, FTC and HHS have also been active enforcers of inaccurate cybersecurity representations in certifications, filings, attestations and disclosures. Recent enforcement activity across federal agencies demonstrates that regulators increasingly view inaccurate cybersecurity certifications as actionable, particularly where contractors had reason to know that their programs were not aligned with their documented posture.

At the same time, the business landscape around defense contracting is shifting in ways that make timely and accurate CMMC compliance a practical necessity. Prime contractors, responsible for validating the CMMC status of their suppliers, are showing a clear preference for subcontractors with final certifications, established governance structures and demonstrably mature security practices. As these preferences solidify, **CMMC compliance will become a competitive differentiator.** Contractors who lag in their readiness may find themselves edged out of teaming opportunities or facing additional scrutiny, documentation requests or contractual conditions that slow down deal cycles or create friction in contract negotiations. In an environment where source-selection decisions can turn on *perceived* risk, an expired, conditional or incomplete certification becomes a visible disadvantage.

Gaps in CMMC readiness can also have operational effects on the organization. When controls are implemented unevenly or documentation lags behind actual practice, teams may find themselves scrambling to recreate evidence during audits or assessments, diverting resources from daily operations. This can be especially challenging for organizations that operate under multiple regulatory frameworks, where inconsistencies in one area may ripple through others. A lapse in asset inventories, for example, may affect CMMC readiness, but it can also impact incident-response timelines or the ability of the organization to adhere to privacy compliance or financial reporting requirements. Maintaining a stable baseline helps reduce risk from these downstream disruptions.

Understanding the risks of CMMC-noncompliance is not just about anticipating enforcement — it is about framing the opportunity to harmonize the organization's obligations, streamline oversight and build a security governance model that can grow and evolve alongside the business.

What Should Organizations Do?

1. Embed CMMC compliance into the company's existing governance structure.

Most companies already have committees or cross-functional bodies responsible for privacy, cybersecurity, internal controls or enterprise risk. Rather than creating new layers of oversight solely for CMMC, integrate CMMC discussions into these existing bodies. This allows leadership to view cyber and compliance issues holistically and ensures that decisions made for one regulatory regime do not inadvertently create conflicts or inefficiencies in another. It also brings CMMC into the orbit of legal, compliance, IT, security and procurement teams that are already collaborating on these issues.

2. Find the overlap and develop a unified control framework.

A useful starting point for an organization looking to begin or improve its CMMC compliance program is to understand the portfolio of frameworks that already govern the organization and find the common ground — the lowest common denominators. Most contractors have longstanding practices for risk assessments, access controls, incident response or vendor management because other regulatory regimes already demand them. A careful inventory often reveals that CMMC aligns closely with many of these existing obligations. The NIST 800-171 controls that anchor CMMC's Level 2, for example, share common DNA with ISO 27001, the HIPAA Security Rule and widely adopted cybersecurity frameworks like NIST CSF. By examining these programs together, organizations can identify natural points of convergence and avoid duplicating work.

This is where a unified control framework becomes especially valuable. Instead of treating each regulatory obligation as a standalone set of requirements, creating a unified framework allows an organization to maintain a single internal collection of controls that are mapped to CMMC, privacy laws, incident-reporting standards, resilience obligations or other sector-specific rules. When changes occur (such as the introduction of a new state privacy law or updated guidance under the SEC's cybersecurity governance rules), the organization can adjust its internal controls once and let those updates flow across all relevant frameworks. This reduces audit fatigue and encourages a more mature, integrated approach to compliance.

3. Develop a unified data governance and classification system.

CMMC requires organizations to define which systems process, store or transmit controlled unclassified information (CUI) or federal contract information (FCI). But these boundary scoping decisions are not unique to CMMC — they mirror the questions companies must consider when handling protected health information, sensitive financial data, regulated personal information or operationally-critical assets. Organizations that take a portfolio view of data classification and system architecture can often design unified enclaves or segmented environments that satisfy multiple regulatory demands simultaneously. This not only reduces the number of systems subject to strict controls but also simplifies incident response, access management and vendor oversight.

4. Enhance existing vendor management programs.

The supply-chain component of CMMC benefits from an integrated perspective as well. Vendor-risk management programs are oftentimes already required to satisfy privacy laws, HIPAA, financial regulations or contractual commitments. Incorporating CMMC flow-down requirements, subcontractor monitoring and documentation obligations into this existing vendor-management structure often results in a more coherent and manageable program. It also avoids placing contracting teams in the position of maintaining multiple parallel processes for vetting the same suppliers.

5. Treat assessments as enterprise events that are broadly applicable.

Internal and external assessments offer another opportunity to strengthen the entire compliance ecosystem. Because CMMC encourages pre-assessments and ongoing internal reviews, organizations can align these efforts with their audit calendars for other frameworks. A gap identified during a CMMC readiness review may be equally relevant for privacy compliance, financial controls or incident-response readiness. Treating assessments as enterprise events rather than CMMC-specific exercises encourages teams to collaborate on efficient solutions that will reduce risk across the organization.

Conclusion

CMMC may originate in the defense-contracting context, but its requirements reflect principles that are foundational to any mature compliance program, like repeatability, documentation, governance and accountability. Approached thoughtfully, CMMC can serve not as another burdensome compliance requirement but as a tool for aligning and strengthening the organization's entire cybersecurity and compliance posture. Polsinelli has a team of experienced professionals who can assist with further questions and help guide your organization through every stage of its CMMC compliance efforts.

AI-Driven M&A Deals: Navigating Data and Model-Centric Acquisitions in 2026

Laila Paszti
Principal
San Francisco

Gregory M. Kratofil, Jr.
Office Managing Partner | Technology Transactions & Data Privacy Chair
Kansas City

Jerita L. Dimaio
Shareholder
Washington, D.C.

KEY TAKEAWAY: AI M&A deals are no longer just about code. As data assets, model architecture and algorithmic risk reshape valuations, deal teams must expand diligence, tailor terms and rethink how they assess legal exposure.

In the early days of artificial intelligence (AI) dealmaking, deal teams treated AI-driven merger and acquisition (M&A) deals like traditional software deals. Due diligence and the legal documents governing the deal focused on familiar software moats such as proprietary code, sticky customer contracts and brand recognition, as well as software-related risks like intellectual property (IP) infringement and cybersecurity. While AI is implemented as software, it is more than *just* software, given the unique legal risks arising from its design, development and use. AI software systems, unlike traditional software, are also heavily dependent on data, algorithms and models, and they often require specialized hardware and intense compute power.

This article analyzes developing best practices for structuring AI-driven M&A deals to address these new risks, informed by recent market developments. Today, acquirers face a fundamental shift. Rather than merely evaluating ownership of software, they must determine which data and AI models underpin a target's competitive advantage and whether these assets can be legally and operationally acquired — and commercialized at scale — to justify the acquisition price. Similarly, sellers and their counsel need to recognize potential acquirer's concerns and be able to anticipate and address these concerns — both before and while undergoing M&A diligence.

Uniqueness of AI-Driven Deals

AI systems learn, adapt and — with the rise of agentic AI — increasingly take actions on their own, potentially making decisions without human approval. Generative AI, like ChatGPT, and highly specialized models, like diagnostic tools trained on medical imaging, bring new assets to the table, including: the datasets used to train, test, validate and refine models (**AI Data Assets**); the structural design choices that determine how a model processes information (**Model Architecture**); and the unique optimization methods and design choices baked into how a model learns and performs (**Algorithmic Innovations**).

This translates into unique risks, including around IP ownership and infringement, privacy and cybersecurity. Increasingly, a patchwork of laws imposes technical and operational obligations on AI systems, creating legal risks across their design, development and use. These novel risks present dealmaking challenges that traditional software-focused

frameworks weren't built to handle. Managing these risks while competing for deals in a market increasingly focused on proprietary data and AI capabilities requires a nuanced approach to diligence and deal terms. The shift is already showing up in the market. Recent transaction analysis of public deals reveals that over 80% of AI-focused deals now include tailored provisions to address these risks, up from less than 25% just three years ago.

