United States Senate

March 17, 2026

Mark Zuckerberg
Chairman and Chief Executive Officer
Meta
1 Hacker Way
Menlo Park, CA 94025

Dear Mr. Zuckerberg,

Meta reportedly plans to integrate facial recognition technology into its smart glasses and release this technology at a moment of political distraction to avoid scrutiny. But scrutiny is clearly warranted: Given Meta's vast data collections, its smart glasses could capture images of thousands of people without their knowledge or consent and then instantly link those faces to names, workplaces, or personal profiles, creating serious risks of stalking, harassment, and targeted intimidation. This frictionless identification and constant monitoring also risks normalizing mass surveillance at a moment when the federal government is using similar tools to intimidate protesters and chill speech. Although facial recognition may offer real benefits for blind and visually impaired users, Meta's history of failing to protect user privacy raises serious questions about its plan to deploy this technology in its smart glasses.

Despite abandoning facial recognition technology across its platforms in 2021 over ethical concerns[1] and never publicly releasing the feature on its smart glasses citing privacy concerns,[2] Meta is reportedly yet again working to deploy this privacy-invasive technology.[3] Meta had previously deployed facial recognition on Facebook to automatically identify individuals in photos and videos without needing to tag them. But in 2021, Meta decided to end its use of facial recognition technology across all its platforms, stating that "the many specific instances where facial recognition can be helpful need to be weighed against growing concerns about the use of this technology as a whole."[4] Five years later, Meta appears less worried about those societal concerns and is reportedly planning to deploy facial recognition technology in one of the most dangerous possible settings: smart glasses. Moreover, Meta is apparently aware of the risks with this technology: An internal memo recommended launching the product "during a dynamic political environment where many civil society groups that we would expect to attack us would have their resources focused on other concerns."[5] In other words, Meta appears to

[1] Jerome Pesenti, *An Update On Our Use of Face Recognition,* Meta Newsroom (Nov. 2, 2021), https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/.

[2] Ryan Mac, *Facebook Is Considering Facial Recognition For Its Upcoming Smart Glasses*, BuzzFeed News (Feb. 25, 2021), https://www.buzzfeednews.com/article/ryanmac/facebook-considers-facial-recognition-smart-glasses.

[3] 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.

[4] Pesenti, *supra* note 1.

[5] Hill et al., *supra* note 4.

recognize the serious privacy and civil-liberties risks of facial recognition but thinks it can avoid attention by slipping the once-abandoned, ethically fraught product back onto the market while the world is distracted by the Trump administration's daily chaos.

Despite Meta's desire to minimize public attention on this product, the deployment of smart glasses equipped with facial recognition technology threatens Americans' privacy rights and civil liberties, and therefore warrants close scrutiny. Smart glasses — often indistinguishable from regular glasses — are designed to be worn throughout the day as its user passes hundreds, if not thousands, of people. In a single day, the user could scan thousands of faces, with no practical way for a bystander to consent or even know about such real-time identification. Americans do not consent to biometric data collection simply by walking down a public street, entering a café, or standing in a crowd. Yet the deployment of this technology would appear to do exactly that — subjecting countless individuals to covert identification without notice, without consent, and without any meaningful opportunity to opt out. This practice would erode longstanding expectations of privacy in public spaces, effectively eliminating public anonymity.

Meta's sweeping access to personal information makes the integration of facial recognition technology into its smart glasses uniquely dangerous. Meta's facial-recognition-enabled smart glasses could allow users to instantly access an individual's name or social media profile, potentially surfacing personal information even if users have switched their profiles to private. Such real-time identification would dramatically lower the barrier to doxxing and persistent tracking, enabling bad actors to connect a face in a crowd to a workplace, name, or online presence within seconds. Granting strangers frictionless access to identifying details raises serious risks of stalking, harassment, and targeted intimidation, particularly for women, LGBTQ+ individuals, and other vulnerable communities. In the hands of a bad actor, this technology could be a remarkably powerful and dangerous tool.

