



Hi ,

This week, The Information reported that Amazon is building consumer augmented reality glasses that aim to rival Meta's — putting smart glasses back in the headlines. Amazon's device could be released as early as next year, according to the report, prompting a world where even more people have microphones, speakers, cameras and a display sitting right on their nose.

Amazon is Developing AR Glasses in Challenge to Meta



Canada helped focus this technology (remember North?). Now, smart wearable tech has moved beyond watches and rings that tracked *us* to glasses that track *everyone else*. Once mocked as niche gadgets for “glass-holes,” smart glasses are now widely available for purchase: Meta's Ray-Ban glasses alone have sold more than two million units. Equipped with hidden HD cameras and AI integration, they can record and analyze the world in real time, often without bystanders knowing.


There are other competitors, too: Even Realities recently launched AI-powered glasses, and Oakley entered the space with its own smart eyewear — signaling this trend is expanding across both tech and lifestyle brands.


These smart spectacles raise urgent questions. Who owns the data they collect? Where is it stored? And why are we tacitly permitting continuous recording of people in both public and private settings with almost no oversight?

Two privacy concerns stand out: The opportunity for companies like Amazon and Meta to collect *even more* information from users, and the potential for abuse through the recording of others. Unlike with smartphones, smart glasses users can record their fellow man without making an obvious action, like holding their phone up. They only need to press a small button or give a voice command. They can quietly film in classrooms, bathrooms or changerooms, or scoop up footage from public spaces for facial recognition or social media monetization.

The capture of personal data by most big tech companies has so far been limited to digital spaces. The quick development and release of software programs and mobile apps has made it hard for governments to keep pace with innovation. But smart glasses are different: they are hardware. And they augment reality with online platforms, like Meta's, that already dominate global data collection.

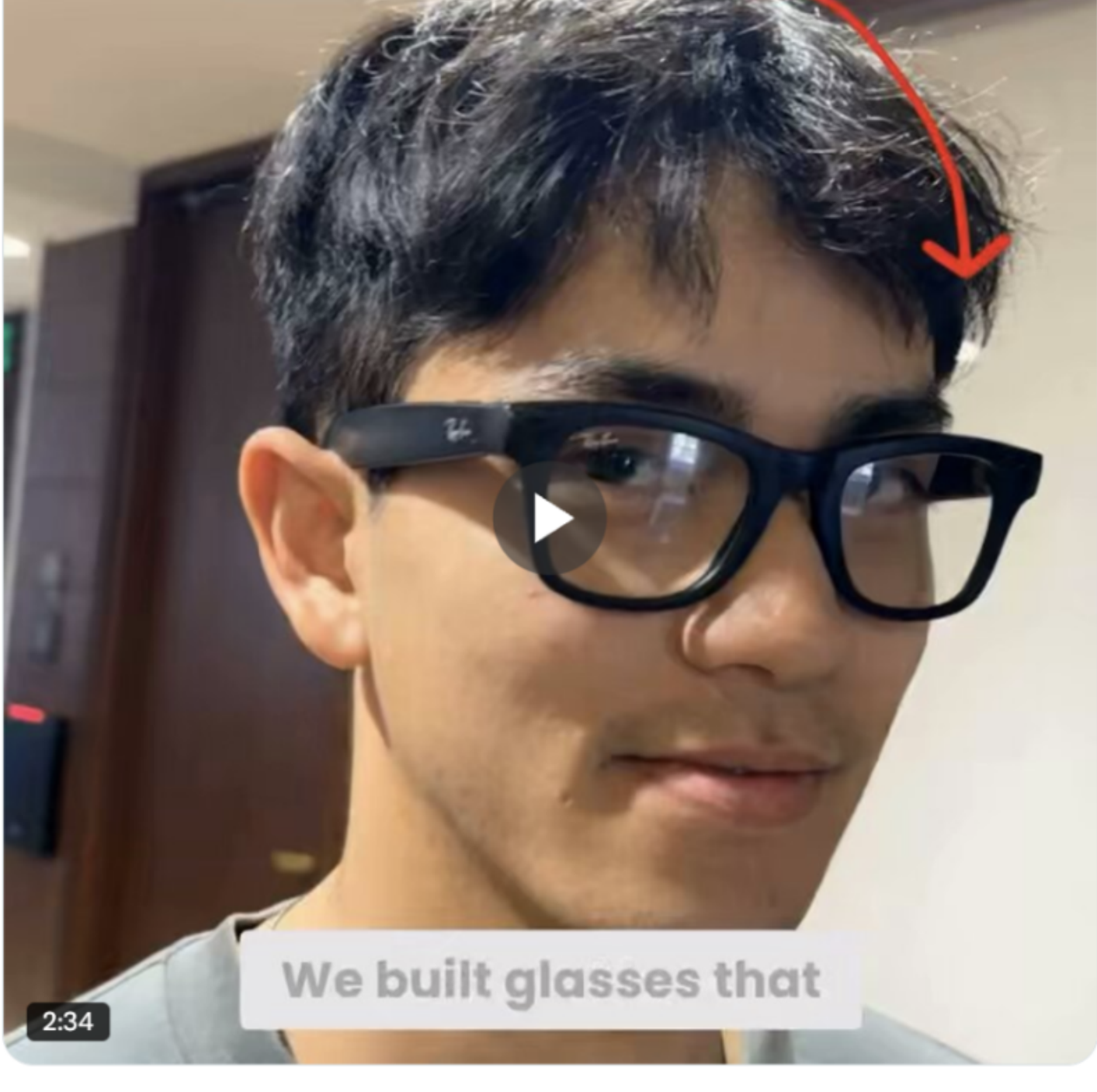
Facial recognition technology (FRT) is the next frontier, moving surveillance capitalism from screens to sidewalks. Last year, an experiment by Harvard University students revealed FRT could be integrated into Meta's Ray-Bans. The result was alarming.



