CLIENT ALERTS & INSIGHTS

Privacy Points: 2024 Recap and What to Watch For in 2025

JANUARY 29, 2025

Authors: Ryan T. Sulkin

Looking forward to 2025, more U.S. states are in line to pass omnibus data protection laws, enforcement of U.S. state data protection laws is likely to increase, and "sensitive data" concepts will similarly grow and take shape.

As we close the book on 2024 and look to 2025, data protection law remains as active as ever. Specifically, 2024 saw a handful of new states omnibus data protection laws become effective; bringing the total number of states with such laws in effect to 14. And 2025 shows no signs of stopping with five state legislatures already taking up consideration of new data protection laws.

This past year also saw major updates to biometric information regulation, Federal government action on the protection of U.S. sensitive personal information and limiting the transfer of such information, a specific focus on the protection of consumer health data by state legislatures, and so much more.

As the page turns into a new year, businesses will need to dive beyond initial data protection law requirements-like website privacy notices-and consider how any and all data is collected and used through the business. Consent and opt out requirements, contract and procurement considerations, specific security requirements, and regular audits and assessments are just the tip of the iceberg of a fully compliant data protection program.

Below are some highlights of key issues and topics to watch as we progress into 2025.

NEW US STATE DATA PROTECTION LAWS

As the clock hit midnight a few weeks ago (and as of the date of this article being published), 14 states have broad, omnibus data protection laws in effect regulating the collection and use of personal data: (1) California, (2) Colorado; (3) Connecticut; (4) Delaware; (5) Florida; (6) Iowa; (7) Montana; (8) Nebraska; (9) New Hampshire; (10) New Jersey; (11) Oregon; (12) Texas; (13) Virginia; and (14) Utah.

In total, there are 20 states with omnibus data protection laws on the books, with the other eight going into effect this year and in the years to come.

2025 and Beyond

Specifically, over the course of 2025, we have three new states to welcome to the party:

2025:

- Maryland: October 1, 2025
- Minnesota: July 31, 2025
- Tennessee: July 1, 2025

Indiana, Kentucky, and Rhode Island are ready to follow suit in 2026. There has also been a flurry of early year, state legislature activity, with five states-New York, Massachusetts, Ohio, Pennsylvania, and Oklahoma-having introduced their own omnibus data protection laws.

It is already difficult to come across a business operating in the U.S. that is not impacted or that does not need to comply with one or multiple U.S. state data protection laws. That will become even more difficult by year end.

U.S. State Data Protection Law Compliance

The privacy policy and notice requirements are often what businesses first think of, and first build out compliance for, regarding U.S. state data protection laws. However, the privacy policies and notices are but the first step towards compliance.

Full compliance with U.S. state data protection laws requires a dive deeper into the layered, complicated, and sometimes contradictory depths of this burgeoning body of law. Compliance programs will need to span, yes, those privacy policies and notices, but also procurement and sales teams to handle vendor management and required privacy provisions in contracts (i.e., Data Processing Addendums), internal consumer relation teams to handle data privacy right requests (e.g., rights to delete, access, correct, opt out, etc.), web developer teams to build out Global Privacy Control compliance, and engagement with information technology teams to conduct risk assessments and to ensure current security measures are sufficient.

Generally, with a growing body of privacy law in U.S. state law-ranging from consumer-facing requirements to procurement and third-party risk management considerations-a business will need to consider privacy and information security across all departments and teams. An understanding of the full scope of how data is being collected and used within a company is a critical first step.

See our past coverage of some of the less talked about requirements here. Additionally, see Benesch's and Data Meets World's interactive U.S. State Privacy Laws website page for a high level overview of what U.S. states have data protection laws on the books and of what such data protection laws cover and will require.

2025 What to Watch For: More U.S. states are sure to follow suit, continuing to increase the number of states with broad data protection laws on the books. As more states come online with these laws, expect businesses across industries to focus on deeper levels of compliance, past the initial work of privacy notices.

