



The Consumer Voice in Europe

Ms Henna Virkkunen
Executive Vice-President
Tech Sovereignty, Security and Democracy
European Commission

BEUC-X-2026-096

21st October 2026

Subject: Covert surveillance through “smart” glasses must not become the norm in Europe

Dear Executive Vice-President Virkkunen,

Following the fast availability of so-called ‘smart glasses’ such as Ray-Ban Meta in the European market, BEUC would like to express its serious concerns about the risks that these glasses and other wearables with hidden surveillance features may pose to consumers and society at large.

These devices pose a **significant risk to fundamental privacy rights** by integrating covert cameras into regular eyewear, allowing wearers to record people hands-free without their knowledge or consent. The recent addition of embedded AI features introduces further risks for society, enabling wearers to identify individuals in real time without their consent. As smart glasses transition from a niche gadget into mainstream retail availability, their impact on consumers’ rights needs to be seriously considered.

Smart glasses operate hands-free and are deliberately designed to resemble standard eyewear, making covert recording effortless and hidden from the public. The only visible warning to bystanders is a small light, which is hard to notice and can be disabled or hidden. This poses a direct threat to consumers’ privacy, who can now be filmed in public without their knowledge, let alone a chance to consent or exercise the rights to object. Such footage can reveal sensitive data concerning a person’s health, beliefs or political views, and be published online within seconds, as well as further harvested to train AI models. Covert filming also creates serious risks of harassment and non-consensual sharing of footage, with women and children being at most risk. These harms require **an immediate and decisive regulatory response at the EU level**.

Meta prominently [highlights](#) the value of smart glasses as accessibility tools for blind and visually impaired individuals to bolster social legitimacy. But restricting smart glasses as mass consumer products does not prevent providing dedicated, privacy-respecting assistive tools for those with specific needs. Persons with disabilities are particularly vulnerable when using such devices for daily assistance, as they will remain the default targets of non-consensual recording in public spaces, compounding a long history of disproportionate surveillance against them. Rights to accessibility and privacy can and



must go hand in hand. As technology is moving beyond recording, we fear these risks may escalate significantly, thanks to ready to use facial recognition capabilities, previously embedded by [Meta](#) without warning. This exposes people to further undesirable behaviours and profiling, as well as extending surveillance to physical spaces. BEUC has consistently [advocated](#) a ban on remote biometric identification under the AI Act, with similar calls made by the EDPS and the EDPB. Urgent action is critical in order to provide legal certainty as other major technology companies are preparing to launch competing devices soon.

BEUC therefore calls on the European Commission and on the European Data Protection Board to examine the risks posed by this technology as an immediate priority and urgently investigate their compliance with existing EU regulatory frameworks. National authorities must be vigilant and closely monitor these products on the EU market and make full use of their powers. Moreover, we recommend an assessment as to whether the current EU digital rules are still fit for purpose to effectively protect consumers from the harm of these technologies. This may include introducing stronger rules concerning manufacturers' responsibility and whether wearables that allow for covert (commercial) surveillance should be restricted in certain public areas altogether.

From our perspective, an effective EU regulatory response must require manufacturers to integrate privacy by design and by default into these products, enabling consumers to use them lawfully while protecting the rights of third parties. Their obligations must cover product design, default settings, data flows and technical safeguards. The ongoing Digital Omnibus negotiations can provide an opportunity to establish such rules, addressing the wider structural challenge posed not only by smart glasses, but also camera-equipped headphones, connected vehicles, and other products that enable covert surveillance.

Europe cannot afford a society where covert surveillance becomes normalised across public and private spaces.

We remain at your disposal should you require additional information. Please note that this letter has also been addressed to Commissioner McGrath and the European Data Protection Board Chair, Anu Talus.

Yours sincerely,

Agustín Reyna
Director General