Sheppard

Eye on Privacy

2025 Year In Review

Sheppard's Eye on Privacy

2025 Year In Review

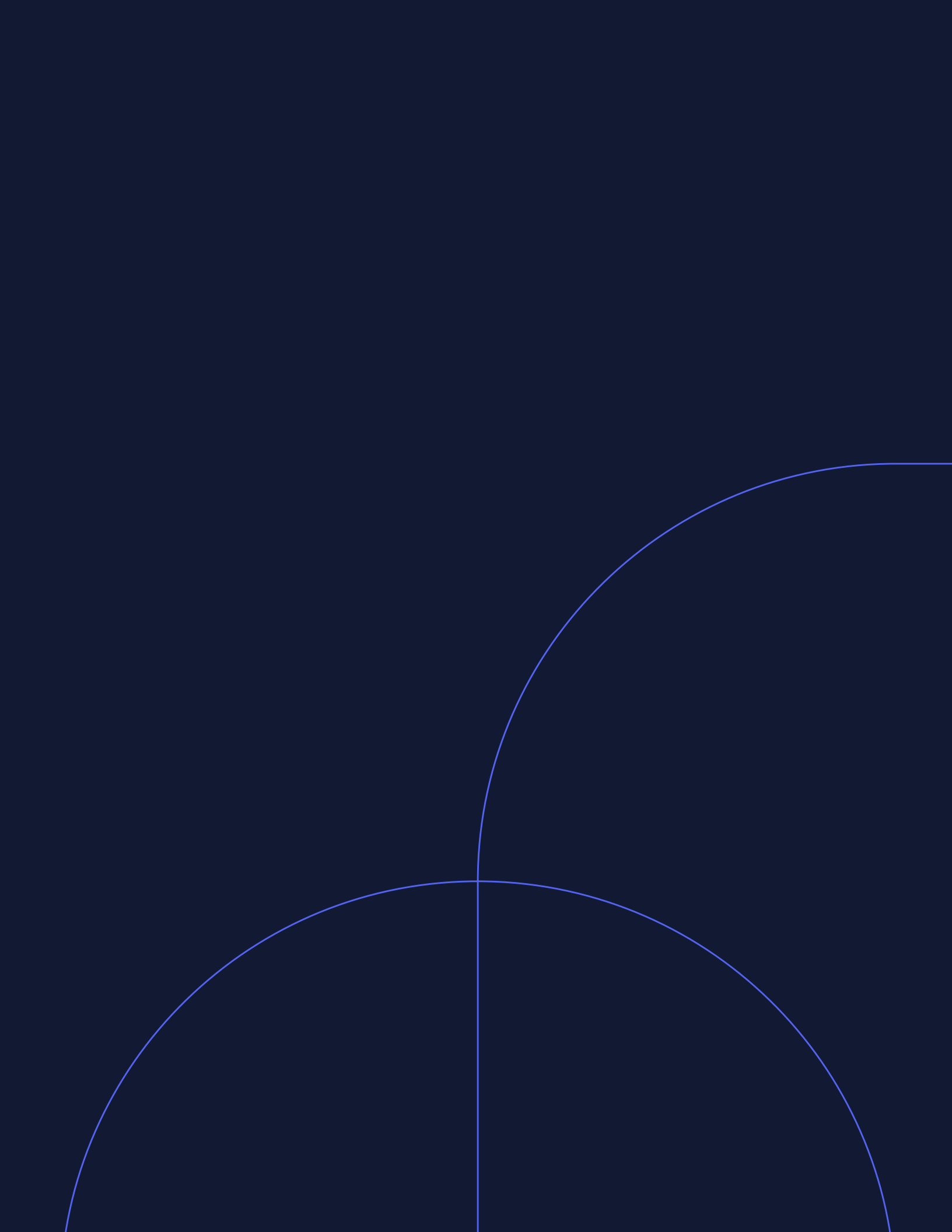
These articles appeared in the "Eye On Privacy" Blog in 2025 (www.eyeonprivacy.com)

As we close out January 2026, 2025 is firmly in the rearview mirror. And what a roller coaster it was. From AI developments to US state enforcement and legislation, it was a hard one to keep up with! The ground shifted under our feet in a way that will inform the rest of 2026 and beyond.

This year in review pulls together all of our posts from 2025, in one place, so you can scan development topic-by-topic. We hope these help you translate these risk areas into legal change and practical action for your organization. Whether you are assessing your approach to AI governance, refreshing privacy notice and choice, contemplating or facing CIPA or other privacy litigation and enforcement, or contemplating children's and location data practices, this compilation is designed as a working tool. It's not just a look-back, it's intended to be a resource to help you prepare for what is next.

Want a peek at the archives?
Here are round-ups from:

2024
2023
2022
2021
2020
2019
2018



Contents

Artificial Intelligence

Protecting Personal Data in the Age of AI: Lessons from the Latest EDPS Guidance

Posted December 2, 2025

The European Data Protection Supervisor (EDPS) AI guidance for EU institutions has lessons for businesses. This includes when inputting personal information into these tools. The recommendations from the guidance fall into five categories, which businesses can take as potential principles. Namely:

- Do your diligence. Know where personal information enters AI processes. Personal information can show up in training, during use, and in the results the AI gives. It is important to check every step for risks to personal data.
- Be transparent. Do not just use public data and hope for the best. Privacy laws impose obligations to tell people why their information is being collected and how it will be used. They also require telling people who will handle their personal data.
- Be accountable. This means making it clear who is responsible for decisions about personal data and keep accurate records. In the guide, the EDPS reminds EU Institutions that as AI changes, security risks like hacking become more common. So, businesses need to update their defenses often.
- Respect the rights of individuals. Let people see, fix, or remove their data, even if the data is hidden in AI systems. This can be technically demanding, but the burden is on the business to make it possible.
- Be thoughtful. Do not use a check-the-box approach to risk assessments. Before deploying a new generative AI system, conduct a full Data Protection Impact Assessment, question whether all data collection is genuinely necessary, and prefer anonymized or synthetic data where possible. Keeping up with regular checks for accuracy and bias, plus open communication with staff and users, helps build compliance.

Putting it into Practice: These recommendations were directed to EU Institutions, not private businesses. However, they may signal what regulators expect of businesses when implementing AI tools. As AI laws and obligations continue to develop, consider basing your privacy program on these principles from diligence to thoughtfulness. Taking a principle-based approach to compliance can allow your company to more nimbly react as laws develop and change.

Illinois AI Employment Law Goes Live Soon: Are Your Hiring Practices Compliant?

Posted November 19, 2025

Illinois employers are reminded that a law addressing the use of AI in the workplace is set to take effect January 1, 2026.

It applies to employers, employment agencies, and labor organizations within Illinois that use AI for decisions like hiring, promotion, discharge, and other terms of employment. It applies to all employers, regardless of whether the company has a physical location in the state of Illinois. AI is defined broadly and includes not only generative AI but any machine-based system that generates outputs influencing employment decisions, with no specific exemptions provided.

The law generally requires two things for organizations using AI in employment related decisions:

- Avoid using AI that results in discrimination based on protected classes, such as race, gender, age, or disability; and
- Provide notice to employees when AI is used for employment decisions, explaining its purpose and the characteristics it assesses.

Putting it into Practice: Any organization using AI for employment purposes with Illinois employees should review current or planned AI practices for potential discriminatory outcomes and to confirm that necessary notices are in place. This includes the use of AI tools internally developed or offered by third party vendors. While the law does not require any creation of formal impact assessments, an AI governance policy to reflect these requirements and educating workforces on the proper use of AI in decision-making processes will help guide compliance. There is no private right of action for the law; the Illinois Department of Human Rights and the state's Human Rights Commission will be charged with enforcing the law.

When in Rome—Make Your AI Do As the Regulators Do

Posted November 18, 2025

Italy became the first EU country to enact a comprehensive national AI law when its AI law (Law No. 132/2025) took effect last month. The law is intended to work with the existing EU AI Act, but with more details and specific obligations. In fact, it mirrors many of the themes that are being implemented in US AI laws (like those in Texas, Virginia (vetoed), and Colorado). This may be one of many similar laws we see coming out of Europe this year, and the potential for a fragmented AI regulatory patchwork in the EU.

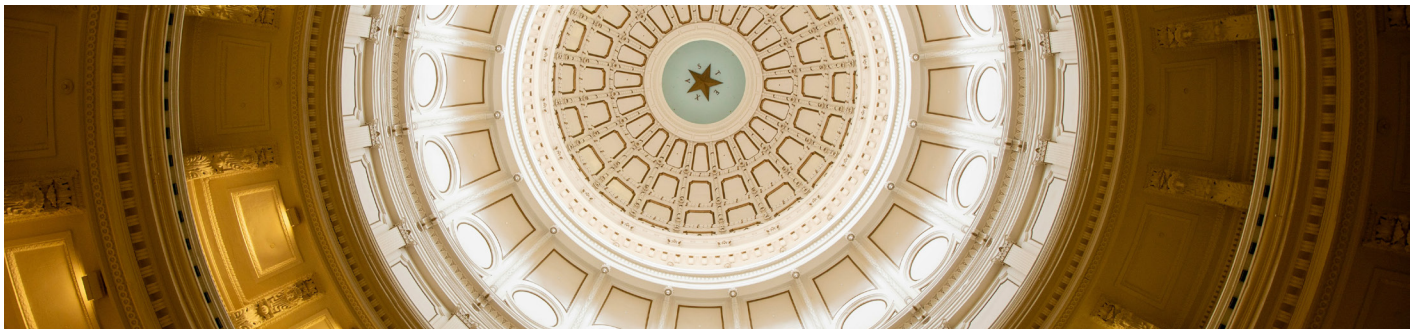
The law imposes more human oversight obligations on healthcare, public administration, and employers than those required under the EU AI Act. For example, AI may assist, but not replace, clinical decision-making. Medical providers must explain both the use and the logic behind AI systems to patients.

The law imposes criminal penalties for deepfakes and create more robust risk management expectations for businesses than under the EU AI Act. It also commits up to € 1 billion in public investments—targeting innovative SMEs and partnerships—and mandates the development of a National AI Strategy, updated biennially.

Putting it into Practice: This law suggests that we may see a more sector-specific approach to AI regulation in the EU. In the face of a sector-specific regulatory regime, global companies can take several steps. These include putting guardrails in place for human oversight of AI output and involving a wide set of stakeholders in the planning process.

Countdown to 2026: What Will the Texas AI Law Mean for Businesses?

Posted July 16, 2025



Texas is getting into the AI action, with a new law (the Texas Responsible Artificial Intelligence Governance Act) that will place restrictions not only on AI use by government agencies, but businesses as well. In particular, it will apply to businesses (a) operating in Texas, (b) those that have products or services used by those in the state, or (c) those that develop or deploy AI systems in Texas. The requirements of the law will take effect January 1, 2026. Some things for companies to keep in mind about the law's requirements:

- **Appropriate Uses.** The law will require that companies take steps to ensure that AI systems are not used, among other things to intentionally incite or encourage criminal activity, self-harm, or harm to others. Covered businesses will also have to review AI system use to make sure it does not violate state of federal discrimination laws. AI systems also cannot, under the law, be used to impair someone's constitutional rights. AI also cannot be used to develop content that simulates child pornography or explicit deepfake imagery.
- **Biometric Data.** The new law will modify the state's existing biometric law to incorporate additional AI provisions. If companies intend to input or otherwise biometric identifiers (e.g., fingerprints, retina scans, facial geometry) in connection with AI for commercial purposes, they will need to get proper consent. These commercial purposes might include, for example, using biometric data to train AI. Data will also need to be destroyed within one year after the purpose for collection expires.
- **Healthcare Providers.** Once in effect, healthcare providers that use AI tools as part of their provision of treatment will need to notify patients of this before starting treatment (or as soon as possible in emergencies). This is similar to Utah's law that requires disclosures for those in regulated professions, including healthcare.
- **New "Regulatory Sandbox" Program.** The law creates a "regulatory sandbox" program that allows approved businesses to test innovative AI systems for 36-month periods. The intent is to allow companies to create and test AI systems in the state. Among other things, as part of the program the Attorney General will not be able to file or pursue charges if a program participant has violated the new AI law during the testing period.

The law will be enforced by the Texas attorney general and does not include a private right of action. There is also a safe-harbor provision in the law: if a company discovers a violation and promptly remediates it, it can avoid liability. There will also be a rebuttable presumption of care if a company follows industry-recognized standards like NIST's AI Risk Management Framework. Finally, the law establishes an AI council, which will provide guidance on AI development and use.

Putting it into Practice: In the months before this law goes into effect, covered businesses may want to review their use of AI systems to assess the extent to which these new laws requirements might apply. This includes training AI on biometric data, as well as -for healthcare providers- using AI as part of the provision of health care services.

Lessons from the FTC: The Cleo AI Settlement

Posted April 29, 2025

The FTC's settlement with Cleo AI gives some indication as to what we might see from the agency in the coming months. The FTC alleged, among other things, that Cleo AI's actions violated Section 5 of the FTC Act. In particular, as reported in our sister blog, Cleo AI required people to enroll in a paid subscription plan, even though they marketed their services as free. It also made it difficult for people to cancel their subscription and made it hard to stop recurring charges. The company also failed to disclose material terms.

Cleo AI agreed to settle by paying $10 million in consumer redress, and a $7 million civil penalty. The company has also agreed not to misrepresent people's ability to cancel negative option charges and must get people's "express informed consent" before collecting money (or other consideration) from consumers. It has also agreed to simplify the subscription cancellation mechanism.

Putting it into Practice: This case suggests that the FTC will be continuing its practice of examining businesses whose user interfaces make it difficult for users to exercise choices, especially those that result in fees being charged. This decision follows the FTC's November 2024 update to the negative option rule.

US State AI Legislation: Virginia Vetoes, Colorado (Re)Considers, and Texas Transforms

Posted March 28, 2025

Virginia's Governor, Glenn Youngkin, vetoed a bill this week that would have regulated "high-risk" artificial intelligence systems. HB 2094, which narrowly passed the state legislature, aimed to implement regulatory measures akin to those established by last year's Colorado AI Act. At the same time, Colorado's AI Impact Task Force issued concerns about the Colorado law, which may thus undergo modifications before its February 2026 effective date. And in Texas, a proposed Texas Responsible AI Governance Act was recently modified.

The Virginia law, like the Colorado Act, would have imposed various obligations on companies involved in the creation or deployment of high-risk AI systems that influence significant decisions about individuals in areas such as employment, lending, health care, housing, and insurance. These obligations included conducting impact assessments, keeping detailed technical documentation, adopting risk management protocols, and offering individuals the chance to review negative decisions made by AI systems. Companies would have also needed to implement safeguards against algorithmic discrimination. Youngkin, like Colorado's Governor Polis, worried that HB 2094 would stifle the AI industry and Virginia's economic growth. He also noted that existing laws related to discrimination, privacy, data usage, and defamation could be used to protect the public from potential AI-related harms.

Whereas Polis ultimately signed the Colorado law, Youngkin did not.

However, even though Polis signed the Colorado law last year, he urged in his statement for legislators to assess and provide additional clarity and revisions to the AI law. And, last month, the AI Task Force issued a report on their recommendations. The task force identified potential areas where the law could be clarified or improved. It divided them into four categories: (1) where consensus exists about changes to be made; (2) where consensus needs additional time and stakeholder engagement; (3) where consensus depends on resolving multiple interconnected issues; and (4) where there is "firm disagreement." In the first are only a handful of relatively minor changes. In the second, for example, is clarifying the definition of what are "consequential decisions" – important because AI tools used to make them are the ones that are subject to the law. In the third, for example, is defining "algorithmic discrimination" and obligations developers and deployers should have in preventing it. And in the fourth, by way of example, is whether or not to include an opportunity to cure incidents of non-compliance.

Texas, like Colorado and Virginia, has been considering legislation that addresses high-risk AI systems that are a "substantial factor" in consequential decisions about people's lives. That bill was recently modified to

remove the concept of algorithmic discrimination, and as currently drafted prohibits AI systems that are developed or deployed with the "intent to discriminate." It has also been modified to expressly state that disparate impact alone is not sufficient to prove that there was an intent to discriminate. The proposed Texas law is similar to Utah's AI legislation (which went into effect on May 1, 2024), insofar as it would require notice if individuals were interaction with AI (though this obligation is only for government agencies.) Lastly, the law would also prohibit the intentional development of AI systems to "incite harm or criminality." The law was filed on March 14 and, as of this writing was pending in the House Committee.

Putting it into Practice: The veto of HB 2094 emphasizes the complex journey towards comprehensive AI regulation at the state level. We anticipate ongoing action at a state level and some time before we see a consensus approach to AI governance. As a reminder, there are currently AI laws in effect focusing on various aspects of AI in New York (likenesses and employment), California (several different topics), Illinois (employment), and Tennessee (likenesses). These laws are set to go into effect at different times in 2024 through 2026. There are also bills sitting in committee in at least 17 states.

Oregon's AI Guidance: Old Laws in Scope for New AI

Posted February 25, 2025

The Oregon AG's Office, along with the state's Department of Justice, issued guidance late last year on how state laws apply to the ways businesses use AI. The guidance may be two months old, but the cautions are still timely. The guidance seeks to give companies direction on times when AI uses might be regulated by existing state laws.