U.S. STATE DATA PROTECTION LAW ENFORCEMENT

Enforcement of U.S. state data protection laws has been fairly slow out of the gate. But businesses should not expect that pattern to hold. If 2024 is a sign of enforcement to come, 2025 could be a turning point year as state attorney general offices and regulations focus on enforcing these new laws.

California Leading the Way

California-being the first on the U.S. scene with an omnibus data protection law with the 2018 California Consumer Privacy Act, amended by the California Privacy Rights Act of 2020 ("CCPA")-has led the way on initial enforcement actions. The California Attorney General's Office continued formal CCPA enforcement actions in 2024. However, California's new Consumer Privacy Protection Agency ("CPPA") also spent 2024 issuing enforcement advisories, highlighting areas of CCPA compliance they viewed many companies failing to adhere to.

The CPPA's first enforcement advisory highlighted the key concept of data minimization-specifically focusing on excessive data collected when consumers make requests pursuant to their data privacy rights under the California data protection laws. In laymen's terms, data minimization means a business is only permitted to: (1) collect and use the minimum amount of data necessary for specific purposes (e.g., those purposes that are stated in that business's privacy notice); and (2) only retain / store such limited data set for the minimum period of time necessary for that specific purpose.

And even then, a business is required to ensure-as with any data collection under the CCPA-that reasonable and appropriate security measures are in place to protect the data.

The enforcement advisory focused on data minimization as applied to a business verifying a consumer privacy rights request. Under the CCPA, a business is permitted to take reasonable steps to verify the identity of a consumer prior to granting or acting on that consumer's privacy rights request (for example, a request to delete, correct, or access their personal data). In the enforcement advisory, the CPPA stated that it was "observing, however, that certain businesses are asking consumers to provide excessive and unnecessary personal information in response to requests that consumers make under the CCPA."

Practically, businesses need to ensure that such verification data is not commingled with other personal data a business generally collects and uses-the latter of which is likely subject to longer retention periods and other use cases. The verification data should only be kept for the period necessary to verify and act on the request-which is likely a shorter period of time.

Other recent enforcement advisories from the CPPA focused on the use of dark patterns. The CCPA defines dark patterns as designs and interfaces used by businesses to subvert or impair a consumers' ability to make a decision or choice. Specifically, the CPPA advised that businesses need to focus on providing consumers with clear, symmetrical, and equal choices with respect to their privacy rights.

The CPPA specifically used the example of a consumer's right to opt out of the sale of their personal information or sharing of their personal information. There, businesses are required under the CCPA to provide users with clear, easy to use methods through which the consumer can opt out of-for example-targeted advertising activities.

If the process to opt out of such activities takes more steps than the process to opt back in, it would be an impermissible dark pattern. Another example would be a targeted advertising cookie notice that only provides the consumer with an "Accept All" option, but no clear option to decline or opt out.

Colorado Advisory Opinions

The Colorado Privacy Act took effect July 1, 2023 and, after California, has been one of the more active U.S. state data protection laws, with the Colorado Attorney General's Office issuing multiple rounds of regulations.

The most recent set of Colorado Privacy Act regulations introduced a new process for opinion letters. The opinion letter process permits a business to proactively reach out to the Colorado Attorney General's Office to request a formal opinion from the Colorado Attorney General's Office on how the Colorado Privacy Act applies to, accepts, or prohibits potential data collection and use activities.

Businesses can request opinion letters, but the request must be (1) prospective in nature, pertaining to an activity that the requestor specifically plans to undertake; (2) must not be based on a hypothetical situation or activity not related to the requestor; and (3) must be in writing. The request for an opinion letter must then substantively contain the following:

- Complete and specific description of the activity and planned processing;
- Description of the personal data in scope, including whether sensitive personal data is in scope;
- Description of the parties who will have access to the personal data;
- Description and draft of any planned consumer-facing disclosures relating to the planned activity;
- A copy of any data protection assessment conducted in anticipation of the planned activity; and
- A designation of trade secrets or confidential information included, if applicable.

If the Colorado Attorney General's Office accepts the request and issues an opinion letter, it will publish an opinion letter pursuant to the request, and the letter will be publicly available.