Understanding Core AI Assets

AI acquisitions challenge deal teams to evaluate asset categories that were largely absent a decade ago. The primary drivers of AI valuations now fall into three main categories, each calling for specific due diligence approaches.

AI Data Assets

In AI acquisitions, proprietary AI Data Assets can be a key differentiator if competitors cannot easily gain access to or replicate the same or similar data and that data is of high quality. An AI model's performance is closely tied to the quality (and sometimes quantity) of the AI Data Assets it learns from — training on well-curated data enables better predictions and outputs. Besides raw data, additional data asset types may also drive value, including:

- Derivative data: cleaned, labeled or enhanced versions of raw data
- Synthetic data: artificially generated data that mimics real-world patterns
- Data pipelines: third-party partnerships and integrations that enable ongoing data capture

Model Architecture

Building robust, finely tuned models demands significant computational investment, expert input and iterative testing. The structural design of a model and ongoing enhancements can take years to perfect. A well-architected model may outperform competitors, even when trained on comparable data.

Models designed to filter potentially infringing, harmful or off-brand content are increasingly attractive to acquirers, particularly those operating in regulated industries or with significant brand exposure.

For certain industries and high-risk applications — like health care, financial services and employment decision support or making — explainability is critical. Regulators and customers may require an explanation of why a model produced a particular output. Models designed without explainability features can be difficult to retrofit post-acquisition, limiting their value in regulated markets.

Algorithmic Innovation

Algorithmic innovation captures algorithmic IP and source code. This includes optimization techniques (methods that make a model train faster or perform better) and other proprietary innovations that differentiate AI systems. Registered IP (e.g., patents covering novel algorithmic methods, copyright registration for code) can command premium values, as registration helps acquirers defend and monetize these assets more easily post-acquisition (e.g., by potentially blocking competitors).

Key Legal Risks Affecting Valuation

AI M&A deals present risk categories that traditional software diligence frameworks do not adequately address. Deal teams must expand their due diligence frameworks to capture these emerging concerns.

AI Data Asset Ownership and Provenance

Chain-of-title analysis for AI Data Assets requires tracing data lineage across multiple sources, auditing license terms for each dataset and verifying consents for data gathered from users (which could have been knowingly submitted by them or gathered from them in less obvious ways). Data may have been acquired through multiple channels, including licensing from third-parties, web scraping or data from customers, patients or end-users. Each source carries different issues and risks for an AI developer to safely use the data. A developer's use of the data must align with the rights under which the data was licensed or otherwise acquired.

Unauthorized scraping of copyrighted content has already generated IP litigation, with plaintiffs arguing that training on their content constitutes infringement. Regulatory enforcement actions by agencies such as the Federal Trade Commission (FTC) and Department of Health & Human Services (HHS) targeting data use without requisite consent are accelerating. Hybrid datasets that combine licensed, scraped and user-generated content pose particular challenges. Improperly acquired data can taint an entire AI product or system — especially when the AI cannot be retrained to exclude problematic sources without adversely impacting desired performance or if the prior training has fundamentally and irreversibly improved the AI in ways that are not practically reversible.

IP Infringement

AI models may exhibit "memorization," in that they reproduce or "leak" substantial portions of training data verbatim. This IP risk is particularly acute for smaller task-specific models, which are prone to data leakage because they have less capacity to generalize.

AI developers often assemble their codebase using third-party code, which may be licensed under commercial or open-source licenses. They may also use generative AI coding tools (which have their own memorization risks) to generate code. Understanding and auditing the underlying third-party code components and ensuring appropriate license rights, including for open-source components, is important to mitigate IP infringement or incompatible license use (e.g., where a viral open-source license requires developers to make proprietary code available at no cost).

AI Compliance

Legal regimes such as the EU AI Act and state legislation in California, Colorado, New York and Utah impose prescriptive technical and operational requirements, including documentation, transparency and human oversight. Violations can result in significant fines and penalties. The EU AI Act, for example, authorizes penalties up to €35 million or 7% of global annual revenue. In the U.S., the FTC has ordered model disgorgement, requiring companies to delete AI models trained on improperly obtained data as a remedy for data collection violations. For an acquirer, this could mean losing the very asset that drove the deal.

High-risk applications such as employment screening, credit decisioning and health care diagnostics and decision support face heightened regulatory scrutiny under a patchwork of federal and state laws, including laws that may not even reference the term AI (e.g., the Federal Trade Commission Act). In addition, the use of AI may trigger other legal

considerations. For example, health care AI systems may fall within the U.S. Food and Drug Administration's (FDA) Software as a Medical Device (SaMD) framework, creating distinct premarket review and ongoing compliance obligations. Noncompliance with these requirements can result in significant regulatory penalties.

Data Privacy and Cybersecurity Compliance

Privacy compliance diligence must consider AI-specific processing obligations (e.g., where an AI system trains on or otherwise processes personal information). This includes mapping data flows, training sources and model use cases against applicable legal regimes. Several state laws, including the California Consumer Protection Act and similar statutes, grant individuals who are the subject of decision-making by an AI system (an AI subject) certain rights, including notice, opt-out mechanisms, access and correction rights and in some cases, a right to appeal or to an explanation of the decision reached by the AI system. Implementing these often requires that AI systems or their outputs include certain features and functionality, such as the ability to provide an AI subject with information about how their personal information is used by the AI system. Sector-specific regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (45 C.F.R. Part 164, Subpart E), create additional compliance obligations that vary depending on how AI systems process personal information (e.g., whether in raw or de-identified form).

AI systems are a particular target for cyberattacks given their broad attack surface. Data pipelines, APIs and model endpoints all serve as access points to malicious actors. AI systems also imply unique attack vectors that do not exist in traditional software. Prompt injection attacks manipulate model behavior by injecting malicious inputs disguised as legitimate queries. Model inversion reverse-engineers training data from a deployed model's outputs. Data poisoning corrupts training datasets, embedding vulnerabilities that persist through updates. Legal and technical diligence must evaluate protections specific to these AI risks.

Structuring Approaches for AI-Specific Risks

Standard transaction documents require significant adaptation for AI-centric acquisitions. The following approaches represent emerging market practice for addressing AI-specific risks.

Preparing for the Deal

At the onset, tailoring due diligence request lists and customizing precedent documents to the target's industry, business, AI use cases and the overall deal thesis can help with competitive deals. For an acquirer with a limited risk profile, letters of intent (LOIs) may delineate the scope of technical and legal due diligence (e.g., software code/AI model audits, data set analysis, data science or statistical analysis of AI performance and cybersecurity).

Due diligence often sets the tone of a deal, and overbroad or unexpected diligence requests result in frustration for both parties. For example, asking for "a list of all AI tools/systems" will generate "noise" — nearly every software tool now has some AI feature or functionality. It is far better to focus requests on the AI assets that actually drive value and risk.

