The Camera on Your Face: India's Privacy Law in the Age of the Watching Wearable

AI Disclosure Statement

The author used an AI solely for language editing, grammar refinement, and formatting assistance. All legal research, analysis, case law interpretation, arguments, and conclusions presented in this manuscript are the author's own work.

Abstract

India's Digital Personal Data Protection Act, 2023 (DPDP Act) was drafted for a world of forms and apps, built around a consent architecture that assumes a known Data principal, a known Data fiduciary, and a specific affirmative act of agreement. This article argues that ambient wearable cameras, epitomised by Reliance Jio's newly announced JioFrames and the privacy controversies surrounding Meta's Ray-Ban smart glasses in Kenya, expose three structural failures in that architecture: the inability of consent to function when a bystander does not know that they are being recorded, an overbroad personal-use exemption under Section 3(c)(i) that may place mass real-time biometric capture entirely outside the Act's reach, and the absence of any heightened protection for biometric data such as facial geometry and voiceprints. Drawing on Reliance Jio's own history of data-handling controversies, the constitutional privacy jurisprudence of Justice K.S. Puttaswamy (Retd.) v. Union of India, the narrow scope of existing voyeurism and image-capture offences under the IT Act and the Bharatiya Nyaya Sanhita, and comparative regulatory responses from the European Union, the United Kingdom, and Pennsylvania, the article contends that India's data protection framework requires targeted legislative correction, including a tamper-evident recording indicator, closure of the personal-use exemption for third-party capture, a distinct consent category for biometric data, and concrete retention and breach-disclosure obligations, before ambient wearable surveillance becomes normalised.

KEYWORDS

Digital Personal Data Protection Act, 2023; Smart Glasses; Biometric Privacy; Consent Architecture; Right to Privacy; Data Protection Law in India

The Camera on Your Face: India's Privacy Law in the Age of the Watching Wearable

In the spring of 2026, the British broadcaster BBC reported on an investigation done by Swedish newspapers Svenska Dagbladet (SvD) and Goteborgs-Posten (GP) that should have unsettled anyone who has ever put on a pair of smart glasses to record a video. Contract workers in Kenya, employed by a firm called Sama to review footage flagged by Meta's AI systems, had been watching clips pulled from Ray-Ban smart glasses, including recordings made inside bedrooms and bathrooms.[1] The footage had not been stolen. It had been uploaded, in the ordinary course of the product working exactly as designed, and then routed to human reviewers on another continent who had no relationship whatsoever with the people appearing in it. Meta's own marketing had promised devices “built for your privacy".[2] Days later, US plaintiffs filed a class action arguing that promise was never true,[3] and by May the Texas Attorney General had opened his own investigation into whether Meta's glasses could unlawfully record bystanders without their knowledge.[4]

This is not a story about Meta. It is a preview, and it is worth pausing on why the device matters as much as the company. A smartphone signals its own function. It has to be pulled from a pocket, held up, and pointed. Everyone nearby can see the gesture and understand what it means, even if they cannot stop it. Smart glasses do away with that signal entirely. They sit on the wearer's face, looking like ordinary eyewear, and they can record on a whispered voice command or the press of a nearly invisible button on the temple. The shift is not really from smartphones to smart glasses; it is from a surveillance you can at least see coming to one you cannot.

---

[1]Chris Vallance, *Regulator Contacts Meta Over Workers Watching Intimate AI Glasses Videos*, BBC News (Mar. 4, 2026), https://www.bbc.com/news/articles/c0q33nvj0qpo (last visited July 17, 2026) (archived at https://perma.cc/N95J-TMQS).

[2] Meta marketed its AI glasses using promises like "designed for privacy, controlled by you," and "built for your privacy," Complaint at 12, *Bartone v. Meta Platforms, Inc.*, No. 3:26-cv-01897 (N.D. Cal. filed Mar. 4, 2026).

[3] Jessica Mathews, *Meta Promised It Wouldn't Spy on You with Its AI Smart Glasses. A Lawsuit Says Humans Are Watching You, Actually*, Fortune (Mar. 27, 2026), https://fortune.com/2026/03/27/meta-smart-glasses-filming-watching-workers-lawsuit-privacy/ (last visited July 17, 2026) (archived at https://perma.cc/MFP7-GG5Y).

