epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

☎ +1 202 483 1140
📠 +1 202 483 1248
🦋 @epic.org
🌐 https://epic.org

February 13, 2026

Attorney General Philip Weiser
Department of Law
1300 Broadway
10th Floor
Denver, CO 80203

Dear Attorney General Weiser,

We write on behalf of the Electronic Privacy Information Center (EPIC) to demand immediate investigation and action in response to today's revelation that Meta Platforms, Inc. intends to add facial recognition and surveillance capabilities to its Ray-Ban Meta glasses.[1] **This feature would pose a grave risk to privacy, safety, and civil liberties and would cause widespread harm to the public. It must not be allowed to reach the market.**

EPIC is a public interest research center in Washington, D.C., established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[2] EPIC has published reports and comments on the dangers of facial recognition technology and the need for greater regulation to protect the public.[3]

This morning, the New York Times reported that Meta has internal plans to embed facial recognition into its Ray-Ban Meta glasses, potentially as soon as this year. In particular, Meta apparently plans to allow wearers of its glasses to identify people around them and receive real-time information about those people. Though Meta has not yet announced the details of this feature, regulators must act now to prevent Meta from rapidly deploying dangerous and likely unlawful facial recognition technology across society.

Facial recognition technology inherently endangers privacy, safety, and liberty, but its integration into commercially available Ray-Ban Meta glasses poses a particularly alarming threat. Ray-Ban Meta glasses are already causing serious, and likely unlawful, privacy harms. They allow unsuspecting—and unconsenting—members of the public to be covertly recorded, with no warning

[1] Kashmir Hill et al., *Meta Plans to Add Facial Recognition Technology to Its Smart Glasses*, N.Y. Times (Feb. 13, 2026), https://www.nytimes.com/2026/02/13/technology/meta-facial-recognition-smart-glasses.html.
[2] *About*, EPIC, https://epic.org/about/.
[3] *See, e.g.*, *EPIC Opposes Dangerous Expansion of Biometric Data Collection and Urges USCIS to Rescind Proposed Rule*, EPIC (Jan. 8, 2026), https://epic.org/epic-opposes-dangerous-expansion-of-biometric-data-collection-and-urges-uscis-to-rescind-proposed-rule/; Comments of EPIC in re. U.S. Dep't of Just. & Dep't of Homeland Sec. Request for Written Submissions on Section 13(e) of EO 14074 (Jan. 19, 2024), https://epic.org/wp-content/uploads/2024/01/EPIC-DOJDHS-Comment-LE-Tech-011924.pdf.

except for a small (and easily circumvented) LED light.[4] Meta has also been increasingly aggressive in its collection, storage, and use of media recorded by the glasses. Just last year, it updated its terms to store audio recorded by the glasses in the cloud and use it to train AI, with no option for consumers to opt out.[5]

Incorporating facial recognition into this already invasive product would dramatically escalate the risks it poses to the public. Giving wearers the ability not just to covertly record members of the public, but also to identify them (and potentially link to the troves of personal data Meta has about them) would represent a profound invasion of privacy and eviscerate any opportunity to keep one's identity private in public. This feature would be ripe for abuse, putting Americans at risk of stalking, harassment, doxxing, and worse. Patients receiving sensitive treatments could be identified and blackmailed; unpopular public officials could become the target of constant and unavoidable harassment in public spheres where they once enjoyed anonymity; members of religious groups could be tracked and targeted whenever they attend their house of worship; and law-abiding protesters could be doxed and punished. These are just some examples of the harms that could be unleashed by Meta's planned roll-out of facial recognition.

The risks do not end with abuse by the wearers themselves. Meta has long developed "shadow profiles" on non-users of its platforms, populated with data collected from contact lists, user-uploaded photos, and tracking pixels.[6] Even if Meta limits whose identity it reveals to individual wearers of its Ray-Ban Meta glasses, its use of facial recognition may still allow Meta itself to engage in mass tracking of unknowing members of the public.

Rather than addressing these concerns and exercising due caution, internal documents indicate Meta's plan was instead to take advantage of today's "dynamic political environment" to roll out the facial recognition features at a time when "many civil society groups that we would expect to attack us would have their resources focused on other concerns," avoiding regulatory attention in the process.[7]

This represents something of a pattern for Meta, which has a sordid history of rolling out policies that violate basic privacy norms—including facial recognition—without due care for the harms they cause. In 2010, Meta hastily began using facial recognition to identify people who appeared in

[4] Elisa Anzolin & Gianluca Lo Nostro, *Ray-Ban Meta Glasses Take Off But Face Privacy and Competition Test*, Reuters (Dec. 9, 2025), https://www.reuters.com/sustainability/boards-policy-regulation/ray-ban-meta-glasses-take-off-face-privacy-competition-test-2025-12-09/.

[5] Chris Welch, *Meta Tightens Privacy Policy Around Ray-Ban Glasses to Boost AI Training*, Verge (Apr. 30, 2025), https://www.theverge.com/news/658602/meta-ray-ban-privacy-policy-ai-training-voice-recordings; Amanda Silberling, *If You Own Ray-Ban Meta Glasses, You Should Double-Check Your Privacy Settings*, TechCrunch (Apr. 30, 2025), https://techcrunch.com/2025/04/30/if-you-own-ray-ban-meta-glasses-you-should-double-check-your-privacy-settings/.

[6] *See* Russell Brandom, *Shadow Profiles are the Biggest Flaw in Facebook's Privacy Defense*, Verge (Apr. 11, 2018), https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy.

[7] Kashmir Hill et al., *Meta Plans to Add Facial Recognition Technology to Its Smart Glasses*, N.Y. Times (Feb. 13, 2026), https://www.nytimes.com/2026/02/13/technology/meta-facial-recognition-smart-glasses.html.

Facebook users' photos and videos, without users' knowledge or consent.[8] Once implemented, it took a decade for civil society and regulators to get Meta to terminate the practice and delete the recorded facial recognition data.

With the prospect of a facial recognition roll-out for Ray-Ban Meta glasses, the stakes are even higher, and it is crucial that regulators act now to prevent this planned feature from being deployed in every bathroom, clinic, classroom, house of worship, and protest in the country. The introduction of commercially available, easily disguised, facial recognition-enabled surveillance devices threatens to cause immense and unavoidable harm to the public. Meta's provision of such technology would constitute an unfair and deceptive trade practice and provide the means and instrumentalities for countless others to engage in the same. And it would raise serious doubts about Meta's compliance with data minimization obligations, opt-in consent requirements for biometric and other sensitive data, safeguards for the data of minors, and restrictions on profiling under the Colorado Privacy Act.

We welcome the opportunity to speak further about this and will follow up again soon with additional details. If you have any questions, please contact EPIC Deputy Director John Davisson at davisson@epic.org.

Sincerely,

/s/ John Davisson
Deputy Director &
Director of Enforcement

/s/ Jeramie Scott
Senior Counsel &
Director, Surveillance Oversight Program

/s/ Calli Schroeder
Senior Counsel &
Director, AI & Human Rights Program

/s/ Sara Geoghegan
Senior Counsel &
Director, Consumer Privacy Program

/s/ Hayden Davis
Redstone Public Service Fellow

[8] *See Facebook Abandons Facial Recognition System Long Targeted by EPIC*, EPIC (Nov. 2, 2021), https://epic.org/facebook-abandons-facial-recognition-system-long-targeted-by-epic/; *see also In re Facebook and the Facial Identification of Users*, EPIC (2011), https://epic.org/documents/in-re-facebook-and-the-facial-identification-of-users/.