ABUNDANCE INSTITUTE

Beyond the Screen: Wearable AI and State Policy

→ Taylor Barkley and Bryce Chinault

INTRODUCTION

The introduction of the iPhone in 2007 ushered in the era of mobile computing. Activities once confined to desks or laptops suddenly became possible anywhere with reliable cellular connectivity. Today, continued advances in hardware efficiency and artificial intelligence are driving another transition: from the hand-held computer to the wearable computer.

This transition goes beyond smart watches and smart glasses. It includes a diverse ecosystem of new computing form factors that can help us better understand ourselves and the world around us. It is finally possible to foresee a world where the rectangular glass pocket computer could be augmented or even replaced by continually present devices that we wear on our face, wrist, or as part of our clothing. Advanced AI models make this innovation possible.

To ensure Americans realize the full benefits of wearables, state policymakers should be cautious not to lock in premature or overbroad regulatory frameworks crafted around previous technologies or speculative harms. Legacy policy approaches intended to govern online data collection are often ill-suited to the continuous, passive, context aware functions of wearable technology. Early policy approaches that target wearables treat them either as generalized "surveillance devices" because they include sensors or cameras, or as "consumer toys" that obscure their significant economic, healthcare, and accessibility value. Neither approach will succeed; both risk sidelining tools that could reduce costs across Medicare and Medicaid, expand workforce participation, improve productivity, and dramatically improve independence for people with disabilities.

The goal of this brief is to outline the wearable AI landscape and provide a use-based, pro-innovation state policy framework. It offers an overview of current and near-term wearable technologies, highlights emerging regulatory risks, and identifies principles that can protect consumers while preserving an environment of abundance and innovation.

WHAT ARE WEARABLES?

Wearable computers, like all computer systems, gather information, process it, and generate outputs. But wearables differ from past computer systems in each of these phases. First, wearables differ in the type and frequency of inputs gathered. Because they have much smaller or even no screens, their outputs are also different.

Below we group wearables into three categories based primarily on the kind of inputs and outputs. But first it is worth talking about the third basic component of computing, processing, briefly. The past few years of AI breakthroughs have unlocked the processing power of wearables, completely transforming what is possible. First, wearables previously struggled with how to adequately interact with users absent a large touchscreen or keyboard and monitor. But LLMs make natural, spoken language interfaces workable. Second, AI has simplified the useful analysis of continuous flows of unstructured data that are common with wearables.

This processing can take place on the wearable device itself, but often the most intensive processing requires accessing cloud services. Thus, many wearables require internet connectivity, either directly or through another device such as a home router or smartphone.

BIOMETRIC WEARABLES

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.

Importantly, most biometric wearables are low-risk general wellness or assistive tools, not Food and Drug Administration (FDA)-regulated medical devices. State policy should avoid sweeping these products into healthcare or medical AI frameworks intended to address higher-risk activities such as diagnosis or treatment. Federal and state oversight remains appropriate where wearable AI performs diagnosis, treatment, or clinical decision-making, but extending medical-device-style regulation to general wellness or assistive wearables risks deterring useful innovation.

As wearable AI evolves, some devices are beginning to measure neural or neuromuscular signals to support accessibility, safety, and assistive functions. A small number of states and advocacy efforts are beginning to explore privacy protections for so-called "neural data." Given the nascent nature of this technology, any risks from collecting such data remain largely hypothetical. Furthermore, there are many different categories of neural data. State policymakers should be cautious not to treat all such signals as inherently sensitive or risky.

AUDITORY WEARABLES

Rather than looking inward at the user's body, many wearable computers look outward. Some wearable AI 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. Many auditory wearables not only collect sound information, but also communicate with the user through sound. These types of wearables include AI-enabled hearing aids, real-time translation earbuds, and audio-enabled glasses. These tools break language barriers, augment hearing, and enable seamless communication with others. Sensors and microphones may be embedded in earbuds, over-ear devices, or eyewear that lacks any visual display.

Wearables that interact with the user through sound can support a wide range of functions, including navigation, scheduling, communication, and entertainment.

