

# The Third Road: Resolving the Privacy Paradox and Surveillance Capitalism Using the DPDP Act, 2023

Utkarsh Nigam<sup>1</sup>

## Abstract

*In the modern digital world, every digital service we utilize or provide is working on a fuel called "data." Data that is like 'digital petroleum' for companies, whether a startup or a mega-corporation, and data that is like 'digital DNA' containing our private lives. It is seen as a piece of life to be protected, and it is also seen as fuel for innovation. We are living in a fast-paced world where we are used to conveniences and waiting for the world around us to get even more convenient, but for that we are paying a price that we are unaware of. To access basic digital services, we are forced to blindly agree to terms and conditions and allow access to our data for purposes that we are not informed about.*

*Our data is then processed and used in a way that can earn profits for the companies. It can range from training their models to extremely targeted ads. When our own data is being used by corporations to target our preferences, then we are not just the customer anymore but the product itself. Treating people's lives as tradable goods is against their right to privacy and right to dignity. Our law protects our right to privacy even from the state, but non-state actors were overlooked, creating a constitutional blind spot.*

*The Digital Personal Data Protection Act, 2023 (the DPDP Act) has been enacted to deal with non-state actors. Things have now changed, since these new laws create strict rules and liabilities for companies handling data. While it is a triumph for civil liberties, the other aspect is causing a clash: startups and mega-corporations argue that these laws ruin their 'ease of doing business' and create an 'innovation chokehold.' This paper discusses new ways to tackle this clash by finding a middle ground. If methods like 'Privacy by Design,' de-identified data, and self-liquidation contracts can*

*be inculcated in the industry, it can become a whole new system of a healthy, fair, and trusted digital economy, because respecting people's privacy is not just about avoiding legal trouble; it builds trust with users, and trust is what leads to sustainable business growth without disturbing civil rights.*

**Keywords:** Digital Personal Data Protection Act 2023, Surveillance Capitalism, Privacy-by-Design, Right to Privacy, Indian Startups, Data Minimization, Consent Fatigue, Digital Economy.

## Introduction -- The Era of Surveillance Capitalism

Does a common person have any idea that they're being monitored with their every move in this digital era? Sounds terrifying but no there are no secret surveillance cameras in your room but a whole system being run by big corporate companies on a large scale called the SURVEILLANCE CAPITALISM. A model in which your data is being used to target you not as a consumer but as a product to the companies willing to buy your preferences that are predicted by none other than your own searches, likes, comments, and each permission you gave to a website or app on your phone. A teenie-tiny phone. Containing a whole blueprint of a person's life is not limited to just that person's use, but is being accessed by companies that are earning profit from those blueprints.

When these companies are asked for accountability and questioned about how they can use someone's data involuntarily, they come up with an incredible idea of asking for consent but in a way that you do not even understand what you're consenting to. "CONSENT FATIGUE" Yes, this term and this phenomenon exist. To explain it in basic terms, imagine if you are asked to say 'yes' to loads of

<sup>1</sup>UG Student, Teerthanker Mahaveer College of Law and Legal Studies.

sentences written in small font that makes you squint your eyes and in complex legal language that a normal person cannot understand easily. To what extent would someone spend time on understanding these when they are in a hurry to access that digital service they are being promised for so they just click on I Agree. This is not a choice, it's an illusion of choice.

Many incidents of data breaches are reported worldwide and even from very trusted companies like Mercor an AI recruiting platform, which confirmed that in an incident Lapsus\$ has stolen 4TB of data that included personal identification documents of over 12 million people. Even a 3.5TB database was just leaked recently in April 2026. Is it not concerning to think that some random attacker has a hold on our vulnerable information that was extracted from us without us knowing just so a few conglomerates could earn profits. They mine our data and can remain unable to protect it.

To tackle these concerns the government has enacted the Digital Personal Data Protection Act 2023. *"An Act to provide for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto."* (Digital Personal Data Protection Act, 2023)

Though we talked about the company's shady ways to track our behavioral data and to use it for purposes that we are unaware of but we also have to consider the other side of the coin that says innovation cannot take place without analyzing human behavior and needs which is absolutely true. While the DPDP act demands strict consent and not illusions or tricks, companies argue that its ruining their ease of doing business by putting on too many restrictions. In this paper, we aim to navigate through this clash which, we termed as the PRIVACY PARADOX.

### **The Digital Drop and the Constitutional Blindspot**

What could go wrong if just a drop is taken out of the sea? That's how it feels each time we allow a simple permission like "access to the gallery". But

what if millions and billions of people give out such a drop? Then the number gets huge. A problem is often undermined by its negligible size and impact that is visible to us but what lies beyond our eyes is not considered part of the problem. BUT let's zoom out and see the bigger picture for once, through an example.