As outlined in the guidance, the Oregon state laws that may apply to a company's use of AI include a variety of consumer protection laws. Namely, the state's "comprehensive" privacy law (the Consumer Privacy Act), its Unlawful Trade Practices Act, the Equality Act, and its data security law (the Consumer Information Protection Act). Some key takeaways from the guidance:

- **Notice.** A reminder to companies that they could be viewed as violating Oregon's "comprehensive" privacy law if they do not disclose how they use personal information with their AI tools. Additionally, the AG may view it as a violation of Oregon's Unlawful Trade Practices Act if they do not explain a potential "material defect" with an AI tool. For example, a business that places a third-party virtual assistant program on its website, but the tool is known to give incorrect information.
- **Choice.** The guidance reminds companies that under Oregon's privacy law, consent is required before processing sensitive information, which may occur if putting that information into AI tools. In addition, the guidance reminds companies that the same law requires giving consumers the ability to (a) withdraw consent (when such consent was required to process information) and (b) opt out of AI profiling for significant decisions. Companies will need to keep this in mind, *inter alia*, when inputting personal information into AI tools.
- **Transparency.**The guidance outlines some potential AI uses that might violate the state's Unlawful Trade Practices Act. For example, not being clear that someone is interacting with an AI tool. Or, misleading individuals about the AI's capabilities or how the company will use AI-generated content. Another example given is using AI-generated voices for robocalling without accurately disclosing the caller's identity.
- **Bias.**The guidance states that using AI in a way that discriminates based on race, gender or other protected characteristics would violate Oregon's Equality Act.
- **Security.** The guidance reminds companies of the obligations of the state's data security law. Thus, if an AI tool incorporates personal information, or a business uses personal information in connection with the tool, it will need to keep that law's obligations in mind. These include obligations to have in place "reasonable safeguards" to protect personal information.

Putting it into Practice: This guidance is a helpful roadmap for companies, by tracking existing state laws' obligations onto AI uses. Most states have unfair and deceptive trade practice laws that mirror those in Oregon, as well as anti-discrimination and security laws. It is thus possible that we will see similar guidance from other states.

Don't Forget the EU: Italy Issued First GenAI Fine of €15 Million Alleging GDPR Violations

Posted January 28, 2025

At the end of 2024 the Italian Data Protection Authority issued a 15 million euro fine in the first generative AI-related case brought under GDPR. According to Garante (the Italian authority), OpenAI trained ChatGPT with users' personal data without first identifying a proper legal basis for the activity, as required under GDPR. The Order also alleges that OpenAI failed to notify Garante about a data breach the company experienced in March 2023. Additionally, the Order states that OpenAI did not provide proper age verification mechanisms for users under age 13.

In addition to the fine, OpenAI must also conduct a six-month public education campaign on how ChatGPT works and how data is used to train AI products. The campaign must also provide individuals with information about their rights and how to exercise their rights. OpenAI intends to appeal the decision.

This decision follows March 2023 temporary ban of ChatGPT in Italy. And in July 2023, the FTC issued a Civil Investigative Demand to OpenAI.

Putting it into Practice: While it is unclear the extent to which AI will receive the same type of scrutiny in the US that it did under the prior administration, this decision is a reminder that the EU regulators are keeping a close eye on AI activities, especially when personal data is used to train the tool. For an ongoing update of executive actions that may impact AI (and much more), check out this tool created by our partner, Jon Meyer.

New Year, New Protections for New York Artists and AI-Generated Replicas

Posted January 6, 2025

New York has a new AI-related law which took effect January 1. The law regulates creation and use of digital replicas of an individual's voice or likeness and is similar to those in California and Tennessee.

The law defines digital replicas as digital simulations of the voice or likeness of an individual that, to the average person, would be indistinguishable from the "real thing." Any contract for personal or professional services that provides for the creation of digital replicas is void and if it does not describe how the contracting party will use the digital replica or the person being "replicated" was either not represented by legal counsel or a labor union. (Both the contract negotiated by legal counsel and the collective bargaining agreement must contain specific provisions relating to digital replicas.)

Putting it into Practice: We anticipate other states will pass similar digital replica/AI laws in 2025. These laws should be kept in mind by companies that engage talent, or use third parties to create content, including for marketing purposes.

Children's Privacy

Texas Sets Sights on Roblox

Posted December 11, 2025

A new lawsuit filed by the Texas Attorney General against Roblox has brought privacy, safety, and data handling into the spotlight for online platforms, especially those used by kids and teens. The allegations followed concerns raised by advocacy groups in 2024 and suggest that Texas will continue to be active in the privacy space.

According to the Texas complaint, the Roblox website does not have a functioning age gate for account creation. Currently, the site allows an account registration for children under 13 collecting only a username and password. The prompt on creation of the account is to "not use your real name." Instead, while birth date is asked, the company does not obtain verifiable parental consent for those who enter an age under 13. This, the AG argued, was a violation of the federal Children's Online Privacy Protection Act.

Other concerns from the AG included the fact that self-reported children could interact with adults. They could also make purchases on its platform. The complaint also alleged deceptive practices insofar as Roblox made statements about how it was taking "every precaution possible" to protect children and had "industry-leading" safety. According to the Texas AG, Roblox is not living up to these promises. Roblox has stated that it takes steps to prevent the sharing of personal information by children and otherwise protect them on its platform.

Putting it into Practice: This case is a reminder that states can bring action under many federal privacy laws, like COPPA. While there may be less activity at a federal level, we expect to see ongoing enforcement by state regulators, which may result in different interpretations of these laws. And when these cases are brought, there is a potential that the state-level regulator may look very closely at security claims, relying on theories of unfair and deceptive trade practices.

Warning! States Continue to Worry About Social Media and Teens

Posted November 19, 2025

If you thought social media needed a warning label, many state regulators agree. California recently passed a new warning label law, which will take effect on January 1, 2027. That is, unless it is challenged. Meanwhile, Colorado is fighting to keep alive a similar law following a NetChoice challenge. Other states (like Arkansas, California, Florida, Utah, Maryland, Mississippi, Ohio, and Texas) have not been successful, seeing similar laws stopped on First Amendment grounds.

The California law (AB 56, i.e., the Social Media Warning Law) was passed and signed by Governor Newsom last month. When the law takes effect, certain social media platforms must display a large pop-up to users under 18 when the users open the platform for the first time that day. The platforms must then display another warning after three hours, and then every hour thereafter. There is required language for the warning, which mirrors tobacco and alcohol warnings. The law does not contain a private right of action.

Colorado tried something similar in June 2024, but with more frequent pop-ups. Namely, every 30 minutes, as well as pop-ups if the platform is used between 10 pm and 6 am. The law is currently stayed, following a recent challenge from NetChoice.

Putting it into Practice: These laws highlight state-level activity around children's online privacy – especially in the perceived absence of federal action. We expect to see this continue in the new year. Companies should keep this in mind, even if they do not run social media platforms. Having a principles-based approach to privacy compliance can help organizations navigate constantly-evolving state regulatory activity.

"How Old Are You, Anyway?" California's New Law Makes Apps Ask... And Remember!

Posted November 17, 2025

California is getting serious about age checks online, and businesses should pay attention. Thanks to the passage of AB 1043, starting January 1, 2027, software makers and app stores will need to know the user's age (or at least their age bracket) and signal it to apps every time a download or launch happens. For businesses that may be unclear whether COPPA or CCPA's provisions for teenagers apply to their app, this law is aimed at clarifying that ambiguity.

How will it work? Under the new law, operating system providers and app stores will need to generate a digital age bracket signal—identifying whether the user is either (a) a minor (with age brackets of: under 13, 13 to 15, or 16 to 17) or (b) 18 and over. This signal must be transmitted securely, and in real-time, not only when the app is downloaded, but each time it is launched.

The law notes that apps that receive this signal will have "actual knowledge" of the users' age. As such, this could impact how California examines COPPA compliance. (Which, as a reminder, applies to collection of information online from children including when the site/app has actual knowledge that the user is a child.) This law should also be viewed in conjunction with CCPA, and its provisions governing minors' personal information.

While there is no private right of action, the law does provide for statutory penalties. Namely, up to $7,500 per intentional violation for each affected child.

Putting it into Practice: Beginning in two years, this law -if not challenged- will impact apps' knowledge of their users' age. This could change the calculus for companies on whether or not COPPA and CCPA's children provisions apply to them. This may be a good time for companies to analyze the impact of these laws on their organizations, even if they have not done so in the past.

What Can We Learn from This Administration's FTC COPPA Settlement

Posted October 10, 2025

Companies can take many lessons from the FTC's recent COPPA settlement with a robot app from the toy manufacturer Apitor Technologies. According to the FTC complaint, the app allegedly allowed a Chinese entity to collect and share children's geolocation information without parental consent – violating COPPA. In particular, children could use the app to program their robots, but to do so, they needed to enable location permissions. Once enabled, a third party SDK (JPush), developed by Chinese-based entity Jiguang, would send the child's location to that entity's Chinese-based servers.

The FTC's concerns stemmed from COPPA's requirements to, among other things, get parental consent before collecting children's personal information, and outlining (in a company's privacy policy) how children's personal information would be used. The FTC based its claims on the fact that geolocation information is personal information, and as such triggers' COPPA's consent and notice obligations. Beyond the COPPA violations, it appears that the FTC's concerns were potentially premised on two issues: that information was being sent to an entity in China, and the sensitive nature of children's geolocation information.

To settle this matter, Apitor agreed, among other things, to delete the geolocation information, modify its privacy policy, and get parental consent moving forward. In addition, the company agreed to delete children's information either if a parent asks, or when it is no longer needed. While the FTC imposed a $500,000 civil penalty, it was suspended for an inability to pay.

Putting it Into Practice: This settlement suggests that, moving forward, the agency may focus on situations where information is being sent offshore, as well as when companies are passively collecting information from children. It serves as a reminder to check what data is being collected passively, as well as to review and understand business partners' practices.

Oregon's Privacy Law Update Adds to Patchwork Approach to Minors and Location Data

Posted July 10, 2025

Oregon will begin to regulate the use of minors' information and sale of users' location data (regardless of age) with an update to its Oregon Consumer Privacy Act. These revisions will go into effect January 1, 2026. As amended, those subject to the law will not be able to profile or serve targeted advertising to anyone under 16. This includes both those the company knows are under that age, as well as those that they should know are under that age. (Currently, restriction that applies to consumers that are at least thirteen but not older than fifteen without their consent.)

As amended, the law will also prohibit sale of information of those under 16. As we previously wrote, Maryland will impose a similar prohibition, but for information of those under 18. Beginning January 2026 covered entities will also be prohibited from selling location data. Namely, data that can show, within a 1,750-foot radius, where a person or their device is or has been in the past. This includes information collected through GPS or other technologies that can track precise locations. This location restriction is for all users, not only that of minors.

Putting it into Practice: These obligations add to the patchwork approach state comprehensive laws are taking to treatment of minors and the location data. Other obligations to keep in mind include social media or online operator restrictions for minors, and potential applicability of existing laws to new practices.

Growing List of States Attempting to Regulate Kids' Online Privacy: Vermont Joins the Group

Posted July 8, 2025

Vermont has joined the list of states attempting to regulate the use of children's information collected online, passing an Age-Appropriate Design Code Act. This law mirrors ones we have seen in other US states as well as the UK, and applies to online services reasonably accessed by minors, that collect personal data. We expect it to be challenged, but if it is not, it would go into effect January 1. Among other things, the law provides the following:

Prohibited Practices

Covered businesses will only be able to collect, use, or keep minor's personal data if it is needed for a service the minor is actively using. They will be prohibited from using this data for new or additional purposes, or from enabling third-party tracking without providing notice and consent. Additionally, they will be limited in the content recommendations they can make to minors based on minors' data. Finally, covered businesses will not be able to send push notifications to minors between midnight and 6 a.m.

Age Verification

The attorney general will be tasked with developing a process and rules for determining if someone is a minor. Covered businesses that collect information as part of the process will need to keep it to the minimum necessary to confirm a user's age and use it only for verification. They will also need to delete the data (except for the age range) after verification. Covered business will need to give minors an appeal process if their age has been determined incorrectly.

Privacy Settings

Covered businesses will need to set the highest privacy settings for minors by default. This includes not letting adults see a minor's posts and locations unless the minor clearly allows it. It also means not letting adults comment on or message minors without permission and not sending push notices to minors. Under the law, search engines will also be prohibited from indexing minors' profiles. Businesses will also need to give minors an easy way to delete their accounts and process the request within 15 days. They also need to ensure that their use of minors' data and the design of their platforms do not cause minors emotional distress or result in compulsive use, among other things.

Be Transparent

Covered businesses will need to clearly display privacy policies and terms of service and make them easily accessible to users. Additionally, businesses will need to explain how any algorithmic recommendations work. This includes giving details about data collection, use, sharing, and data retention for features targeted at minors.

Putting it into Practice: While we anticipate that this law will be challenged, it is a reminder that US states continue to attempt to regulate social media platforms' interactions with children. Companies may want to keep the concepts of these laws, which include default privacy settings and data minimization, in mind when developing interactive platforms that might be accessed by minors.

Growing List of States Attempting to Regulate Kids' Social Media Accounts: Nebraska Husks Up

Posted June 16, 2025

Nebraska's governor signed a bill into law that, among other things, creates the Parental Rights in Social Media Act. The provisions of the law will go into effect July 1, 2026, unless challenged. The law is similar to several other states, most of which have been challenged (including Arkansas, California, and Utah) and some struck down.

If the law goes unchallenged, unlike other states it creates a private right of action. Anyone who violates the act may be subject to a lawsuit brought by an injured party. They may be ordered to pay damages, attorney's fees, and other relief. In addition, the Nebraska Attorney General can enforce the law and seek penalties of up to $2,500 per violation.

Obligations placed on social media companies under the law include:

- **Age Verification:** Social media companies (or their vendors) will need to verify the ages of all people that attempt to create an account. It would restrict anyone under 18 from creating an account. And, the law specifically requires that social media companies delete identifying information they get when checking user ages.
- **Parental Consent:** The law requires parental consent before minors can create social media accounts. They must also give parents mechanisms to revoke their consent. If a parent revokes their consent, the social media company must remove the account of that parent's child and must stop a child from creating a new account unless the parent provides consent.
- **Parental Supervision:** Parents will need to be given a way to supervise their children's social media use. This includes access to their children's posts and messages, and controls over their privacy and account settings. In addition, parents must be able to monitor and limit the amount of time the minor spends using the social media site.

Putting it into Practice: Nebraska joins a growing number of states attempting to regulate children's use of social media. We will continue to monitor the status of this new Nebraska law before mid-2026, but anticipate seeing other similar legislation from other states.

Virginia Will Add to Patchwork of Laws Governing Social Media and Children (For Now?)

Posted May 15, 2025

Virginia's governor recently signed into law a bill that amends the Virginia Consumer Data Protection Act. As revised, the law will include specific provisions impacting children's use of social media. Unless contested, the changes will take effect January 1, 2026. Courts have struck down similar laws in other states (see our posts about those in Arkansas, California, and Utah) and thus opposition seems likely here as well. Of note, the social media laws that have been struck down in other states attempted to require parental consent before minors could use social media platforms. This law is different, as it allows account creation without parental consent. Instead, it places restrictions on account use for both minors and social media platforms.

As amended, the Virginia law will require social media companies to use "commercially reasonable" means to determine if a user is under 16. An example given in the law is a neutral age gate. The age verification is similar to those proposed other states' social media laws. (And it was that requirement that was central to the court's decision when striking down Arkansas' law.) Use of social media by under-16s will default to one hour per day, per app. Parents can increase or decrease these time limits. That said, the bill expressly states that there is no obligation for social media companies to give those parents who give their consent "additional or special access" or control over their children's accounts or data.

The law will limit use of age verification information to only that purpose. An exception is if the social media company is using the information to provide "age-appropriate experiences" – thought the bill does not explain what such experiences entail. Finally of note, even though these provisions may increase costs on companies, the bill specifically prohibits increasing costs or decreasing services for minor accounts.

Putting it into Practice: We will be monitoring this law to see if the Virginia legislature has success in regulating children's use of social media. This modification reflects not only a focus on children's use of social media, but also continued changes to US State "comprehensive" privacy laws.

Arkansas' Kids Social Media Law: Another One Bites the Dust

Posted April 10, 2025

Arkansas' second attempt at regulating minor's access to social media – in the form of the Social Media Safety Act (SB 689) – has again been struck down as unconstitutional. The court permanently enjoined the state from enforcing the law. It was a modified version of Arkansas' 2023 SB 396, that was also blocked. The plaintiff in both challenges was NetChoice, a group familiar to anyone following kids' social media laws. As a result of NetChoice's efforts, similar laws have been blocked in California, Utah, Maryland, Mississippi, Ohio, and Texas. Courts in those states, as in Arkansas, found that the laws were unduly burdensome on free speech, with overly broad content restrictions not tailored to prevent harm to minors.

