

Memo on State Policy Barriers to AI Wearable Use: Louisiana

→ Kevin Frazier | Senior Fellow for AI Policy

SUMMARY

Louisiana legislators passed the [Louisiana Data Privacy Act \(LDPA\)](#), SB 386, in 2026. When the law goes into effect in 2027 it will significantly complicate the regulatory landscape for AI wearable companies. Imprecise coverage thresholds may impose the heaviest burdens on responsible companies while letting those least likely to maintain robust safety checks escape the LDPA's reach entirely. Additionally, the law imposes arbitrary barriers on data collection that may undermine the utility of AI wearables for Louisianans who stand to benefit from these innovations. The result is a regulatory climate that favors the adoption of less safe and less efficacious AI wearables.

Lawmakers interested in helping their constituents gain access to these transformative tools should consider various amendments.

BACKGROUND ON WEARABLES

AI wearables, like all computer systems, gather information, process it, and generate outputs. There's an increasing diversity of such tools but they can be loosely grouped into three categories:

- 1. Biometric wearables focus inward on the wearer's body.** Such devices include continuous glucose monitors, smart rings, and smartwatches. These devices gather information about the user's body to provide activity and exercise performance metrics, support predictive health insights, and facilitate chronic disease management.
- 2. Auditory wearables look outward rather than looking inward at the user's body.** Some AI wearable products—such as the now-discontinued Humane AI Pin—are worn on the body and use audio as an input, operating via voice commands without a traditional screen. Future consumer AI devices may take similar forms, including pins or necklaces. These are commonly labeled as auditory wearables.
- 3. Visual wearables observe the world around the user.** Smart glasses offered by companies such as Ray-Ban Meta and Envision are a prime example of this kind of wearable. These tools often feature one or more integrated cameras and a small screen visible only to the user.

Read more from the Abundance Institute on the state wearable policy landscape [here](#).

REFORMING THE LDPA

Background: The LDPA replicates privacy laws enacted in other states and includes some of the common faults with those laws.

Nearly half of US states have enacted a variant of a common template for comprehensive privacy law. This template, first enacted by California as the [California Consumer Privacy Act \(CCPA\)](#), was developed during an earlier technological era. The CCPA was enacted in 2018, primarily to address social media and internet concerns. Generative AI has since transformed the landscape.

How this type of privacy law clashes with AI wearables: The technological shifts that have transpired in the eight years since the CCPA was enacted have changed the costs and benefits of various data collection practices. Advances in AI, especially in generative AI, have resulted in tools, such as AI wearables, that drastically improve the quality of life for users.

Advances made possible by wearables, such as helping users see, operate more safely at work, and track bodily functions, depend on AI wearable companies being able to engage in a wide range of data processing activities. The development of AI wearables, as with other AI tools built on modern AI training tactics, requires vast troves of high-quality data.

Absent representative data, AI tools may not work as well for individuals of diverse backgrounds. This is because the underlying AI model will not have been trained on relevant information; this shortcoming is somewhat akin to asking a teenage driver who learned to drive in Southern California to navigate a snow storm in Montana. Data privacy laws that fail to account for this important, novel use of data risk replicating already documented instances of new technological advances benefiting certain communities more than others.

Vague and excessive data collection, usage, and storage limitations also invite unintended, negative consequences. Limits on those data activities can make AI wearables less useful. For example, prohibiting AI-equipped glasses from retaining personalization data could diminish the otherwise transformative impact of AI-equipped glasses for members of the visually impaired community.

POLICY RECOMMENDATIONS

1. Consider a exemption for AI wearable companies: The LDPA applies to entities doing business in Louisiana that satisfy one or more of the following criteria: (1) annual gross revenues of more than \$25 million; (2) engaging in at least one of many of personal information data processing activities for a commercial purpose of 75,000 or more consumers, households, or devices; or (3) deriving at least half of annual revenues from the sale of consumers' personal information.

This approach may drag small AI wearable companies into the regulation and expose them to regulatory expenses that are comparatively de minimis for larger firms. Lawmakers may want to consider an exemption that allows smaller firms to operate provisionally under a less burdensome set of requirements. More generally, it's critical that lawmakers realize that metrics based on ad-tech business practices may not align well with the hardware tech sector.

