



UPSC & STATE PCS CURRENT AFFAIRS · UJIYARI.COM

EDITORIAL ANALYSIS

Smart Glasses and the Bystander the Privacy Law Forgot

 THE HINDU

25 August 2026 ·

SCIENCE & TECH

POLITY

GS2

GS3

CURATED & WRITTEN BY

**Bharat Choudhary**

UPSC Educator & Content Creator

 [linkedin.com/in/epicbharat](https://www.linkedin.com/in/epicbharat)

ALSO FROM THE CREATOR

BharatNotesFree UPSC notes, MCQs, PYQ analysis. **100% Free.**bharatnotes.com → **ADVERTISE****Advertise with Ujiyari**

Reach thousands of UPSC aspirants daily.

 epicbharat@gmail.com

Smart Glasses and the Bystander the Privacy Law Forgot

 The Hindu

25 August 2026

GS2

GS3



INTERVIEW ANGLE

"The DPDP Act exempts personal data processed by an individual for a purely personal or domestic purpose. When that individual is wearing a camera in a public street, does the exemption still make sense?"

Source: [Original editorial](#)

The Hindu

 Every fact web-verified against primary sources

THE LIFT LINE

A law built on asking permission cannot protect the one person who was never going to be asked.

WHY THIS EDITORIAL MATTERS FOR YOUR EXAM

This connects a live technology story to the constitutional right to privacy and to India's principal data protection statute. It is examinable in GS2 as rights and legislation, and in GS3 as technology governance.

GS Paper 2: Fundamental Rights; Article 21; government policies and interventions; [statutory](#) and regulatory bodies.

GS Paper 3: Awareness in the fields of IT and emerging technology; challenges to internal security through communication networks.

CONCEPT	MEANING	WHY IT IS TESTABLE
Data Principal / Data Fiduciary	The individual to whom personal data relates, and the person determining the purpose and means of processing	The two roles around which the DPDP Act is built
Personal or domestic purpose exemption	The Act does not apply to personal data processed by an individual for a purely personal or domestic purpose	The provision that arguably leaves the wearer unregulated
Proportionality test (Puttaswamy)	Legitimate aim, rational nexus, necessity, and balancing	The constitutional standard for privacy intrusion

BACKGROUND AND CONTEXT

The Constitutional Foundation

Justice K. S. Puttaswamy (Retd.) v. Union of India (2017) was decided by a **nine-judge bench**, which held unanimously that the **right to privacy is a fundamental right** protected under **Article 21** and as part of the freedoms in Part III. It recognised **informational privacy** as one dimension of the right and laid down a **four-part proportionality test** for any intrusion: a legitimate aim, a rational nexus between the measure and the aim, necessity in the sense that no less restrictive alternative exists, and a balancing of the intrusion against the benefit.

The Statute

MILESTONE	DETAIL
Justice B. N. Srikrishna Committee	Constituted 2017; reported 2018 with a draft Bill
Personal Data Protection Bill, 2019	Introduced, then withdrawn in August 2022
Digital Personal Data Protection Act, 2023	Enacted August 2023
DPDP Rules	Notified 2025

The Act's architecture:

ELEMENT	CONTENT
Data Principal	The individual to whom the personal data relates
Data Fiduciary	The person who alone or with others determines the purpose and means of processing
Significant Data Fiduciary	A class notified on the basis of volume and sensitivity, carrying additional obligations including a Data Protection Officer and audits
Consent Manager	A registered intermediary through which a principal may give, manage and withdraw consent
Data Protection Board of India	The adjudicatory body for breaches
Penalties	Up to ₹250 crore for specified breaches

Processing is lawful where it is for a lawful purpose and is based either on **consent** that is free, specific, informed, unconditional and unambiguous, or on certain **legitimate uses**. Critically, the Act **does not apply to personal data processed by an individual for any personal or domestic purpose**.