Like prior social media laws, the Arkansas Social Media Safety Act would have required social media companies to verify that users were at least 18 years old. Or obtain verifiable parental consent for the minor to create an account. Companies that did not implement such checks would face monetary penalties. Social media companies would also have been required to use third-party vendors to perform reasonable age verification, which can include digitized identification cards, government-issued identification, or any commercially reasonable method. Social media companies would also have been prohibited from retaining any identifying information after access to the platform has been granted.

The story on children's privacy and social media does not end here. States have continued to pass laws attempting to regulate kids' use of social media. The Virginia legislature is seeking to amend the state's data privacy law to restrict 16 year olds to one hour of social media use a day, along with requiring age screening mechanisms. The amendment is awaiting signature. Arkansas has also rolled out additional legislation targeting social media companies and children. Utah recently implemented app store age limits, with effective dates under the law ranging from May 2025 to December 2026. And Texas – despite prior social media challenges – has introduced House Bill 186. If passed, the law would require age verification to create accounts.

Florida has also introduced legislation (SB 868) that would, among other things, permit law enforcement to view messages relevant to an investigation, allow parents to read all messages in a minor's account, and prohibit minors from using accounts that have "disappearing" messages.

Putting it into Practice: While these laws have not thus far been successful, state legislatures continue to propose laws to regulate kids' use of social media. We anticipate this flurry continuing, both from state law makers as well as efforts to push back on overly broad provisions.

Utah Pioneers App Store Age Limits

Posted March 27, 2025

Utah's governor recently signed the first law which puts age restrictions on app downloads. The law (the App Store Accountability Act, SB 142), was signed yesterday (Wednesday, March 26, 2025). We anticipate that the law may be challenged similar to NetChoice's challenge to the Utah Social Media Regulation Act and other similar state laws.

Once in effect, the law will apply to both app stores and app developers. There are various effective dates – May 7, 2025, May 6, 2026 and December 31, 2026— as outlined below. Among its requirements are the following:

- **Age Verification:** Under the new law, beginning May 6, 2026, ***app stores*** will need to verify the age of any user located in the state using "commercially reasonable" measures. Prior to that time, the Division of Consumer Protection will need to create rules that outline how age can be verified. Also starting May 2026, ***app developers*** will need to verify age categories "through the app store's data sharing methods." Age categories are children (users under age 13), younger teenagers (users between the ages of 13 and 15), older teenagers (users aged 16 or 17), and adults (users aged 18 and up).
- **Parental Consent/Notification:** Beginning May 6, 2026, ***app stores*** will need parental before a minor can download or purchase an app, or make in-app purchases. Consent is to be obtained through a parental account that links to the child's account. At the same time, ***app developers*** will need to verify that app stores have parental consent for minors' accounts. They also have to notify app stores of any significant changes to their apps. When this happens, the app stores will need to notify users and parents of these changes and get parents' renewed consent. App stores will also need to notify developers any time parents revoke their consent.
- **Contract Enforcement:** Under the new law, beginning May 6, 2026, app stores will not be able to enforce contracts against minors unless they already have consent from the minors' parents. This applies to app developers as well, unless they verify that the app store has consent from the minor's parents.
- **Safe Harbor:** The new law contains safe harbor provisions for app developers. Developers won't be responsible for violating this law if they rely in good faith on information provided by the app store. This includes age information as well as confirmation that parents provided consent for minors' account. For the safe harbor to apply, developers also need to follow the other rules set out for them by the law (described above).

Putting it into Practice: While we anticipate that this law will be challenged, it signals that states are continuing their focus on laws relating to children in the digital space. This is the first law that is focused on app stores, but we expect to see more in the future.

New York AG Settles with School App

Posted March 24, 2025

The New York Attorney General recently entered into an assurance of discontinuance with Saturn Technologies, operator of an app used by high school and college students. The app was designed to be a social media platform that assists students with tracking their calendars and events. It also includes connection and social networking features and displayed students' information to others. This included students' location and club participation, among other things. According to the NYAG, the company had engaged in a series of acts that violated the state's unfair and deceptive trade practice laws.

In particular, according to the attorney general, although the app said that it verified users before allowing them into these school communities, in fact anyone could join them. Based on the investigation done by the AG, the majority of users appeared not to have been verified or screened to block fraudulent accounts. In other words, accounts that were not those of students at the school. This was a concern, stressed the AG, as the unverified users had access to personal information of students. The AG argued that these actions constituted unfair and deceptive trade practices.

Finally, the AG alleged that the company did not make it clear that "student ambassadors" (who promoted the program) received rewards for marketing the program. As part of the settlement, the app maker has agreed to create and train employees and ambassadors on how to comply with the FTC's Endorsements Guides by, among other things, disclosing their connection to the app maker when discussing their use of the app.

Putting it into Practice: This case is a reminder to review apps directed to older minors not only from a COPPA perspective (which applies to those under 13). Here, the NYAG has alleged violations stemming from representations that the company made about the steps it would take to verify users. It also signals expectations in New York for protecting minors if offering a social media platform intended only for that market.

FTC COPPA Rule Updates: On Hold?

Posted February 26, 2025

In the waning days of the Biden administration, the FTC published an update to its COPPA Privacy Rule. The status of this update, however, is unclear. The revisions to the rule were posted on the FTC website prior to the Trump administration, but had not yet been published in the Federal Register.

Trump's Presidential Memorandum freezing pending federal regulations means that it has not yet been published. And publication is the next step towards it going into effect. Second, and relatedly, the current FTC chair (Ferguson) had expressed concerns about the rule. It is thus likely that it will not be published, at least as currently drafted. As we wait for next steps, for those companies that offer websites directed to or appealing to children, a quick recap. First, the items that were not of concern for Ferguson (and thus likely to be implemented as are):

- **Website Notice (privacy policy):** The content of website notice for those subject to COPPA under the rule as revised will require new content. This includes steps a site takes to make sure persistent identifiers used for operational purposes are not used for behavioral advertising. Additionally, for sites collecting audio files, the privacy policy must indicate how the files are used and deleted.
- **Verifiable Parental Consent:** The revised rules provide for new methods of parental verification. This includes comparing a parent's authenticated government ID against their face (using a camera app, for example). It also includes a "dynamic, multiple-choice" question approach, if the questions would be too hard for a child 12 or under to complete. The revision also permits texting for what has been traditionally known as the "email-plus" verification process, which can be used when children's information is not disclosed. Also added is another "one time use" exception to parental consent. Namely collecting and responding to a question submitted by a child through an audio file.
- **Security:** The new rule will require sites to have a written information security program. This goes beyond the current obligation to have "reasonable measures" in place. The security obligations are detailed, and mirror security obligations that exist under various state data security laws.

- **Definitions:** As revised the rule will add "biometric identifiers" to the list of personally identifiable information. These are elements like fingerprints or voiceprints that can be used to identify someone. The definition also includes someone's "gait." The rule will also include the definition of "mixed audience" site, a term currently used by the FTC in its COPPA FAQs.

Putting it into Practice: While we await the publication of the revised rules, whether in the format that they took before the new administration, or in a revised format, companies that operate websites subject to COPPA can keep in mind the parts of the new rule that were not of concern to Ferguson. These include new content in privacy policies.

California's Kids' Social Media Law Wrangling Continues, and Maryland Too!

Posted February 5, 2025

The Ninth Circuit continued the pause on California's SB 976 (Protecting Our Kids from Social Media Addiction Act) as of late January 2025. The law was signed by Governor Newsom in September 2024, and challenged by NetChoice shortly thereafter.

A federal judge first enjoined the law until February 1, 2025. The case continued in the courts, and most recently the Ninth Circuit blocked the law until April of 2025. At that time, it will examine substantively whether the law infringes free speech rights. This delay will impact the AG's drafting of rules for the law.

This is not NetChoice's first attempt to stop kid-focused social media laws. It took similar steps in Utah in 2024, and has challenged similar laws in Arkansas, Ohio, Mississippi, Texas, and most recently, as of Maryland's similar Age Appropriate Design Code Act.

Putting it into Practice: These decisions are a reminder that the social media laws being passed at a state level are continuing to be challenged. We will be continuing to monitor them for further developments.

Comprehensive Privacy

2025 Brought Us Eight U.S. "Comprehensive" Privacy Laws, What's Next?

Posted October 13, 2025

For those keeping track of the growing list of U.S. state "comprehensive" privacy laws, you know that the Maryland law (the Maryland Online Data Privacy Act or MODPA) went into effect on October 1st. This rounds us out for US state privacy laws in 2025, bringing the total to 17 (or 16, if you discount Florida). Next up will be Indiana, Kentucky, and Rhode Island (all on January 1, 2026).

While we have provided extensive information about these laws as they were passed, including this post and our online state law tracker, it's worth keeping in mind a few practical steps, especially as we wait for our next round, and undoubtably ongoing changes to the existing laws.

Have a regular cadence for reviewing your privacy policy. States -like Maryland- have specific content requirements. There is also exposure under deceptive trade practice laws if the policies are incorrect.

Review how and when you will provide "rights" like access and correction. Will the fact that a growing number of jurisdictions provide these rights tip you into the realm of offering them to all individuals?

Review your collection and storage practices. How are you addressing data minimization requirements, like those in Maryland? What about your treatment of sensitive information and your data sales practices? Are you meeting the growing patchwork of obligations that apply to digital targeting? What about the complex matrix of obligations for collection and use of children's information?

Maryland -and other states- have attempted to reduce risk for businesses by creating cure periods (in Maryland the cure period is 60 days, but that sunsets on April 1, 2027) and not providing private rights of action. However, not all privacy risks in the U.S. stem from these comprehensive state laws. And those laws do not necessarily have cure periods, and may also provide for private rights of action. The steps above may thus help in the face of this complex state patchwork.

Putting it into Practice: October for many entities is the height of planning for the coming year. The growth of the U.S. privacy law patchwork does not seem to be slowing down, and putting in place methods for addressing privacy notice, choice, and other data practices is a good thing to have on the schedule for 2026.

CPPA Adopts ADMT, Cybersecurity and Risk Assessment Regulations

Posted August 26, 2025

The CPPA scratched another task off the to-do list last month when it officially adopted proposed regulations under CCPA. These rules focus on three major areas: automated decision-making technology, risk assessments, and cybersecurity audits. We discussed the requirements of the proposed rules in this post in May, when they were still in draft form.

Since then, few substantive changes were made. As a reminder, here are a few of the rules' highlights:

- **Automated Decision-Making Technology:** Requirements around use of this technology will not go into effect until January 1, 2027. At that time, obligations will include, among other things, notification and choice if using these technologies for major decisions on financial services, housing, school admissions, employment, or healthcare. Use of the technologies for behavioral advertising is excluded.
- **Risk Assessments:** Beginning April 1, 2028, companies will need to submit risk assessments (including those conducted in 2026 and 2027) to the CPPA for processing poses "significant risk"—including selling/sharing data, processing sensitive data outside employment, using ADMT for major decisions, or profiling that reveals sensitive traits.
- **Cybersecurity Audits:** Annual cybersecurity audits will be mandatory for entities meeting "significant risk" thresholds based on size and data volume. The timing of these requirements is between 2028–2030, depending on revenue. Reports must justify any security safeguards not implemented and be available for review.

Putting it into Practice: Now that we have final rules (pending Office of Administrative Law approval, which is anticipated to come soon), businesses that meet CCPA's thresholds will want to review their use of automated technologies, update policies for risk assessments, take stock of their security controls, and train staff on their new obligations. Unfortunately, although these rules are final, they were not without controversy (hundreds of comments came in during the public consultation period) so further changes may be in store for these regulations.

Privacy Compliance Insights from Connecticut's First Privacy Law Settlement

Posted August 4, 2025

Can we take any insights from Connecticut's first settlement under the state's Data Privacy Act, reached with TicketNetwork, an online ticket marketplace? The AG concerns mirrored priorities outlined in Connecticut's 2025 CTDPA Enforcement Report. This suggests that future cases may also draw from that report.

In its press release about the matter, the AG argued that the company's privacy policy was "largely unreadable," missing required consumer rights information under Connecticut's privacy law, and failed to provide a functioning mechanism for consumers to exercise their data rights even after receiving a notice of violation in late 2023.

Under the settlement, TicketNetwork has agreed to pay an $85,000 penalty, as well as to maintain records regarding the number and types of consumer rights requests received and its response timelines and outcomes—metrics the AG uses to assess compliance. As a reminder, the Connecticut cure period has now expired, but some other states still have them. Namely: Indiana, Texas, Utah, and Virginia (30 day); Tennessee (60 day); Iowa (90 day); Oregon (30 day, expires January 1, 2026); Delaware (60 day, expires January 1, 2026); and Montana (60 day, expires April 1, 2026).

It is hard to tell exactly what concerns the AG had with the privacy policy. The AG did not provide any detail in its press release. However, since the AG first began its investigation of TicketNetwork (in 2022), the company made many modifications to its privacy policy (based on a comparison of its July 1, 2025 and 2023 policies, the latter available here.) Changes included adding section headers, giving more detail about rights and information collection practices, and listing the Connecticut law by name.

Putting it into Practice: This settlement suggests that the AG may rely on the priorities set out in its enforcement report when assessing if companies are in compliance with the Connecticut Data Privacy Act. If you have not done so already, you may want to review your organization's privacy policy, including how you describe rights to consumers.

Connecticut, the Provisions State, Adds New Provisions to its Privacy Law

Posted July 28, 2025

Connecticut has revised its privacy law for the third time since it was passed in 2022. With SB 1295, the state has mirrored others (like Colorado and Montana) in making ongoing changes to its law. Many of the changes incorporate either in concept, or wholesale, provisions that exist in other states. Connecticut makes these changes following 2024 and 2025 AG reports, which reports included recommendations to lawmakers, some of which ended up in SB 1295.

Among the changes that will take effect July 1, 2026 are the following:

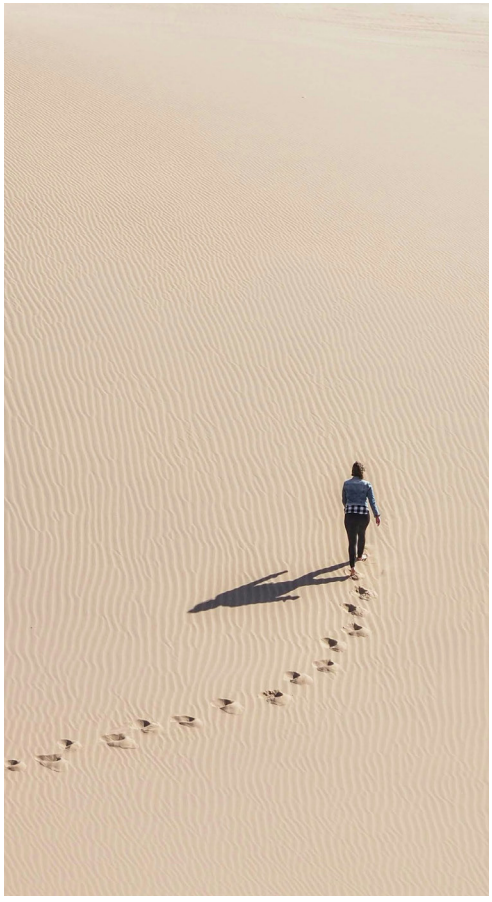
- **Expanded Scope:** Like Montana, the threshold will be lowered. Rather than 100,000 consumers, it will be processing information of 35,000 consumers. This lowered threshold aligns with other states such as Delaware, New Hampshire, Maryland, and Rhode Island. The law will also cover entities that process any sensitive consumer data, and expands the definition of that term. It will also apply to those offering personal data for sale in trade or commerce. Connecticut has also replaced its broad GLBA exemption with more targeted exemptions for certain types of regulated entities (including banks, insurers, and investment advisors).
- **Consumer Rights and Profiling Protections:** As revised, consumers will be able to access inferences made about them, including marketing profiles or other information derived from their data. They will also be able to contest profiling decisions (mirroring Minnesota). As revised, they will have a right to know if their information is being used for certain types of profiling that can have real-world effects, such as decisions relating to employment or housing. Among other things, consumers will be able to review or question certain results of automated tools used to make significant decisions. Connecticut will also join Minnesota and Montana in placing restrictions on how much sensitive data businesses can disclose in response to access requests.
- **Data Minimization:** Once the changes are in effect, businesses will only be able to collect personal data that is "reasonably necessary and proportionate" to the purposes disclosed. Businesses that process sensitive data will need both a valid purpose and consumer consent, with separate consent needed to sell such data. If a business plans to use data in a manner not reasonably aligned with what was first disclosed to the consumer, extra factors (such as the consumer's reasonable expectations) must be considered.
- **Profiling and AI:** Businesses will need to conduct impact assessments for profiling used in decisions with legal or significant effects, such as denying a loan or a job. These assessments must disclose the purpose, potential risks, performance metrics, and safeguards associated with the profiling activities.
- **Protections for Minors:** Like Maryland and Oregon, businesses will be prohibited from engaging in targeted advertising to minors, as well as selling minors' personal data (currently, these activities are permitted with parental or, depending on the age of the child, minor consent). For these purposes, in Maryland a minor is defined as someone under 18, and in Connecticut under 16.