The opinion letter process may offer businesses a helpful avenue to clarify the law's requirements and to proactively address concerns prior to enforcement actions.

2025 What to Watch For: More states will jump into the enforcement fray as the laws and regulations mature. With many U.S. state data protection laws including mandatory or discretionary cure periods, expect many states to send out cure letter requests to businesses identifying areas of potential non-compliance.

U.S. SENSITIVE DATA TRANSFERS

In late October, the Department of Justice issued a new proposed rule that would implement regulations prohibiting the transfer of certain categories of bulk data about U.S. individuals to persons entities, or locations connected to "counties of concern", which include China, Cuba, Iran, North Korea, Russia, and Venezuela. The rule is made pursuant to Executive Order 14117 on "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern". The executive order called on the US Department of Justice and relevant federal agencies to build out requirements surrounding the transfer of specific categories of personal data to "countries of concern" and "covered persons" as defined in the rule.

DOJ-Proposed Rule

The proposed rule focuses on two categories of data:

1. **Sensitive Personal Data:** Defined to include human genomic data, biometric identifiers, precise geolocation data, personal health data, personal financial data, and-the broadest sub-category-covered personal identifiers.

    a. "Covered personal identifiers" is subsequently defined to include government identification numbers (e.g., Social Security numbers), financial account numbers or personal ID numbers associated with a financial service, device-based identifiers such as IMEIs, SIMs or MAC addresses, demographic or contact data, advertising identifiers, account credentials, network identifiers (e.g., IP addresses), and CPNI.

2. **U.S. Government-Related Data:** Defined as any data that either (1) is considered precise geolocation data for any of the DOJ's designated Government-Related Location Data List; or (2) any amount of sensitive personal data that is marketed as linked or linkable to current U.S. government current or former employees, contractors, or officers.

This new proposed rule and the Executive Order mark a clear understanding by the federal government that regulating personal data and transfers thereof are critical. They impose substantial new due diligence obligations on U.S. businesses, and U.S. companies that transmit, store, or process utilizing the services of third party vendors will need to maintain keen eyes on the rulemaking process as new final regulations may impose significant new obligations and penalties.

The proposed rule includes robust security measures related to sensitive data transfers but also goes on to (1) prohibit data transactions or transfers with respect to bulk sensitive personal data and U.S. government-related data where "countries of concern" or "covered persons" are involved; and (2) restrict any data transactions or transfers with respect to bulk sensitive personal data and U.S. government-related data unless certain requirements are met.

See more information in our recent alert detailing the proposed rule and its implications.

2025 What to Watch For: While the U.S. still lags behind other prominent jurisdictions-such as the European Union, United Kingdom, and China-in that the U.S. lacks a comprehensive federal level cross-border data transfer regulation, the U.S. has stepped up measures related to national security. This proposed rule is the latest update in furthering that trend.

BIOMETRIC INFORMATION

This past year saw major changes on the biometric information privacy front-and a sea change in comparison to past years.

Illinois' BIPA Amendments

Since the advent of Illinois' Biometric Information Privacy Act ("BIPA"), litigation regarding the collection and use of biometric information grew. Litigation and risk under BIPA subsequently increased in 2023 when the Illinois Supreme Court handed down its decision in the *White Castle* case that found claims accrue ***each time*** a business improperly collected an individual's biometric information. The ruling was seen as a boon for plaintiffs' attorneys, broadening the potential damages plaintiffs could claim.

The court acknowledged that such damages could be crippling to businesses, but that the existing language of the law presented little leeway for other interpretations. BIPA imposes liquidated damages of $1,000 per violation and $5,000 per "reckless or intentional" violations. Under the White Castle precedent, a business was potentially liable for damages every time a biometric information data point was collected or disclosed without consent.

Heeding the court's analysis, Illinois amended BIPA in 2024. The new amendments state that when a business collects or otherwise processes biometric information about "***the same person***" in more than one instance but "***using the same method of collection***", the business can only be liable for a single violation of BIPA. The amendments essentially equate to "per violation" meaning "per person," which has the potential to lower the number of damages plaintiffs seek under BIPA. Damage claims in BIPA cases had ballooned in recent years to hundreds of millions of dollars and even into the billions.