The recently popularized AI app 'ChatGPT' stands among users' favourite AI apps. A recent marketing stunt disguised as a social media trend - the Ghibli-style animated photos. Millions of users worldwide provided their personal pictures like free candy, letting it collect tons of biometric data with no guarantee of safety. OpenAI's standard policy states that they may use content provided to ChatGPT including photos to improve and train their models while users do have the option to opt out of this but here is the twist: This isn't the default setting for many users. Unless and until a user manually goes into their settings to turn off "Chat History & Training," the photos uploaded for "Ghiblification" (Turning images into soft Ghibli-style art) are technically eligible to be used as training data. I want to put the light on a simple question. What would happen if this data were leaked or sold? If the database of that company is attacked, then the attacker has access to the AI database, and they could probably use a real photo of the user to create unimaginable hazards for common people or *maybe* famous people. You are probably now aware of the impact of giving out just a drop from the sea.

Now imagine the amount of involuntary data extraction happening every second in this fast-paced world and the consequences it could bring. Supreme Court of India views privacy not just as a collective right but as a Fundamental Right to Dignity (Article 21) (Constitution of India, Art. 21). Even if it's "just a drop" that drop is a piece of your human dignity that the Constitution says is inviolable.

This strong sense of protection of our dignity comes from a landmark case: *Justice K.S.Puttaswamy (Retd) vs Union of India, 2017* (10 SCC 1 (Supreme Court of)). A legal milestone in Indian history regarding digital rights. It is even called the "PRIVACY JUDGEMENT" since it changed the relationship between the Indian

Citizen and the State. Before 2017, the government argued that the Constitution did not explicitly mention privacy and so the citizens couldn't claim it as a basic right. But the Supreme Court disagreed. It was ruled by a nine-judge bench of the Supreme Court that the Right to Privacy is a Fundamental Right. The Supreme Court held that privacy is not a "gift" from the government but an "intrinsic part" of the Constitution. One cannot have liberty or dignity if they do not have basic privacy.

This is our constitutional bedrock of privacy, where even our government cannot breach our privacy, but while the State is now bound by this high constitutional stone, before extracting a single byte of citizen data, private tech companies have been operating in a totally wild manner. Mega corps have been acting up like wild horses, running around in the jungles of our behavioral data, collecting every digital footprint just in case it becomes profitable later. Basically, a constitutional blind spot, where the non-state actors are not taken into consideration. Tech companies exploited this loophole. To fix this, the Supreme Court recognized this void within the Puttaswamy judgment and demanded an accurate modern data protection regime to regulate non-state actors.

The Puttaswamy judgment created the legal energy for the enactment of the Digital Personal Data Protection (DPDP) Act, 2023.

### Deconstructing the DPDP Act 2023

India's first attempt to leash these wild horses running around in a wild manner. The non-state actors and their unregulated data mining. The Digital Personal Data Protection (DPDP) Act, 2023, addresses the constitutional blind spot identified in the Puttaswamy judgment. It fundamentally redefines the relationship between the user and the corporation by introducing two new legal identities: the "Data Principal" and the "Data Fiduciary".

*"Data Principal means the individual to whom the personal data relates and where such individual is - (i) a child, includes the parents or lawful guardian of such a child; (ii) a person with disability, includes her lawful*

*guardian, acting on her behalf." "Data Fiduciary means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data." (Digital Personal Data Protection Act, 2023)*

As soon as one gives their consent to a term or condition and hands over a piece of data, what happens to it afterwards? How do we make sure that it will not be misused later on for the purposes that we are not aware of? To address this concern, the DPDP Act provides an exact framework for the use of data consented to by the data principal. According to Section 4 of the DPDP Act,

*"A person may process the personal data of a Data Principal only in accordance with the provisions of this Act and for a lawful purpose, (a) for which the Data Principal has given her consent; or (b) for certain legitimate uses. For the purposes of this section, the expression "lawful purpose" means any purpose which is not expressly forbidden by law." (Digital Personal Data Protection Act, 2023)*

But if one is giving access to their phone's camera, how do we make sure how much data it's capturing and exactly what purpose it's being used for? We are not supposed to give our consent without knowing the purpose for it, so Section 5 (1) & (2) of the DPDP Act provides:

*"Every request made to a Data Principal under section 6 for consent shall be accompanied or preceded by a notice given by the Data Fiduciary to the Data Principal, informing her, (i) the personal data and the purpose for which the same is proposed to be processed; (ii) the manner in which she may exercise her rights under sub-section (4) of section 6 and section 13; and (iii) the manner in which the Data Principal may make a complaint to the Board, in such manner and as may be prescribed." "The Data Fiduciary may continue to process data until and unless the Data Principle withdraws her consent." (Digital Personal Data Protection Act, 2023)*