Deal Structure and Type: Purchasing the Stock or Assets of a Company

The choice between an asset purchase, stock purchase or other structure matters in AI deals. In a stock purchase, the acquirer buys the entire entity, including all AI assets, data rights and liabilities. In an asset deal, the acquirer selects specific assets to acquire (or license), which can be advantageous when isolating valuable AI components from unwanted liabilities. However, asset deals require careful analysis. The seller may retain valuable IP, IT infrastructure or data that is critical to model use and performance. Additionally, data licenses, API agreements and other third-party contracts may not be assignable — some data rights may be non-transferable or require consent, potentially leaving critical AI assets behind. Additionally, the target's asset may be a compilation of open-source assets and know-how related to that, which others could replicate, which is increasingly important when development teams/management do not transfer as part of the deal. Best practices for managing risk include:

- **Scheduling AI assets.** AI assets should be scheduled with specificity in the transaction agreements, beyond traditional IP schedules. This includes model versions (with documentation of changes between versions), training methodologies, datasets used in each training cycle and dependencies on third-party tools or infrastructure. Without this detail, acquirers may not fully understand what they are actually acquiring.
- **Ancillary agreements**. Sometimes the IP, IT infrastructure or personnel critical to an AI system fall outside the perimeter of an asset deal. Ancillary agreements can bridge these gaps.
  - *Transition services agreements (TSAs).* A TSA allows the acquirer to temporarily access the seller's resources — personnel, systems or infrastructure — for a defined period post-closing. When key personnel are essential to ongoing development or maintenance, TSAs can facilitate knowledge transfer. Where a target's AI systems rely on specific cloud providers or specialized hardware, TSAs can provide continuity while acquirers plan for data migration, pipeline integration and infrastructure compatibility. Acquirers may also consider retention arrangements for essential technical staff.
  - *IP licenses.* Where datasets or proprietary know-how are retained by the seller or cannot be transferred outright (due to third-party restrictions, consent requirements or contractual limitations), IP licenses between the seller and acquirer can provide the rights needed to (i) continue operations while longer-term solutions are negotiated or (ii) jump-start developing and commercializing the next generation of the target's AI product or tool.
  - The scope and duration of non-competes relating to founders and other key resources may also be especially important if the AI related assets could be recreated using third-party or open-source materials relatively easily.

Enhanced Representations and Warranties

Relying on traditional IP or software protections is insufficient to limit the risks posed by AI assets. Transaction analysis[1] shows that over half of recent AI-focused deals included specific representations addressing the provenance of training data and compliance with applicable license terms. Approximately one-third now include representations regarding ethical or responsible AI use, and nearly one-quarter specifically address the use of generative AI tools/systems. Comprehensive representations might address AI-specific risks, including:

- Validated data provenance and chain of title for all AI Data Assets;
- Training data obtained through lawful means with sufficient rights for any personal data included;
- Absence of infringement claims related to training data or model outputs;
- Compliance with AI-specific regulations;
- Adequacy of AI governance frameworks, including bias testing and ethical use policies;
- Disclosure of material/external/customer-facing third-party AI tools/systems and foundation models used, with confirmation of compliance with applicable license terms;
- No personal, confidential or proprietary information or source code input into third-party generative AI tools/systems;
- No use of generative AI to create material company IP without human review;
- Adequate technical documentation sufficient for model modification, debugging, statistical analysis and retraining/tuning; and
- No pending or threatened regulatory inquiries or investigations related to AI practices.

Special Indemnities and Liability Exposure

When a significant risk is identified during diligence, an acquirer may require the seller to indemnify it for losses arising from those risks through a specific special indemnity in the M&A agreement. Special indemnities are distinct from general indemnification and often have separate caps on liability and time periods during which claims can be asserted. They are not the norm and are heavily negotiated. They may address claims relating to certain active proceedings or arising from AI Data Asset provenance, privacy violations related to specific datasets, open-source license violations in AI components, cybersecurity risks or regulatory enforcement actions targeting AI practices.

From a liability perspective on AI-related representations, warranties and indemnities, buyers and sellers may have conflicting views on liability exposure. Buyers may want to treat AI- and other IP-related representations and indemnities as fundamental to the deal, with exposure up to the purchase price, while sellers may seek to limit exposure to a modest percentage of the purchase price or the amount escrowed. What is appropriate for a specific deal can depend on many factors, and there are a variety of potential compromises.

Pre-Closing Remediation Covenants

Pre-closing remediation covenants — when the seller agrees to fix identified issues between signing and closing — are rare, but not unheard of. Where diligence identifies specific data provenance concerns, pre-closing remediation covenants may require sellers

1. This article draws on a review of publicly available transaction documents involving AI-driven acquisitions from 2021 to 2025.

to retrain models on verified clean datasets; delete or replace problematic training data; implement enhanced documentation of data lineage; and complete third-party audits of AI systems. An acquirer may want to include a right to verify that remediated models maintain acceptable performance, accuracy and functionality.

Representation & Warranty Insurance (RWI)

RWI has become a standard feature in M&A transactions, allowing acquirers to seek recovery from insurers rather than sellers for breaches of representations. It's generally seen as a win-win for both parties. RWI underwriters are taking a closer look at AI-related risks, reflecting the complexity and novelty of these exposures. They may require additional diligence into AI assets, and certain AI-related risks may be excluded from coverage or subject to enhanced retention requirements or sub-limits. Where coverage is available, enhanced retention requirements or sub-limits may apply.

Parties should engage with insurers early to understand available coverage and tailor representations accordingly. Acquirers may need to adjust deal terms, such as escrows, indemnity caps or purchase price holdbacks, to account for risks that fall outside RWI coverage. Sellers can improve insurability by maintaining robust documentation of data provenance, AI governance practices and regulatory compliance efforts.

Post-Closing Compliance

Many AI M&A deals involve larger companies acquiring smaller companies without mature systems, products or governance practices. Documentation may be incomplete, compliance frameworks may be informal and institutional knowledge may reside with a handful of individuals rather than in written policies. Gaps identified during diligence don't disappear at closing — acquirers should plan for post-closing remediation and integration work to address these risks:

- Regulatory compliance monitoring should extend beyond closing, given the evolving legal landscape
- AI governance frameworks should incorporate ongoing monitoring for model drift, bias emergence and regulatory developments
- Documentation requirements continue post-closing — building out and maintaining auditable records of training data, model modifications and performance metrics supports both operational excellence and regulatory compliance
- Cybersecurity response plans should address AI-specific scenarios, including model failures, adversarial attacks and data contamination events

Additionally, for many AI M&A deals, the acquirer may be planning to scale the target's business or offering, and whether the target's AI technology is truly commercially scalable may not be certain until after the deal closes. Accordingly, acquirers could limit their risks (and targets could increase their upside) by considering earn-outs or other similar incentives or mechanisms based on future results.

Conclusion

The rise of AI-driven mergers and acquisitions demands a new playbook. Traditional diligence frameworks and historical standard-form documents are inadequate for evaluating and structuring transactions in which competitive advantage derives primarily from data assets and AI capabilities. M&A transaction data confirms this evolution. The vast majority of technology-focused deals now address AI matters explicitly, with increasingly sophisticated treatment of training data provenance, ethical AI use and generative AI tool usage — issues that were barely contemplated in transaction documents just a few years ago. Deal teams that develop AI-specific competencies will be positioned to execute successful transactions in this evolving landscape.

Current Trends in Data Breach Notification Laws: Increased Regulator Scrutiny Leads to Greater Responsibilities for Companies

Pavel (Pasha) A. Sternberg
Principal
Los Angeles, San Francisco

Tyler S. Kraft
Associate
Kansas City

KEY TAKEAWAY: Data breach laws are expanding on all fronts. New state and federal updates broaden what counts as personal information, tighten timelines and increase regulator involvement — raising the stakes for incident response and reporting accuracy.

As companies' reliance on technology continues to evolve and the amount of data companies keep continues to grow, so do the scale of data breaches and their associated costs. According to a recent study by IBM, the average cost of a data breach in the U.S. has climbed to $10.22 million USD — an all-time high not only for the country but for the entire world. While the continued evolution of disruptive-threat actor activity is partially responsible for driving up the costs of these events, the increased price tags are also due in part to higher state regulatory fines and more frequent class-action litigation filed against entities experiencing the breaches.

The higher regulatory fines and increased litigation activity are no coincidence, as various state legislatures have continued to focus their attention on data security and data breaches impacting consumer information. In 2025, Oklahoma's state legislature amended its state data breach protection law for the first time since its inception in 2008. New York passed an amendment to its data breach protection law in late 2024, only to pass another amendment to the same law three months later in early 2025. These are just two examples of various changes to data breach notification laws and regulations over the course of 2025. This article summarizes the changes to the data breach regulation landscape and trends that can be identified heading into the upcoming year.

