SOLD. WITHOUT YOUR CONSENT

Kushagra More, Nirma University

Krity Upadhyay, Nirma University

Before you have even had your first cup of tea, your phone already knows more than you'd like about where you slept, the news you consumed, the product you were about to buy at midnight. Every single thing you do online, every tap, every scroll, every hesitant search, is quietly flowing out to companies you have never heard of, on privacy policies you never actually read. The most unsettling part? You never even noticed the pattern.

Yes, India has more than 900 million internet users.[1] That's a whole lot of people creating a lot of data every day. But until recently, there had been virtually no dedicated law to safeguard any of it. That all changed with the passage of the Digital Personal Data Protection Act, 2023[2] ("**DPDPA**") on paper, though. However, there is a disconnect between laws and reality. . The real challenge was never passing the law, but ensuring that it rightly protects the citizens in an evolving technology driven society.

The coming into existence of the DPDPA marked not just a legislative development but also a constitutional realisation, influenced in part by the landmark judgment of *Justice K.S. Puttaswamy v. Union of India.*[3] judgement, where a nine-judge bench of the Supreme Court that unanimously held that the right to privacy is a fundamental right under Article 21[4] of the Constitution. The legislation includes several important mechanisms. It sets out a tiered system of responsibility with "data fiduciaries" and "data principals". The rights accorded to the individual are similar at least in some respects to those of the General Data Protection Regulation ("**GDPR**")[5] of the European Union: they include the right to access their data, the right to correct their data and the right to have their data deleted, and they are to be heard by a Data Protection Board of India, which is envisaged as a body for the investigation of complaints

[1] Telecom Regulatory Authority of India, *Telecom Subscription Data as on 31st March, 2024* (Mar. 2024), https://www.trai.gov.in.
[2] Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).
[3] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1.
[4] INDIA CONST. art. 21.
[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), arts. 15–17, 2016 O.J. (L 119) 1.

and the imposition of fines of up to ₹250 crore. It is possible. Indian citizens now have personal rights over their personal data that are codified and enforceable for the first time. The incentive for businesses is to adopt a privacy-conscious design. Data restrictions for cross-border transfers indicate that India wants to play a serious role in the global data governance discourse. But the problems are not without significance either. The Data Protection Board is not an independent statutory body like the Election Commission but is appointed by the Central Government, raising concerns about insulation from political pressure.[4] Furthermore, the Act does not explicitly cover algorithmic profiling, surveillance technologies or the use of AI systems to process data in a country that is fast making use of AI in areas such as welfare delivery, law enforcement and financial services. Data protection as a constitutional right may turn into a 'pie in the sky' objective, not a reality.

The battle between individual privacy and the state's surveillance is nothing new. Now what's new is the magnitude, complexity and stealth of the contemporary surveillance system. India has built a huge digital monitoring network. Data is collected in the Aadhaar biometric database and is used to connect with more than 1.3 billion residents, allowing the government to monitor access to welfare, financial transactions and, increasingly, mobility.[6]

The Crime and Criminal Tracking Network and Systems ("**CCTNS**") and the National Intelligence Grid ("**NATGRID**") consolidate data from various law enforcement and intelligence agencies. In 2021, an unprecedented volume of the most intrusive spyware was allegedly used to target journalists, activists and political figures; this was a matter of great concern that the government has neither substantiated nor refuted in Parliament.[7]

In reality, these three tests of the *Puttaswamy*[8] that is legality, necessity and proportionality are not applied.[9] The Indian Telegraph Act, 1885[10], a colonial law, still regulates the interception of communications with procedural protections that would be unthinkable in a modern democratic society. It is interesting to compare it with the international measures. The GDPR, despite its restrictions, imposes strict procedures on state access to personal data. The ECHR has ruled that mass surveillance programmes violate the proportionality principle. In contrast, the Section 17[11] Exemptions in India do not need any judicial supervision, do not require a

[6] Unique Identification Authority of India, *Aadhaar Dashboard* (2024), https://uidai.gov.in
[7] Forbidden Stories & Amnesty International, *The Pegasus Project* (July 2021); *Manohar Lal Sharma v. Union of India*, Writ Petition (Crl.) No. 314 of 2021 (S.C. India).
[8] *Supra Note at 3.*
[9] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1, ¶ 325 (per Chandrachud, J.).
[10] Indian Telegraph Act, 1885, No. 13 of 1885 (India).
[11] Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 17 (India).

sunset clause, and do not provide an individual remedy. The issue is not whether the state has a legitimate security interest; it does. But can security interests be pursued outside the court, in the absence of accountability, transparency and consent from a democratic citizenry? The answer in a constitutional democracy is NO.

