# Meta reignites facial recognition in smart glasses amid rising privacy fears



In 2021, Facebook announced a significant shift in its strategy regarding facial recognition technology, deciding to halt efforts to integrate such systems into its emerging smart glasses due to pervasive concerns about privacy and ethics. Fast forward four years, and Meta, the parent company of Facebook, has reignited development on this controversial feature, particularly focusing on a function known as "super sensing." According to reports from The Information, this feature could enable the glasses to continuously record the user's environment, triggering various reminders based on their day-to-day activities, all while potentially infringing on the privacy of those around them.

The technology behind super sensing entails a combination of AI and facial recognition capabilities. This raises troubling possibilities: for instance, users might identify acquaintances at social events or monitor family members, arguably harmless applications that could swiftly devolve into serious privacy invasions. A wearer could inadvertently or intentionally use these tools to compromise the anonymity of unsuspecting individuals in public spaces. Scenarios abound where misuse could lead to public doxxing, unwarranted surveillance, or even harassment, particularly in sensitive situations like protests or crowded venues.

Meta's renewed focus on facial recognition technology aligns with a broader shift in the political landscape regarding surveillance and privacy. Rob Leathern, a privacy expert and former product manager at leading tech companies including Facebook and Google, notes that societal attitudes toward privacy appear to be fluctuating, with certain corporate practices facing diminished scrutiny compared to just a few years ago. The technology industry, as it stands, seems set on redefining the parameters of acceptable data usage amidst shifting public perception.

Compounding these concerns is the troubling experience already witnessed in various cases involving Meta’s current smart glasses. In a chilling instance reported by the FBI, smart glasses were used by a suspect to scout locations ahead of a planned attack in New Orleans, illustrating the potential for the technology to be weaponised in harmful ways. With built-in cameras and microphones, the glasses can record not only the user’s perspective but also the experiences of those around them, raising questions about consent and ethical use.

Moreover, Meta's existing AI-powered smart glasses have already faced significant backlash for their handling of user data. When photos or videos are captured, they are processed in the cloud, presenting substantial risks regarding privacy infringement. Concerns grow when considering Meta's history with data misuse, particularly in light of a recent $1.4 billion settlement with the state of Texas regarding the unlawful harvesting of biometric data without informed consent. Such legal precedents highlight both the regulatory landscape that tech companies must navigate and the inherent risks tied to biometric surveillance technologies.

The situation becomes even more dire when one considers the evolution of similar technologies. Recent demonstrations of an application named I-XRAY illustrate just how sophisticated—and potentially dangerous—these systems can become. Utilising real-time video feeds from smart glasses to identify individuals and aggregate personal data from the internet, I-XRAY exemplifies a concerning trajectory in which personal privacy can be breached in an instant. This capability poses serious implications for identity theft and social engineering, allowing individuals with malicious intent to exploit this technology to manipulate or harm others.

As Meta reinvigorates its ambitions within the wearable tech space, the intersection of AI and facial recognition stands at a critical juncture. While advancements may provide exciting new functionalities for users, they also beg a fundamental question: at what cost to privacy and personal security? Without stringent safeguards, the proliferation of such technologies could lead society into uncharted—and unsettling—territory, where the line between convenience and ethical use becomes disturbingly blurred.

