EXPRESS OPINION

Is someone recording you? Why AI Smartglasses are a threat to privacy and women's safety

As companies race to integrate AI into everyday life, concerns around consent and limits on data collection persist. Without effective safeguards, AI-enabled eyewear risks transforming public spaces into a permanently surveilled environment

Smartglasses enable users to capture a broad range of personal information, including audio, video, and geolocation, stored on the user's phone. Portions of this information may be collected by companies providing data-processing services.

6 min read
Jun 9, 2026 05:33 PM IST

Print

By Shivani Mago and Rishiti Choudaha

Imagine you're travelling by the metro, or a bus and notice someone looking at you, only this is not an ordinary glance. The person looking at you is wearing glasses. Glasses that can record, upload your face to a database, and learn everything about you – your name, address, and phone number – before the next station. This is no longer dystopian fiction but a reality that Harvard students demonstrated using Ray-Ban Meta smartglasses.

Competing with Ray-Ban Meta and the Chinese Qwen, Google has now announced its "intelligent eyewear". The Indian "B by Lenskart" has entered the market with over 30,000 preorders. Marketed as a shift in consumer technology, accessibility and content creation, these smartglasses record from a first-person view, translate, describe surroundings, and make calls with just voice commands. The advent of this technology aggravates concerns about privacy, women's safety, and surveillance.

Erosion of consent in public spaces and women's safety

Unlike smartphones and cameras that are recognisable while recording, AI glasses are designed to be invisible. They resemble regular eyewear, leaving bystanders unaware when being filmed. The Ray-Ban Meta glasses, for instance, feature a white light, indicating recording — a signal largely unnoticeable and easily covered up. Moreover, global compliance requirements around recording indicators are inconsistent. While South Korea mandates stronger recording alerts and shutter notifications for camera-enabled devices, the US has weaker requirements, relying on LED indicators, whereas India currently has a regulatory gap. This lowers overall standards, thus decreasing barriers to covertly capturing footage on campuses, workplaces, and other semi-public environments.

STORIES YOU MAY LIKE

Mahhi Vij recalls the one demand ex-husband Jay Bhanushali's parents made

'Married simple men with no money': Neelima Azeem opens up about marital choices; expert weighs in

'Hit with an iron rod': Manjari Fadnis breaks down over brutal killing of society dog

Also Read | My generation understands technology. We just don't understand privacy

In India, women already face high rates of harassment and voyeurism in public places. In a world where Grok can undress women with just one prompt, Google's "put funny hats" command cloaks harm as quirkiness. AI-enabled eyewear further invisibilises non-consensual recording, creating new forms of digital gender-based violence and amplifying fears of harassment.

Beyond individual privacy, there are concerns of covert recording in places with explicit prohibition on photography. In 2025, a visitor to a Kerala temple was detained after personnel identified a concealed camera glare in his smartglasses in violation of their no-photography rule.

Together, these challenges are compounded given the limitations posed by India's current legislation. While the Digital Personal Data Protection (DPDP) Act requires explicit consent to process and use personal data (including for AI training), publicly accessible data is outside the purview of the law. Intimation for recording individuals in public has not been accounted for despite the country's 2017 landmark Puttaswamy judgment acknowledging privacy in public spaces within the right to life and personal liberty.

Data processing, use and limits of consent

Consent is complicated when considering questions of processing and storing data. Smartglasses enable users to capture a broad range of personal information, including audio, video, and geolocation, stored on the user's phone. Portions of this information may be collected by companies providing data-processing services. A Swedish investigation revealed footage collected by Meta was reviewed by outsourced workers in Kenya, prompting a subsequent lawsuit in the US. Workers responsible for footage-labelling claim to have seen people in intimate settings such as "going to the toilet or getting undressed".

Although Meta maintains that it discloses its data-handling practices, the assumption that an ordinary consumer can comprehend the full scope of privacy and consent risk is arguably illogical, especially since the marketing indicates "privacy-first" products.

The risks posed by emergent technologies multiply when pre-existing capabilities are integrated into newer and more accessible systems, opening up avenues for mischief. Harvard students illustrated how Meta's Ray-Ban smartglasses could be used to identify and "dox" people in real time. This system combined the glasses' livestreaming capabilities with facial recognition software and public databases to instantly retrieve personal information such as names, phone numbers, and addresses. Additionally, an

independent researcher found that Meta's updated coding – yet to be operationalised – can now notify when a face is recognised and store unknown faces' data.

Systematic monitoring of individuals

Beyond interpersonal concerns, a broader question arising out of the use of recording technologies is legitimacy of facial recognition technology and the probable use of smartglasses in capturing and training systems feeding into privatised or public surveillance systems.

States have previously used facial recognition as a surveillance tool to track and arrest protesters. During the Black Lives Matter demonstrations, US authorities used recognition software to follow demonstrators' locations to their homes and make preemptive arrests. Similarly, in China, the CCTV network and real-time smartphone monitoring enabled mass surveillance, leading to targeted arrests.

Footage captured on AI glasses could make it harder to evade identification during public protests, and their deceptive nature would allow authorities to blend in as participants and use the data against activists, which is additionally problematic. While surveillance can help in maintaining public security and law and order, authoritarian governments may misuse such justification to curb freedom of speech, expression and association.

Further, under domestic laws, governments can demand data stored on manufacturers' servers, and those interlocked in geopolitical tensions may leverage corporate ownership of private foreign data to serve political ends. India has introduced rules for digital security around footage from made-in-China CCTVs. Russia has shut parts of presidential security surveillance systems after Israeli intelligence's reported use of video footage from Tehran's traffic cameras to track movements of Khamenei and his aides just before killing top Iranian officials. This brings up questions on what kind of

rules should regulate non-consensual filming and pseudo-surveillance of individuals.

As companies race to integrate AI into everyday life, concerns around consent and limits on data collection persist. Without effective safeguards, AI-enabled eyewear risks transforming public spaces into a permanently surveilled environment. While creating standards for a meaningful safeguard mechanism, it is imperative to combine regulation on technology companies with stricter measures of verification for users and methods of improving digital literacy.

While Meta's user guide advises respecting opt-out requests and turning off the glasses in private spaces like changing rooms or public washrooms, this transfers the onus onto the wearer. Therefore, the question is whose privacy are we safeguarding – the wearer's, the company's, or everyone subjected to being filmed? The advent of technology empowering the wearer should not come at the cost of anonymity in public spaces.

Mago is Project Officer/Communications Officer and Choudaha is Programme Officer at Centre for Communication Governance, NLU Delhi

YOU MAY LIKE

1 Longer than Nehru: How Narendra Modi transformed India in 4,399 days

2 Chandrababu Naidu writes: 12 years on, leadership that endured, India that emerged

3 Four challenges that demand attention in India's FTAs

4 Is India ready for a mandatory shift to electric vehicles by 2028?

5 Chirag Paswan writes: From Ladakh, a sea buckthorn parable about enterprise

CURATED FOR YOU


Congress tries moving MLAs to Karnataka – in vain – as Meenakshi Natarajan's Rajy...


'Hope Pakistan held accountable': India reacts after 11 killed in PoK

Artificial Intelligence # Data Privacy # Data Protection

Share Comments Print