Increased Scrutiny on Regulator Reports, Timelines

One common trend in updated data breach notification laws dealt with clarification of reporting deadlines to regulators for notices, and in some cases, instituting regulator reporting requirements where there were previously none. Oklahoma's former data breach notification law did not include notice to a state regulator in the event of a data breach. The updated law, which took effect Jan. 1, 2026, requires notice to Oklahoma's Attorney General within 60 days of notice to impacted Oklahoma residents if a data breach involves the information of 500 or more Oklahoma residents.[1]

New York's amendment involves similar changes. While the requirement to notify the New York Attorney General is nothing new, a 2025 amendment introduced a reporting requirement for financial institutions regulated by the New York State Department of Financial Services (NYDFS) to report data breaches to the NYDFS as well. The updated New York law also introduced a specific time element to the Attorney General reporting requirement. Instead of the previously malleable requirement for a report to occur without unreasonable delay, notification of a breach involving New York residents' personal information must now occur within 30 days of discovery of the breach.

This heightened scrutiny in reporting timelines is common across states. California, which passed an amendment to its data breach notification law in October 2025, will require notice to California residents within 30 days of an identified breach and a notification to its attorney general no later than 15 days after notification to the residents. Fannie Mae, the federally sponsored mortgage purchaser, amended its reporting requirements for lenders that experience a data breach to notify Fannie Mae within 36 hours of a known or suspected data breach involving Fannie Mae "confidential information."

The various amendments indicate that regulators not only increasingly want to know about data breaches, but they also want to know about them in a timely manner. With data breaches continuing to become more common, companies and entities at risk of experiencing them will need to ensure their protocols are up-to-date to ensure their reporting plans not only include the right entities, but also that those notifications are made within the correct timelines.

Growing Definitions of "Personal Information"

In a similar vein of regulators seeking more information on data breaches, multiple regulators increased the scope of what they consider "personal information" for the purposes of triggering a data breach. Oklahoma enhanced the scope of its "Personal Information" definition to include government-issued identification numbers, unique electronic identifiers allowing access to an individual's financial accounts and biometric data.[2]

Fannie Mae took perhaps the largest step in enhancing its scope of what is considered information that could create a data breach if subject to unauthorized exposure.

Under Fannie Mae's updated guidelines, lenders must notify Fannie Mae of unauthorized exposure or acquisition of "Confidential Information." Confidential Information includes "information that is not a matter of public knowledge or

1. *See* Okla. SB 626 (2025)
2. *Id.*

which is specifically designated as confidential." This can include not only information regarding borrowers that is non-public, but also information regarding the lender itself such as financial information, customer lists or any other information the lender itself holds in confidence. The definition is obviously extremely broad, and when combined with Fannie Mae's definition of a "Data Breach," which explicitly names common data breach occurrences such as ransomware attacks and business email compromises, can be expected to put significant strain on lenders trying to comply with Fannie Mae's updated timeline for reporting data breaches discussed earlier in this article.

The end result is that regulators are identifying more information as sensitive and expanding their definitions of "personal information" to account for it. This will undoubtedly result in more incidents rising to the level of a data breach, and in combination with the regulatory notice requirements discussed earlier in this article, lead to greater burdens created by data breaches.

Takeaways for Companies: The Case for Strengthening Data Breach Protections and Action Plans

Recent years have seen record increases in costs stemming from data breaches, and we anticipate 2026 figures to be no different given the increased scope and scrutiny given to data breaches by regulators and litigators. Proactively investing in measures to mitigate risks of experiencing a data breach and knowing whom to notify — and when — in the event of a breach is becoming increasingly valuable. It may also save companies from adding to the increasing costs that result from data breaches. In the event companies do experience a data breach, companies will need to keep in mind the timeframe and reporting requirements for any regulator that oversees them to ensure any costs already incurred from the breach are not exacerbated by avoidable fines and penalties for non-compliance.

Leveraging Cyber Insurance Trends to Strengthen Information Security Programs: Insights from M3 Insurance

Alexander D. Boyd
Shareholder
Kansas City

Caitlin A. Smith
Associate
Philadelphia

KEY TAKEAWAY: M3 Insurance and Polsinelli provide insights on how companies can adapt to a changing cyber insurance market and reduce the risks associated with data security incidents.

The cyber-threat landscape continues to demand a layered risk-management approach — one that both reduces the likelihood of an incident and enables an efficient, well-coordinated response when one occurs. Cyber liability coverage continues to be one of the most impactful tools organizations can invest in as part of their risk-reduction strategy. When purchased and used effectively, a cyber insurance policy not only transfers costs but also incentivizes proactive cybersecurity initiatives and provides access to specialized resources during a crisis.

To explore how the cyber insurance market is evolving and how organizations can better align their information security programs with these developments, Polsinelli spoke with Alex Friedl, CCIC, CIC, CISR, Brokerage & Cyber Liability Client Executive with M3 Insurance, a leading advisor in cyber liability coverage. His insights highlight important market trends and actionable steps that Polsinelli clients and other companies should take today to ensure they are holistically addressing their cybersecurity risks.

A Firming Market: Tougher Underwriting, Limited Coverage and Higher Costs

Across the industry, the cyber insurance market is firming, and flat renewal premiums are increasingly rare. Insurers are exiting high-risk classes of business, including health care, and are taking a closer look at certain controls such as specific VPN configurations. That being said, there is still excess capacity in the marketplace, especially among insuretechs and managing general agents, which is slowing an overall market hardening.

Practical Guidance for Companies Seeking or Renewing Cyber Insurance

- **Plan for Your Insurance Renewal During Incident Response.** If an organization experiences an incident, insurers will ask what steps are being taken to prevent similar events in the future. Documenting technological, policy and procedural improvements can improve the renewal process and insurance coverage outcomes.
- **Strengthen Cybersecurity and Privacy Programs Before Seeking Coverage.** Investing in and universally deploying tools like multifactor authentication (MFA), strong backup controls and endpoint monitoring, detection and response (EDR) does more than reduce the risk of a widespread incident. The effective implementation of these tools may be able to unlock better coverage, lower premiums and smoother renewals. However, purchasing access to tools that are not fully enforced or paired with fulsome employee training and incident response planning limits the effectiveness of the spend.

- **Know Your Privacy Practices, Especially on Your Website.** Tracking technologies, cookies, pixels and third-party scripts are frequent sources of privacy litigation. Organizations should evaluate how these tools are deployed, what data they collect and whether disclosures and configurations align with regulatory expectations.

Rising Claims Driven by Litigation Costs

According to M3, the largest cyber insurance claims tend to follow from those incidents that also result in data breach class action litigation. Organizations need to deploy a proactive, layered approach to address this risk.

Practical Guidance for Addressing Litigation Risk

- Organizations need to take technical steps to reduce the risk and scope of potential incidents and align those safeguards with any available state law safe-harbor provisions.
- Depending on the organization, mandatory arbitration and class action waiver provisions may be tools to manage some of these litigation risks.
- When an incident does occur, organizations must be ready with a tailored notification strategy to ensure that legally required notifications are provided without unnecessarily increasing the organization's litigation risk.
- As defense and settlement costs rise, organizations should reevaluate their policy's limits to ensure it is still sufficient to cover the current risk landscape.

The Consistent Threat of Business Email Compromise and Financial Fraud

While not a new risk, M3 reports an increase in business email compromise and related financial fraud claims. These incidents can be financially devastating and can be subject to low policy limits or strict terms limiting coverage only if certain steps were taken leading up to the incident.

Practical Guidance for Organizations Seeking to Avoid Fraudulent Funds Transfers

- **Implement a Comprehensive Payment Verification Process:** Create and train employees on a structured workflow for validating payment instructions through telephone calls placed to known contacts. This reduces the risk of fraud and increases the likelihood of insurance recovery if an incident occurs.
- **Audit Autopay and Vendor Invoicing:** Oftentimes organizations do not realize there has been an email compromise that led to a manipulation of payment instructions until several autopay cycles have passed. Organizations should regularly audit changes in instructions and verify them with the payor or payee before implementing.
- **Report Fraud Immediately:** Promptly notifying the Secret Service, FBI and your financial institution can significantly increase the chance of recovering funds.

