HINSHAW

Hot Topics in Data Privacy: Staying Cool and Compliant This Summer

Mid-Year Check-In for Compliance Teams

Privacy, Cyber & AI Decoded Alert | 6 min read
Jun 12, 2026

By: Cathy Mulrow-Peattie, *Elyssa Eisenberg

This edition of Hinshaw's *Privacy, Cyber, and AI Decoded* highlights several newly enacted pieces of legislation in 2026 that businesses and our clients should include in their growing list of compliance planning, along with key enforcement information.

As we enjoy the start of summer, remember that maintaining privacy compliance—similar to gardening—requires planning and a strategic approach.

Key Privacy Law Effective Dates to Note

- **July 1, 2026:**
  - *Virginia's Precise Geolocation Data Amendment*
- **January 1, 2027:**
  - *Louisiana's Data Privacy Act*
  - *Oklahoma's Consumer Data Privacy Act*
- **May 1, 2027:**
  - *Alabama's Personal Data Protection Act*

Virginia Precise Geolocation Data Amendment (SB 338)

Default Effective Date: *July 1, 2026*

Virginia has become the third state—after Maryland and Oregon—to prohibit the sale of precise geolocation data. Under the amendment, a controller shall not "sell or offer for sale precise geolocation data concerning a consumer." The amendment does not include an effective date, so it will go into effect on July 1, 2026, by default.

Previously, the Virginia Consumer Data Protection Act (VCDPA) classified geolocation data similarly to any other sensitive data, meaning controllers could process and sell the data so long as they obtained consumers' informed, opt-in consent. However, SB 338 replaces this approach with an outright ban on the sale of precise geolocation data, covering data that identifies a person's specific location within a 1,750-foot radius.

It is important to note that Virginia's definition of the **"sale of personal data"** is narrower than Maryland's and Oregon's. While Maryland and Oregon extend the definition to exchanges for **"other valuable consideration,"** Virginia limits it to the exchange of personal data for monetary consideration only.

For companies that transfer geolocation data as part of advertising, human services, or other service-provider contracts, please note these ongoing restrictions on the use of geolocation data.

The VCDPA is enforced by the Attorney General, and there is no private right of action. There is a 30-day right to cure, after which fines begin at $7,500 per violation.

Oklahoma's Consumer Data Privacy Act

Effective Date: *January 1, 2027*

On March 20, 2026, Oklahoma's governor signed the state's comprehensive new privacy law. It is very similar to other state privacy laws, but, like Alabama, it is also more business-friendly.

Thresholds

The law applies to businesses that, during a calendar year, either:

- Controls or processes personal data of at least one hundred thousand (100,000) Oklahoma consumers, or
- Controls or processes personal data of at least twenty-five thousand (25,000) Oklahoma consumers and derives over fifty percent (50 percent) of gross revenue from the sale of personal data.

Key Provisions

The law takes a narrow approach to defining the **"sale of personal data,"** limiting a sale to apply only in the context of monetary consideration and does not include exchanges for "other valuable consideration" like other state privacy laws.

- Businesses ***are not required*** to honor Global Privacy Control (GPC) or other universal opt-out preferences (OOP).
- Businesses ***are required*** to develop data protection assessments for targeted advertising and profiling, any processing activity that presents heightened harms to consumers, the use of sensitive data, and the sale of data, and they are to be produced upon demand by the Attorney General.
- Specific contracts with required contractual terms ***are required*** with processors.

- Sensitive data may be processed by controllers with the consumer's informed and opt-in consent.

Exemptions

Oklahoma's privacy law includes several broad exemptions for businesses, including entity exemptions for organizations regulated by the Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), and nonprofits.

It also exempts employment and business-to-business data.

Enforcement

The law is enforced exclusively by the Attorney General, and there is no private right of action. There is a permanent right to cure, meaning before the Attorney General can take action, they must provide the business with written notice, and the business has 30 days to "cure" the violation. If the violation remains uncured for 30 days, the business can be fined up to $7,500 per violation.

Louisiana Data Privacy Act

Effective Date: *January 1, 2027*

- Enforcement begins on August 1, 2027

On May 29, 2026, Louisiana enacted the Louisiana Data Privacy Act (LDPA).

Key Implications

Unlike Oklahoma and Alabama, which use consumer-count thresholds, Louisiana borrows California's broader applicability framework, applying the LDPA based on revenue and data volume. This is significant to note because businesses that do not meet the consumer-count thresholds in other state privacy laws may still be subject to Louisiana's law based on revenue alone.