### Reference Map

1. Paragraphs 1, 2, 3
2. Paragraphs 4, 5
3. Paragraph 6
4. Paragraph 7
5. Paragraph 8
6. Paragraph 9, 10

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://futurism.com/facial-recognition-meta-plan> - Please view link - unable to able to access data
2. <https://www.reuters.com/business/meta-expands-ai-access-ray-ban-smart-glasses-europe-2025-04-23/> - Meta Platforms announced the expansion of its AI assistant, Meta AI, to Ray-Ban smart glasses users in seven additional European countries: Germany, Austria, Belgium, Denmark, Norway, Sweden, and Finland. This AI functionality allows users to engage with the assistant via voice commands to receive answers to general inquiries. The expansion is part of a broader rollout of Meta’s AI technology in Europe, which began in March 2025 after delays caused by regulatory concerns regarding data protection and privacy. Initially launched in the U.S. in 2023, Meta AI’s European release faced challenges due to the European Union's stringent privacy and transparency rules. The expansion introduces new features, including live translation and a real-time visual assistant, enabling users to query objects they see and receive immediate responses. These enhancements follow Meta’s December 2024 update, which added AI-powered video and translation capabilities to the smart glasses. This initiative aligns with Meta’s ongoing efforts to enhance wearable technology and attract users while investing heavily in AI development.
3. <https://theconversation.com/metas-ai-powered-smart-glasses-raise-concerns-about-privacy-and-user-data-238191> - Meta's AI-powered smart glasses have raised significant privacy and user data concerns. The glasses, developed in collaboration with EssilorLuxottica, feature cameras, open-ear speakers, microphones, and touch panels. Users can operate the glasses using voice commands or the built-in Meta AI assistant. When users capture photos or videos, they are sent to Meta’s cloud for AI processing. Meta states that all photos processed with AI are stored and used to improve Meta products and train its AI with the help of trained reviewers. This practice has led to concerns about how images captured without consent might be used by the company, especially given Meta's history with privacy issues. The integration of AI into the glasses adds another layer to these concerns, as AI technologies have been criticized for potential biases and inaccuracies.
4. <https://www.ft.com/content/faedc975-7a9b-4632-bc6e-3e2ea71587c1> - Meta, the owner of Facebook, has agreed to pay $1.4 billion to the state of Texas to settle claims that the company harvested millions of citizens' biometric data without proper consent. The settlement, to be paid over five years, is the largest ever obtained from an action brought by a single US state. The original complaint accused Facebook's now-closed facial recognition system of collecting ... from photos and videos posted on ... informed consent, in breach of a 200 ... Meta launched a feature in 201 ... 'tag suggestions' that recommended to users who to ... 'facial geometry' of those pictured. The complaint accused Facebook of ... billions of times, with at least $10, ... . In 2021, Meta announced it was shutter ... , including the tag suggestions feature, and wiped the biometric data it had ... billion users, citing legal 'uncertainty'.
5. <https://apnews.com/article/cf0f94a8ed9e21421735adf0d15d312a> - The suspect in the New Orleans New Year's Day attack that killed 14 people used Meta smart glasses to scout the French Quarter beforehand, the FBI revealed. Shamsud-Din Jabbar recorded video with these glasses on October 31 while planning the attack. On the day of the incident, he wore but did not activate the glasses' livestream function. Meta, the parent company of Facebook, did not comment. Meta glasses, developed with Ray-Ban, feature a built-in camera, speakers, and AI capabilities, controlled via voice, buttons, or gestures. They allow users to capture images and videos, make calls, message, and listen to music. The glasses cannot execute complex tasks or provide turn-by-turn directions and lack a display in the lens for framing photos or videos. An LED indicator light informs bystanders when the camera is in use.
6. <https://www.theverge.com/2024/10/2/24260262/ray-ban-meta-smart-glasses-doxxing-privacy> - Dubbed I-XRAY, the tech works by using the Meta smart glasses’ ability to livestream video to Instagram. A computer program then monitors that stream and uses AI to identify faces. Those photos are then fed into public databases to find names, addresses, phone numbers, and even relatives. That information is then fed back through a phone app. In the demo, you can see Nguyen and Caine Ardayfio, the other student behind the project, use the glasses to identify several classmates, their addresses, and names of relatives in real time. Perhaps more chilling, Nguyen and Ardayfio are also shown chatting up complete strangers on public transit, pretending as if they know them based on information gleaned from the tech. Facial recognition tech has been frighteningly accurate for a while now, and I-XRAY is largely just chaining together a bunch of existing technologies. It relies in part on PimEyes, which The New York Times described in 2022 as an 'alarmingly accurate' face search engine that 'anyone can use.'
7. <https://www.forbes.com/sites/johnkoetsier/2024/10/03/metas-ray-ban-smart-glasses-used-to-instantly-dox-strangers-in-public-thanks-to-ai-and-facial-recognition/> - They call it I-XRAY and have demonstrated its concerning power to get phone numbers, addresses and even social security numbers in live tests. 'We stream the video from the glasses straight to Instagram and have a computer program monitor the stream,' AnhPhu Nguyen said in a demo video on X. 'We use AI to detect when we’re looking at someone’s face, then we scour the internet to find more pictures of that person. Finally, we use data sources like online articles and voter registration databases to figure out their name, phone number, home address and relatives’ names.' Nguyen and fellow Harvard student Caine Ardayfio then stream that information to an app on their phones. 'Using our glasses, we were able to identify dozens of people, including Harvard students, without them ever knowing,' said Ardayfio. The system is perfect for scammers, because it detects information about people that strangers would have no ordinary means of knowing, like their work and volunteer affiliations, that the students then used to engage subjects in conversation. In the wrong hands, this could very easily lead to dangerous or compromising situations. Imagine a sexual predator who gains the trust of a target by appearing to know them and claiming to have met them at an event in the past. Most of us have fairly hazy memories of years-ago events, so if someone claims to have met us and knows our name and a few facts about us, we’re likely to believe them and engage with them, offering them at least a little bit of trust.