

---

## Privacy will die to deliver us the thinking and knowing computer

### Description

We're getting a first proper look at much-hyped [Humane's "AI pin" \(whatever that is\) on November 9](#), and personalized AI memory startup [Rewind](#) is launching a pendant to track not only your digital but also your physical life sometime in the foreseeable future. Buzz abounds about OpenAI's Sam Altman meeting with Apple's longtime design deity Jony Ive regarding building an AI hardware gadget of some kind and murmurs in the halls of VC offices everywhere herald in breathless tones the coming of an iPhone moment for AI.

Of course, the potential is immense: A device that takes and extends to many other aspects of our lives what ChatGPT has been able to do with generative AI — hopefully with a bit more smarts and practicality. But the cost is considerable; not the financial cost, which is just more wealth transfer from the coal reserves of rich family offices and high-net-worth individuals to the insatiable fires of startup burn rates. No, I'm talking about the price we pay in privacy.

The death of privacy has been called, called-off, countered and repeated many times over the years (just Google the phrase) in response to any number of technological advances, including things like mobile device live location sharing; the advent and eventual ubiquity of social networks and their resulting social graphs; satellite mapping and high-resolution imagery; massive credential and personal identifiable information (PII) leaks and much, much more.

Generative AI — the kind popularized by OpenAI and ChatGPT, and the kind that most people are referring to when they anticipate a coming wave of AI gadgetry — is another mortal enemy of what we think of as privacy, and it's one of its most voracious and indiscriminate killers yet.

At our recent TechCrunch Disrupt event in San Francisco, Signal President Meredith Whittaker — one of the only major figures in tech who seems willing and eager to engage with the specific realistic threats of AI, rather than pointing to eventual doomsday scenarios to keep peoples' eyes off the prize — said that [AI is at heart "a surveillance technology"](#) that "requires the surveillance business model" in terms of its capacity and need to Hoover up all our data. It's also surveillant in use, too, in terms of image recognition, sentiment analysis and countless other similar applications.

All of these trade-offs are for a reasonable facsimile of a thinking and knowing computer, but not one that can actually think and know. The definitions of those things will obviously vary, but most experts agree that the LLMs we have today, while definitely advanced and clearly able to convincingly mimic human behavior in certain limited circumstances, are not actually replicating human knowledge or thought.

---

But even to achieve this level of performance, the models upon which things like ChatGPT are based have required the input of vast quantities of data — data collected arguably with the “consent” of those who provided it in that they posted it freely to the internet without a firm understanding of what that would mean for collection and re-use, let alone in a domain that probably didn’t really exist when they posted it to begin with.

That’s taking into account digital information, which is in itself a very expansive collection of data that probably reveals much more than any of us individually would be comfortable with. But it doesn’t even include the kind of physical world information that is poised to be gathered by devices like Humane’s AI pin, the Rewind pendant and others, including the [Ray-Ban Meta Smartglasses](#) that the Facebook-owner released earlier this month, which are set to add features next year that provide information on-demand about real-world objects and places captured through their built-in cameras.

Some of those working in this emerging category have anticipated concerns around privacy and provided what protections they can — Humane notes that its device will always indicate when it’s capturing via a yellow LED; Meta revamped the notification light on the Ray-Ban Smart glasses versus the first iteration to physically disable recording if they detect tampering or obfuscation of the LED; Rewind says its taking a privacy-first approach to all data use in hopes that’ll become the standard for the industry.

It’s unlikely that will become the standard for the industry. The standard, historically, has been whatever the minimum is that the market and regulators will bear — and both have tended to accept more incursions over time, whether tacitly or at least via absence of objection to changing terms, conditions and privacy policies.

A leap from what we have now, to a true thinking and knowing computer that can act as a virtual companion with at least as full a picture of our lives as we have ourselves, will require a forfeiture of as much data as we can ever hope to collect or possess — insofar as that’s something any of us can possess. And if we achieve our goals, the fact of whether this data ever leaves our local devices (and the virtual intelligences that dwell therein) or not actually becomes somewhat moot, since our information will then be shared with another — even if the other in this case happens not have a flesh and blood form.

It’s very possible that by that point, the concept of “privacy” as we understand it today will be an outmoded or insufficient one in terms of the world in which we find ourselves, and maybe we’ll have something to replace it that preserves its spirit in light of this new paradigm. Either way, I think the path to AI’s iPhone moment necessarily requires the “death” of privacy as we know it, which puts companies that ensconce and valorize privacy as a key differentiator — like Apple — in an odd position over the next decade or so.

**Date**

03/02/2025

**Date Created**

31/10/2023

**Author**

susantwain1