HINSHAW

Alerts

July 2025 Privacy Compliance Countdown: Key Deadlines for Five State Privacy Laws and DOJ's Bulk Sensitive Data Rule

July 8, 2025
Privacy, Cyber & AI Decoded

In this *Privacy, Cyber & AI Decoded* alert, we cover Colorado's Biometric Identifier Requirements, Delaware's Data Protection Assessment Requirement, Minnesota's new comprehensive privacy law going into effect, Tennessee's comprehensive data protection law going into effect, New York's Child Data Protection Law, and a reminder that the Department of Justice's (DOJ) Bulk Sensitive Data Law requirements will be enforced in July 2025.

Colorado's Biometric Identifiers Requirements

Effective Date: *July 1, 2025*

Colorado amended the Colorado Privacy Act to cover Biometric Identifiers.

A **"Biometric Identifier"** is defined as set forth in C.R.S. § 6-1-1303(2.4) and means data generated by the technological processing, measurement, or analysis of an individual's biological, physical, or behavioral characteristics, which data can be processed for the purpose of uniquely identifying an individual.

A Biometric Identifier includes:

- a fingerprint;
- a voiceprint;
- a scan or record of the eye retina or iris;
- a facial map, facial geometry, or facial template;
- or other unique biological, physical, or behavioral patterns or characteristics.

As of **July 1, 2025**, any business that collects or processes biometric identifiers or data of Colorado residents, including employers collecting biometric data from employees or job applicants, must:

- Provide a written policy that includes specific requirements for retention schedules, data incident response, and data deletion;
- Prohibit the collection and further disclosure of biometric identifiers unless the business does not fulfill the requisite requirements of transparency, including having a separate biometric identifier policy or including such

Attorneys

Sabrina Janeiro

Cathy Mulrow-Peattie

Jason J. Oliveri

Justyna H. Regan, Ph.D.

Service Areas

Privacy, Security & Artificial Intelligence

disclosures clearly within its existing privacy policy, obtaining the applicable consents as required under Colorado law, and developing applicable retention schedules;
- Implement security controls for controllers and processors of biometric identifiers or biometric data, including certain incident response plans; and
- Obtain consent from workers prior to collecting their biometric identifiers. In certain circumstances, employers can condition continued employment on consent in situations where employers most commonly collect biometric identifiers;

Companies that collect and disclose biometric identifiers should confirm that they have the appropriate written policies, consents, and disclosures in place.

Delaware Data Protection Assessment Requirement

Effective Date: *July 1, 2025*

Certain Delaware controllers subject to the Delaware Personal Data Privacy Act that controls or processes the data of no less than 100,000 Delaware consumers are required to regularly conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer. This includes any of the following activities:

(1) The processing of personal data for the purposes of targeted advertising.

(2) The sale of personal data.

(3) The processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of any of the following:

1. Unfair or deceptive treatment of, or unlawful disparate impact on, consumers.
2. Financial, physical, or reputational injury to consumers.
3. A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person.
4. Other substantial injury to consumers.

(4) The processing of sensitive data.

These requirements go into effect on **July 1, 2025**, and Delaware's Attorney General can require such assessments for production.

Minnesota

Effective Date: *July 31, 2025*

Minnesota's comprehensive privacy law goes into effect on **July 31, 2025**. View our prior alert for a comprehensive analysis and compliance considerations of this state privacy law.

Tennessee Information Protection Act

Effective Date: *July 1, 2025*

Businesses that meet the thresholds of the Tennessee Information Protection Act (TIPA) are required, among other obligations and similar to other comprehensive state privacy laws, to:

- Provide consumers with a reasonably accessible privacy notice;
- Limit the collection of consumer personal information to what is adequate, relevant, and reasonably necessary for the disclosed processing purpose;
- Establish, implement, and maintain reasonable administrative, technical, and physical data security practices;
- Obtain consent before processing sensitive data of a consumer or of a child; and
- Have written contracts in place with processors meeting the TIPA requirements.

An affirmative defense to a violation of TIPA is that the controller's written privacy policy conforms to NIST's privacy framework and provides a consumer with the substantive rights in TIPA.

Companies subject to TIPA should review their privacy compliance processes.

New York Child Data Protection Act (CDPA)

Effective Date: *June 20, 2025*

New York recently joined states such as California, Connecticut, Maryland, and Vermont, passing legislation around the protection of minor data (*i.e.*, data from a user under 18 years of age). However, the New York law stands out as it blends frameworks found under the federal Children's Online Privacy Protection Act (COPPA) and state comprehensive privacy laws to address minor data. Critical provisions of this law include the following:

- Operators are prohibited from collecting, using, or selling the personal data of users under 18 unless the covered user is 12 years of age or younger and processing is permitted under the Children's Online Privacy Protection (COPPA); the covered user is 13 years of age or older and processing is strictly necessary for certain specified activities; or informed consent has been obtained;
- The definition of "operator" is broad and includes "any person who operates or provides a website on the internet, online service, online application…and who…controls the purposes and means of processing personal data;"
- A covered user under NYCDPA is a user who is "actually known by the operator…to be a minor;"
- The law protects the personal data of anyone under the age of 18 or if an "age flag" signals that the user is a minor;
- Personalized ad targeting, behavioral profiling, or engagement-driven content feeds will require opt-in consent and are generally prohibited for users under 13 unless COPPA compliant;
- The law does not disrupt the framework in place for personally identifiable information covered by the New York Education Law, or the federal Family Educational Rights Privacy Act (FERPA), and their respective implementing regulations.

The law will be enforced by the New York Attorney General, and civil penalties are $5,000 per violation. Notably, there is no private right of action.

Interest groups such as Netchoice have routinely challenged laws like the NYCDPA on First Amendment grounds. Although Netchoice has been vocal with its criticisms of the law, it has not yet taken any legal action in New York. In response, supporters of the law point to the Supreme Court's decision in *Moody v. Netchoice*, which gives states the flexibility to pass laws like the NYCDPA as long as they do not regulate viewpoints or speech.

Bulk Sensitive Data Rules

Companies subject to the Department of Justice's Bulk Sensitive Data Rule must show good faith efforts to comply with the Rule by **July 8, 2025**.

This Rule prohibits and restricts the transfer of sensitive data to certain entities, vendors, persons, and employees in covered countries, including China, Russia, and Venezuela.

The DOJ will not "prioritize" civil enforcement actions against organizations that are engaging in "good faith efforts." **Some key good-faith efforts referenced by the DOJ include:**

- Conducting internal reviews of access to sensitive personal data, including whether transactions involving access to such data flows constitute data brokerage or fall with the Rules;
- Reviewing internal data flows to determine if they are potentially subject to Rules;
- Renegotiating and reviewing vendor agreements with vendors who handle bulk sensitive data;
- Adjusting employee work locations, roles, or responsibilities that are implicated by the Rules; and
- Implementing the Cybersecurity and Infrastructure Agency Security Requirements, including the combination of data-level requirements necessary to preclude covered person access to regulated data for restricted transactions.

For further information on the Bulk Sensitive Data Rule, read our June 4, 2025 edition of the *Privacy, Cyber & AI Decoded* publication.

Law clerk Elyssa Eisenberg contributed to this alert. She is not admitted to practice law.