Putting it into Practice: Between now and next July, companies that are subject to Connecticut's expanded scope will want to take the time to review their rights processes, as well as their approaches to automated decision making and sensitive information processing. These modifications are a reminder that the US may not have one "most stringent law" and instead, each state adds to the increasingly complicated patchwork of obligations facing companies.

U.S. Privacy Footprint Continues to Expand: Tennessee and Minnesota Join the State Law Club

Posted July 9, 2025

The U.S. "comprehensive" law landscape continues to expand, with two more states—Tennessee (July 1) and Minnesota (July 31) —joining the "comprehensive" privacy law club. Five of these -Delaware, Iowa, Nebraska, New Hampshire, and New Jersey- took effect in January. As the patchwork of state-level "comprehensive" privacy laws expands, what should business keep in mind? As outlined below, perhaps the biggest takeaway is that the laws add to a patchwork, one which consists of many overlapping requirements.



Here are a few highlights from these two latest laws:

- **Privacy Notice:** Both Tennessee and Minnesota -as with other states- require businesses to publish a clear and accessible privacy policy. These policies must explain what data is collected, how the information is used, with whom information is shared, and how consumers can exercise their privacy rights. Minnesota, though, unlike Tennessee, requires businesses to include data retention periods in their privacy policies. Tennessee uniquely offers an affirmative defense in the event of an enforcement action if a business has a privacy policy that reasonably conforms to NIST's privacy framework or equivalent safeguards.
- **Options:** Both states grant consumers the right to access, correct, delete, and port their personal information, as well as to opt out of the sale of their information, targeted advertising, and high-risk profiling. Additionally, both laws require businesses to obtain consent before processing sensitive information and to follow data minimization principles—collecting and using only the data necessary for the stated purpose. These mirror existing requirements in other states. Minnesota goes further by granting consumers the right to review, correct, and request reevaluation of information used in high-risk automated decision-making. It also requires letting consumers know -and opt out of- material changes to privacy practices that will impact them in the future.
- **Compliance Documentation:** Minnesota requires businesses to maintain privacy policies, compliance documentation, contact details for responsible personnel, and records of consumer appeals for at least 24 months. This is similar to requirements in California and Colorado.
- **Enforcement and Cure Periods:** Neither Tennessee nor Minnesota provides a private right of action, and each offers a cure period. Minnesota's cure period is 30 days, but sunsets January 31, 2026. Tennessee's is 60 days, and there is no sunset.

Putting it into Practice: Businesses operating in or collecting data from these states' residents should keep in mind the nuances and differences between these states' laws and those in other jurisdictions (for more comparisons see our tracker). These include responding, in Minnesota, to a request to review information used in high risk automated decision making (if the company engages in that practice).

Big Sky State Makes Big Privacy Updates

Posted June 24, 2025

Montana's privacy law has received a refresh and updates will go into effect October 1, 2025 – exactly one year since the law took effect. The law was modified with SB 297, and changes include coverage, approach with minors, and more:

- **Broadening Who is Covered:** Previously, Montana's privacy law applied only to those controlling or processing the personal data of at least 50,000 Montanans. SB 297 cuts those numbers in half, bringing in any business handling the data of just 25,000 state residents or making substantial revenues off the personal data of at least 15,000 people.
- **Minors:** As amended, businesses offering online services, products, or features to those under 18 must use reasonable care to avoid heightened risks of harm to minors. Data protection impact assessments -will also be needed if engaging in activities that might create a risk of harm to minors. As revised, companies will need to get consent from those 13-18, or from their parents if the minor is under 13, to process minors' information for targeted advertising, certain profiling activities, or selling of personal data. There are also restrictions on geolocation information collection and using "system design feature[s]" to increase use of online services.
- **Narrowed Exemptions:** Montana has removed the broad GLBA entity-level exemption that exists in most states (joining California, Minnesota, and Oregon). There will still be an exemption for GLBA-covered information, but the only types of financial institutions that receive the entity-level exception are banks and credit unions. Montana's law also previously exempted non-profits, but now narrows this to only non-profits that detect and prevent fraudulent acts in connection with insurance. Delaware and Oregon's privacy laws contain similar carveouts for non-profits.
- **Privacy Policy Updates:** Under the law's revisions, privacy policies will need to explain what rights consumers have (not just that the consumer has rights) and the types of data and third parties to whom data is shared or sold. Like California, Colorado, Minnesota, and New Jersey, Montana businesses must also state the date the privacy notice was "last updated." Privacy notice content will need to be accessible to individuals with disabilities and available in each language in which the business provides a product or service. Links to the notices must be conspicuously posted. Material changes must communicated to consumers for prospective data collection and they must be allowed to opt out of such changes.
- **AG and Right to Cure:** Finally, as amended, businesses will no longer have a statutory cure period. Previously, when the AG issued a notice of violation, businesses were given 60 days to cure.

Putting it into Practice: Montana joins California, Colorado, and Virginia in making changes to its comprehensive privacy laws. Provisions to keep in mind include privacy policy content, approach with minors' information, and who and what is covered under the law.

Oregon Extends Privacy Law to Specifically List Auto Makers

Posted June 18, 2025

In ongoing tweaks to state privacy laws, Oregon has amended its state privacy law to cover auto manufacturers. Specifically, those that process or control personal information that they get from a person's use of a car. As most are aware, the law requires disclosures when collecting personal information, provision of rights to consumers (including the ability to delete and port personal information), and limits on profiling among other things. While the Oregon law, like most state "comprehensive" laws, includes applicability thresholds, there are no thresholds for this new applicability to car manufacturers. The law is slated to go into effect in September of this year.

Putting It Into Practice: This amendment demonstrates a growing concern by law makers and regulators around data collected in motor vehicles. We anticipate seeing similar developments in coming months.

California Regulator Releases Updated Draft Regulations, Scales Back Proposed AI Privacy Rules

Posted May 28, 2025

California appears to be changing its approach to how it regulates artificial intelligence, likely reflecting its reaction to challenges seen recently in other states. Namely, the California Privacy Protection Agency recently released an update to its draft regulations which change how the Agency plans to regulate Automated Decisionmaking Technology, or ADMT. This comes after the Agency's original proposal faced intense opposition from industry groups, state lawmakers and Governor Newsom.

The public has until June 2, 2025 to submit comments. As now proposed, some of the key changes include:

Narrowed Scope of ADMT Rules

The definition of automatic decisionmaking technologies would now only cover technologies that "replace or substantially replace human decision-making." Technologies that just help or support human decisions would not be covered. The update also makes clear that the ADMT rules would only apply to decisions that result in a "significant decision" about a consumer—like those involving housing, employment, credit, or access to essential goods and services. Advertising to a consumer is specifically excluded from what counts as a "significant decision."

Eased Risk Assessment Burden

The new rules would make it easier for businesses when it comes to conducting risk assessments. For example, profiling a consumer for behavioral advertising would no longer requires a risk assessment. Similarly, using personal data to train ADMT would not trigger a risk assessment unless the business does it intentionally for certain specific purposes.

Cybersecurity Audits

As revised, businesses would have more time to complete initial audits, depending on how much money they make. Some of the tougher rules have also been relaxed. For example, businesses can use existing audits and report the results up to executive management instead of the board of directors.

Putting it into Practice: While we await the final regulations, this is nonetheless a reminder for businesses to review their uses of automatic decisionmaking technologies.

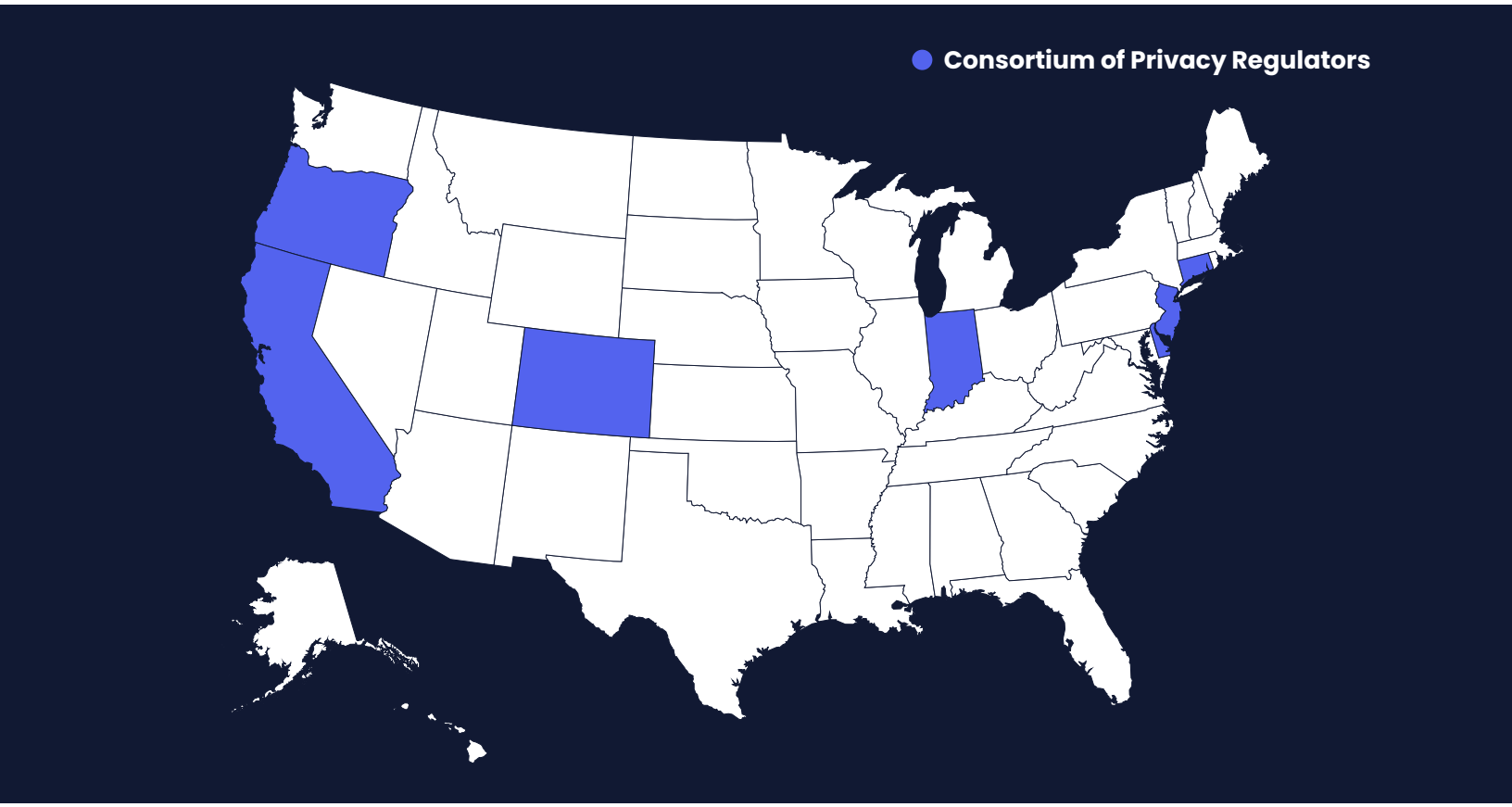
New Era of Collaboration? States Team Up to Coordinate on Privacy Laws

Posted April 28, 2025

The California Privacy Protection Agency announced this month that it, along with six other states, will be forming a new group called the "Consortium of Privacy Regulators." (The other states are Colorado, Connecticut, Delaware, Indiana, New Jersey, and Oregon.) Members include the Attorneys General from these states, as well as California's privacy regulator (the CPPA).

While these states may have slightly different privacy laws (see our U.S. State Comprehensive Privacy Law tracker for an overview), the group in its announcement reminded readers that there are many to ways in which the laws are similar. These include giving consumers rights -like access and deletion. Through the consortium, members intend to share resources and coordinate enforcement. They also announced their plan to use the consortium to promote a consistent interpretation of laws across jurisdictions. The CPPA press release indicated a goal is to minimize harm from data misuse, particularly health, geolocation and children's data.

Putting it into Practice: We anticipate that there may be cross-state action for violations of state "comprehensive" privacy laws, which could result in larger penalties. Companies may want to review their current practices, especially in areas that have been identified as issues of focus.



Oregon's Privacy Law: Six Month Update, With Six Months to End of Cure Period

Posted March 26, 2025

Oregon's Attorney General released a new report this month, summarizing the outcomes since Oregon's "comprehensive" privacy law took effect six months ago. A six-month report isn't new: Connecticut released a six month report in February of last year to assess how consumers and businesses were responding to its privacy law.

The report summarizes business obligations under the law, and highlights differences between the Oregon law and other, similar state laws. It also summarizes the education and outreach efforts conducted by the state's Department of Justice. This includes a "living document" set of FAQs answering questions about the law. The report also summarizes the 110 consumer complaints received to-date, and enforcement the Privacy Unit has taken since the law went into effect. On the enforcement side, Oregon reports that it has initiated and closed 21 privacy enforcement matters, with companies taking prompt steps to cure the issues raised.

As a reminder, these actions are being brought during the law's "cure" period, which gives companies a 30-day period to fix violations after receiving the Privacy Unit's notice. The Oregon cure provision sunsets on January 1, 2026. Other states with a cure period are Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Tennessee, Texas, Utah, Virginia. (Of these, Minnesota, New Hampshire, New Jersey, Oregon, Delaware, Maryland, and Montana will expire, with varying expiration dates between December 31, 2025 (Delaware) and April 1, 2027 (Maryland). Those without or where the cure period has expired are California, Colorado, Connecticut, and Rhode Island. For an overview of US state "comprehensive" privacy laws, visit our tracker.

Common business deficiencies identified by Oregon in the enforcement notices included:

- **Disclosure Issues:** This included not giving consumers a notice of their rights under the law.Also, of concern, has been insufficiently informing Oregon consumers about their rights under the law, specifically the list of third parties to whom their data has been sold.
- **Confusing Privacy Notices:** By way of example, Oregon pointed to -as confusing- notices that name some states in the "your state rights" section of the privacy policy, but not specifically name Oregon. This, the report posits, gives consumers the impression that privacy rights are only available to people who live in those named states.
- **Lacking or Burdensome Rights Mechanisms:** In other words, not including a clear and conspicuous link to a webpage enabling consumers to opt out, request their privacy rights, or inappropriately difficult authentication requirements.

Putting it into Practice: This report is a reminder to companies to look at their disclosures around consumer rights. It also sets out the state's expectations around drafting notices that are "clear" and "accessible" to the "average consumer." Companies have six months before the cure period in Oregon sunsets.

Colorado Rolls Out Updated Privacy Rules Ahead of 2025 CPA Amendments

Posted January 7, 2025

The Colorado AG's office adopted draft amendments to the Colorado Privacy Act rules last month. The adopted draft reflected input from the public to AG's September 2024 version and addresses three key issues. First, on opinion letters and interpretive guidance from the AG. Second, changes resulting from the passage of a bill related to biometric (HB 24-1130) data. And third, a bill related to children's (SB 24-041) privacy. (Both of which amend Colorado's privacy law.)

Opinion Letters and Interpretive Guidance

Colorado's privacy law allows the Colorado AG to issue opinion letters and interpretive guidance by January 1, 2025. These are tools that can provide insight and clarity to businesses and the general public. A business can request an Opinion Letter containing the AG's advice on how the CPA would apply to prospective processing activities. If the AG declines to issue an Opinion Letter, they can issue Interpretive Guidance. Both will be published on the Colorado AG website (Opinion Letters in redacted form). Interpretive Guidance is general advice that is not binding. The rule amendments state how to request an Opinion Letter, what information to provide in the request, and the factors the AG can consider when determining whether to respond to a request. The rule amendment also establishes a "good faith reliance defense" for businesses that receive an Opinion Letter (there is no such defense for relying on an Interpretive Guidance). Among other things, the business can legally rely upon the Opinion Letter in the event an enforcement action for the activity presented in the Opinion Letter.

Biometric Data

Effective July 1, 2025, Colorado's privacy law (as amended by HB 24-1130) will require that businesses adopt a written policy relating to biometrics. Part of the required process will be having a retention schedule, handling data incidents that impact biometrics, and deletion requirements. With certain exceptions, businesses must make this written policy available to the public. The new rule amendments address some of these changes, including:

- **Notice:** The creation of a "biometric identifier notice." Such notice must comply with all privacy notice requirements under CPA. This means the notice must be accessible, and detail in plain language the collection, purpose, length of retention, and any disclosure of biometric identifiers. It must be given at or before the collection of biometric information, and can be a separate document or part of the company's privacy policy.
- **Consent:** Consumers must give consent before their biometric data is sold, leased, traded, disclosed, or otherwise disseminated. Employers will need to get consent from employees and prospective employees before they collect or use biometric information. Employers must also provide notice. While the CPA rules generally require that businesses "refresh" consent every 2 years, but an employer does not need to refresh the employee's biometric consent – unless the biometric information will be used for new purposes.