The issue of 'consent fatigue' induced by the companies to indirectly force us to agree to their terms and conditions that are provided in a

complex legal language is also addressed in the DPDP Act, as Section 5 (3) of the DPDP Act additionally states:

*"The Data Fiduciary shall give the Data Principal the option to access the contents of the notice referred to in sub-sections (1) and (2) in English or any language specified in the Eighth Schedule to the Constitution. (1) The consent given by the Data Principal shall be free, specific, informed, unconditional, and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose." (Digital Personal Data Protection Act, 2023)*

Not only this, but the DPDP Act also takes care of consent withdrawal. Meta (Facebook/Instagram) recently updated their terms to use personal posts for AI training under the legal basis of "Legitimate Interests." To stop this, users in some regions must navigate a multi- step "Objection Form" requiring proof of impact. If it takes one click to join but ten clicks to leave, it is a "Dark Pattern" and an illusion of choice that opting out exists but induces mental fatigue to do so. Section 6(4) of the DPDP Act clearly states:

*"Where consent given by the Data Principal is the basis of processing of personal data, such Data Principal shall have the right to withdraw her consent at any time, with the ease of doing so being comparable to the ease with which such consent was given." (Digital Personal Data Protection Act, 2023)*

We also get to know about what happens if we no longer want to provide access to our particular data. It used to be a crooked system before, where we had no security that our data would not be processed if we did not use that service anymore, but Section 6(6) of the DPDP Act explicitly adds:

*"If a Data Principal withdraws her consent to the processing of personal data under sub-section (5), the Data Fiduciary shall, within a reasonable time, cease and cause its Data Processors to cease processing the personal data of such Data Principal unless such*

*processing without her consent is required or authorised under the provisions of this Act or the rules made thereunder or any other law for the time being in force in India." (Digital Personal Data Protection Act, 2023)*

Enforcing a law is easy, but making people obey it is the tough part. If people do not fear the punishment, they'll simply consider it as a cost of doing a certain activity and do it anyway. So Section 33(1) of the DPDP Act strengthens our protection by imposing certain penalties as it states:

*"If the Board determines on conclusion of an inquiry that breach of the provisions of this Act or the rules made thereunder by a person is significant, it may, after giving the person an opportunity of being heard, impose such monetary penalty specified in the Schedule." (Digital Personal Data Protection Act, 2023)*

With fines reaching up to ₹250 crore for major breaches, such as failure to secure personal data, as per the Schedule of the DPDP Act.

### **The Startup Friction: Compliance Tax and the Innovation Chokehold**

While it's a huge triumph for civil liberties, it has caused a huge ruckus in the digital startups ecosystem of India. For years, our data was like a fuel, we can even call it the digital petroleum, which was fueling the market, with no limits of exhaustion and a huge surplus amount being received per day, just waiting to be extracted. But to shatter these fast-paced dreams, the DPDP Act has nationalized this digital petroleum and placed it back into the hands of the individuals. This sudden legal shift has caused a clash between the privacy protection concerns and the ease of doing business.

For a baby start-up that's just putting its foot down on the floor and learning to walk in this fast- paced industrial system, the DPDP Act does not just represent a set of rules. It's basically an 'out of the decided budget' operational expense. This is often called the 'compliance tax' in the corporate world. A startup cannot simply store user data anymore in a generic cloud or so instead they have to build a whole Consent Management Architecture in the

company. Users can now go through the terms and conditions in simple effective language for the data they are consenting to. The tough part is that developing these systems needs high-end engineering that could have been used for innovation and growth otherwise.

Now they need real humans and pay them a real salary in addition to the already existing workforce. Data Protection Officer (DPO) and even a Grievance Redressal Mechanism where they can not afford a mistake when penalties can reach up to ₹250 crore for mishandling data and failure to protect it. Absolutely scary for small-scale setups. An even more concerning complaint is that with these many restrictions and regulations for the companies based on Indian lands, how are they going to compete with those who have much more freedom worldwide? Studying larger amounts of data that was collected with ease can help generate more techs and innovation compared to those who are spending money on protecting themselves from legal hurdles.

Apart from growth and innovation data is also collected to identify target audience for a particular advertisement and the new laws mean less data to collect = less ads which means LESS REVENUE. Ads were the primary source of generating revenue for many digital services which allowed them to stay free for public use but now the primary source of funding is gone or not that effective, leading to tension in the companies. Some even say that the new laws favor the Mega-Corp companies like Google, Meta and OpenAI since they already have pre 2023 collected data and has the capacity to bear the cost in case of a lawsuit. Well they basically have enough revenue to not be affected by these new laws. The real cost of protecting privacy might have to be India losing its edge in the global AI race.