[4]Office of the Att'y Gen. of Tex., *Attorney General Ken Paxton Launches Investigation Into Meta Glasses to Protect Texans' Privacy From Unlawful Monitoring and Collection of Facial Data* (May 20, 2026), https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-launches-investigation-meta-glasses-protect-texans-privacy-unlawful (last visited July 17, 2026) (archived at https://perma.cc/W34S-V63X).

Roughly six months earlier, Reliance Industries had unveiled JioFrames at its Annual General Meeting: AI-powered smart glasses with HD recording, livestreaming to Jio's cloud, and voice-activated capture, pitched explicitly as an Indian answer to Ray-Ban.[5] Targeted at a market of over 1.4 billion people, in a country where a single company already sells the SIM card, the streaming app, and now the eyewear, JioFrames is not a niche gadget. It is built for mass adoption. JioFrames is not really the subject of this article, though; it is the occasion for it. The argument is not about the hardware of a single company. It concerns a law that was never designed to withstand contact with such hardware. It also concerns what happens when that hardware enters a nation that is still putting together the legislation intended to regulate it.

I. A law built for a world that no longer exists

The Digital Personal Data Protection Act, 2023, was India's first serious attempt at a comprehensive privacy statute, and in the world of forms and apps it was written for, its logic mostly holds. A person opens an account. A company asks for consent. The person says yes or no, and if things go wrong later, there is at least a paper trail showing who agreed to what. The Act calls this person the “Data Principal” and the company the “Data Fiduciary", and Section 6 insists that whatever consent passes between them be “free, specific, informed, unconditional and unambiguous with a clear affirmative action.”[6]

Put a camera on someone's face and that entire architecture becomes unworkable.

A commuter on the Metro does not know that the person across the aisle is wearing a recording device. They cannot ask what the footage will be used for, because they do not know it exists. They cannot withdraw consent under Section 6(4), because they never gave any. They cannot even identify who the “fiduciary” is. Is it Reliance Jio, which built the cloud infrastructure and the AI models, or is it the wearer, who pressed record? The Act assumes a negotiation between two known parties. Smart glasses introduce a third person into the room who was never invited to the table, and the statute has no vocabulary for them at all.

---

[5]The Hindu Bureau, *Reliance Announces AI Powered Smart Glasses JioFrames*, The Hindu (Aug. 29, 2025), https://www.thehindu.com/sci-tech/technology/reliance-announces-ai-powered-smart-glasses-jioframes/article69988556.ece (last visited July 17, 2026).

[6]Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023, §§ 2(i), 2(j), 6(1) (India).

It gets worse. Section 3(c)(i) exempts personal data "processed by an individual for any personal or domestic purpose," a carve-out considerably broader than its European counterpart, which is confined to "purely personal or household activity."[7] The exemption was written with an obvious and reasonable target in mind: a parent photographing their child's birthday party should not have to comply with a corporate-grade data protection regime. Nobody drafting that clause in 2023 was picturing a device capable of continuously harvesting the faces of every stranger on a crowded metro platform, twenty-four hours a day, at the scale of a mass-market consumer product. Read literally, though, an ordinary person filming their commute on JioFrames for their own enjoyment may fall entirely outside the Act's reach, even as the footage of dozens of strangers sits on a corporate server the moment it syncs to the cloud. Reliance Jio's own processing, as manufacturer and cloud host, remains regulated. The individual wearer's real-time capture of everyone around them may not be regulated at all. That is not a small gap. It is a hole large enough to walk an entire surveillance economy through, and it exists not because Parliament wanted it to, but because nobody updated the exemption once the hardware caught up to it.

And there is a third failure, quieter than the first two but arguably more consequential. Nowhere does the DPDP Act treat biometric data (facial geometry, voiceprints, gait, the particular way a person's face moves when they laugh) as anything other than ordinary personal data. The GDPR's Article 9 classifies biometric identifiers as "special category data" demanding a higher bar of explicit consent.[8] India's Act draws no such line. A device that is, by its very design, harvesting facial geometry from every face that crosses its lens receives exactly the same statutory treatment as a form asking for someone's email address.