THE ANALYSIS

- 1. Consent presupposes a relationship, and ambient capture has none.** The notice-and-consent sequence requires an identifiable fiduciary to approach an identifiable principal before processing begins. Wearable capture inverts every element: the fiduciary is not identifiable to the subject, the subject is not identified in advance, and processing begins the moment the person walks into frame. This is not a compliance failure. It is a design mismatch.
- 2. The exemption was written for a different world.** The personal-or-domestic exemption exists so that ordinary private life is not converted into regulated data processing. That rationale is sound for a family photograph album. It sits uncomfortably with a networked camera worn continuously through public space, where the motive is personal and the effect is public. The wearer is personally motivated, and therefore arguably exempt, while being the proximate cause of the intrusion.
- 3. Processing, not capture, is where the harm scales.** Being photographed in public is an old and largely tolerated condition. What is new is that footage can be run through face matching, gait recognition and location inference to produce **identification and tracking**. A thousand ordinary photographs are a nuisance; a thousand photographs plus a matching model is a surveillance system. Any regulation aimed at the camera rather than at the model is therefore aimed at the wrong stage.
- 4. Puttaswamy points the right way but was aimed elsewhere.** The proportionality standard was articulated principally to discipline **State** intrusion. Horizontal application against private actors runs through statute, and the statute here is the DPDP Act, which is precisely the instrument the editorial says does not reach the case. The constitutional principle is available; the statutory vehicle is not.

5. The counter-argument is substantial and should not be dismissed. Photography in public has never required the consent of everyone in frame, and a rule that made it so would criminalise journalism, citizen evidence-gathering and ordinary life. Regulating a device category is overbroad, technologically brittle and largely unenforceable. The strength of this objection is exactly why the workable remedy targets **biometric processing** and **notice through indicators**, rather than the act of recording itself.

DATA AND INSTITUTIONS VAULT

PRELIMS-GRADE FACTS:

Justice K. S. Puttaswamy v. Union of India (2017): nine-judge bench; privacy a fundamental right under Article 21; four-part proportionality test.

Digital Personal Data Protection Act, 2023, enacted August 2023; DPDPA Rules notified 2025.

Preceded by the Justice B. N. Srikrishna Committee (constituted 2017, reported 2018) and the Personal Data Protection Bill, 2019, withdrawn in August 2022.

Key roles: Data Principal, Data Fiduciary, Significant Data Fiduciary, Consent Manager.

Adjudicatory body: Data Protection Board of India. Maximum penalty: ₹250 crore.

The Act does not apply to personal data processed by an individual for a purely personal or domestic purpose.

*The DPDPA Act, 2023 applies to **digital** personal data, and to non-digital data only once digitised. It is not a general privacy statute: it does not cover anonymised data, and it contains wide exemptions for State instrumentalities. Do not describe it as India's equivalent of a comprehensive right-to-privacy law.*

THE DEBATE

FOR (the law leaves a real gap): The protective mechanism is consent, and the bystander is definitionally outside any consent relationship. The personal-or-domestic exemption removes the wearer from the Act's reach entirely. Downstream AI processing converts casual footage into an identification capability that no existing provision addresses.

AGAINST (existing law suffices and device regulation is overbroad): Public photography has never required universal consent. Voyeurism, stalking and harassment are already offences. State surveillance is governed by Puttaswamy proportionality. Regulating an object rather than a use is unenforceable, technologically obsolete on arrival, and chills legitimate recording.