However, one important point of caution for businesses that leverage biometric information technology: the amendments make clear this narrowing of "per violation" only applies where the information was collected from the same person **using the same technology**. If, for example, the business collects the same biometric information about a consumer using two different technologies-for example, in the employee context through a timekeeping system **and** through on-premises facial recognition security cameras-the business would be liable for more than one violation.

The BIPA amendments also addressed what type of consent qualified as a "release" required prior to collecting or using biometric information under BIPA. Specifically, BIPA was amended to include electronic consent (e.g., check box consent and electronic signatures) within the definition of "Written Release". Courts previously left unaddressed whether the original text required wet signatures.

Colorado Biometric Data Amendments

In 2024, Colorado passed amendments to the Colorado Privacy Act in 2024 diving deeper into what businesses can and cannot do with biometric data-aligning the Colorado Privacy Act's biometric provision closer to BIPA. Importantly, the amendments did not create a private right to action, continuing to limit enforcement to the Colorado Attorney General's Office.

With these new amendments, Colorado also joined California-at least with respect to biometric data-as one of the only U.S. state data protection laws imposing at least some requirements on employee personal information.

With the new slate of biometric data amendments, the Colorado Privacy Act now applies to an employer's use of employee and independent contractor biometric data.

Like the landmark Illinois Biometric Information Privacy Act, the biometric data amendments to the Colorado Privacy Act require a business to transparently disclose to consumers how biometric data is collected, used and shared by the applicable business. Unlike the Illinois Biometric Information Privacy Act, there is no private right of action allowing consumers to sue businesses for violations of Colorado law.

The new biometric data requirements will apply to ***any*** business operating in Colorado and collecting any biometric data about Colorado consumers. The traditional Colorado law applicability thresholds do not apply.

See more coverage about the Colorado Privacy Act's consumer and employee biometric data requirements here.

2025 What to Watch For: The 2024 BIPA amendments will likely see litigation-and at the very least, claimed damages-decrease. But the Colorado Privacy Act amendments are a good reminder that activity with respect to legislating the collection and use of biometric data and identifiers remains a focus and is a critical topic that any business's privacy program should consider.

HEALTH DATA FOCUS

Over the course of 2024, a handful of states ushered in a new wave of health-focused data protection laws, with many focused on the repeal of *Roe v. Wade* and others focused on the advent of new technology.

My Health My Data Acts

Washington's and Nevada's "My Health My Data" acts focus on prior written consent for any processing of consumer health data and applies to any collection or processing of consumer health information in the respective states, or about such states' residents.

It is important to note that neither Washington's nor Nevada's new laws apply to entities governed by HIPAA. However, the type of data generally covered by these laws is broadly defined. "Health data" is generally defined under both laws to include personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present or future physical or mental health status. This could include, for example, (1) individual health conditions, treatment, diseases, or diagnosis; (2) social, psychological, behavioral, and medical interventions; (3) health-related surgeries or procedures; (4) use or purchase of prescribed medication; (5) bodily functions, vital signs, symptoms, or measurements of such information; (6) gender-affirming care information; and (7) reproductive or sexual health information.

Consumer health data can also include information derived from non-consumer health data, if such non-consumer health data is processed with any data falling into the above categories. Meaning,

any processing of consumer health data with non-consumer health data may pull in consent and other data protection requirements to data not otherwise falling into the above categories.

The biggest shift in practices will certainly stem from the new law's consent requirements. A business is only permitted to collect and process consumer health data in two circumstances:

1. Where it has obtained the consumer's prior consent; or
2. It is necessary to provide a product or service the consumer requests from the specific business.

The same circumstances apply when a business is permitted to share or disclose consumer health data to a third party-meaning a business either needs to obtain a separate consent for sharing the consumer health data, or the consumer needs to request such sharing as part of the provision of services.

Consent under these laws must be obtained via prior, express opt-in consent. Businesses cannot rely on implied consent, pre-checked boxes, or combined consent (e.g., consent for marketing activities combined with consent for collecting consumer health data under one check box option).