The widespread deployment of facial-recognition-enabled smart glasses also risks accelerating the normalization of mass surveillance in the United States. Federal agencies are already using facial recognition tools to identify individuals engaged in lawful protest activity and potentially to assemble databases of those exercising their First Amendment rights. This abuse of facial recognition tools demonstrates how easily real-time identification technologies can be repurposed to discourage political expression, target vulnerable communities, and chill lawful dissent. Embedding facial recognition into consumer wearables would vastly expand this surveillance infrastructure, enabling continuous, decentralized identification of members of the public without their knowledge or consent. The deployment of facial recognition technology in smart glasses risks entrenching a system in which Americans are routinely scanned, catalogued, and analyzed as they move through daily life — an outcome fundamentally incompatible with a democracy.

To help the public better understand Meta's plans and privacy policies regarding facial recognition in its smart glasses, please respond in writing to the following questions by April 6, 2026:

1. Please detail Meta's facial recognition and biometric data practices for its smart glasses:

   a. How would Meta obtain affirmative express consent from a user to enable facial recognition?

   b. How would meta obtain affirmative express consent from every individual whose biometric data its smart glasses capture, including bystanders, and other non-users?

   c. How would Meta notify individuals that its smart glasses may collect their biometric data without their consent when they appear in the device's field of view?

   d. How long would Meta retain biometric data collected through its smart glasses products, and what policies govern deletion?

   e. Can individuals—both device owners and people whose images the glasses capture—request deletion of their biometric data? If so, how does Meta ensure timely and complete deletion?

   f. Does Meta use biometric data collected through its smart glasses to train machine learning models or improve facial recognition algorithms? If so, how does Meta inform individuals and provide an opportunity to opt out?

   g. Has Meta conducted any internal privacy impact assessments or commissioned third-party audits of its biometric data practices related to smart glasses facial recognition?

2. Please clarify whether Meta intends to match faces captured by its smart glasses to any existing databases or user-provided images:

   a. Does Meta plan to allow users to upload images of known individuals — such as friends, family members, coworkers, or public figures — to create a personalized database for facial recognition matching?

   b. If Meta intends to support user-uploaded face libraries, how will the company verify that the user obtained informed consent from every individual included in that library?

   c. Does Meta plan to match faces captured by its smart glasses to profiles, images, or identifiers stored on Meta-owned platforms, including Facebook and Instagram?

   d. If Meta intends to match captured faces to social media profiles, images, or identifiers, what categories of information would Meta display to the user (e.g., name, username, profile photo, location, connections, or other personal details)?

   e. Does Meta plan to store biometric templates derived from smart glasses captures in a centralized database? If so, will that database connect to any existing Meta data systems?

3. Please identify any controls that Meta intends to provide users to prevent or limit Meta's smart glasses from matching them and their profile:

   a. Will Meta allow smart glasses users to disable any matching between smart glasses captures and Meta's broader social media ecosystem? If so, how will Meta ensure that the default settings do not enable cross-platform biometric matching without explicit consent?

   b. Will Meta allow Facebook and Instagram users to disable any matching between smart glasses captures and Meta's broader social media ecosystem?

   c. What safeguards will Meta implement to prevent unauthorized or covert matching of bystanders' faces to social-media profiles or other Meta-controlled datasets?

   d. Has Meta evaluated the civil liberties risks associated with linking real-time facial recognition to its social media platforms, including the potential for stalking, harassment, doxxing, or government misuse?

4. Please describe how Meta evaluates and mitigates harmful biases and discrimination in its facial recognition systems:

   a. Does Meta test the accuracy and error rates of its facial recognition technology across demographic groups? If so, does Meta publicly disclose those results?

   b. What steps does Meta take to ensure its facial recognition systems do not disproportionately harm communities of color, immigrants, religious minorities, LGBTQ+ individuals, or other vulnerable populations?

5. Does Meta intend to share biometric data — or any outputs generated by facial recognition features in its smart glasses — with federal, state, or local law-enforcement agencies, including the Department of Homeland Security?

Thank you for your prompt attention to this important issue.

Sincerely,

Edward J. Markey
Edward J. Markey
United States Senator

Jeffrey A. Merkley
Jeffrey A. Merkley
United States Senator

Ron Wyden
Ron Wyden
United States Senator