Children and Minors

Beginning October 1, 2025, the Colorado privacy law (as amended by SB 24-041), will include new obligations on companies relating to minors (those under 18). These changes were also incorporated into the new rule amendments, and include:

- **Data Protection Impact Assessments:** Data protection impact assessments will be required where there is a heightened risk to minors from offering online services or products to minors.
- **Consent:** Businesses will need to get consent from minor consumers, or from a minor's parents if the minor is a child before using a system or design feature that will increase or sustain the use of an online platform. SB 24-041 also amends the CPA to require parental consent before processing a minor's data for targeted advertising, sale, or used for risky profiling.

Putting it into Practice: These new rules are a reminder that Colorado's Privacy Act continues to expand and grow. Companies should keep in mind these upcoming obligations for biometric and minor data, going into effect later this year. For some companies, the opportunity to receive an Opinion Letter about proposed activities may be useful, but only after careful consideration of the pros and cons of requesting such a letter (which include disclosure to the AG of planned -but not implemented- activities).

Data Breach

The Ghost of Employees Past: The Data Breach Risks from User-Credential Management

Posted December 3, 2025

A recent settlement with an education service provider and three states – California, Connecticut, and New York – serves as a reminder to deactivate the credentials of departed employees. The case arose following a data breach suffered by Illuminate Education, which provides assessment software to K-12 school systems. As part of its services, the company stores sensitive details like students' special education and accommodation needs.

In 2021, a hacker accessed the company's network using the administrative-level credentials of a former employee. The hacker created new accounts and exfiltrated the personal information of millions of students. The states alleged that failing to turn off the credentials of the former employee directly led to the 2021 breach. This, they argued, was a violation of their respective student privacy laws and was an unfair trade practice.

To settle the matter, the company agreed to pay $5.1 million: California will receive $3,250,000, Connecticut $1,700,000, Connecticut, and $150,000 will go to New York. The company also agreed to modify its security measures. Among other things, it will create and maintain data inventories, as well as limit data retention periods. It will also strengthen its access control and authentication processes.

Putting it into Practice: Threat actors are using more sophisticated tools to identify vulnerabilities. This settlement serves as a reminder to establish a clear process for removing credentials of departing employees. Especially those who may have been systems administrators.

2026 Data Breach Law Updates – California and Oklahoma

Posted October 29, 2025

California recently passed an amendment accelerating how quickly businesses must notify following a data breach. Previously, the requirement was to notify affected individuals "without unreasonable delay." Beginning January 1, 2026, the law mandates that businesses notify individuals within 30 calendar days after the discovery or notification of a breach. (New York also shortened its reporting this earlier this year). While some flexibility remains for law enforcement needs or to fully investigate the incident and restore data systems, this change places a clear emphasis on prompt action and accountability. Businesses in California will also face a new requirement when a data breach impacts over 500 residents. The law also calls for a copy of the notice sent to consumers to be submitted to the California Attorney General within 15 days of notifying individuals. Previously, there were no specific deadlines for sending a copy of the notice to the AG office.

Oklahoma also amended its data breach law with Senate Bill 626 earlier this year, with the amendment to also take effect January 1, 2026. This marks the first time Oklahoma has updated its breach notification law since its original passage in 2008. The law significantly broadens the types of personal information that could trigger notification. In addition to names and account numbers, now, government-issued identification numbers, unique electronic identifiers, and biometric data such as fingerprints and iris scans are also "personal information". Entities will also need to notify the Attorney General when a breach affects 500 or more residents within 60 days of notifying affected individuals. This aligns with several other states that require AG or regulator notification.

Putting it into Practice: For businesses operating in these states, these changes signal the growing focus on incident response times. As 2026 approaches, now is a good time for businesses to review their incident response processes—from detection and assessment to addressing notification, communication, and regulatory submission requirements.

Incident Response Defenses: Can You Take Advantage of a Cyber Program Safe Harbor?

Posted October 15, 2025

We are in the final quarter of the year, which is typically budgeting and planning for many issues, including -hopefully!- data incident preparedness. Is your organization able to take advantage of one of the growing number of states' safe harbor provisions? In particular, Connecticut, Iowa, Ohio, Oklahoma (beginning January 1, 2026), Oregon, – as of September 2025 Texas (for entities with less than 250 employees) – and Utah provide certain affirmative defenses against claims resulting from data breaches. The safe harbor is available if the company has a "qualified" cybersecurity program. What that means varies by state.

For Connecticut, Ohio, Utah, and Texas, the program must protect the confidentiality and security of personal information against threats, as well as against unauthorized access or acquisition that could result in material fraud. In Oregon, the business must use "reasonable" security measures. In Iowa, the program must evaluate and protect against risks, annually calculate the probable loss due to a breach, and communicate to impacted parties how they can reduce damages. Additionally, in Texas companies must meet specific operational requirements (like access controls and training) with specifics that depend on the size of the organization.

In Connecticut, Iowa, Ohio, and Utah, businesses can also qualify if they comply with industry-recognized cybersecurity frameworks (such as the NIST's Cybersecurity Framework) or, if applicable, laws like the Gramm-Leach-Bliley Act or HIPAA. Texas, however, makes compliance with one of these programs a *requirement* for the program.

Finally, Tennessee and Nebraska both provide a safe harbor not based on a company's security program, but instead as long as the incident was not based on a company's willful misconduct or gross negligence.

Putting it into Practice: Now is a good time to review your current cybersecurity program. Many are planning incident response tabletops, but examining if you qualify for a safe harbor is another good way to look for risk mitigation for the "not if but when" of data incidents.

New York Modifies Data Breach Law Heading Into 2025

Posted January 3, 2025

As 2024 came to a close, New York Gov. Hochul signed two bills (A8872A and S2376B) amending New York's data breach law. The modifications change both what constitutes personal information under the law, as well as modifying notification timing. The notice modification is now in effect; the change to the definition of personal information does not take effect until March 21, 2025.

As amended, companies will now have 30 days from discovery of a breach to notify impacted individuals. Previously, the law required notice to individuals "in the most expedient time possible and without reasonable delay." The regulator to notify has also changed. Previously, businesses needed to provide notice to the NY Attorney General, the Department of State, and the Division of State Police. A fourth group has been added. Now notice must also be sent to the New York Department of Financial Services. Notification to each agency can be done via form on the New York AG website.

The law's definition of personal information has been expanded to include both medical information and health insurance information. New York joins a growing list of states to include these elements in their breach laws.

Putting it into Practice: For those who keep a running list of notification timing, they will need to add this New York change to their list. New York also adds a regulatory authority to its notification list. Keep in mind the expended definition of personal information for assessing breaches this year.

Data Broker

California Continues to Expand Data Broker Requirements

Posted October 23, 2025

Companies are become increasingly concerned about being viewed as "selling" personal data. In the midst of these worries, California's governor signed SB 361, which will change the California Delete Act starting January 1, 2026. The law applies to those who sell personal information about consumers with whom they do not have a direct relationship. For covered entities, the amendment will add to compliance complexities.

The bill adds more disclosure obligations when a data broker registers with the state. Currently, data brokers must disclose when registering if they collected five different kinds of information. These include children's information or reproductive health information. That list has now been almost tripled. New elements to disclose as part of registering include if the broker collects biometric data and mobile advertising IDs. As amended, data brokers will also need to state if they sell information to foreign actors or US governmental bodies or law enforcement. They will also have to state if they sell any of the listed identifiers to GenAI models.

Separately, the California Privacy Protection Agency finalized its DROP regulations. That tool, the "Delete Request and Opt-Out Platform," will go live for consumers on January 1, 2026. Once live, consumers can go to the registry and opt out of brokers' sale of their information. Brokers will need to start regularly scrubbing against the platform August 1, 2026. "Regularly" defined as every 45 days. These finalized regulations have been modified from the last round. Specifically, to change the percentage matching threshold between what is in the DROP platform and what the broker holds before opting someone out. The final regulations call for a 100% match, not the previous 50% threshold.

Putting it into Practice: This amendment (and final rule) is a reminder of US state regulators' concerns about the sharing personal information. The requirements suggest that covered companies could be well served if they use their organizations' broader risk and compliance frameworks to address these obligations, while keeping in mind the legal exposure incorrect reports might create.

New Year, Old Tradition: CPPA Focuses on Unregistered Data Brokers

Posted February 18, 2025

The California privacy regulator recently settled with a data broker (Key Marketing Advantage LLC) that it alleged had violated the state's data broker law. Under the Delete Act, data brokers must, among other things, register annually by January 31 and pay an annual fee. According to the agency, the company failed to register or pay the fee. The broker agreed to pay $55,800 as part of the settlement.

This settlement follows an industry investigation sweep the agency announced in October of last year, after which it reached similar settlements with other data brokers. For those keeping track, the agency focused on data broker compliance at the beginning of last year as well.

What's coming up next for data brokers? The Act will require companies to access an online portal once every 45 days for consumer deletion requests. The portal is aptly called the Data Broker Delete Requests and Opt-Out Platform, or the DROP. It will launch to consumers on January 1, 2026. It opens to data brokers on August 1, 2026. As a reminder, Vermont, Texas, and Oregon also have similar data broker registration requirements.

Putting it Into Practice: This settlement is a reminder that California, like other states, is focused on entities that collect and sell personal information about individuals with whom they do not have a relationship (i.e., data brokers). If engaged in these practices keep the law's requirements in mind.

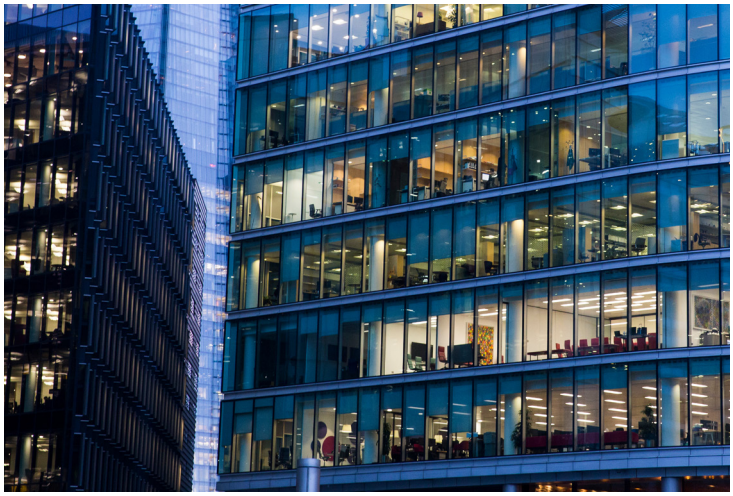
Data Transfers

DOJ Announces 90-Day Grace Period for Companies to Comply with New Data Security Rules on Foreign Adversary Access to U.S. Sensitive Data

Posted April 16, 2025

The U.S. Department of Justice (DOJ)'s new data security rule went into effect April 8, 2025. This rule requires companies to take measures to prevent U.S. sensitive personal and government-related data from falling into the hands of foreign adversaries. The rule targets transactions (including data brokerage, vendor agreements, employment agreements, and investment agreements) involving access to bulk sensitive personal data or government-related data when those transactions involve identified covered persons or countries of concern (China, Russia, Iran, North Korea, Cuba, and Venezuela).

On April 11, 2025, the DOJ's National Security Division (NSD) issued a Compliance Guide, a Frequently Asked Questions (FAQs) document, and its Implementation and Enforcement Policy, offering critical clarity on how it will assess compliance and approach enforcement of the rule. One of the most significant elements of the policy is the DOJ's announcement of a 90-day grace period (between April 8, 2025 and July 8, 2025) for companies making good faith efforts to comply (willful violations may still be pursued).This grace period is intended to encourage early cooperation and foster a compliance-first mindset across industries.



Companies should take action now, if they have not done so already, to engage in compliance efforts (many of which are identified by DOJ as evidence of "good faith") such as:

- Assessing datasets and datatypes that might be covered by the rule
- Reviewing data flows and data transactions, particularly those that might constitute data brokerage as defined in the rule
- Analyzing vendor agreements to determine the need for new contractual terms; renegotiation of agreements; and potential transfer of products and services to new vendors
- Instituting vendor due diligence practices aligned with the rule
- Evaluating employee access and potentially modifying roles, responsibilities, or work locations
- Assessing investments and investment agreements relating to countries of concern or covered persons
- Revising or creating internal policies and procedures
- Implementing security controls as set forth in the requirements established by the Cybersecurity and Infrastructure Agency (CISA)

The DOJ guidance confirms the effective dates in the rule and expectation for full compliance with initial requirements after the 90-day grace period. While the core rule took effect April 8, 2025, additional compliance obligations (e.g., audits, reporting, due diligence) must be in place by October 6, 2025.

Putting it into Practice: Organizations that collect, store, or transmit sensitive personal data—especially with cross-border implications—should begin engaging in the activities listed above. The rule is effectively a form of national security data control and applies to a broad array of actors, from data brokers and cloud infrastructure providers to businesses with international partnerships or data transfers.

Employment Privacy

New Jersey Updates Discrimination Law: New Rules for AI Fairness

Posted February 20, 2025

The New Jersey AG and the Division on Civil Rights' new guidance on algorithmic discrimination explains how AI tools might be used in ways that violate the New Jersey Law Against Discrimination. The law applies to employers in New Jersey, and some of its requirements overlap with new state "comprehensive" privacy laws. In particular, those laws' requirements on automated decisionmaking. Those laws, however, typically do not apply in an employment context (with the exception of California). This New Jersey guidance (which mirrors what we are seeing in other states) is a reminder that privacy practitioners should keep in mind AI discrimination beyond the consumer context.

The division released the guidance last month (as reported in our sister blog) to assist businesses as they vet automated decision-making tools. In particular, to avoid unfair bias against protected characteristics like sex, race, religion, and military service. The guidance clarifies that the law prohibits "algorithmic discrimination," which occurs when artificial intelligence (or an "automated decision-making tool") creates biased outcomes based on protected characteristics.

Key takeaways about the division's position, as articulated in the guidance, are listed below, and can be added to practitioners' growing rubric of requirements under the patchwork of privacy laws:

01 **The design, training, or deployment of AI tools can lead to discriminatory outcomes**. For example, the design of an AI tool may skew its decisions, or its decisions may be based on biased inputs. Similarly, data used to train tools may incorporate the developers bias and reflect those biases in their outcomes. When a business deploys a new tool incorrectly, whether intentionally or unintentionally, the outcomes can create an iterative bias.

02 **The *mechanism* or *type* of discrimination does not matter when it comes to liability**. Whether discrimination occurs through a human being or through automated tools is immaterial when it comes to liability, according to the guidance. The division's position is if the covered entity discriminates, they have violated the NJLAD. Additionally, the type of discrimination, whether disparate or intentional, does not matter. Importantly, if an employer uses an AI tool that disproportionately impacts a protected group, then they could be liable.

03 **AI tools might not consider reasonable accommodations and thus could result in a discriminatory outcome**. The guidance points to specific incidents that could impact employers and employees. An AI tool that measures productivity may flag for discipline an individual who has timing accommodations due to a disability or a person who needs time to express breast milk. Without taking these factors into account, the result could be discriminatory.

04 **Businesses are liable for algorithmic discrimination even if the business did not develop the tool or does not understand how it works**. Given this position, employers, and other covered entities, need to understand the AI tools and automated decision-making processes and regularly assess the outcomes after deployment.

05 **Steps businesses, and employers, can take to mitigate risk**. The guidance recommends that there be quality control measures in place for the design, training, and deployment of any AI tools. Businesses should also conduct impact assessments and regular bias audits (both pre- and post- deployment). Employers and covered entities should provide notice about the use of automated decision-making tools.

Putting it into Practice: This new guidance may foreshadow a focus by the New Jersey division on employer use of AI tools. New Jersey is not the only state to contemplate AI use in the employment context. Illinois amended its employment law last year to address algorithmic bias in employment decisions. Privacy practitioners should not forget about these employment laws when developing their privacy requirements rubrics.

EU/UK Privacy

Might We See a Streamlining of EU Digital Compliance?

Posted December 23, 2025

For those operating in the European Union, the list of digital technology laws is becoming daunting. Compliance with GDPR to the AI Act — with stops along the way for the ePrivacy Directive and many more – is a significant undertaking. To simplify this confusion, the European Commission is proposing modifications to many of its data laws. It released the first attempt of these changes in the Digital Omnibus Regulation Proposal.

The proposal takes a multi-pronged approach. If passed, it will impact GDPR, simplify rules around AI, data sharing, and modify the EU's approach to cybersecurity, to name but a few. This proposal is far from final: the European Parliament and the European Council must review and debate the proposed changes before any are implemented into law. What is potentially on the horizon?

With respect to GDPR, there are many things under consideration. A few highlights include making it easier for businesses, in low-risk situations, to give less detailed information in response to a rights request. Also on the horizon is the potential of a 96-hour breach-notice window, instead of 72 hours. Related to this is the possibility for a single point of notification for breaches. And, modify GDPR to clarify that if a business cannot re-identify an individual in practice, that information is not personal data. There is also the potential for a new legitimate interest for data processing of developing or operating AI systems—provided certain safeguards are followed.

For the ePrivacy Directive (Cookies), changes include incorporating it into the GDPR. As part of this would be new rules to make it easier for users to give or refuse consent and manage choices.