While the laws touch on similar concepts raised in broader, omnibus data protection laws-like individual privacy rights, they also usher in new requirements on tracking individuals. The laws make it unlawful for any business to use geofencing in or around any facility that provides in-person health care services. A "geofence" is defined to mean technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency identification, Wi-Fi data, or any other form of spatial or location detection to either (1) establish a virtual boundary around a specific physical location, or (2) to locate a consumer within a virtual boundary.

For purposes of this definition, "geofence" means a virtual boundary that is within a certain perimeter (2,000 feet or less for Colorado, 1,750 feet or less for Nevada).

Under these laws, it is unlawful for a business to use such geofencing technology to (1) identify or track consumers seeking health care services; (2) collect consumer health data; or (3) send notifications, messages, or ads to consumers related to or derived from their health data or use of health care services.

Colorado Neuro-Privacy Amendments

In spring of 2024, Colorado became the first state to issue laws and requirements directly related to the collection and use of biological and neural data.

The laws were actually an amendment to the Colorado Privacy Act. The amendments added to the definition of what constitutes "sensitive data" under the Colorado Privacy Act to include "Biological data". "Biological data" is then subsequently defined under the amendments to include: (1) is generated by technological processing, measurement, or analysis of (i) an individual's biological, genetic, biochemical, physiological, or neural properties, compositions, or (ii) an individual's body or bodily functions; and (2) which data is used or intended to be used by itself or in combination with other data, for identification purposes.

Biological data is then defined to expressly include another subset of data deemed "neural data", which is subsequently defined as any data that: (1) is generated by the measurement of the activity

of an individual's central or peripheral nervous systems; and (2) that can be processed by or with the assistance of a device.

2025 What to Watch For: U.S. state data protection laws are quickly expanding. As those laws become more and more commonplace-with businesses now more familiar with requirements such as robust privacy notices, privacy rights, security requirements-U.S. states are looking to specific subsets of new technologies and identifiable information that may warrant greater protection.

CHILDREN'S DATA PRIVACY PROTECTION

The Federal Trade Commission ("FTC") spent much of 2024 working on a proposed amendment to its Children's Online Privacy Protection Act rules ("COPAA Rule"), and also looked on as Congress kicked the tires on amending federal law more broadly.

FTC Rule Amendments

It appears that already, 2025 has been and will be active in legislation and new updates with respect to children's personal data privacy and security requirements.

In early 2025, the FTC finalized its COPPA Rule amendments. It is the first amendment and update to the COPPA Rule since its implementation back in 2013. One of the amendments includes a new, specific opt-in consent requirement for targeted advertising and disclosures of children's personal information to third parties. This consent would need to be obtained via separate, verifiable parental consent.

This would be an additional consent requirement on top of the existing COPPA requirement that parental consent be obtained for any collection and use of children's personal information.

The COPPA Rule amendments also impose new data retention requirements on how long a business can retain children's personal information. The data retention requirements align to the data minimization principle that personal information only be retained for so long as necessary to fulfill a specific purpose (with such purpose specifically identified at the time of collection.

2025 What to Watch For: The FTC's final COPPA Rule amendments come as U.S. states are also increasingly passing laws aimed to making social media less addictive, requiring parental consent for social media accounts for users under the age of 18, or banning accounts for certain age groups. Expect state legislatures, and even the U.S. Congress, to continue to be active in regulating minors' use of the Internet and social media.

Conclusion

The breakneck speed at which data protection laws are being passed, coming into effect, and changing can be difficult for businesses to keep track of as one business can often find itself navigating compliance with multiple, and substantively different, data protection legal regimes.

This new year will likely prove to continue the trend of an exponentially growing body of data protection law as use of and reliance on technology, data, and artificial intelligence grows. Make sure to check back throughout the year for specific updates on all data protection topics.

As data protection law updates continue to roll in throughout the new year and new data protection legal requirements take shape, the Benesch Data Protection team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Ryan T. Sulkin at rsulkin@beneschlaw.com or 312.624.6398.

Luke Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.