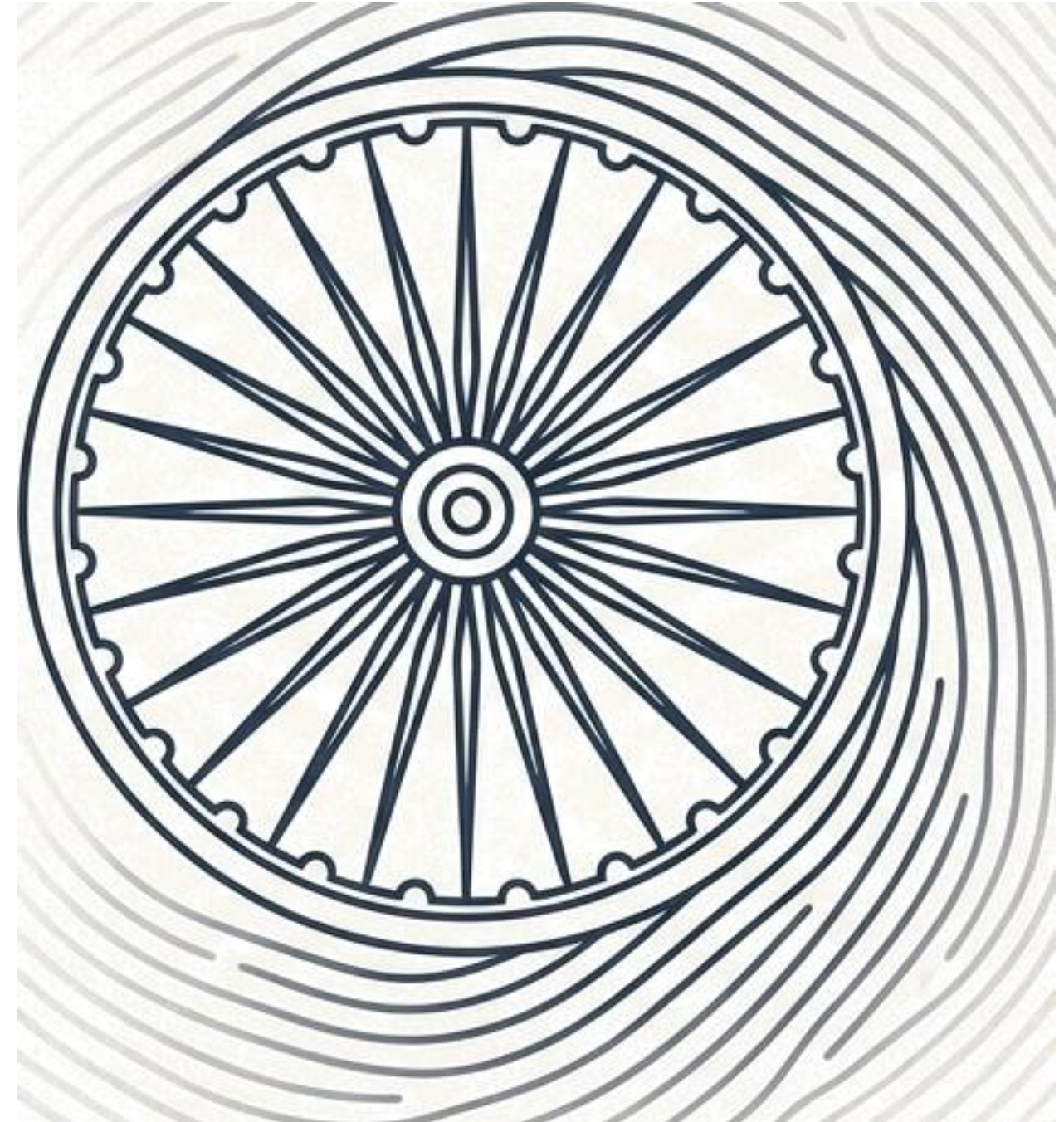


The Ethics of Data Privacy

From 'Datafication' to Data
Protection
in the Indian Context

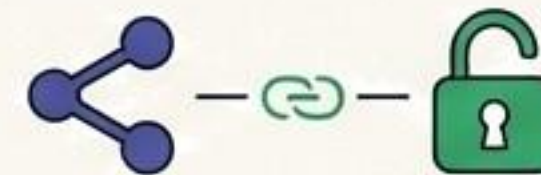


The Privacy Paradox: A Price for



The Truecaller Example:

To identify spam, we grant the app access to our **entire contact** list.



In doing so, you gave away **your** family's and friends' phone numbers **without their consent**.



Is our **privacy** the price we pay for a **'free'** or **'convenient'** service?

The Lock and The Curtains: Understanding the Difference



Data Security (The Lock)

Protecting your data from unauthorized access, like hackers or thieves. It's about building strong walls.