There is also a timing problem layered on top of the drafting problems, and it makes everything above worse rather than better. MeitY notified the DPDP Rules only in November 2025, alongside a staggered enforcement timeline: the Data Protection Board of India came into existence immediately, consent-manager obligations follow a year later, and the bulk of substantive compliance duties for data fiduciaries do not bite until May 2027.[9] JioFrames will be

[7] *Id.* § 3(c)(i); Regulation (EU) 2016/679, art. 2(2)(c), 2016 O.J. (L 119) 1 (GDPR).
[8] *Id.* art. 9.
[9] Ministry of Electronics & Info. Tech., Notification, G.S.R. 843(E)–846(E) (Nov. 13, 2025), https://www.meity.gov.in/static/uploads/2025/11/c56ceae6c383460ca69577428d36828b.pdf; Shahana Chatterji & Kirti Mahapatra, *Enforcement of the DPDP Act and Notification of the DPDP Rules*, Shardul Amarchand Mangaldas

on Indian faces years before the statute meant to constrain it is even fully switched on. A regulator without a full mandate, enforcing a law without most of its teeth, against a device engineered specifically to make consent unworkable. That is not a coincidence of bad timing so much as a structural pattern in how India has always legislated on privacy: reactively, and usually a technology cycle too late.

II. Not just the bystander: the wearer too

Most of the commentary on smart glasses fixates on the stranger caught in frame, and rightly so. But there is a second person being quietly exposed here, and it is the customer who actually bought the device.

Reliance Jio is not a company entering the data economy for the first time. In 2017, reports surfaced that the personal details of over 100 million Jio subscribers, including names, phone numbers, and email addresses, had appeared on a website that came to be known as 'Magicapk.' Jio initially denied a breach had occurred at all, calling the reports 'unsubstantiated claims' and insisting its subscriber data was safe and protected by the highest levels of security. Yet on the very same day it issued those denials, Jio filed a police complaint with the Navi Mumbai Police alleging 'unlawful access to its systems'. Several local news outlets cross-checked the leaked records and concluded a leak had occurred.[10] India, unlike the European Union, imposed no legal obligation on companies at that time to disclose breaches to the people affected by them, and, tellingly, that basic transparency gap is one the DPDP Act still does not fully close. Three years later, when Facebook took a stake in Jio Platforms, the architect of India's own draft data protection framework, Justice B.N. Srikrishna, publicly raised concerns that the deal was proceeding precisely because India still lacked a functioning data protection law and regulator to scrutinise it.[11]

& Co. (Nov. 2025), https://www.amsshardul.com/insight/enforcement-of-the-dpdp-act-and-notification-of-the-dpdp-rules/ (last visited July 17, 2026) (archived at https://perma.cc/S3BW-FSEM).

[10]Reuters, *Jio Breach Prompts Calls for New Cyber Law*, The Hindu (July 15, 2017), https://www.thehindu.com/business/jio-breach-prompts-calls-for-new-cyber-law/article19286261.ece (last visited July 17, 2026) (archived at https://perma.cc/UQD9-72HR).

[11]Aman Rawat, *Architect of Data Protection Bill Raises Privacy Concerns Over Jio-Facebook Deal*, Inc42 (May 13, 2020), https://inc42.com/buzz/architect-of-data-protection-bill-raises-privacy-concerns-over-jio-facebook-deal/ (last visited July 17, 2026).

Now hold that history up against what JioFrames actually does: livestream footage to "Jio AI Cloud," process voice commands through an integrated assistant, and, inevitably, because this is how every AI product improves, retain some share of that data to train and refine the very features the device is sold on. A company with a documented history of under-disclosed breaches and data-sharing arrangements with the world's largest advertising businesses is now positioned to become the custodian of its own customers' facial geometry, voiceprints, location trails, and a continuous audio-visual record of daily life. That is a meaningfully different risk profile from a breach of names and phone numbers. Facial geometry and voiceprints cannot be reset the way a password can; once they sit in a compromised or carelessly shared database, the exposure is close to permanent.