- 2. Provide guidance around the general data processing limitation:** AI wearable companies must limit the collection of personal information to what is "adequate, relevant, and reasonably necessary" under the LDPA. This well-intentioned limitation will likely chill data practices that may improve AI wearables both in general thanks to the collection of more representative and diverse data as well as in individual use cases by virtue of identifying more unique aspects of a user's preferences and needs.

Minimally, Louisiana regulators should provide more granular guidance as to how these limitations will apply in particular instances of data collection. State legislators may also want to consider safe harbor provisions as well as a permanent cure period that ensures companies that attempt to comply with the spirit of this prohibition are not excessively punished. This recommendation is explored further below.

- 3. Update consent requirements:** The LDPA mandates that an AI wearable company receive the consent of the user prior to collecting sensitive information. Again, this is a well-intentioned effort to safeguard user autonomy. However, the law's mandates stretch too far in the context of AI wearables.

Sensitive information is defined as "personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexuality, or citizenship or immigration status," as well as "genetic or biometric data that is processed for the purpose of uniquely identifying an individual." The Act specifies that user consent is provided when the user takes a "clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement" to the relevant data processing activity. The LDPA explicitly forecloses "[a]cceptance in a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information."

Some of the most important uses of AI wearables involve exposure to and potential processing of sensitive information. Compliance with the LDPA's consent requirements may therefore involve repeatedly and serially prompting users to consent to data processing activities.

These pervasive reminders may cause users to become numb to what is intended to be a thoughtful and intentional process. Other users may forgo use of AI wearables to avoid the constant consent prompts. In either instance, the net result is not the outcome aspired to by state legislators.

This likely shortcoming justifies amendment to the LDPA. Louisiana is home to [well more than 150,000 visually impaired](#) individuals and others who stand to benefit significantly from AI wearables. Consent requirements designed for prior generations of technologies should not block their ability to make deliberate and intended use of AI wearables.

- 4. Clarify the extent of the right to delete information:** LDPA authorizes users to request that a company delete their personal information. Companies must respond to such requests in a timely fashion (45 calendar days). Whether and to what extent the right applies to personal data relied on to train an AI model and, therefore, embedded within a model's weights is an open question.

From a technical standpoint, personal data is not stored as a standalone, accessible data unit within a model. User or regulator demands that personal data be "deleted" from trained AI models are thus technically difficult (if not impossible) and do not improve user privacy.

Regulators should rapidly confirm that data deletion rights do not require the modification, retraining, or deletion of AI models trained on user data.

- 5. Provide for a permanent cure period:** The Attorney General treats violations of the LDPA as unfair and deceptive trade practices. There is no private right of action. There is a thirty-day right to cure that sunsets on July 31, 2027.

The legislature should seriously weigh making permanent the thirty-day cure period, especially with respect to novel technologies that do not fit neatly within the technological assumptions held by the authors of the LDPA.

UPSHOT

Louisiana set out to advance the well-being of its residents but instead built a privacy regime that may leave Louisiana residents unable to enjoy the full benefits of AI wearables. The LDPA borrows a template drafted before generative AI existed, and that mismatch now shapes outcomes the legislature never intended. Its ad-tech-based thresholds do not map neatly onto hardware companies, while its data minimization and consent rules fall hardest on the larger labs best positioned to build safe, powerful, representative tools. The visually impaired Louisianans who stand to gain the most from AI glasses (among many other communities) are precisely the users a consent-prompt treadmill will frustrate or drive away.

Regulators can and should address these flaws. Clear guidance on the minimization standard, an explicit answer that the right to deletion does not compel model retraining, and a permanent cure period for novel technologies would align the law with the benefits it claims to protect.

In short: a privacy law worth enacting should make safe and effective wearables easier to adopt, not harder.

**GET IN
TOUCH**

🌐 abundance.institute
✉️ [@abundanceinst](https://abundanceinst.org)
📄 [@abundanceinstitute](https://abundanceinstitute.org)

Kevin Frazier
Senior Fellow for AI Policy
kevin@abundance.institute

Bryce Chinault
Director of State Government Affairs
bryce@abundance.institute