The omnibus proposal also contemplates changes to the AI Act. These include delaying full application of high-risk rules until necessary standards and guidance are ready, providing phased transition periods and fallback dates. Also, under consideration are changes to bias testing, and extending lighter regulatory requirements from small firms to small-mid caps. The omnibus proposal also contemplates shifting certain training responsibilities from companies to the Commission and Member States.

With respect to the Data Act, among the proposed changes are limiting business data-sharing obligations with government to public emergencies. And, expanding rules for switching between cloud providers to include Small Mid-Cap Companies (SMCs), not just small and medium-sized enterprises. Also being contemplated are making the law's smart contract data sharing less strict and easier to follow.

Putting it into Practice: This is the first step of process that will continue to develop throughout 2026. We will be monitoring for future developments. In the meantime, for companies that operate in the EU, this is another reminder of the importance of a principles-based approach to compliance.

Are Your Online Terms Enforceable?: Lessons from California

Posted December 1, 2025

The Southern District of California recently reminded companies that it has concerns about steps to take to make online terms binding. The case arose from a putative class action over alleged false pricing practices brought against Maggy London International Ltd. an online clothing retailer.

In an attempt to compel individual arbitration, the company pointed to a mandatory arbitration provision in its website terms. In California, to enforce an online agreement, a website operator must show one of two things. First, that a consumer had either actual knowledge of the terms of the agreement. Or second, that the company gave the consumer reasonably conspicuous notice of the terms and the consumer took action to unambiguously agree to the terms. Here, the company argued that the font, color, placement, and underline of the link to the terms under the "Pay Now" button on the checkout page was reasonably conspicuous. Additionally, the complaining customer by clicking "Pay Now" to buy product had agreed to the website terms.

The court agreed that the notice was conspicuous. However, relying on several Ninth Circuit cases, the court held that the conspicuous hyperlink to website terms was not enough to bind the consumer to the terms. The court's rationale was that it was not clear to the consumer that by clicking "Pay Now," they agreed to the website terms. Instead, the court determined the company should have had another step, like having words along the lines of "*by clicking pay now, you confirm you have read, understood, and agree to the Terms,*" to make it clear to the website user that they were agreeing to legal terms by clicking "Pay Now."

Putting it into Practice: This case underscores court concerns over on-screen consent flows. The company here had taken steps to make their terms prominent, but nevertheless, having a conspicuous link alone was insufficient. In designing platforms where you are linking to terms, think beyond having prominent links. To address court concerns, look at how you might tie a user's affirmative action to term acceptance.

EU Weighs in on Pseudonymized Data

Posted October 20, 2025

A thorny issue for companies has been how to handle data derived from personal information. Is it still personal information? Do privacy laws apply? The EU Court of Justice of grappled with this issue in a September decision. The case arose following a Spanish bank's financial difficulties. Its regulatory agency, the European Single Resolution Board, stepped in to attempt to value some of the bank's investments and otherwise determine next steps. As part of the process, the board hired a consulting firm to analyze feedback from the bank's shareholders and creditors. The board collected the information, pseudonymized the data, and then sent the pseudonymized data set to the consulting firm.

At issue was whether the entity should have told shareholders the sharing with the consulting firm would happen. In other words, treating the pseudonymized data as personal and following notice obligations under a privacy law applicable to entities like the board (Regulation 2018/1725, which is like GDPR but applicable to EU institutions like the board). Which, according to the Court, included telling individuals at the time information was collected, of "potential recipients of that data" (para. 108). The Court held that if pseudonymized data can be combined with other information and identify the individual, it still counts as personal data. The Court noted that this analysis should be made separately for each entity: the original company and the data recipient.

Putting it into Practice: Knowing when personal information is no longer "personal" will impact what legal obligations apply. As courts -like the one here- often point out, this is a factual analysis, and thus develop proactive processes and procedures can be tricky. In particular, because an entity may not have a full picture of all of the different data flows or intended internal or external uses. Remembering that any organization is made up of individuals with different needs and practices can help. Consider regular check-ins and conversations with business leaders and business teams to understand their current and future data uses and needs.

Belgian DPA Finds Certain Tax Information Transfers to IRS Unlawful

Posted May 12, 2025

The Belgian Data Protection Authority recently ruled that a Belgian government entity, FPS Finance, cannot transfer the personal data of "accidental Americans" to the IRS. According to the decision, the transfers needed to cease for several reasons.

The case was brought by a dual US-Belgian citizen, who, while a US citizen by birth, did not reside in the US or otherwise have any significant connections to the US (i.e., an "accidental American"). He argued that his personal information should not be transferred to the US, even though the US's Foreign Account Tax Compliance Act requires all US citizens to report their tax information to the US to combat terrorism and prevent tax evasion. That law is enforced in Belgium through a 2014 bilateral treaty, which was entered into before the GDPR's effective date. The Belgian tax authority argued that it could make the transfer under a GDPR exception (Article 96), which allows pre-GDPR international agreements, such as this one, to remain in place if they comply with the law in effect at the time. Thus, the Belgian DPA examined not only whether the transfer violated GDPR (as the individual argued) but also whether it violated the laws in existence at the time the treaty was signed.

The Belgian DPA found that the transfers did not comply with pre-GDPR law because the amount of information being transferred exceeded what was necessary to meet the specified purposes. Further, the FATCA was not compliant with current GDPR standards. The Belgian DPA also emphasized that FATCA, as implemented, lacked sufficient safeguards to protect the personal data of EU residents, especially those with tenuous or accidental ties to the US. The Belgian DPA gave FPS Finance a year to modify its transfer process. This included minimizing the amount of data transferred, conducting a data transfer impact assessment, and giving individuals more information about its data processing activities.

Putting it into Practice: This decision is a reminder that there may an increase in scrutiny of data transfers to the US. While the facts in this case were narrow, we expect that there may be other, similar, decisions in the future.

Forget It!: EDPB Announces Focus on Right to Erasure in 2025

Posted March 11, 2025

Right of erasure (or "right to be forgotten") has been selected by the European Data Protection Board as its priority enforcement topic for 2025. This work is being done under the "Coordinated Enforcement Framework" or "CEF." The EDPB created the CEF in 2022 as a way to streamline and coordinate enforcement across EU data protection authorities. Past topics have included the right of access, and the role of data protection officers in organizations.

Data Protection Authorities in the various member states (and seven state-level authorities in Germany) this year will examine how companies are complying with GDPR obligations around erasure requests. The topic was selected, the EDPB indicated, because it is the most common right requested by individuals . . . and also the one about which DPAs often receive complaints.

As they did with the actions for right of access, DPAs will take steps ranging from fact finding to formal investigations. The DPAs will also work together to analyze the results of the initiative, and the EDPB will publish a report at the conclusion of the initiative. This will be similar to the report issued on the 2024 right of access actions (adopted this January).

Putting it into Practice: The announcement about the right of erasure priority, as well as the release of the right of access report, can serve as a reminder for companies to revisit their process for responding to rights requests.

EU Fines EU?!: Alleged Unlawful Data-Transfer Dust-Up

Posted February 3, 2025

Following a German case brought against the EU Commission, the EU General Court found that the Commission had made an improper transfer of personal information to the U.S. The plaintiff, a German citizen, alleged (among other things) that his information was sent through the EU Commission's website to the U.S. through an automated social media login option when he registered for a Commission event. He further alleged that this violated the government-agency equivalent of GDPR (EUDPR), as it occurred during a period in time when the Privacy Shield had been found inadequate, and the replacement program was not yet in place.

The court noted that the Commission, in making the transfer, relied only on website terms for the US data recipient. It did not enter into a contract that included standard contractual clauses or otherwise have "appropriate safeguard[s]." The court ordered the Commission to pay the individual €400.

Putting it into Practice: This case -brought against the EU entity that oversees GDPR compliance- is a reminder of EU concerns with data transfers to the US. As we await further developments with the Data Privacy Framework under the new administration, companies may want to re-examine the mechanisms (including standard contractual clauses + additional safeguards) EU-U.S. data transfers.

Financial Privacy

North Dakota Passes New Data Security Law for "Financial Corporations"

Posted June 17, 2025

North Dakota recently passed a law establishing new rules for certain financial companies operating in the state – specifically "financial corporations." The new obligations will take effect on August 1, 2025. They will apply to businesses that the North Dakota department of financial institutions regulates. Financial institutions (like banks and loan companies) and credit unions are not regulated by that entity.

Under the new requirements, covered entities must create a written information security program and designate a person to oversee that program. Covered entities must base their information security programs on a written risk assessment that identifies risks to their customers' information. The program includes breach response and reporting provisions for incidents that impact customer information. Covered entities will also have to periodically complete new risk assessments to evaluate their security measures and monitor the efficacy of the program.

The law also creates new rules for reporting data breaches. Namely, covered financial companies must notify the North Dakota Commissioner of the Department of Financial Institutions if there is a "notification event." A notification event occurs when an unauthorized person accesses unencrypted customer information. If this event involves the information of at least 500 customers, the company must notify the Commissioner as soon as possible, but no later than 45 days after discovering the issue. The law states that a covered entity "discovers" an event as soon as any employee, officer, or agent of the corporation learns about it.

Putting it into Practice: Financial corporations regulated by the North Dakota department of financial institutions should take note of these changes and make updates as might be needed to their security program and incident response plan prior to August 1st.

Insurance Cybersecurity Certifications: An (Updated) State Roundup

Posted April 14, 2025

Over half of US states require annual compliance certifications from insurance providers. While the filing time frames for this year draw to a close, companies may want to keep them in mind not only for next year, but as a reminder of the information security programs that are expected to be in place.

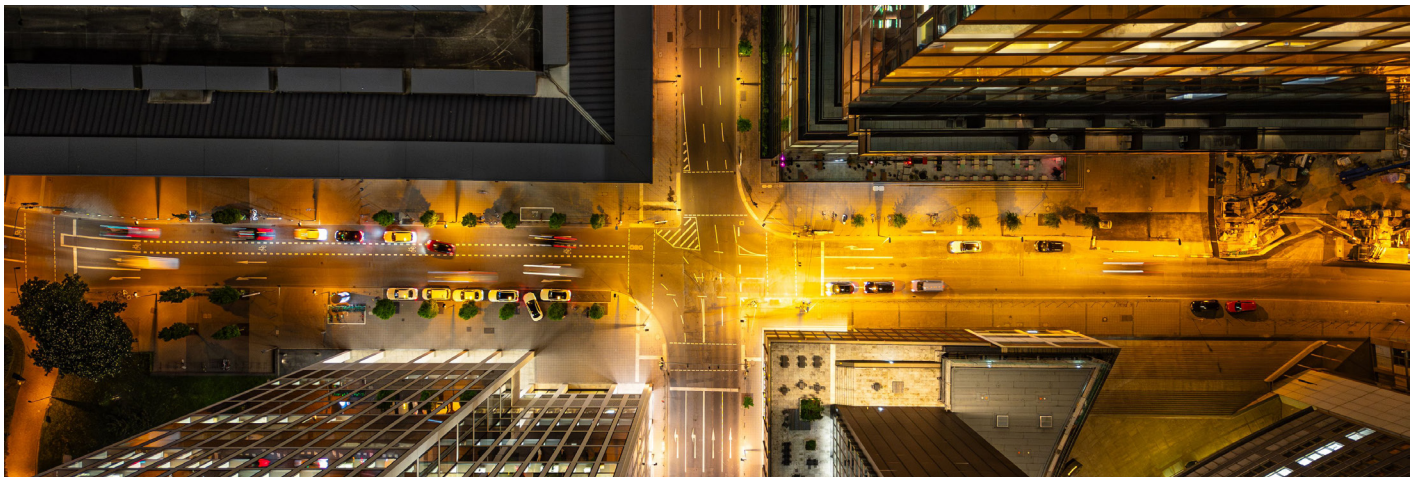
When we last wrote about this, in 2021, only nine states (Alabama, Delaware, Louisiana, Michigan, Mississippi, New Hampshire, Ohio, South Carolina, and Virginia) had adopted certification obligations. Since then, 17 more states have followed suit, adopting the Insurance Data Security Model law (from which the obligations stem). These states are Alaska, Connecticut, Hawaii, Illinois, Indiana, Iowa, Kentucky, Maine, Maryland, Minnesota, North Dakota, Oklahoma, Pennsylvania, Rhode Island, Tennessee, Vermont, and Wisconsin. Additionally, while New York has not adopted the NAIC model law, it imposes a similar annual filing requirement.

Filing deadlines are set out below:

Deadline	States
February 15	Alabama, Alaska, Delaware, Kentucky, Louisiana, Michigan, Mississippi, Ohio, South Carolina, Virginia
March 1	New Hampshire, Wisconsin
March 31	Hawaii
April 15	Connecticut, Illinois, Indiana, Iowa, Maine, Maryland, Minnesota, New York, North Dakota, Oklahoma, Pennsylvania, Rhode Island, Tennessee, Vermont

Those who might need to certify are those registered under the various state insurance laws. This includes insurance companies and insurance professionals, like agents and brokers. When making their filing, covered entities must certify that they have an Information Security Program in place. That program must include risk management and incident response procedures, as well as board oversight. Certification records and supporting materials need to be retained for five years after submission.

Putting it into Practice: Those with insurance certification obligations should keep in mind the varying filing deadlines, as well as the accompanying obligations like having a compliant information security program in place.



Auto Insurer Settles With New York AG Over Insurance Application Platform Security Issues

Posted April 4, 2025

The New York Attorney General recently entered into an assurance of discontinuance with Root Insurance Company following a 2021 data incident. According to the AG, the threat actors obtained people's drivers' license numbers by exploiting a website error on its car insurance application portal. Namely, upon entering a publicly available name and address, the site would generate a prefilled PDF that included that person's drivers' license number, which numbers were pulled from third-party databases. Threat actors used an automated bot to exploit this vulnerability, and gathered drivers' license numbers of 44,449 New Yorkers (more than half of the total 72,852 people impacted). The threat actors then used many of these people's information to file fake unemployment claims with New York, which according to the AG, was the goal of the attack.

According to the AG, the company was not aware of the design feature issue. Instead, the situation was discovered when company personnel noticed unusual application activity. Upon discovery, the company took measures to address the issue, including using CAPTCHA to ensure the application was made by a human, and masking the license numbers. The AG nevertheless brought this case, claiming that the incident occurred because the company did not have appropriate risk assessment measures in place to identify the design error. It also should have, according to the AG, used measures like masking sensitive data and detecting and deterring automated traffic. These failures, it alleged, constituted a violation of the state's data security law, which requires that companies develop, implement and maintain "reasonable safeguards" to protect covered information. This information includes names and drivers' license numbers.

Similar to past settlements, the AG required that the company implement of additional security measures (see, for example, our posts about settlements with a social media app last month, ENT in December 2024, a biotech company in mid-2024, and Herff Jones in 2022). Included in these are developing and maintaining a written information security program, designating a chief information security officer to oversee the program, engaging in network monitoring and employing multi-factor authentication, and maintaining compliance records for six years that the attorney general can access. The company has also agreed, among other things, to develop a data inventory, have a written process to ensure secure software development processes, to monitor network activity, and to promptly investigate suspicious activity. The company has also agreed to pay $975,000.

Putting it into Practice: This settlement outlines expectations from the New York attorney general of the proactive measures companies it believes companies should have in place if handling sensitive personal information. As companies launch new platforms, or revamp existing ones, this is a reminder to think not only about platforms where they collect personal information directly from individuals, but also where that information might be gathered from third party sources.

SEC Creates New Tech-Focused Enforcement Team

Posted March 28, 2025

On February 20, the SEC announced the creation of its Cyber and Emerging Technologies Unit (CETU) to address misconduct involving new technologies and strengthen protections for retail investors. The CETU replaces the SEC's former Crypto Assets and Cyber Unit and will be led by SEC enforcement veteran Laura D'Allaird.

According to the SEC, the CETU will focus on rooting out fraud that leverages emerging technologies, including artificial intelligence and blockchain, and will coordinate closely with the Crypto Task Force established earlier this year (previously discussed here). The unit is comprised of approximately 30 attorneys and specialists across multiple SEC offices and will target conduct that misuses technological innovation to harm investors and undermine market confidence.

The CETU will prioritize enforcement in the following areas:

- Fraud involving the use of artificial intelligence or machine learning;
- Use of social media, the dark web, or deceptive websites to commit fraud;
- Hacking to access material nonpublic information for unlawful trading;
- Takeovers of retail investor brokerage accounts;
- Fraud involving blockchain technology and crypto assets;
- Regulated entities' noncompliance with cybersecurity rules and regulations; and
- Misleading disclosures by public companies related to cybersecurity risks.

In announcing the CETU, Acting Chairman Mark Uyeda emphasized that the unit is designed to align investor protection with market innovation. The move signals a recalibration of the SEC's enforcement strategy in the cyber and fintech space, with a stronger focus on misconduct that directly affects retail investors.

Putting it into Practice: Formation of the CETU follows Commissioner Peirce's statement on creating a regulatory environment that fosters innovation and "excludes liars, cheaters, and scammers" (previously discussed here). The CETU is intended to reflect that approach, redirecting enforcement resources toward clearly fraudulent conduct involving emerging technologies like AI and blockchain.

Government Privacy

Leveling Up: Will CMMC Contract Obligations Impact Your Organization?