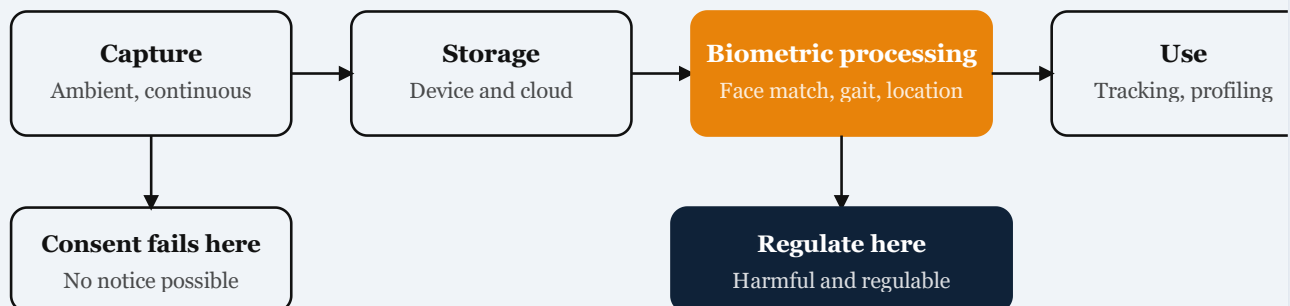
Balanced verdict: The gap is real but it is narrower than a device ban would assume. The intrusion that genuinely lacks a remedy is **biometric identification of non-consenting bystanders**, not recording as such. Regulation should therefore attach to processing: mandatory and non-defeatable recording indicators to restore notice, a prohibition on real-time biometric identification of bystanders outside narrowly defined and supervised circumstances, and an express clarification that the personal-or-domestic exemption does not extend to continuous capture in public space or to biometric processing of the resulting footage.

HOW TO THINK ABOUT THIS

When a technology appears to defeat a legal framework, resist the instinct to regulate the object. Instead, decompose the activity into stages and ask at which stage the harm actually arises, and which stage is practically regulable.

Here the stages are capture, storage, processing and use. Capture is impossible to police and largely lawful. Use is where the damage lands but is detected only after the fact. **Processing is the stage that is both harmful and regulable**, because it requires models, infrastructure and identifiable operators. Locating the intervention at the regulable stage nearest the harm is the general principle, and it applies well beyond privacy law.

DIAGRAM-IN-WORDS



Personal-or-domestic exemption removes the wearer from the Act entirely

Capture is unpoliceable; use is detected too late; processing needs models and operators that can be identified, licensed and held to account

Consent breaks at the first stage and the harm lands at the last, but the only stage with identifiable operators to regulate is the third.

TAKEAWAY BOX

A law built on asking permission cannot protect the one person who was never going to be asked.

Puttaswamy (2017), nine-judge bench, privacy under Article 21, four-part proportionality test; DPDP Act 2023 enacted August 2023, Rules notified 2025; Srikrishna Committee 2017-18; PDP Bill 2019 withdrawn August 2022; Data Protection Board of India; penalties up to ₹250 crore; personal-or-domestic purpose exemption.

Does a person walking through a public street retain any reasonable expectation of privacy once every passer-by may be wearing a camera capable of identifying them?

Connects to past UPSC Mains questions on the right to privacy after Puttaswamy and on the governance of emerging technologies.

“India’s data protection law regulates relationships, while modern surveillance technology operates without them.” Critically examine with reference to ambient wearable devices.

Source: Smart Glasses and the Bystander the Privacy Law Forgot — Ujjyari.com | Free UPSC & State PCS Editorial Analysis

● KEY ARGUMENTS AT A GLANCE

The Hindu argues that AI-powered smart glasses enable continuous, covert capture of bystanders who never consent and often never know they have been recorded, and that the Digital Personal Data Protection Act, 2023 does not squarely address this because its notice-and-consent architecture presupposes a bilateral relationship between a data principal and a data fiduciary that simply does not exist between a wearer and a stranger on the street.



SUPPORTING

- The Act's central mechanism is notice followed by consent, which requires an identifiable data fiduciary to approach an identifiable data principal before processing, a sequence that is structurally impossible where capture is ambient, continuous and directed at whoever happens to be in frame.
- The exemption for personal data processed by an individual for a purely personal or domestic purpose was drafted with private, small-scale activity in mind, but a person wearing a networked camera through public space is engaged in something that is personal in motive and public in effect.
- Capture is only the first stage: once footage is processed by AI systems capable of face matching, gait recognition and location inference, an ordinary recording becomes an identification and tracking capability, which is a qualitatively different intrusion from being photographed.



COUNTER

The counter-view is that the harm is not novel and that existing law already reaches it, since the Puttaswamy proportionality standard governs State surveillance, criminal law addresses voyeurism and stalking, and photography in public places has never required the consent of everyone in frame. On this reading, regulating a device category rather than the harmful use invites overbreadth, chills legitimate recording including journalism and evidence-gathering by citizens, and would be largely unenforceable in practice.