VISUAL WEARABLES

Visual wearables observe the world around the user. These include smart glasses by companies such as Meta/Ray-Ban, Vuzix, and Envision. These include one or more integrated cameras, and newer products are also including small screens visible only to the user.

For example, Meta's Ray-Ban glasses have featured cameras and audio form factor, but newer models have a small display in one lens. The Meta Ray-Bans have been a consumer hit, selling over 20 million units and with sales described as "exponential."[1] Google is reportedly developing

1 Lo Nostro, Gianluca, and Elisa Anzolin. "*Ray-Ban maker shares hits all-time high as investors bet on Meta AI glasses boom.*" *Reuters*, 17 October 2025. https://www.reuters.com/business/shares-ray-ban-maker-essilorluxottica-soar-after-meta-ai-glasses-drive-revenue-2025-10-17/.

a similar augmented reality glasses product for release in 2026. Other similar technologies are focused on accessibility uses. Envision Glasses, for example, use an integrated camera and artificial intelligence to interpret the visual world. They read text aloud, identifying objects and people and describing scenes to help people who are blind or have low vision.[2] Innovative uses of visual wearables continue to emerge. In 2024, the New York Academy and Sciences' Innovation Challenge awarded a prize to students for their VisionXcelerate smart glasses, which help dementia patients perform every-day tasks independently.[3]

State-Level Policy Barriers

While wearable AI technology is advancing rapidly, state regulatory frameworks often remain calibrated to more traditional types of computing. Existing privacy, biometric, and AI safety frameworks were designed to address social media platforms, data brokers, or government surveillance—not personal, user-controlled wearable devices. This mismatch creates uncertainty, and the patchwork creates high compliance costs.

BARRIERS TO BIOMETRIC WEARABLES

Wearables currently face a regulatory scope creep that treats simple wellness nudges like high-stakes medical decisions. Emerging laws, such as the Colorado AI Act, require expensive risk assessments for AI for "consequential decisions," a term defined to include healthcare services. In practice, this can trigger extensive documentation, governance, and risk-management requirements even for basic wellness features. For example, if a smart ring analyzes sleep data and suggests a user "take a walk to reduce stress," regulators could classify this as a healthcare decision. Proving such a simple wellness algorithm is bias-free via formal assessment will impose compliance costs, which could be prohibitive for small firms and raise the cost of products from larger firms. This financial burden could likely force innovators to "dumb down" devices, removing proactive AI coaching to avoid liability and leaving users with mere data logs instead of life-improving guidance.

Similarly, statutes such as Washington's My Health My Data Act define "health data" broadly enough to capture non-clinical metrics such as step counts or location-based activity logs. The resulting compliance often requires distinct, aggressive "opt-in" consents that differ from federal standards. This added friction frequently causes users to opt-out of "passive monitoring" features out of fear or annoyance, effectively neutralizing the device's ability to detect falls or heart arrhythmias in the background.[4]

2 Will Wei, "*Envision glasses use ChatGPT and Google Glass to help blind and low vision*," *Business Insider*, December 15, 2023, https://www.businessinsider.com/envision-glasses-chatgpt-google-glass-help-blind-visually-impaired-2023-12.

3 Nicole Pope, "Assisting Dementia Patients with AI and AR," *The New York Academy of Sciences* (blog), August 14, 2024, https://www.nyas.org/ideas-insights/blog/using-artificial-intelligence-and-augmented-reality-to-assist-dementia-patients/.

4 Rea S. Hederman Jr. and Logan Kolas, *A Healthcare World Reimagined: How Big Government Threatens Healthcare AI and What to Do About It* (Columbus, OH: The Buckeye Institute, April 1, 2024), https://www.buckeyeinstitute.org/library/docLib/2024-04-01-A-Healthcare-World-Reimagined-How-Big-Government-Threatens-Healthcare-AI-and-What-to-Do-About-It-policy-report.pdf.

BARRIERS TO AUDITORY WEARABLES

States have adopted AI transparency mandates to prevent deception in automated interactions. Wearables with auditory interfaces designed to facilitate natural conversation could get tangled in transparency mandates originally written for text-based chatbots.Continuous verbal disclosures (“I am an AI”) interrupt real-time translation, hearing assistance, and cognitive support. While disclosure requirements can be appropriate to prevent fraud or deception, continuous verbal disclosures for real-time translation and assistive audio tools don’t help users and harm the functionality of such systems. Transparency should be contextual—not constant.