Posted October 16, 2025

Will a final rule issued by the Department of Defense on September 10, 2025 (available here) cause companies to rethink their compliance approach? The rule –relating to the Cybersecurity Maturity Model Certification program or CMMC – will impact how defense contractors engage with the Department of Defense. (We wrote previously (here) about the separate, but related, CMMC rule that addressed substantive CMMC program requirements.)

This final rule will require defense contractors to affirm CMMC compliance on a phased approach, with full implementation by November 2028. The requirement will place a significant hurdle on defense contractors, who will need to affirm their CMMC compliance in order to contract with the Department of Defense. The first implementation phase begins November 10, 2025 and addresses self-assessment and affirmation for entities that handle "FCI" (or basic Federal Contract Information) and "CUI" (or Controlled Unclassified Information). More detail about the requirements are in our sister blog post here.

Performing assessments and obtaining certification will likely require organizational change on many levels. It will include C-suite attestations and flow down obligations to subcontractors. While obligations were already in effect before this rule, we expect CMMC to result in increased exposure under the False Claims Act if attestations are inaccurate.

Putting it into Practice: Failing to get through the CMMC assessment and certification process can result in defense contractors losing their DoD business. Rushing through the assessment process, failing to involve key stakeholders, or otherwise mis-stepping, however, can expose entities to legal exposure. In the face of this, companies should consider organizational change principles: engage key stakeholders, conduct reviews under privilege, and treat CMMC as a key governance risk, not an IT problem.

Healthcare Privacy

Keep Out! California Draws the Privacy Fence Around Health Data

Posted November 20, 2025

California has set what may be an emerging trend with AB 45, restricting collection and use of personal information collected near family planning facilities. The law was signed recently by h Governor Newsom and is set to go into effect January 1, 2027. It provides for penalties of $25,000 fine per violation.

Under the law, personal information collected at these locations can be used only for purposes necessary to provide a requested service. For example, checking someone in for their appointment. All other uses are specifically prohibited. This includes not only advertising uses, but also tracking foot traffic. Similarly prohibited is geofencing and selling location data. The law will also prohibit releasing reproductive health records ("research records") to law enforcement or out-of-state entities seeking to enforce laws in other jurisdictions (like abortion bans).

Putting it into Practice: While designed to protect those who are seeking reproductive health services, the law underscores a broader trend. State lawmakers are modifying or adopting laws to address evolving technologies. Especially if they think there is "a high risk to the rights and freedoms of natural persons," to borrow an EU term. This will grow the US patchwork, something multinational companies should keep in mind as they design their compliance programs.

New Texas Law Requires Storage of Electronic Health Records in U.S.

Posted August 1, 2025

Starting January 1, 2026, health care practitioners in Texas are required to store electronic health records in the United States under a new Act. It applies to all records- regardless of the date on which the record was first prepared. his requirement is found in a recently enacted law that also includes requirements for practitioner's AI use.

Health care practitioners include providers licensed, certified, or otherwise authorized to provide health care services in Texas. Many practitioners use third party software for electronic health record solutions. This localization requirements also applies to those arrangements with vendors and cloud storage providers. The Act also requires that health care practitioners implement reasonable and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic health records. The law does not specifically contemplate what those safeguards might be. The law also prohibits collection and storage of individual credit scores or voter registration information in electronic health records.

Putting it into practice: While historically, there had not been many laws expressly requiring that EHRs be hosted in the U.S., Texas joins Florida in enacting this law. Before this law goes into effect, health care practitioners in Texas should assess storage of electronic health records to ensure records are maintained in the United States. Providers will also want to confirm that the necessary safeguards are in place to protect EHRs. Lastly, credit scores or voter registration records should not be collected or stored in electronic health records. In addition, health care practitioners should assess vendor relationships to confirm compliance with the Act. Practitioners may also want to update template agreements to account for these offshoring considerations (if not done so already).

New Texas Law Permits Use of AI In Health Care

Posted July 29, 2025

Texas recently enacted a pair of laws aimed at AI governance in the public sector and in healthcare. Starting September 1, 2025, there will be statutory authorization for health care practitioners (HCPs) in Texas to use AI for care-related purposes. This includes a practitioner's ability to develop courses of treatment and to diagnose patients.

For HCPs using AI, the Act has four key requirements:

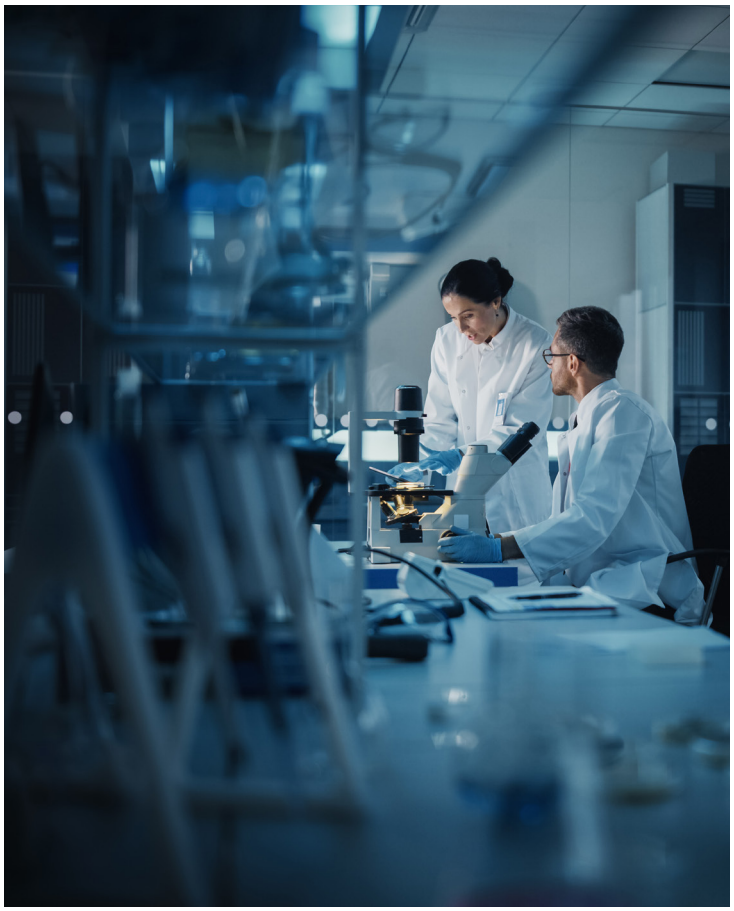
01
the HCP using AI must be acting within the scope of his/her license, certification, or authorization;

02
use of AI must not otherwise be restricted or prohibited by applicable laws;

03
the HCP must review all medical records created by AI to ensure they conform to records standards established by the Texas Medical Board; and

04
the HCP must disclose to patients that he/she uses AI for care-related purposes.

As for the notice requirement, the Act does not impose specific content requirements nor does it require that the disclosure be verbal versus written. The Utah Artificial Intelligence Policy Act has a similar requirement, which requires that businesses who are in "regulated" occupations (such as HCPs) make a prominent disclosure that they are using AI in the provision of those services. Texas HCPs should also be mindful of the overlap between this act and the companion bill enacted (i.e., the Texas Responsible Artificial Intelligence Governance Act (TRAIGA) (which we wrote about here)). Notably, TRAIGA also requires that HCPs notify patients when using AI tools for treatment.



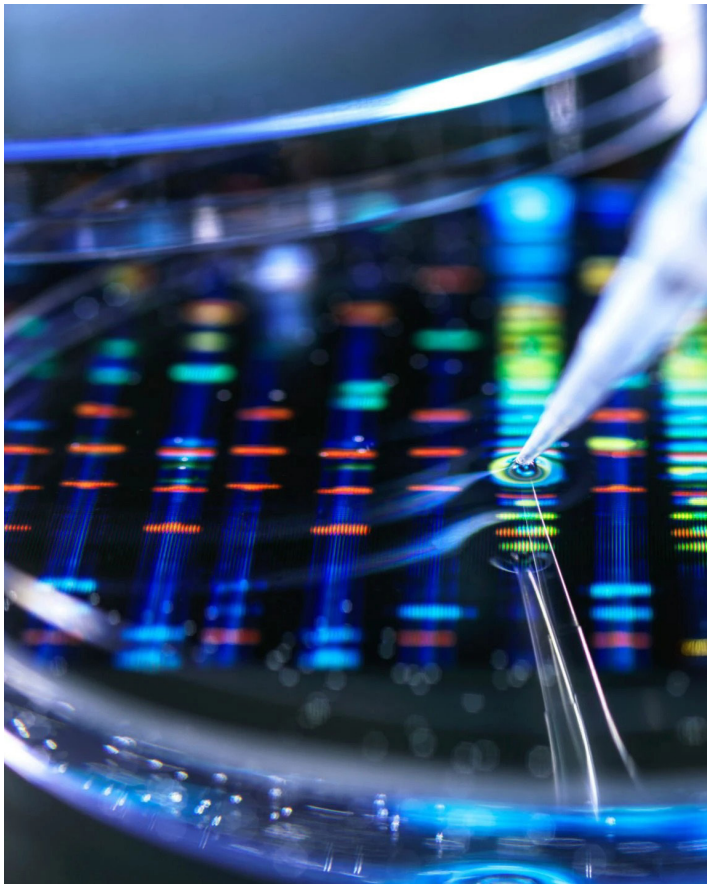
Putting it into Practice: Texas HCPs currently using (or open to using) AI for care-related purposes should consider what steps should be taken to comply with this law. For example, practices should be established requiring require review of medical records contributed to by AI to ensure conformance with professional standards. In addition, HCPs should consider the content and method of delivery for notices to patients about AI-use.

Montana Amends Law to Cover Collection and Use of Neural Data

Posted May 27, 2025

Montana recently revised its Genetic Information Privacy Act to address neural data. The law went into effect in 2023, and applies to both entities that offer genetic testing services as well as entities that use genetic data.

Under the current law, covered entities must provide notice and also have choice obligations. This includes getting consent about collection, use and sharing of genetic data. Covered entities must include specific content in the consent request. They also need to give separate notice in several circumstances. This includes if they want to share genetic information with non-vendor third parties, or use it for marketing purposes. There are also data security obligations under the law, as well as access obligations.



The Montana governor signed SB 163 on May 1 to amend the Genetic Information Privacy Act. As a result, beginning October 1, 2025, there will be several changes to the law. They include:

- **Neural Data will be Covered by the Law:** As revised the law will cover "neurotechnology data." This is information capable of "recording, interpreting, or altering the response of an individual's central or peripheral nervous system" to its external environment. (This definition is slightly different than that which California and Colorado added to their comprehensive privacy laws.)
- **De-identified Neural Data Out of Scope:** As modified, the law will also except from coverage deidentified neural data that is used for research purposes. To be deidentified, among other things, the information cannot be reasonably linked to the individual, and measures must be taken to ensure that the data cannot be reassociated with an individual.
- **Exceptions Added to Right of Access:** Also as modified, the law will provide for exceptions to the obligation to give individuals access to covered data, including if express consent was obtained from an individual participant in a clinical trial which was obtained following the provisions specified in the law (these include content and font size obligations, among other things).

Putting it into Practice: This modification to Montana's Genetic Information Privacy Act reflects regulators' concerns with uses of neural data, which companies might use when offering wearable technology or engaging in advertising that measures emotional engagement. This modification is a reminder for those who engage in these activities to review their notice process, and consider whether consent might be needed under this or similar laws.

New Ohio Transparency Pricing Rules for Hospitals Comes with Limits to Target Advertising

Posted March 21, 2025

Starting April 3, Ohio hospitals will have to navigate new requirements under House Bill 173. This law mandates greater transparency in healthcare pricing. It also includes rules for selling or targeted advertising related to personal information hospitals collect from price estimator tools (discussed in more detail below). The law applies to hospitals in Ohio, which is any facility providing inpatient medical services for periods longer than twenty-four hours.

Transparent Pricing for Services

HB 173 requires hospitals to provide consumers with public pricing information for all hospital items and services. Hospitals need to create a digital list of all standard charges for their services. This list must be easy to access, free of charge, and cannot require any personal information from the user. These provisions are designed to help patients understand how much they will have to pay for medical services. Hospitals also have to offer information about "shoppable services" e.g., – services that can be scheduled in advance.

To meet this transparency requirement, hospitals either must provide a list of shoppable services, *or* provide an internet-based price estimator tool that helps patients estimate costs for these types of procedures.

Targeted Advertising

For hospitals that decide to use a price estimator tool, there are restrictions on how personal information the tool collects can be used. Specifically, the law prohibits hospitals from using personal information collected from the use of the tool for targeted advertising. The law defines targeted advertising as displaying an ad that is selected based on personal data obtained from the use of a hospital's internet-based price estimator tool by a person in Ohio. This means that hospitals cannot show consumers specific ads based on the information a person provides to estimate healthcare costs. Hospitals are also not allowed to sell personal information collected from price estimator tools. While "sell" is not defined under the law it is most likely to be interpreted closer to HIPAA definitions than state consumer privacy laws. Sell under HIPAA means direct or indirect renumeration in exchange for PHI.

The law provides specific exclusions for what is considered targeted advertising. Hospitals can still advertise based on a user's direct request for information or their activities on the hospital's own websites. Ads that are shown based on the context of a user's search or visit are also excluded. Additionally, using data to measure how effective ads are is not considered targeted advertising. However, covered entities must continue to be mindful of OCR's guidance with respect to the use of tracking technologies as well.

Putting it into Practice: Hospitals in Ohio may need to adopt new practices to remain compliant with the law. This includes making sure their websites provide easy-to-find pricing information for patients. Additionally, hospitals should confirm personal information from price estimator tools isn't used for targeted advertising.

Online Privacy

Minnesota May Be First to Require Social Media Warning Label

Posted July 11, 2025

Minnesota has a new law that, beginning a year from now, will require that social media companies warn users of the potential negative mental health effects of social media use each time a user accesses a social media platform. The warning label will need to include specific content, including information about mental health resources (like the national suicide prevention and mental health crisis hotline). The law also specifically prohibits including "extraneous information" in the warning label. It must be on-screen (not in a company's website terms) and remain on screen until the user either acknowledges and agrees to it, or leaves the site.

Unless challenged, the law will take effect on July 1, 2026. Prior to going into effect, the commissioner of health is tasked under the law with creating guidelines by March 1, 2026.

Putting it into Practice: While we anticipate that these social media label requirements will be challenged prior to the 2026 effective dates, they demonstrate ongoing concern from US state law makers over the impact of social media use.

Michigan AG Sues Roku Over Alleged Privacy Violations

Posted May 28, 2025

The Michigan Attorney General has filed a complaint against Roku, a popular TV content platform, alleging, among other things, violations of the Children's Online Privacy Protection Act and the Video Privacy Protection Act (and a similar Michigan law). As most are aware, COPPA requires prior parental consent before collecting information from children online. It gives standing to both the FTC and to states' attorneys general, but no private right of action. Most cases brought since COPPA's passage have been brought by the FTC, however, and not by states. This current Michigan case comes after a group of 43 states, including Michigan, sent a letter to the FTC urging it to strengthen and update its COPPA Rule.

In this lawsuit, Michigan claims that Roku collected children's names, device IDs, locations, voice recordings, and other personal information without getting parental consent. Roku also shared this information with advertisers and data brokers to serve targeted ads to children. This activity occurred on the kids and family channel of Roku, and other areas of the Roku service that were targeted to children. Unlike competitors' services, the complaint alleges, Roku does not have the ability to create child profiles, which profiles would have permitted parents to moderate and control their children's use of the services.

According to the Michigan AG, Roku knew that it was collecting personal information from children, and was an operator of an "online service" as defined by COPPA. As such, it should have gotten parental consent from parents before collecting and sharing personal information from children. It also should have had appropriate notice of these practices in its privacy policy as contemplated under COPPA. The AG also alleged violations of the state's unfair and deceptive trade practice laws, as well as counts relating to VPPA as – it alleged – Roku is a video tape service provider under that law, which impacts the ability to disclose information about people's viewing habits to third parties.

Putting it into Practice: For companies that are directed to or have actual knowledge of collecting information online from children under 13, this case is a reminder that state attorneys general can bring COPPA cases. We may see other, similar, actions in the future. It also suggests what AGs will view as an "online service" under the law, beyond a mere website.

Ninth Circuit Upends Internet Personal Jurisdiction Law–Briskin v. Shopify

Posted May 5, 2025

In a landmark ruling, the Ninth Circuit expanded the application of specific personal jurisdiction principles to the realm of nationwide e-commerce. On April 21, 2025, an en banc panel issued a 10–1 decision ruling that allegations that Shopify embedded cookies that tracked a California consumer's location data were sufficient to establish specific personal jurisdiction over Shopify in California (reversing the Court's prior opinion on this exact issue). In the wake of this decision, businesses may face increased legal challenges in various states. To protect against far-flung lawsuits in unwanted jurisdictions, e-commerce businesses should, if practicable, refrain from collecting location data and engaging in other online activities that may be seen as targeting consumers of a particular state.