WAY FORWARD

The proportionate response is to regulate the processing rather than the device: mandate unambiguous and non-defeatable recording indicators, prohibit real-time biometric

identification of bystanders outside narrowly defined and judicially supervised circumstances, and clarify that the personal-or-domestic exemption does not extend to continuous capture in public space or to any subsequent biometric processing of the resulting footage.


MAINS ANSWER FRAMEWORK
QUESTION

The consent-based architecture of the Digital Personal Data Protection Act, 2023 presupposes a relationship between the data principal and the data fiduciary. Examine whether this architecture can protect bystanders captured by ambient wearable devices. (250 words)

INTRODUCTION

The arrival of AI-enabled smart glasses has exposed a structural limitation in India's data protection framework. Writing in The Hindu, the argument is made that the Digital Personal Data Protection Act, 2023 leaves a lacuna for ambient wearable surveillance, because its protective mechanism is consent and the person most exposed by such devices is the one from whom consent cannot meaningfully be sought.

BODY

The DPDP Act, 2023 organises protection around a relationship. A data fiduciary determines the purpose and means of processing, a data principal is the individual to whom the data relates, and the Act requires that the fiduciary give notice and obtain free, specific, informed and unambiguous consent before processing, subject to certain legitimate uses.

This design works where the parties know each other and the processing is discrete. It does not work where capture is ambient.

A person wearing networked camera glasses through a market records dozens of individuals continuously; there is no moment at which notice could be given, no practicable means of obtaining consent, and often no awareness on the part of the recorded person that anything has occurred. Two features of the statute deepen the gap.

First, the Act does not apply to personal data processed by an individual for any personal or domestic purpose, an exemption drafted for private and small-scale activity but capable of covering a person who is personally motivated yet publicly intrusive. Second, the Act's obligations attach to the fiduciary, so a wearer who falls within the exemption carries no obligations at all, while the device manufacturer and the platform processing the footage may be at one remove from the capture.

The deeper shift is what follows capture. Justice K. S. Puttaswamy v. Union of India (2017) recognised informational privacy as part of Article 21 and laid down a proportionality standard, but that standard was articulated principally against State action.

When private footage is processed through face matching and location inference, the aggregate result is a private tracking capability that no single act of photography would have produced.

CONCLUSION

A balanced answer should concede that photography in public has never required universal consent and that device-level prohibition would be overbroad and unenforceable. The defensible reform is to regulate the processing rather than the object: mandatory recording indicators, a bar on real-time biometric

identification of bystanders, and an express clarification that the personal-or-domestic exemption does not cover continuous capture in public space.

RELATED DAILY ARTICLES

25 Aug **Current Affairs Today — August 25, 2026**

25 Aug **Prime Minister Chairs 53rd PRAGATI Meeting, Reviews Six...**

25 Aug **Centre Constitutes Committee to Finalise a Permanent...**

25 Aug **CSIR-NAL Unveils Three Indigenous Micro and Small Gas...**



CURATED & WRITTEN BY

Bharat Choudhary

UPSC Educator & Content Creator

[in linkedin.com/in/epicbharat](https://www.linkedin.com/in/epicbharat)[Read Full Article on Ujiyari →](#)<https://ujiyari.com/editorials/2026/08/th-smart-glasses-privacy-law-gaps-2026/>

ALSO FROM THE CREATOR

BharatNotes

Free UPSC study platform — subject-wise notes across all 4 GS papers, Prelims MCQs, Mains answer frameworks, PYQ analysis & progress tracking. **100% Free • No Login Required.**

[Start Preparing → bharatnotes.com](#)

📌 OPPORTUNITY

Advertise with Ujiyari

Reach **thousands of serious UPSC & State PCS aspirants** daily through our PDFs, website, and social channels.

Ideal for: Coaching institutes • EdTech platforms • Book publishers • Exam prep apps

[✉ epicbharat@gmail.com](mailto:epicbharat@gmail.com)

Write to us for rates & media kit

Free UPSC & State PCS Current Affairs · ujiyari.com · bharatnotes.com