Section 8(7) of the DPDP Act requires fiduciaries to erase personal data once its purpose is served, but sets no concrete timeline, no retention ceiling, and no independent audit mechanism to verify that erasure actually happens.[12] In practice, that leaves the question of how long a wearer's footage sits on Jio's servers, and who can access it in the meantime, almost entirely to Jio's own internal policy, the same kind of self-regulation that, historically, has not served Indian users especially well. Meta's Kenya scandal shows precisely what fills that vacuum when nobody outside the company is watching: footage that was supposed to stay on-device or under user control instead ends up in front of contracted human reviewers, thousands of miles away, with no relationship to and no accountability toward the people appearing in it. There is no principled reason to assume an Indian company, operating under a newer and weaker statute, with less press scrutiny and a regulator still finding its feet, would behave any differently once its own cloud infrastructure is doing comparable work at comparable scale.

III. What the Constitution already knew

None of this is territory the Indian legal system is encountering for the first time. In 2017, a nine-judge bench of the Supreme Court decided *Justice K.S. Puttaswamy (Retd.) v. Union of India*, recognising privacy as a fundamental right flowing from Articles 14, 19, and 21.[13] Justice Chandrachud's plurality opinion did something particularly useful for this argument: it identified

[12] Digital Personal Data Protection Act, 2023, § 8(7) (India).
[13] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, 121, 180, 202 (India).

several distinct zones of privacy, including "behavioural privacy," which protects a person's interest in controlling access to themselves even while they are visibly, publicly doing something ordinary: riding a train, walking down a street, sitting in a café. The Court was explicit that people "do not lose their right to privacy simply by being in public arenas."

Smart glasses are, in a sense, a direct technological challenge to that sentence. A JioFrames wearer filming a crowded metro platform is not doing anything that Section 66E of the IT Act, 2000 was built to punish. That provision criminalises capturing images of "private areas," defined narrowly as genitals, pubic area, buttocks, or breasts, and only in contexts analogous to a changing room.[14] Fully clothed commuters whose facial geometry is extracted for biometric identification sit entirely outside that definition, no matter how invasive the underlying capture actually is. Section 77 of the Bharatiya Nyaya Sanhita, 2023, which replaced the old Section 354C IPC voyeurism provision, suffers the identical limitation: it still requires a "private act" performed with a reasonable expectation of not being observed.[15] Ambient recording of ordinary public conduct, for the purpose of biometric extraction, simply was not contemplated by either provision.

What that gap makes possible is not hypothetical. In 2024, two Harvard students connected a pair of Ray-Ban smart glasses to publicly available facial recognition tools and large language models, then walked around campus identifying strangers in real time, pulling up names, phone numbers, and home addresses from nothing more than a glance.[16] Nobody involved broke into anything. Every tool they used was legal to buy, and every technique they combined was already public. That is precisely the point: the harm does not require malicious hacking or a data breach. It requires only ordinary, off-the-shelf capability, aimed at an ordinary crowd, in a jurisdiction where nobody's face is legally protected the way their bedroom would be. If two students in a dorm room could build that in an afternoon, it is not difficult to imagine what a company holding hundreds of millions of subscriber records, and now a camera on hundreds of thousands of faces, could build with actual resources behind it. The Constitution recognised the underlying harm

[14]Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, § 66E (India).
[15]Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023, § 77 (India).
[16]John Koetsier, *Meta's Ray-Ban Smart Glasses Used to Instantly Dox Strangers in Public,* Forbes (Oct. 4, 2024), 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/ (last visited July 17, 2026); Harvard L. Sch. Libr., *I-XRAY: The AI Glasses That Reveal Anyone's Personal Details* (Jan. 29, 2025), https://lil.law.harvard.edu/events/i-xray-lunch/ (last visited July 17, 2026).

nearly a decade ago in *Puttaswamy*. The criminal statutes have not caught up, and the DPDP Act, the one law that could plausibly have caught up on the civil side, was drafted around a consent model that assumes the harm away entirely.

IV. How other jurisdictions are responding

It is worth being clear that India is not unusually behind because the problem is unusually novel; wearable cameras have existed for years. It is behind because comparable democracies are now actively legislating around exactly this technology, while India's framework remains silent.