The LDPA applies to a person or entity that does business in the state that satisfies at least one of the following thresholds:

- Annual gross revenue exceeds $25 million, or
- Annually buying, receiving, selling, or sharing personal information of 75,000 or more Louisiana consumers, households, or devices, or
- Derives 50 percent or more of its annual revenues from selling Louisiana consumers' personal information.

Key Definitions

"Sale of personal data" means the exchange of personal data for monetary or other valuable consideration by the controller to a third party.

"Sensitive data" means a category of personal data that includes any of the following:

- Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexuality, citizenship, or immigration status;
- Genetic or biometric data that is processed for the purpose of uniquely identifying an individual;
- Personal data collected from a known child; and
- Precise geolocation data

There are specific disclosure requirements for consumers in the LDPA for the sale of sensitive data, even with opt-in consent.

Exemptions

- Financial institutions subject to the GLBA;
- Covered entities or business associates subject to HIPAA;
- Nonprofit organizations; and
- Employee data

Enforcement

The law is enforced exclusively by the Louisiana Attorney General as a violation of the Unfair Trade Practice and Consumer Protection Law. There is no private right of action and no specific civil penalty amount included.

The law includes a 30-day cure period that sunsets on July 31, 2027. Unlike Oklahoma's permanent right to cure, after July 31, 2027, the Attorney General may pursue enforcement action without prior notice.

Alabama's Personal Data Protection Act (APDPA)

Effective Date: *May 1, 2027*

Alabama enacted a comprehensive consumer data privacy law when Governor Kay Ivey signed **House Bill 351** in April 2026. The statute largely follows the Virginia/Connecticut privacy model but includes several business-friendly and structurally unique provisions, particularly its low compliance thresholds, a narrow definition of sale of personal data, and a 45-day cure period.

Thresholds

The APDPA applies to persons or entities that conduct business in Alabama or target products or services to Alabama residents and meet either of the following criteria:

- Control or process personal data of more than 25,000 Alabama consumers, excluding data processed solely to complete payment transactions; or
- Derive more than 25 percent of gross revenue from the sale of personal data, regardless of the number of consumers affected.

The APDPA adopts a notably narrow definition of "sale" of personal data. A "sale" includes:

- Exchange of personal data for monetary consideration, or
- Exchange for other valuable consideration only if:
  - *The controller receives a material benefit, and*
  - *The third party is not restricted in its subsequent use of the data.*

Express exclusions from "sale" include disclosures made for:

- Analytics services,
- Certain marketing services, and
- Processors acting under contractual restrictions.

The APDPA does not require data protection impact assessments but does require processing contracts with specific provisions for service providers.

Exemptions

Alabama's exemptions are among the broadest in the state-privacy landscape and include:

- Financial institutions governed by GLBA;
- HIPAA-covered entities and business associates;
- FERPA personal data; and
- Employment and business-to-business data.

Enforcement

There is exclusive enforcement by the Alabama Attorney General, with no private right of action and a 45-day cure period after notice of alleged noncompliance.

Texas' Meta AI Smart Glasses Investigation

On May 20, 2026, Texas Attorney General Ken Paxton issued a Civil Investigation Demand into Meta's AI Glasses to determine whether Meta has deceptively misrepresented the extent of its use of personal data from consumers in violation of Texas law.

Meta's glasses are equipped with cameras and speakers. Paxton's office has raised several privacy concerns:

1. First, although Meta's privacy policy acknowledges that the smart glasses have an "always enabled" mode, which continuously processes video data, the LED indicator is designed to alert bystanders when recording is not active while in this mode, and is easily hidden; bystanders can inadvertently be captured without their consent.
2. Second, Paxton alleges that the glasses collect biometric data without consent.

The outcome of this investigation could have significant implications for similar products on the market, as it may help define how products equipped with cameras, speakers, or other data collection tools are regulated under existing biometric privacy and consumer protection laws.

**Elyssa Eisenberg is a law clerk and is not admitted to practice law.*

Hinshaw & Culbertson LLP is a U.S.-based law firm with offices nationwide. The firm's national reputation spans the insurance industry, the financial services sector, professional services, and other highly regulated industries. Hinshaw provides holistic legal solutions—from litigation and dispute resolution, and business advisory and transactional services, to regulatory compliance—for clients of all sizes. Visit www.hinshawlaw.com for more information and follow @Hinshaw on LinkedIn and X.

Related People

Cathy Mulrow-Peattie

Partner

212-655-3875

Related Capabilities

Data Privacy, AI & Cybersecurity

Regulatory & Compliance

Website Data Privacy

Related Insights

AI Governance Expectations on the Rise for Insurers Amid New Regulatory Activity