Vendor-Caused Incidents are Increasing and Draw Greater Scrutiny

A growing portion of cyber incidents originate from third-party vendors. These incidents could involve sensitive data held by an organization's vendor or could involve misuse of the vendor's direct access to the organization's computer network. Insurers are more closely evaluating vendor management programs, aligning with Polsinelli's own experience advising clients on these complex exposures.

Practical Guidance for Vendor Management

- Classify and evaluate vendors based on cybersecurity impact, data access and retention and network connectivity.
- Require written agreements that include clear security obligations, breach notification responsibilities, data privacy requirements, indemnification provisions and adequate cyber insurance coverage and limits.
- Perform periodic reassessments and maintain documentation of vendor off-boarding, data deletion and access termination.

Cyber insurance will remain a dynamic component of mature information security strategies in 2026 and beyond. By proactively aligning technical controls, vendor management and privacy compliance with underwriting expectations, organizations can not only obtain stronger coverage but also enhance their readiness to respond to evolving threats.

When Breaches Bring Regulators to Your Door: Preparing for Heightened Scrutiny of Your Security Compliance Program

Michael J. Waters
Shareholder
Chicago

Jessica L. Peel
Associate
Kansas City

KEY TAKEAWAY: Regulators are digging deeper after breaches. Investigations now often go beyond questions about the underlying incident and general security practices and are diving deep into the specifics of an organization's cybersecurity program — making robust controls, documentation, consistency and internal alignment critical.

The prospect of dealing with a data breach can be frightening. Depending on the nature of the incident, a data breach can result in significant business disruption, loss of customers, loss of goodwill, substantial expenses and class action lawsuits. If that were not enough, data breaches can also result in regulatory investigations that serve as de facto audits of an organization's data security practices.

For years, most organizations have been subject to various state and federal laws that impose obligations to protect the security of personal information. However — other than entities in a small number of highly regulated industries like health care and financial services — there has often been little scrutiny into whether organizations are complying with these obligations.

That is starting the change. With increasing frequency, after receiving notice of a data breach, state and federal regulators are using the incident as an opportunity to conduct a deep dive on an organization's cybersecurity compliance program. Historically, these investigations have asked questions about the underlying incident, sought confirmation that the organization notified individuals in accordance with relevant breach notification laws and requested copies of various cybersecurity policies and procedures. More recently, and with

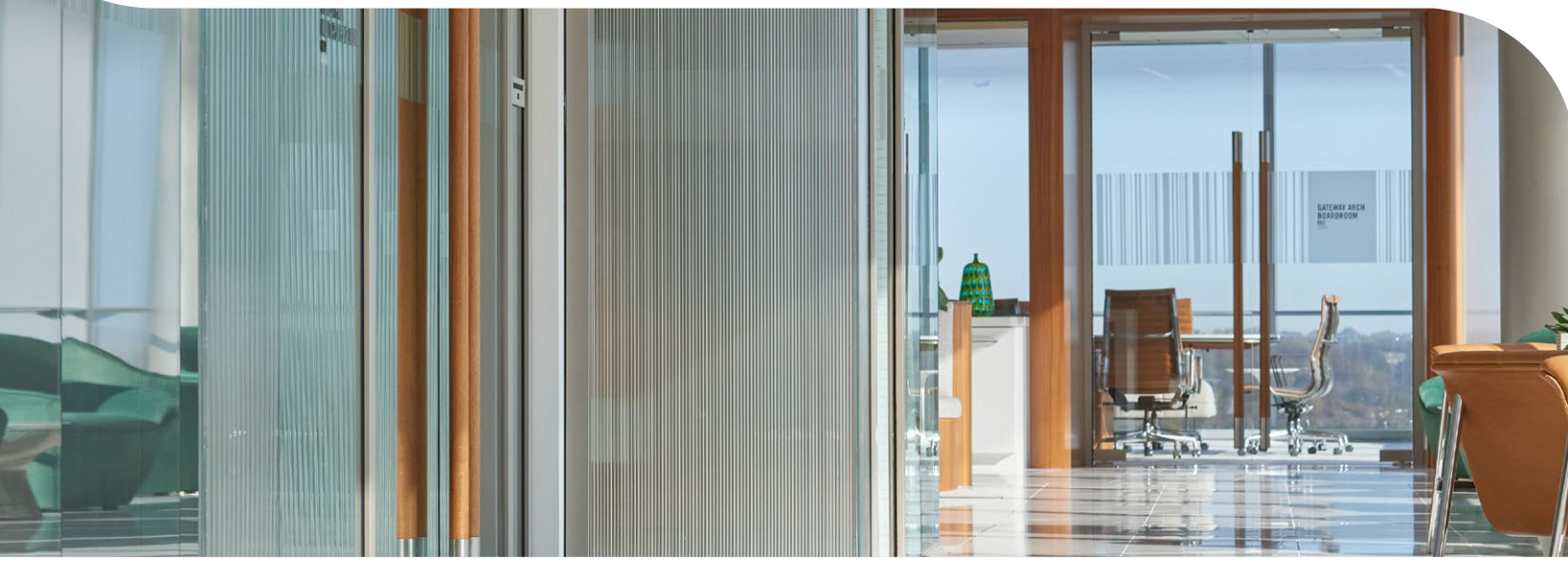
greater frequency, regulators are asking extremely detailed questions about organizations' administrative and technical controls.

Importantly, the regulators are not only asking what controls are in place, but they are requesting evidence that the organization is adhering to their security policies and procedures. For example, a regulator may request "a description of how long your company retains personal information and the originating date of the oldest information in this breach" to determine not only if the organization has an existing record retention policy, but if the entity is complying with that policy.

Additional examples of the expanded information requests are below.

- At the time of the incident, did the organization have an endpoint detection and response (EDR) agent installed? If not, why not? If yes, were any alerts generated regarding threat actor activity?
- Was two-factor/multi-factor authentication (MFA) enabled at the time of the breach? If not, explain why.
- Per your previous response, the organization has a policy to conduct yearly security audits. Please provide a copy of the security audits from the last X years.
- Per your previous response, the organization has a policy to regularly review the firewall status and security policies. Please provide a copy of all such reviews conducted in the six months prior to the incident.
- Please provide any reports or analyses regarding the technical security of your company's system that were generated up to a year before the breach.
- At the time of the incident, did the organization have any controls in place to restrict and/or monitor the use of file transfer software? If yes, please describe the controls.
- At the time of the incident, was data encrypted at-rest? If not, why not?

Further, regulators are increasingly issuing fines and entering into settlements based in significant part on the regulators' belief that entities did not take



sufficient steps to protect information pre-incident. For example, on Oct. 15, 2025, the New York Department of Financial Services (NYDFS) secured more than $19 million in penalties from eight separate auto insurance companies following cyber incidents for violations of NYDFS's cybersecurity regulation and NYDFS's finding that the companies maintained inadequate security controls.

Given the extent to which regulators are scrutinizing organizations' cybersecurity compliance efforts, organizations should consider:

- Maintaining a *written* information security program and documenting the organization's efforts to protect the security of personal data to ensure they can demonstrate those efforts to regulators.
- Confirming the organization is adhering to its policies and procedures. If your policies state the organization will conduct yearly risk assessments, make sure it is conducting yearly risk assessments. If the organization's record retention policy states that certain categories of data will be deleted after a set period, make sure data is timely deleted.
- If you determine the organization is not complying with its own policies and procedures, consider whether to update the organization's practices to ensure compliance or revising policies to reflect the organization's practices.
- Ensuring that legal counsel and risk management personnel are partnering with the information security team on cybersecurity compliance. For example, all stakeholders should work together to ensure compliance with the organization's written information security program. In addition, the information security team should be informed that, if the organization experiences a data breach, it may receive information requests along the lines of those discussed above, and all stakeholders should feel confident in the organization's ability to respond to those requests.