AnhPhu Nguyen 
@AnhPhuNguyen1

Are we ready for a world where our data is exposed at a glance?
[@CaineArdayfio](#) and I offer an answer to protect yourself here:


tinyurl.com/meet-ixray





2:34


We built glasses that


Last edited 12:10 PM · Sep 30, 2024 · 1.2M Views

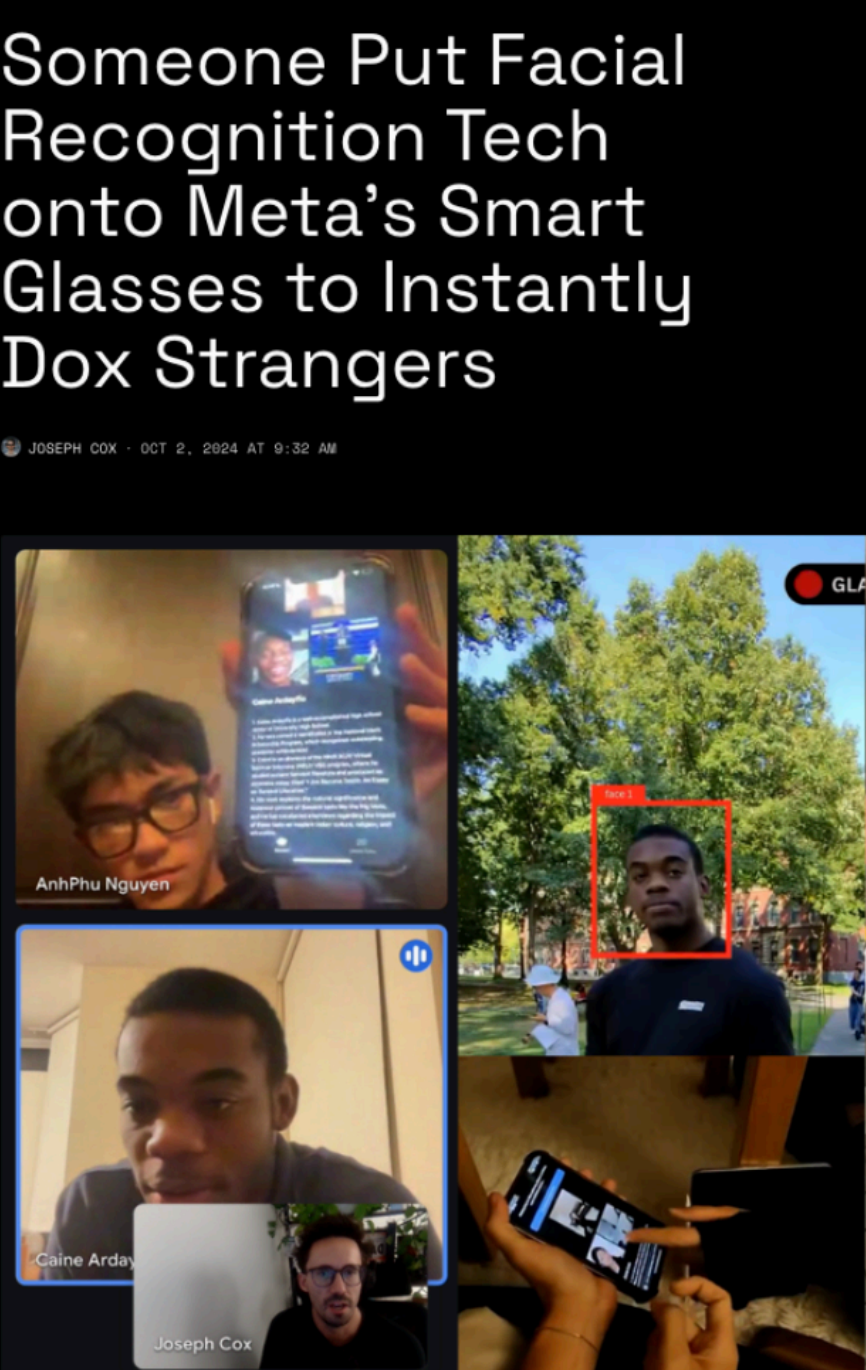
 394

 2.7K

 5.4K

 4.2K





Someone Put Facial Recognition Tech onto Meta's Smart Glasses to Instantly Dox Strangers

The technology, which marries Meta's smart Ray Ban glasses with the facial recognition service Pimeyes and some other tools, lets someone automatically go from face, to name, to phone number, and home address.

try it on a REAL person in the subway

her results on my phone

try it on a REAL person in the subway

her results on my phone

We're not ready for this, but we need to be. Canada's privacy laws were designed for visible cameras and discrete data collection, not ambient, always-on surveillance.

While federal privacy law regulates the collection and use of personal data by a vendor, it does not regulate the collection of personal data by another individual for non-commercial purposes — meaning it's the wild west for video captured by smart glasses.

The Criminal Code only captures narrow and extreme cases of privacy invasion (like voyeurism or sexual exploitation), and privacy torts such as “intrusion upon seclusion” are limited and costly to enforce. Civil claims are reactive, not preventative. Meanwhile, Ottawa has (so far) failed to modernize federal privacy law, leaving a patchwork of protections that simply don't address the realities of wearable AI devices.

Influencers are already using smart glasses to capture unsuspecting strangers in public, turning their likeness into monetized content without permission. In this new environment, consent is rendered meaningless — those filmed rarely even realize they are being recorded, let alone agree to have their image broadcast to thousands online. Our current legal and ethical frameworks, built for an era of visible cameras and explicit data collection, are outdated and ill-equipped to confront the covert, everyday surveillance these technologies normalize.



Sunday Project

SNEAKY SURVEILLANCE

In Australia, an American TikTok influencer is being investigated for filming beachgoers using smart glasses without their consent.

If privacy laws are not strong enough to protect Canadians, what about consumer protection laws? Smart glasses are, simply put, physical consumer products that present significant privacy concerns. Product liability frameworks tend to focus on the harm to the individual consumer and are mostly concerned with health risks. Smart glasses force us to ask how a product can cause privacy harm to *others*.