I have read and agree to the Terms and Conditions. It's in some ways the most prevalent lie on the internet. As it is being implemented, reading all of the average internet user's privacy policies annually would take more than 200 hours.[12]

It becomes a serious issue in AI and big data analytics. In the traditional consent models, it is assumed that there is a relatively straightforward exchange of specific data for a specific purpose. Modern AI systems are not only using the data you feed them, but they are also deriving data that you never gave them. Based on what you buy, a health insurance AI can make an educated guess on your medical risks. According to a Harvard study, a hiring algorithm can predict your political party from your online reading habits. If you give the machine permission to locate you for navigation, you also give it permission to reveal your religious practices, your relationships, and your mental health.[13]

This is 'contextual integrity' information should be distributed appropriately to match the norms of the context from which it originated, a principle that scholar Helen Nissenbaum has identified.[14] If you share a location with a mapping app, you don't want it to display ads or political information or sell your information to a data broker. You technically "consented", but you have broken the "rules of the game", as it were.

While the DPDPA calls for "free, specific, informed, unconditional and unambiguous" consent to data processing, it does not deal with dark patterns, which are interface designs used to trick users into agreeing to data processing. It doesn't require the transparency of the algorithms; people don't know when AI is used to infer. It doesn't validate automated decisions for users as Article 22[15] of the GDPR does.

In the era of AI, consent cannot be taken for granted. It demands clear explanations in plain language, effective opt-outs with no loss of service, restrictions on secondary uses of data, and

[12] Lorrie Faith Cranor & Aleecia McDonald, The Cost of Reading Privacy Policies, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543 (2008).
[13] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 14–17 (Harvard Univ. Press 2015).
[14] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* 129 (Stanford Univ. Press 2010).
[15] Regulation (EU) 2016/679, art. 22, 2016 O.J. (L 119) 1.

an explanation when technologies are used to affect your life. These are the conditions that transform consent into a theatre, played out by users, acted out by corporations, and authorised by a deficient law.

Data protection cannot be achieved if law, technology and society don't work together. *First*ly, it is important to ensure that the Data Protection Board is truly independent. It should consist of members appointed through a transparent process that is not under the control of the executive branch, similar to the Comptroller and Auditor General, with security of tenure, and a broad mandate to investigate government entities as well as the private sector. If institutions are not independent, the Board may end up being a protector of the population at large, rather than of the population at risk from state over-reach. *Secondly*, the Act needs to be amended to address the accountability of algorithms. All AI systems making decisions with a bearing on the rights of others, such as in credit, employment, healthcare and welfare, must be subject to a Data Protection Impact Assessment, publish their decision-making methodology in an accessible format and give individuals a meaningful right to a human review. India does not have to reinvent the wheel; it can learn from the EU's Artificial Intelligence Act. *Thirdly*, surveillance must be placed under the rule of law. A new dedicated Surveillance Reform Act, which mandates judicial pre-authorisation for targeted interception and parliamentary oversight of mass surveillance programmes, would make India more democratic and recognise the Puttaswamy proportionality standard. *Fourth*, digital literacy must be recognised as a citizen's right. The power of the law rests in the hands of the people and can only be as effective as the people's capacity to protect it. Data literacy initiatives in schools and public institutions, mandated by the government, that teach citizens about the data being gathered, how to read privacy notices, and their right to exercise them, are critical pieces of the infrastructure rather than afterthoughts. Last, but not least, industry needs to do more than simply comply it needs to be ‘privacy by design.’ Meaning: Products in development must incorporate principles of data minimisation and purpose limitation, and not just be added as an ‘afterthought' after regulators tap.

So we started with a straightforward idea: Your phone sold you before breakfast. We conclude with a tougher one that law, technology and society will have to answer: who owns your digital self?

The DPDPA 2023 is not a destination; it is a starting point. It puts India in the list of countries that respect Data Protection. Nonetheless, it opens up far too many avenues for state abuse, corporate exploitation, and the insidious erosion of consent at the hands of AI systems we are

barely familiar with. Privacy isn't a luxury or a technicality. It is, as the Supreme Court said, the precondition of the existence of all other freedoms. There would be no freedom of expression without it; it would be self-censorship. Freedom of association translates to "traceable dissent. The right to dignity turns into a set of data. Today's digital age has provided us with tools and opportunities for connection, knowledge and progress that are truly extraordinary. However, tools are created by the hands that hold them. People in India are young, connected, and more aware; they need to hold those in power accountable. The law exists. The rights exist. Will we make use of them or pass by them in between terms, or will we skip reading and the data we forgot to submit?