Most organizations are working hard to protect the data that is entrusted to them, but knowing those efforts may be subject to detailed scrutiny, organizations should work pre-incident to get comfortable with the defensibility of their compliance programs.

Trends in AI and Privacy Litigation: How AI Is Impacting the Privacy Litigation Space in 2026

Mark A. Olthoff
Shareholder
Kansas City

Courtney P. Klaus
Associate
Kansas City

KEY TAKEAWAY: AI-related privacy litigation is accelerating. From notetakers to customer service bots and facial recognition tools, courts are allowing claims to proceed — especially where consent, disclosure or data use practices are unclear.

Since ChatGPT launched as an experimental technology about three years ago, the popularity of artificial intelligence (AI) has exploded. So, too, has the popularity of AI-related lawsuits.

Discourse surrounding the ethics and legal implications of AI continues to evolve as AI becomes more prevalent in everyday business. Many companies have already implemented AI in one form or another, whether that AI is simply used to take notes during meetings, to provide customer service or to design whole websites. However, each of these common uses of AI can present litigation risks.

One common theme of plaintiffs who bring AI-related lawsuits revolves around how AI learns. AI often learns by being trained on vast amounts of data, using algorithms to identify patterns and make decisions without being explicitly programmed for every task. Where an AI collects or is provided with unfettered access to large amounts of consumer data, privacy concerns are likely to arise.

Several trends have developed in privacy litigation motivated by the rise of AI use.

AI Notetaker Litigation

Those who are used to meeting virtually via Zoom, Teams or any other video conferencing software have probably encountered some form of "AI notetaker." An "AI notetaker" is an AI-powered tool that automatically transcribes, summarizes and organizes audio or video content, such as meetings, lectures or interviews. They often integrate with other tools like video conferencing platforms or other productivity apps.

In August and September of 2025, plaintiffs sued a popular AI notetaker in four class action lawsuits in the Northern District of California, generally alleging violations of the federal Electronic Communications Privacy Act (ECPA), the Computer Fraud and Abuse Act (CFAA), the Illinois Biometric Information Privacy Act (BIPA) and the California Invasion of Privacy Act (CIPA). These suits allege that the AI notetaker violates individuals' privacy rights by transmitting call content to servers in real time and using participant conversations to train its machine-learning models while retaining recordings indefinitely, without proper disclosure. In addition, some of the plaintiffs allege that the AI notetaker violates BIPA by capturing and storing unique biometric identifiers during video-conference calls and using those voiceprints to identify speakers in later meetings.

The court recently consolidated all four lawsuits but has yet to decide on the viability of these claims past the pleading stage.

GenAI and "Virtual Customer Service Agent" Litigation

Some AI products assist with customer service by communicating directly with consumers. These products have become a prime target for class action litigation.

Generative AI, or "GenAI," is a type of artificial intelligence that creates new content, such as text, images, audio and code in response to a user's prompt. GenAI tools can offer "conversation intelligence," which can transcribe customer conversations in real time, analyze their context and respond.

But plaintiffs are claiming this technology violates their rights under CIPA because the technology allows for the "eavesdropping upon private communications" where consumers are unaware that their conversations are being tracked by a third-party AI product. These AI-based arguments are similar in structure to previous lawsuits, where plaintiffs have focused on "pixel tracking" or third party "chatbot" technology for the past several years.

On Feb. 10, 2025, a Northern District of California Court found these eavesdropping allegations satisfied federal pleading requirements and could proceed. Notably, the Court stated that when a GenAI "'learns' the content of the call, that is the same as [the defendant] 'learning' it." As a result, plaintiffs have filed more lawsuits in 2025 that characterize "virtual customer service agents" as "third-party eavesdroppers," while bringing claims under both CIPA and the Federal Wiretap Act.

Image Data Collection Meets Biometric Privacy Litigation

AI does not just "learn" from audio or written data. It also can learn with images of bodies and faces.

Earlier last year, parties reached an unusual settlement for $51.75 million involving claims against a prominent AI company that used machine learning, specifically neural networks and advanced algorithms, to power its facial recognition platform. The underlying lawsuit had alleged that the company scraped facial images from the web and then sold information without consent. The company faced claims under BIPA, the Virginia Computer Crimes Act, California's Unfair Competition Act and other various California, Virginia and New York privacy laws. The class size was estimated to be between 65,000 and 125,000 members.

AI, Privacy Policies and User Consent

The pertinent issue of whether consumers should be required to "opt-in" or provide their consent before a company employs new AI technology is at the center of several recent lawsuits.

One November 2025 lawsuit against a design software company evokes both privacy and copyright-adjacent issues simultaneously. Plaintiffs in this lawsuit allege that the design software company automatically opted users into allowing the company to use their data to train its new AI software without receiving permission or updating the company's privacy policy. In this case, the plaintiffs brought claims for breach of contract and misappropriation of trade secrets, among various other statutes. The plaintiffs argue that they developed, uploaded and stored confidential and proprietary business information within the company's platform (including trade secret materials) that were then accessed and disclosed via AI-generated outputs provided to third parties.

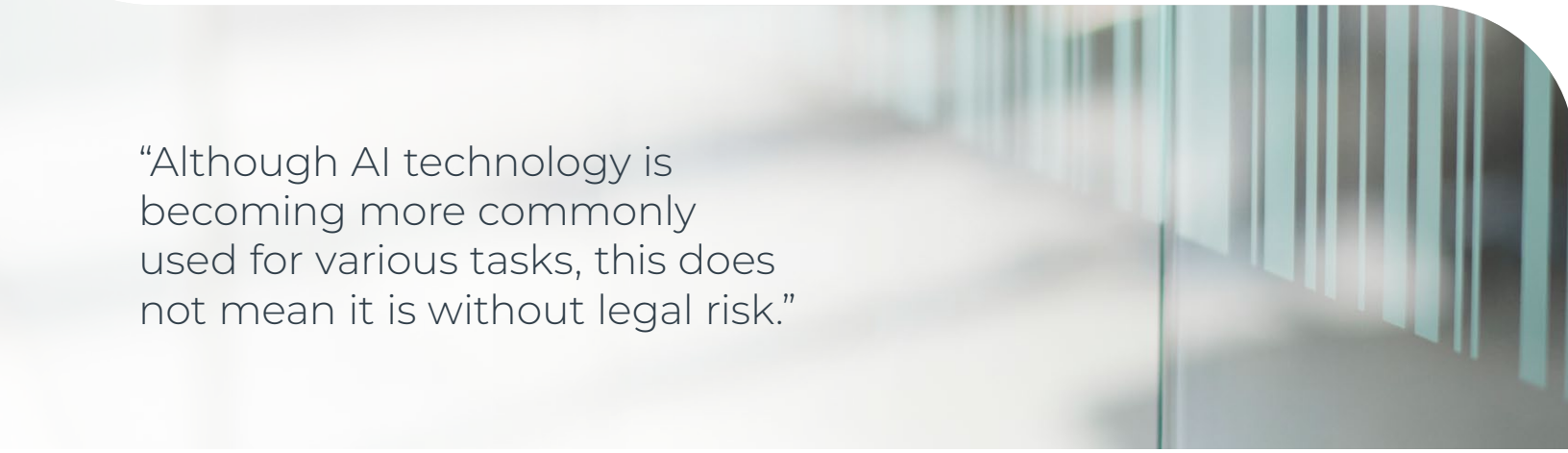
Another lawsuit filed in late 2025 against a graphic design company alleges that a defendant violated the terms of service of

a popular video-sharing platform by "circumventing technological measures to access and scrape millions of copyrighted videos . . . in order to feed, train, improve and commercialize" the defendant's large-scale GenAI. This lawsuit is particularly unique because, although the only cause of action is brought under the Digital Millennium Copyright Act (DMCA), a copyright law, the suit invokes privacy-related concerns regarding the exploitation of stored user-created content and underlying audiovisual files and relies on the website's particular "terms of service." The DMCA provides that "no person shall circumvent a technological measure that effectively controls access to a work protected under this title." Thus, where a website's terms of service prohibit data-mining and bulk downloading, the suit says, a defendant using an automated tool designed to scrape audiovisual content from a website's users necessarily violates the DMCA.