BARRIERS TO VISUAL WEARABLES

Assistive reality tools that "see" for the blind are currently being blocked by privacy laws intended to stop police surveillance.

State biometric privacy laws—most notably Illinois’ Biometric Information Privacy Act (BIPA) and Texas’ Capture or Use of Biometric Identifier Act (CUBI)—were designed to curb mass surveillance and commercial exploitation.

When applied to user-directed wearable devices, these laws create strict-liability exposure even when no data is retained, shared, or misused.

The result is a de facto ban on accessibility features in strict-liability states as users cannot possibly obtain written consent from every stranger passing by on the street.

Clearing the Path: Targeted State Law Fixes

DISTINGUISH CONSUMER USE FROM DATA COLLECTION AND GOVERNMENT SURVEILLANCE

→ **The Barrier**: One-size-fits-all regulatory approaches subject user-directed assistive tools to the same restrictions and requirements as tracking or surveillance systems.

→ **The Fix**: State policy should avoid hindering consumer-directed features that process data solely on behalf of the individual user, for the user’s benefit, without profiling or sharing with third-parties for separate purposes.

CREATE SAFE HARBORS FOR ON-DEVICE AND EPHEMERAL PROCESSING

→ **The Barrier**: Laws often fail to distinguish between cloud-based aggregation and local or transient processing.

→ **The Fix**: Clarify regulated collection does not include 1) processing biometric or sensory data locally; 2) data retained only for a short technical interval in order to provide the user with their requested service.

REPLACE STRICT LIABILITY WITH ACTUAL HARM STANDARDS

→ **The Barrier**: Strict liability and private rights of action chill innovation even without injury.

→ **The Fix**: State law should avoid codifying strict-liability regimes for incidental biometric processing and should focus enforcement on demonstrable harm or misuse.

LIMIT COMPELLED SPEECH TO HIGH-RISK CONTEXTS

→ **The Barrier**: Blanket disclosure mandates disrupt real-time assistive and translation tools.

→ **The Fix**: Rely on existing deception and consumer protection authority, requiring disclosures only where necessary to prevent fraud or material deception.

STRENGTHEN CIVIL LIBERTY PROTECTIONS

→ **The Barrier**: Current Fourth Amendment precedent (and the third-party doctrine) means that almost any information that has become legible to a service used by a user is legally available to state law enforcement without a warrant. Wearables will greatly expand that scope of information, shifting the practical balance toward government surveillance.

→ **The Fix**: State legislation to restore the full effect of the Fourth Amendment protections to individuals while ensuring lawful access to information in appropriate circumstances.

What States Should Do in the 2025–26 Legislative Cycle

State policymakers should:

1. Audit existing biometric and AI statutes for unintended impacts on wearables
2. Add explicit consumer-wearable carve-outs where appropriate
3. Align AI transparency rules with context and risk
4. Engage disability and accessibility communities early in policymaking

Conclusion: Choosing Abundance in the Ambient Era

Wearable AI is moving computing off the screen and into the real world: augmenting human capability, restoring independence, and reducing costs across healthcare, workforce participation, and public services. For many Americans, these tools will not be mere conveniences but essential assistants.

As state policymakers debate the future of AI governance, decisions made now will determine whether wearable AI is governed by flexible, use-based standards or constrained by fragmented and precautionary rules that are difficult to unwind.

Policymakers face a consequential choice. By providing clarity, resisting precautionary overreach, and focusing on actual harms rather than speculative risks, the state governments can ensure wearable AI becomes a force for empowerment rather than a casualty of regulatory lack of vision. A use-based, innovation-friendly federal approach will position the United States to lead the next chapter of computing: expanding accessibility, lowering public costs, and preserving individual agency in the era of wearable AI.

GET IN TOUCH

abundance.institute
@abundanceinst
@abundanceinstitute

Taylor Barkley
Director of Federal Government Affairs
taylor@abundance.institute

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