The case—Brandon Briskin v. Shopify, Inc.—involves Brandon Briskin, a California resident, who accused Shopify, Inc., a Canadian corporation, along with its U.S. subsidiaries, of privacy violations during an online transaction. Briskin alleged that Shopify unlawfully collected and used his personal information, including location data, without consent, focusing on Shopify allegedly installing tracking cookies and creating consumer profiles from collected data. The district court dismissed the case for lack of specific personal jurisdiction, ruling that an e-commerce platform such as Shopify, which operates nationwide, does not specifically target California residents. The Ninth Circuit affirmed the district court's ruling but later agreed to reconsider the personal jurisdiction determination en banc.

Applying traditional personal jurisdiction principles to Shopify's e-commerce activities, the Ninth Circuit panel held that because Shopify's geolocation technology allowed it to know where Briskin's smartphone was located in California when it installed cookies on his device, Shopify's conduct of intercepting Briskin's information deliberately targeted a California resident, meeting the purposeful direction requirement for specific personal jurisdiction. Accordingly, per the Ninth Circuit, an interactive platform "expressly aims" its wrongful conduct toward a forum state when its contacts are its "own choice and not 'random, isolated, or fortuitous," even if that platform cultivates a "nationwide audience" for commercial gain.

A significant aspect of the decision was the panel's rejection of the necessity for "differential targeting," which refers to the concept that a defendant's actions within a forum state create specific personal jurisdiction only if the defendant acted with "some prioritization of the forum state"—rather than a general, nationwide focus. This ruling indicates that a business model like Shopify's, which operates nationwide and utilizes consumer data, can be subject to jurisdiction in any state where it (1) gathers data from a resident of such state and (2) the business has some indication of the resident's physical location when interacting with the business.

Judge Callahan dissented, expressing concerns that Shopify's conduct was not expressly aimed at California. The dissent cautioned that the majority's approach could lead to companies facing jurisdiction based solely on the plaintiff's location during transactions and noted "[b]y holding that California courts can exert specific jurisdiction over Shopify because Briskin used his iPhone while 'located in California,' […] the majority opinion departs from the longstanding principle that jurisdiction turns on 'the defendant's contacts with the forum State itself, not the defendant's contacts with persons who reside there."

Putting it into Practice: The Ninth Circuit's decision is a major sea change to personal jurisdiction of businesses in the digital age, particularly e-commerce businesses. This ruling serves as a reminder for e-commerce platforms to consider their interactions with consumers in various states, as their business activities may subject them to jurisdictions across the map. To lessen the impact of the Shopify ruling and the likelihood of personal jurisdiction being established in states in the Ninth Circuit businesses can consider geofencing, refraining from collecting online location data, and making sure that other aspects of the business's online activities are not purposefully directed at a particular state.

FTC Requests Input from Tech Platform Users About Speech

Posted March 10, 2025

The Federal Trade Commission recently requested public comment from users of tech platforms. In particular, the impact the platforms may have on user speech. Input is sought -by May 21- on the extent to which tech firms are engaging in potentially suppressing free speech.

Using terms like "censorship," "demonization," and "shadow banning," this request for public comment signals a new direction of the agency under Andrew Ferguson. The direction being taken reflects the concern expressed before the new administration: that tech platforms were using their roles to censor speech (see *Murthy v. Biden*).

The request is unlike those we had seen in the past from the FTC, insofar as it requests comment about the tech platforms not from the platforms themselves, but instead directly from users. As of this writing, the agency had received over 1,000 comments. Among other things, the agency has asked people to provide input on:

01

Impact: Whether tech platforms banned users from the platform because of the content of their speech, or took other adverse actions and the extent to which those actions adversely impacted them. Relatedly, the request asks if people were given a "meaningful" way to challenge adverse decisions.

02

Moderation: Whether there were moderation policies in place, and if the platform told people (even implicitly) that they could appeal the platforms' decisions. Also asked was whether the platforms used "opaque" or "unpredictable" processes to restrict access.

03

Pressure: Interestingly, the request asks potential commenters to speculate on "factors [that] motivated platforms' decisions." Included in these might be measures that resulted in them getting banned from the platform. This includes suggestions like pressure from advertisers, state or local governments, or foreign governmental action.

04

Competition: If the tech platforms were coordinating directly or through trade associations about policy and adverse actions.

Putting it into Practice:
Private platforms' moderation policies date to the early days of the Internet, and the Digital Millennium Copyright Act and the Communications Decency Act. These policies typically indicate that content that violates the policy will be removed (the alternative -modifying content- would run the risk of the platform participating in the creation of the content, losing the shield of the DMCA or CDA). We anticipate comments from industry groups, in addition to the many already received from users themselves. The comment period closes May 21.

Privacy Management

Top Tips for Non-US Companies to Address U.S. Privacy Laws

Posted December 16, 2025

In a recent webinar, we gave practical recommendations for those non-U.S. companies who are looking to expand their U.S. operations. We are thrilled to announce publication of a white paper, which summarizes the recommendations from our webinar. In it, we provide an overview of the U.S.'s patchwork approach to regulating privacy.

We designed this guide to help non-U.S. entities prioritize their compliance efforts. We walk through sector-specific risks (like healthcare, kids' use of social media, and government contracting), activity-specific risks (such as tracking technologies and vendor management), and practical strategies for building a flexible, principle-based compliance framework. Rather than advocating generic and impractical approaches, we focus practical strategies. From programs based on core principles, to cross-functional collaboration, we suggest change-management concepts that can help navigate the U.S. environment.

Putting it into Practice: This guide can help non-U.S. organizations navigate what we anticipate will be an increasingly confusing and complex privacy and cybersecurity landscape in the United States in 2026, and potentially beyond.

More Privacy Compliance Considerations for the 2026 Budget Process

Posted August 25, 2025

Now is the time that many are putting together their 2026 budgets and considering how much to allocate next year to address the constantly evolving privacy and data security landscape. In the last article in this series we looked at three change management tools that can help effectuate privacy compliance. Here are three more, and things to consider -and potentially budget for- in the new year.

- **Build Practical Roadmaps:** As you create your program and goals for 2026, have actionable milestones and measurable objectives. Both will help you keep track of your progress, and help assess the extent to which the initiative has been successful. There are many change management tools -like balanced scorecards- that can help with alignment and tracking.
- **Appreciate Individual Impacts and Readiness**: When designing training or developing employee compliance requirements, remember that everyone has a different experience with change. How do people in a given group learn best? It might be through in-person and interactive sessions, or an online, gamified approach. What will the impact be on a given compliance requirement? If it makes it more difficult to do one's job duties -or have a perception of difficulty, there may be more resistance. Surveys and check-ins can provide valuable insight into potential challenges.
- **Identify and Work With Key Stakeholders**: Identify who holds formal and informal influence within the organization. These are the individuals on whom the success of your compliance initiative often rests. Understanding the extent to which they are committed to your compliance vision – and developing a roadmap to get their buy-in if there are not – can have an outsized impact on your success.

Putting it into Practice: As you develop your privacy and data security compliance budget for 2026, keeping in mind these tips for what makes for a successful change management process can help you identify what activities you want to budget for in the new year.

Setting Your Privacy Compliance Strategy in Advance of the 2026 Budget Process

Posted August 22, 2025

Today's compliance landscape is more crowded—and more complex—than ever. As the pace of regulatory change accelerates, companies need to find effective paths forward. As I detailed in a Law360 article from earlier this year, change management tools can help. Here are three areas to consider as you begin to think about your compliance plans (and budget) for 2026.

- **Diagnose Before You Act:** Rushing to launch "solutions" for perceived compliance programs can backfire. From wasted resources to missed opportunities, rushing can result in programs that do not have sufficient buy in, or are simply not actionable. It may be painful, but taking the time to fully diagnose the problem and the business rationale can have big payoffs. That may mean mapping out compliance priorities, reviewing the compliance needs unique to your organization, or exploring multiple approaches before settling on the path forward.
- **Align With Your Company's Core Values:** Those who research organizational change have found time and time again that initiatives that are grounded in an organization's mission and values is more likely to take root. Making sure the compliance program resonates with stakeholders means that it is more likely to be successful.
- **Listen and Adapt:** A program built only by the compliance or legal team can lose the buy-in that you need to make change happen. Organizational change practitioners know that to accomplish change, you need to involve the right stakeholders in the development of the program. This includes getting and incorporating feedback. This will foster trust, surface real-world concerns, and result in workable and supported compliance programs.

Putting it into Practice: The next post in this series will include three more tips and ideas drawn from change management research.

Common Privacy Pitfalls in M&A Deals

Posted March 12, 2025

Many expect that deal activity will increase in 2025. As we approach the end of the first quarter, it is helpful to keep in mind privacy and data security issues that can potentially derail a deal. We discussed this in a webinar last week, where we highlighted issues from the buyer's perspective. We recap the highlights here:

- **Take a Smart Start Approach:** Often when privacy "specialists" are brought into deals, it is without a clear understanding of the goal of the deal and post-acquisition plans. Keeping these in mind can be crucial to conducting appropriate and risk-based diligence. (Along with having a clear understanding of the structure of the deal.) Questions to ask include the extent to which the target will be integrated into the buyer. Or, whether privacy assets (mailing lists) are important to the deal.
- **Conducting Diligence:** Diligence can happen on a piece-meal basis. There are facts about the target that can be discovered even before the data room opens. What information has it shared about operations and products on its website? Has there been significant press? Any publicly-announced data breaches? What about privacy or data security related litigation? When submitting diligence question lists, keep the scope of the deal in mind. What are priority items that can be gathered, and how can that be done without overwhelming the target?
- **Pre-Closing Considerations:** There are some obvious things that will need to happen before closing, like reviewing and finalizing deal documents and schedules. There may also be privacy-specific issues, such as addressing potential impediments to personal information transfers.
- **Post-Closing Integration:** In many deals, the privacy and cybersecurity team is not involved in the integration process. Or, a different team handles these steps. Issues that might arise- and can be anticipated during the deal process- include understanding the data and processes that will be needed post integration, and the personnel who can help (whether at the target or buyer).

Putting it into Practice: Keeping track of the intent of the deal and the key risks can help the deal flow more smoothly. This checklist can help with your next transaction.

Sheppard's 2024 Eye on Privacy Year in Review

Posted January 21, 2025

January brings us new year's resolutions, and an opportunity to look back at the prior year. As we have done in years past (2023, 2022, 2021, 2020, 2019 and 2018), we have created a comprehensive resource of all our www.eyeonprivacy.com posts from 2024. Articles address new US state laws, artificial intelligence, data transfers, and more. As you move forward with your privacy program and risk management for 2025, we hope that this compilation of developments from 2024 is helpful. We hope that this is again a useful tool to help prepare for privacy and cybersecurity program plans for the year.

Tracking

Is Your Website's Cookie Banner Up to Date? New Guidance from Dutch DPA

Posted December 4, 2025

The Dutch Data Protection Authority recently updated its cookie banner guidance. This comes after the agency, the Autoriteit Persoonsgegevens (or AP), promoted a goal earlier this year to monitor 500 websites a year to ensure their use of cookies complies with GDPR. The Dutch are not the only ones concerned about cookie banners. See, for example, activity from the UK that we wrote about last year. Of note, the Dutch authority stresses in its guide that even if a company uses third-party consent management platforms, the site operator is still responsible for compliance.

In its guidance, the Dutch authority has reminded companies that if they use cookies that collect personal information, they need a banner that clearly tells people what personal information the site collects and if the company shares that information with anyone else. This content must be in the banner's first layer. If visitors want more details, they can find more layers with extra information. The guide gives as a suggested banner one with three choices: "Accept," "Reject," and "Set It Yourself."

Once the user clicks to the second layer -where they can control their options- the Dutch authority cautions that for consent to be valid, sliders, toggles, or other choice mechanisms must be easy to understand. If there are check boxes, they cannot be pre-checked. It also must be just as simple for users to withdraw consent as it was to give it.

The Dutch authority's guidance also addresses categorizing cookies, stressing that they should be organized between those where consent is required and those where it is not. The Dutch authority reminds companies in its guide that cookies that are placed based on a "legitimate interest", for example functional or analytic cookies, do not require consent.

Putting it into Practice: This guide is a reminder that regulators are focused on the level of control companies give over website tracking tools. Keep in mind that cookies are dynamic: lower risk by avoiding a "set it and forget it" approach to cookie categorization. Other techniques can include regularly testing banners for user ease and functionality.

Behind the Pixel: Not Always Personal Information Under VPPA

Posted October 21, 2025

Many courts have held that that information gathered by video-related pixels are not "personal" for purposes of the Video Privacy Protection Act. Nevertheless, plaintiff class action attorneys continue to file these VPPA actions in federal court.

This issue came up in a recent case against the National Basketball Association (Salazar v. NBA). The plaintiff argued that video-related pixels used by the NBA gathered personally identifiable information and sent it to third parties. The New York federal court, looking at the case on remand, disagreed. It held that the information gathered – lines of computer code – was not personal. In reaching its decision, the court relied on Second Circuit precedent (Solomon v. Flipps Media). Namely, that personal information is limited to what an ordinary person – as opposed to a sophisticated technology company – can use to identify someone.

Putting it into Practice: This decision is helpful and good news for those who have video pixels on their sites. However, the ongoing litigation in this area is a reminder that to be prepared. Have a full picture of your site's tracking tools. This means more than just asking IT, as the tools may be placed by different internal teams or outside vendors. You will likely need a working relationship across many groups, not only IT, legal, and compliance.

U.S. Privacy

State Privacy Action Grows: Consortium Expands, California Launches Data Broker Strike Force

Posted November 24, 2025

The Consortium of Privacy Regulators is growing. Meanwhile, CalPrivacy has announced a new program, a data broker "strike force."

Minnesota and New Hampshire have joined with Colorado, Connecticut, Delaware, Indiana, New Jersey, Oregon, and the California Privacy regulatory body (CalPrivacy) to coordinate on their enforcement of "comprehensive" privacy laws. The consortium was created earlier this year, with the stated goal of coordinating privacy law enforcement efforts. Since the consortium was created, California, Colorado and Connecticut joined together in September to investigate companies' alleged failure to honor sale opt-out requests and honor GPC signals.

Meanwhile, CalPrivacy announced that it will increase its oversight of data brokers. It has created a special team called the Data Broker Enforcement Strike Force. This team will ensure that companies are following rules about protecting consumer privacy and registering as data brokers. The strike force will have more resources to investigate violations. The strike force creation follows recent actions brought by the agency under California's Delete Act.

Putting it into Practice: The state-level actions are a reminder to those operating in the US. As we enter into 2026, expect more state level coordination and enforcement. This is a good time to assess if your privacy program takes an adaptive and principles-based approach. Do your training efforts go beyond memorization? Do you reward "small wins" and otherwise take an organizational change lens to your compliance efforts?

While you may not be able to future-proof regulatory changes, you can future-proof your culture. The most resilient programs take into account regulatory developments and pair them with a principles-based approach to compliance.

2025 Blog Contributors

Liisa Thomas
Partner, Privacy and Cybersecurity Practice Group Leader
+1.312.499.6335
lmthomas@sheppard.com
Bio

Townsend Bourne
Partner, Aerospace, Defense & Government Services Industry Team Leader
+1.202.747.2184
tbourne@sheppard.com
Bio

Snehal Desai
Partner
+1.415.774.2960
sdesai@sheppard.com
Bio

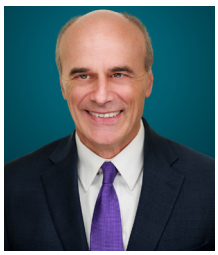
Wynter Deagle
Partner, Intellectual Property Practice Group Leader
+1.858.720.8947
wdeagle@sheppard.com
Bio

A.J. Dhaliwal
Partner, Blockchain and Fintech Industry Team Leader
+1.202.747.2323
adhaliwal@sheppard.com
Bio

James Gatto
Partner, Artificial Intelligence Industry Team and Blockchain and Fintech Industry Team Leader
+1.202.747.1945
jgatto@sheppard.com
Bio

Julia Kadish
Partner
+1.312.499.6334
jkadish@sheppard.com
Bio

Carolyn Metnick
Partner
+1.312.499.6315
cmetnick@sheppard.com
Bio



Jonathan Meyer
Partner
+1.202.747.1920
jmeyer@sheppard.com
Bio

David Poell
Partner
+1.312.499.6349
dpoell@sheppard.com
Bio

Mehul Madia
Special Counsel
+1.202.747.2301
mmadia@sheppard.com
Bio

Maxwell Earp-Thomas
Associate
+1.714.424.2880
mearp-thomas@sheppard.com
Bio

Samuel Hyams-Millard
Associate
+1.415.774.2973
shyams-millard@sheppard.com
Bio

Kathryn Smith
Associate
+1.312.499.6355
kasmith@sheppard.com
Bio

Michael Sutton
Associate
+1.469.391.7455
msutton@sheppard.com
Bio

Brittany Walter
Associate
+1.858.876.3525
bwalter@sheppard.com
Bio

Sheppard

Brussels • Century City • Chicago • Dallas • Houston • Los Angeles • London • New York • Orange County
San Diego (Del Mar) • San Diego (Downtown) • San Francisco • Seoul • Shanghai • Silicon Valley • Washington, DC

sheppard.com