In another recent class action lawsuit against a popular internet service provider, plaintiffs allege that they were automatically and unlawfully "opted in" to the service provider's AI program. This AI program used machine learning with the goal of allowing users to better personalize their experience with the service provider's products. However, the allegations suggest this service provider "def[ied] social norms and invade[d] reasonable privacy expectations" by automatically allowing the AI program to "track" private personal information without first providing notice or a choice to consumers. The plaintiffs brought claims under CIPA, the federal Stored Communications Act (SCA), the California Constitutional Right to Privacy, the California Comprehensive Computer Data and Access Fraud Act (CDAFA) and for common law intrusion upon seclusion.

Conclusion

In sum, AI's ability to learn from massive amounts of code, text, audio and visual data collected from individuals has proven controversial. Although AI technology is becoming more commonly used for various tasks, this does not mean it is without legal risk. As with any new technology, the future of AI regulation and what will become generally accepted practice remains uncertain. To help protect against potential litigation, companies should keep abreast of the legal landscape of AI while maintaining an appropriate level of transparency with individuals regarding its use.



"Although AI technology is becoming more commonly used for various tasks, this does not mean it is without legal risk."

Online Tracking Litigation: The Risks Keep Evolving

Tyler G.D. Anders
Associate
Nashville

Xeris E. Gregory
Associate
Birmingham

KEY TAKEAWAY: Online tracking litigation remains active — but unsettled. Courts are tightening standing requirements, questioning how old statutes apply to new tech, and reaching different conclusions on key issues like VPPA scope, making this an area to watch.

Litigation involving online tracking is here to stay. But the persistence of online-tracking lawsuits does not necessarily reflect more stability in the evolving legal landscape. The number of plaintiffs' firms pursuing web-tracking suits grew during the past year, and web-tracking litigation continues to challenge businesses across industries.

Tracking Technologies that Create a Legal Risk

There are numerous names — like pixels, beacons and tags — and functionalities for online tracking technologies. However, there are three broad classes of third-party tracking technologies that primarily feature in lawsuits: analytics (including cross-channel and data enrichment technologies), chatbots and retargeting technologies. While all three types create legal risk, analytics and retargeting technologies are seen most frequently on websites and therefore in web-tracking litigation. Businesses leveraging these tools often use them to track user engagement and to re-engage prior website visitors.

Special Issues in Online Tracking Litigation

The unifying theory in alleging that web technologies violate state or federal statutes is that tracking technologies allegedly disclose private information to third parties without consent. Despite this relatively straightforward premise, the legal landscape is still turbulent in how web-tracking lawsuits are handled.

Plaintiffs' firms have found repeated success in litigating web-tracking claims, causing disruption for businesses of all sizes and in every sector. This is based, in part, on the ease of access to the information needed to bring a claim and the strict liability penalties that accompany statutory violations.

In the past year, special issues have come to the forefront in these cases.

1. Standing

In web-tracking lawsuits, courts are increasingly requiring plaintiffs to show individualized harm to establish Article III standing. In other words, some federal courts are tightening the screws on "no-injury" cases.

First, courts are increasingly unwilling to find Article III standing where a plaintiff's only injury is an alleged statutory violation. Both the Third Circuit and the Ninth Circuit reiterated this principle in two separate web-tracking cases in August. The Third and Ninth Circuits affirmed dismissal in both cases, reiterating that "Article III standing requires a concrete injury even in the context of a statutory violation." In other words, merely alleging that a defendant's website violated a statute does not automatically mean a plaintiff has standing to sue. There must still be some real-world harm to the plaintiff.

Second, courts are also increasingly unwilling to find standing where the information allegedly transmitted by web-tracking technologies is not inherently private or sensitive. In both cases before the Third and Ninth Circuits, the plaintiffs alleged injury based on loss of privacy. However, the Ninth Circuit likened the defendant's monitoring of user interactions on its website to "a store clerk's observing shoppers in order to identify aisles that are particularly popular or to spot problems that disrupt potential sales." And the Third Circuit noted that "none of the information entered on the defendant's website was personal or sensitive." Thus, neither plaintiff had adequately alleged there was an invasion of privacy.

The takeaway from these recent decisions is that courts can be skeptical about plaintiffs in web-tracking lawsuits. It is not enough to simply allege that a website transmits information to a third party. Plaintiffs must also have suffered some real-world harm as a result. While these decisions offer hope on the horizon for businesses confronted with web-tracking demand letters or lawsuits, businesses should still be wary. The inquiry is still fact-specific, and the categories and type of information transmitted to third parties are crucial for determining whether a lawsuit can proceed past the motion-to-dismiss stage.

2. The untenable state of the California Invasion of Privacy Act (CIPA)

Frustrations with the current application of CIPA — California's wiretapping statute first enacted in 1967 — in online tracking litigation came to a head last year for at least one federal district court judge. In *Doe v. Eating Recovery Center LLC*, Judge Chhabria of the U.S. District Court for the Northern District of California called the "language of CIPA" a "total mess." Judge Chhabria noted that "it's often borderline impossible to determine whether a defendant's online conduct fits within the language of the statute." The problem, according to Judge Chhabria, is that "the statutory language was drafted with very different technology in mind, and it does not map properly onto the internet."

Two other decisions in the U.S. District Court for the Northern District of California echoed Judge Chhabria's frustrations, succinctly identifying the inherent contradiction at the heart of CIPA "trap-and-trace" lawsuits filed in California in recent years. Judge Noël Wise addressed two trap-and-trace class actions involving allegations of CIPA violations through the defendants' websites' use of a TikTok tracking tool. Although the Court found that plaintiffs lacked Article III standing in both cases, its findings did not stop there. Judge Wise went on to find that the defendants' website and the related software did not constitute a "trap-and-trace device" as defined by Cal. Penal Code § 638.50(c).

Judge Wise summarized her reasoning as follows:

> If Defendant only collects information regarding the "metadata" of the communication, Plaintiff's right to privacy is not invaded because he has no expectation of privacy as to that type of data (e.g., his IP address or general geographic location). If Defendant instead collects content information from communication between the parties (e.g., information provided from Plaintiff to Defendant directly), then the TikTok software is not a trap and trace device and § 638.50 does not apply.

CIPA defines a "trap-and-trace device" as "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 the communication." By definition, a "trap-and-trace device" captures identifying information "about" a communication (i.e., the metadata) but not the "contents" of the communication. This distinction "crystalizes the futility of plaintiff's suit (and the myriad identical cases plaintiff's counsel has filed in both federal and state courts)" as it forces plaintiffs into a catch-22. To sufficiently allege standing, a plaintiff must allege the at-issue device captured the contents of their communication. But, by doing so, § 638.50 would no longer apply because § 638.50 only applies when information "about" a communication is captured.

It remains to be seen whether the California legislature will ultimately take action to update the outdated language of CIPA. In the meantime, these recent cases should hopefully give companies another tool to use should they find themselves facing actions involving allegations of CIPA violations.

3. Expanding scope of ECPA claims

Plaintiffs have brought numerous class action lawsuits against health care entities alleging theories under the Electronic Communications Privacy Act (ECPA) where an alleged transfer of protected health information (PHI) to third parties through website trackers allegedly violated the Health Insurance Portability and Accountability Act, other similar state statutes and various common law torts.

Recently, plaintiffs have increased efforts to expand ECPA claims into new contexts, and some courts appear to be receptive to allowing these claims to proceed in these new contexts. For example, a judge in the Northern District of California allowed a putative class action against a shoe retailer to proceed on claims under the federal Wiretap Act.