There's also a sovereignty dimension. Footage collected by these devices can be stored abroad and accessed under U.S. laws like the CLOUD Act, feeding foreign databases and FRT systems. What looks like a subtle, futuristic fashion accessory is in fact an unregulated global data pipeline.

In a trade war context where the U.S. is explicitly seeking AI dominance, do we really want to volunteer more data for American companies' artificial intelligence models? What do these devices mean for national security?

By blurring the line between convenience and coercion, fashion and surveillance, consumer choice and state security, **smart glasses represent a regulatory blind spot in Canada.**

Only responsive public policy can shield Canadians from unwanted recording and identification. Some fixes are obvious: exploring bans in sensitive settings (like schools, or a dance venue just issued one), mandatory recording disclosures (through lights or sounds), or point-of-sale regulations that treat smart glasses less like quirky fashion items and more like medical or safety devices.

Sovereignty is more than a vibe or a slogan. It's the hallmark of an ambitious state that updates its rules to match the world we actually live in. If new consumer devices can ambly capture bystanders, infer identities, and ship that data to foreign clouds governed by foreign law, then we're not “adopting innovation,” we're outsourcing control.

A nimble and responsive government would set terms quickly: establishing that recording must be visible to others, data collection must be minimized and governed locally, and liability must extend beyond the buyer to the manufacturer. If those conditions can't be met, we need to ask whether these kinds of glasses should be for sale at all.

Do we really want hardware designed to surveil and subordinate Canadians flowing unchecked into our market? We believe determining this is in the national interest.

What do you think: should Canada regulate these at the point of sale, or let the market dictate adoption?

Let us know. Thanks for reading,

Vass

(I'm the Managing Director, and you can just reply to this newsletter to get in touch with me)

Below is “Put a Little Light on the Wretch That Is Me” from Vancouver-based Frog Eyes. Send us the Canadian music you've been listening to lately!



F R O G E Y E S

THE OPEN UP



SEND TO A FRIEND