### **Resolving the Paradox -- The Third Road**

The exact dispute between companies' ease of doing business and people's fundamental right to privacy is what we call the PRIVACY PARADOX. The way that data can be both digital petroleum as well as the digital DNA is a paradox in itself that needs to be addressed if we want sustainable growth without compromising people's

private lives. We have all read the poem by Robert Frost, titled as "The Road Not Taken". The author could see two roads in that poem the one that everyone chose and the one that no one did. Similarly harvesting data massively with or without informed consent can be seen as the road that everyone takes and valuing privacy and customers' trust can be the one that no one wants to step on. But we are saying that there is a third way the one that the author didn't see. The middle way out. The "Neither yours nor mine."

The companies complain about the Innovation Chokehold by arguing that having tough access to data will make it harder to train models and new innovations can not happen in such a strict environment. But to grant them data brings us back to our original problem of privacy breach and uninformed uses. I would say both can be solved on a middle ground named "DE-IDENTIFIED DATA". Suppose your behavioral data does reach the company about what kind of content you consumed and how you responded to it and what you explored but, it separates YOU from that data. Data now simply belongs to an individual and who is it? That part will never be stored. Storing only the preference and the necessary statistics and deleting the personal identifiable info will allow the company to train their models as well as understand the market and grow and it will also significantly bring down the risks of data breaches when the identifiable info is never stored. Basically splitting the person and their behavioral patterns.

We already discussed consent fatigue which is addressed by the DPDP act but it still does not solve the problem of giving permanent consent to a service that we needed just for two minutes. To solve this companies can adapt to the concept of 'Self Liquidation Contract' (SLC). In this system, consent would not be a permanent permission instead a time bound contract that is agreed for only a particular period of time. For example, 30 days are mentioned in a particular contract to use a person's data to train models or so and the contract automatically self-destructs after 30 days. This reduces the risk of data breaches significantly during an attack. It also brings down the unfair advantage of mega companies like Google and Meta in almost every field, for having previously collected data in a massive quantity. From now on

if we apply SLC in India, then they won't be able to store data for a long time just like any other startup in the Indian ecosystem. Effectively solving the favoritism acquisitions on the DPDP Act regarding mega-corps

All the methods we discussed till now are to find a balance but it can not be forced additionally instead, it can be integrated into the system from the very start and this is what we call "Privacy-By-Design". Dr. Ann Cavoukian developed this system way back in the 90s which has 7 core principles which are as follows:

- Proactive, not reactive -- It demands that action must be taken before a privacy invasive even takes place, because it's no use crying over spilled milk.
- Privacy as default -- Unlike most applications today like Instagram making it a default setting that their models can train from users' personal data, the default setting should be no permission until the user willingly changes it.
- Embedded design -- It means that privacy should be built-in while developing a software itself and not added later as a formality.
- Full functionality -- Ensures that the functionality of a service is not traded for privacy. It shouldn't be No permission = No service and both should be achieved together.
- End-to-end security -- Like WhatsApp chats that are end-to-end encrypted, information must be secured from its collection to destruction.
- Transparency -- The user must be informed of the policies and purposes for which their data is being taken so that they can make an informed choice.
- User-centric -- Applications should be programmed primarily on the basis of user interest not the company's profit.

With the considerate and well-balanced system of Privacy by Design, Self Liquidation Contracts and De-Identified Data, we can ensure a healthy

growth of industries, innovations, and technology without compromising basic human dignity. It can be concluded that the DPDP Act is definitely a Hero for our civil rights but to solve the problem in its entirety we bring a fresh layer of perspective in which we choose the THIRD road. With advanced solutions like the De-Identified Data system, SLC and Privacy-by-design, we can incorporate user trust in the ever-existing beautiful relationship of a Producer and a Consumer. The lore of Data Fiduciary and the Data Principal can have a happy ending by building a healthier, fairer and sustainable digital economy.

---

## References

- Digital Personal Data Protection Act, 2023, Preamble*
- Turning images into soft Ghibli-style art
- Constitution of India, art.21.
- 10 SCC 1 (Supreme Court of India)
- Digital Personal Data Protection Act, 2023, ss. 2(i), 2(j)*
- Digital Personal Data Protection Act, 2023, s. 4
- Digital Personal Data Protection Act, 2023, ss. 5(1), 5(2)
- Digital Personal Data Protection Act, 2023, s. 5(3)
- Digital Personal Data Protection Act, 2023, s. 6(4)
- Digital Personal Data Protection Act, 2023, s. 6(6)
- Digital Personal Data Protection Act, 2023, s. 33(1)