In denying defendants' motion to dismiss, the court found that plaintiffs plausibly alleged that the defendant "intentionally used" "intercepted" communications in violation of 18 U.S.C. § 2511(1) of the federal Wiretap Act and used those communications to support its targeted advertisement strategy, and that the "alleged disclosure and use of Plaintiffs' personally identifiable information for advertising, in contradiction to the commitments it made in its privacy policy," was "tortious."

4. Growing circuit split on the meaning of a "consumer" under the Video Privacy Protection Act (VPPA)

The VPPA creates civil liability for any "video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider." 18 U.S.C. § 2710(b)(1). The VPPA defines a "consumer" as "any renter, purchaser or subscriber of goods or services from a video tape service provider." *See* 18 U.S.C. § 2710(a)(1). In 2024, the Second Circuit in *Salazar v. NBA*, 118 F.4th 533 (2d Cir. 2024), construed the definition of "consumer" broadly, holding that a broad scope of individuals who may not have purchased video services could still be considered "consumers" under the VPPA. In 2025, courts continued to grapple with the meaning of "consumer," reaching different conclusions and leading to a growing circuit split on this issue.

On the one hand, the Seventh Circuit followed the Second Circuit's approach. The

defendant operated a website where people can watch classic video programming. Plaintiffs alleged they "signed up" with the defendant and provided the defendant with their email addresses and zip codes. The court concluded that "when a person does furnish valuable data in exchange for benefits, that person becomes a 'consumer' as long as the entity on the other side of the transaction is a 'video tape service provider.'" Under the court's expansive reading, a "consumer" includes subscribers to any goods or services from a video-tape service provider.

On the other hand, the Sixth Circuit in *Salazar v. Paramount Global* reached the opposite conclusion. Looking at a "virtually indistinguishable complaint filed by the same plaintiff" in the Second Circuit's *Salazar v. NBA* decision, the court held that an individual is a "consumer" under the VPPA "only when he subscribes to 'goods or services' in the nature of 'video cassette tapes or similar audio visual materials.'" In other words, the court tethered the phrase "goods and services" to "audiovisual," rejecting the expansive reading applied by the Second and Seventh Circuits. VPPA litigation looks to remain unpredictable, as there is no indication this growing split will be resolved soon. Companies who operate websites that stream video should continue to look for ways to limit their liability, including obtaining consent from their users sufficient to satisfy the VPPA, assessing pixel usage and evaluating what information is collected from website users.

Can State Legislation Help Stem the Onslaught of Data Breach Lawsuits?

Shundra Crumpton Manning
Associate
Nashville

Mary K. Longenbaker
Associate
Kansas City, Washington, D.C.

KEY TAKEAWAY: More states are enacting safe harbor laws that limit liability after data breaches, especially for companies that follow recognized cybersecurity standards. As courts begin to interpret these statutes, their impact on class actions and litigation strategy is one to watch.

Data breaches continue to plague companies across industries nationwide. Year after year, the number of reported data breaches continues to rise or remain steady. Despite an increased focus on cybersecurity and privacy protections in the corporate sector, companies still face a seemingly insurmountable burden in trying to protect personal information from cyber attacks. In 2024 alone, there were 3,158 total reported compromises — resulting in more than 1.72 billion notices.

Traditionally, companies have seen little relief from liability in the event of a data breach, even when they have implemented industry-standard systems and processes to protect customers' and employees' personal information. More than 1,400 data breach class actions were filed in 2024. Yet hope may be on the horizon, as more states consider legislation offering safe harbors to businesses facing data breach litigation.

During the past seven years, nine states — Connecticut, Iowa, Nebraska, Ohio, Oklahoma, Oregon, Tennessee, Texas and Utah — have enacted statutes designed to shield companies from liability for a data breach.

To date, these protections have taken many forms but invariably follow one of three models:

1. The affirmative defense,
2. The punitive damages limitation or
3. The class action bar.

State legislatures proposing similar safe harbor legislation frequently draw on the language used in earlier statutes, so future legislation will likely continue to follow these models.

In 2018, Ohio enacted legislation providing an affirmative defense to liability if a business creates, maintains and complies with an industry-recognized cybersecurity framework — e.g., National Institute of Standards and Technology (NIST) guidelines — that is of an appropriate scope and scale for the company's size and resources. Iowa and Utah have adopted legislation similar to this "Ohio model," offering an affirmative defense to businesses with cybersecurity frameworks meeting baseline requirements, albeit with slight variations.[1] A number of other states have proposed, but not enacted, similar legislation following the "Ohio model."[2]

1. *See* Iowa Code § 554G.2 (2023) (requiring cybersecurity investment be at least equal to "maximum probable loss," as defined by the statute to take advantage of the defense); Utah Code § 78B-4-701 (2021) (denying the defense if it is determined a business had actual notice of the threat, but failed to act within a reasonable time to prevent the breach).
2. *See, e.g.*, Georgia H.B. 260 (2021)/S.B. 52 (2021); Illinois H.B. 3030 (2021); Michigan S.B. 672 (2021); Florida H.B. 473 (2024); Mississippi H.B. 1380 (2025).

Other states, such as Connecticut and Texas, have taken a different approach, adopting legislation that only protects against punitive damages in litigation following a data breach. For example, Connecticut protects companies against punitive damages in actions alleging the company failed to implement reasonable security controls. Similarly, under Tex. Bus. & Comm. Code § 542.003, small businesses with fewer than 250 employees are shielded from punitive damages if they implement a cybersecurity program that conforms to a recognized cybersecurity framework. Meanwhile, in Oklahoma, businesses that implement safeguards that meet recognized cybersecurity standards can assert this compliance as an affirmative defense and can leverage it to cap civil penalties at $75,000 plus actual damages.

Within the last two years, Tennessee and Nebraska have also enacted statutes that help protect businesses by barring class actions under certain circumstances.

Effective May 21, 2024, Tennessee enacted Tenn. Code Ann. § 29-34-215 which states in pertinent part:

> A private entity is not liable in a class action lawsuit resulting from a cybersecurity event unless the cybersecurity event was caused by willful and wanton misconduct or gross negligence on the part of the private entity.

A private entity is broadly defined as "a corporation, religious or charitable organization, association, partnership, limited liability company, limited liability partnership, or other private business entity, whether organized for-profit or not-for-profit." The statute further defines a cybersecurity event as "an event resulting in unauthorized access to, or disruption or misuse of, an information system or nonpublic information stored on an information system."

Nebraska adopted a nearly identical statute, effective Sep. 3, 2025.

The Tennessee and Nebraska statutes are in their infancy, so there have been few indications as to how the courts will interpret these statutes in practice. To date, the Tennessee courts have determined only that this type of "class action bar" does not apply retroactively to litigation concerning breaches that occurred prior to the passage of the statute.

And although many of these statutes have already been in place for a few years, there is very little court interpretation of any of them to date. To take advantage of these statutes when the time comes, companies should ensure their cybersecurity programs and practices align with industry standard frameworks. Additionally, advancing and endorsing similar legislative efforts in other states could also help reduce the volume of data breach litigation nationally, as the existence of these laws may serve as a lawsuit filing deterrent.

About Our Technology Transactions & Data Privacy Practice

Polsinelli's Technology Transactions and Data Privacy team is comprised of over 70 lawyers with significant experience in the technology, privacy and cybersecurity industries.

We work with companies of all sizes and at all stages of development to provide strategic guidance as they create, acquire, use and commercialize technology. Our clients include businesses with domestic and international operations as well as governments, universities, hospitals, financial services institutions, startups and nonprofit organizations.

The Polsinelli team provides industry-leading data privacy counseling, incident response and breach litigation legal services. Our lawyers include former in-house data privacy attorneys, alumni of law enforcement agencies, attorneys with international backgrounds and some of the most experienced incident response lawyers in the country.

Contact one of our team members today to learn how we can help you and your organization with its technology, privacy and cybersecurity needs.

Stay Connected

Polsinelli frequently writes about topics related to these materials. Click here to subscribe to receive news and webinar updates.

POLSINELLI | What a law firm *should* be.™