The European Union's AI Act prohibits real-time remote biometric identification in public spaces for law enforcement purposes, bans the untargeted scraping of facial images into recognition databases, and classifies biometric identification systems generally as "high-risk," triggering mandatory conformity assessments and human oversight requirements.[17] The European Data Protection Board has opened a dedicated workstream on smart glasses after the Sama revelations, with its chair noting publicly that the devices bring recording "into a new level" compared with smartphones.[18] The UK's Information Commissioner's Office moved on a parallel track, writing to Meta directly after the BBC's reporting and insisting that any device processing personal data at this scale must put users "in control" with "appropriate transparency" that is a standard that a bystander, by definition, is never given the chance to meet.[19]

Pennsylvania offers the clearest example of a narrower, more immediately achievable fix. House Bill 2603, introduced in mid-2026, would require every pair of smart glasses sold or used in the state to carry a visual indicator that cannot be disabled while recording, a direct legislative response to the fact that, as the bill's sponsor put it, these devices can "easily record or stream without anyone noticing."[20] The bill's drafters were candid about the scale of the workaround problem: an underground market already exists for disabling those indicators, with modifiers

[17]Regulation (EU) 2024/1689, arts. 5(1), 6, 2024 O.J. (L 2024/1689) (AI Act).
[18] Anu Talus, Chair, Eur. Data Prot. Bd., Interview with POLITICO (June 2026) (on file with author); see also Zlatko Delev, *Smart Glasses and GDPR: Why Europe Is Cracking Down on Camera-Equipped Eyewear*, GDPRLocal (June 10, 2026), https://gdprlocal.com/smart-glasses-and-gdpr/ (last visited July 17, 2026).
[19] Thomas Claburn, *Meta Smart Glasses Face UK Privacy Probe*, The Register (Mar. 5, 2026), https://www.theregister.com/security/2026/03/05/meta-smart-glasses-face-uk-privacy-probe/5165427 (last visited July 17, 2026).
[20]Pa. H.B. 2603, 2026 Leg., Reg. Sess. (Pa. 2026).

reportedly charging around seventy-five dollars to drill out the recording light altogether. Legislating a light on a pair of glasses will not solve ambient surveillance by itself. But it restores, at minimum, the one thing a smartphone already gives a bystander for free: the ability to see it coming.

None of these frameworks is perfect, and none translates cleanly onto Indian soil, where enforcement capacity and regulatory bandwidth are already stretched thin. But they share a common instinct that India's DPDP Act currently lacks: that a device capable of ambient, undetectable biometric capture cannot be regulated using the same consent checkbox built for a shopping app.

V. Where this leaves India

If there is a single thread running through everything above, it is this: India does not have a technology problem. It has a consent problem, and JioFrames simply happens to be the product that will expose it fastest.

A visible, tamper-evident recording indicator, the kind Pennsylvania is legislating into existence, would at least restore the bystander's ability to know what a smartphone user's raised camera already tells them instinctively. Closing the Section 3(c)(i) personal-use exemption for wearables that capture third parties, rather than the wearer alone, would stop an entire category of biometric collection from falling outside the Act by accident of drafting. Treating facial geometry and voiceprints as a distinct, higher-consent category of data, the way the GDPR already does, would finally give the DPDP Act a vocabulary for the thing these devices are actually built to harvest. Some spaces probably need a flat prohibition rather than a heightened consent standard at all. A classroom, a hospital ward, a courtroom, a place of worship are not settings where “informed consent” from thirty strangers at once is a realistic proposition, and the law should say so plainly rather than leaving it to a fiduciary's internal policy. These are spaces where power asymmetries or vulnerability make collective consent impossible, and where *Puttaswamy's* 'behavioural privacy' is most easily destroyed. And on the consumer side, concrete retention ceilings for cloud-stored wearable footage, paired with a genuine, enforceable breach-disclosure obligation,

would go some way toward ensuring that a company with Jio's own history is not simply trusted to police itself with the same footage it is also commercially profiting from.

India does not need to invent new constitutional theory here. *Puttaswamy* already supplied the reasoning almost a decade ago; what is still missing is the legislative follow-through. JioFrames will not wait for Parliament, or for the Data Protection Board, or for this article, to catch up, and neither, in all likelihood, will the next device after it. The choice in front of India was never really whether ambient, wearable surveillance would arrive. It already has on faces in the Metro, in office corridors, in college classrooms, right now. The real choice is narrower and less comfortable: whether the law that is supposed to govern this technology gets written before the damage becomes visible, or whether India does what it has so often done with data protection: legislate against the harm only after someone has already been hurt by it.