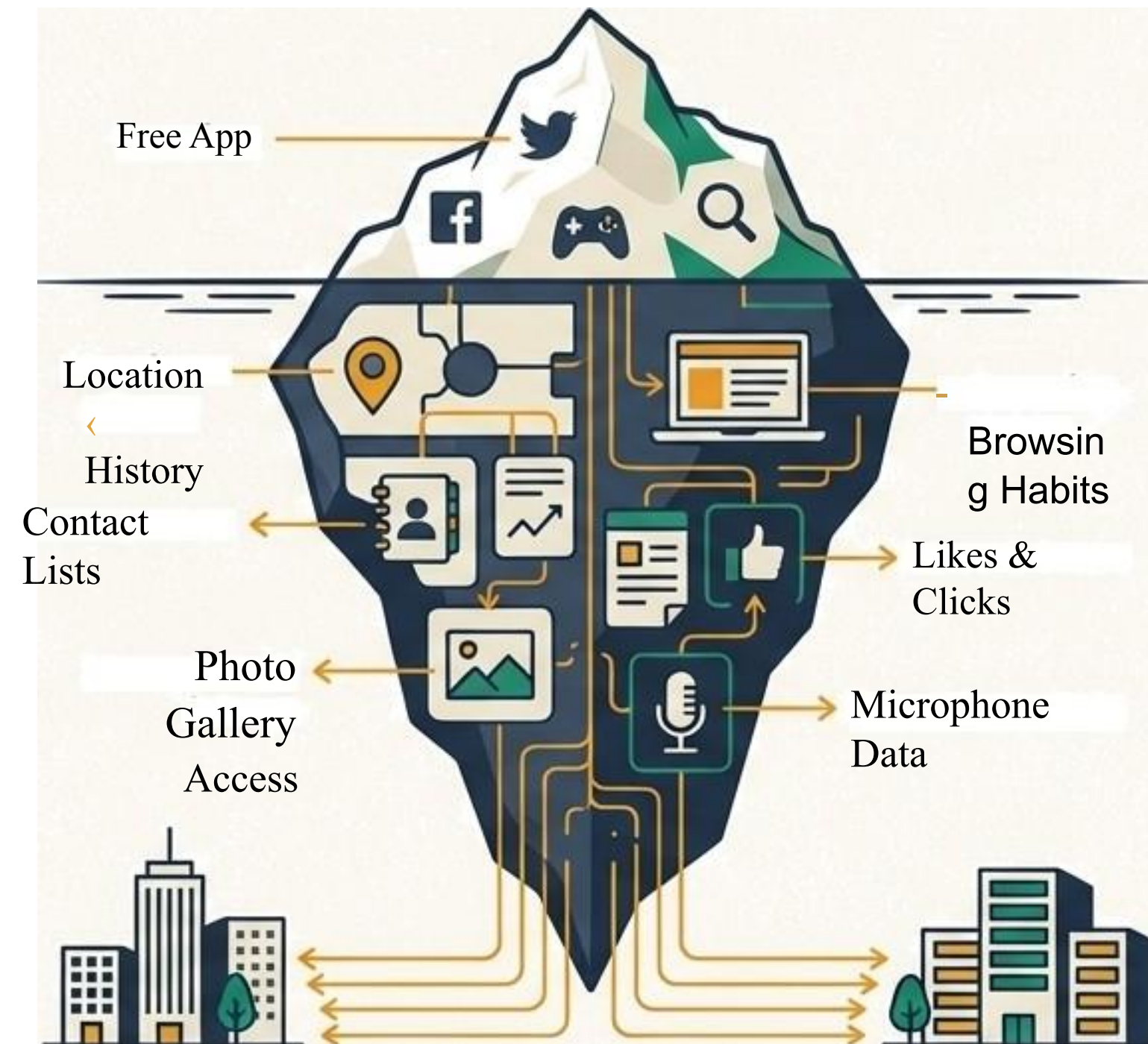


Data Privacy (The Curtains)

Controlling who has the right to see your data and what they can do with it, even if they have legitimate access. It's about your right to decide who can look inside.

You can have security without privacy, but you cannot have privacy without security.

The “Free” App Economy: If the Service is Free, You Are the Product.



Sold to Advertisers, Data Brokers, and Profilers

This economic model is called **Surveillance Capitalism**. Your data is used to create a “Prediction Profile” to influence your behavior.

Our Digital Backbone: Convenience with Great Responsibility



Aadhaar

Your biometrics (fingerprint, iris scan) are permanent passwords. They cannot be changed if compromised.

The Risk

Mentions the real-world threat of AepS (Aadhaar Enabled Payment System) fraud using duplicated silicone fingerprints.



UPI

Every transaction creates a map of your life (school fees, medical bills, travel, food choices).

The Risk

This financial data can reveal deeply personal information about your health, lifestyle, and associations.

A Fundamental Right is Born

Key Event: The landmark Supreme Court judgment in the Justice K.S. Puttaswamy (Retd.) vs Union of India (2017) case.

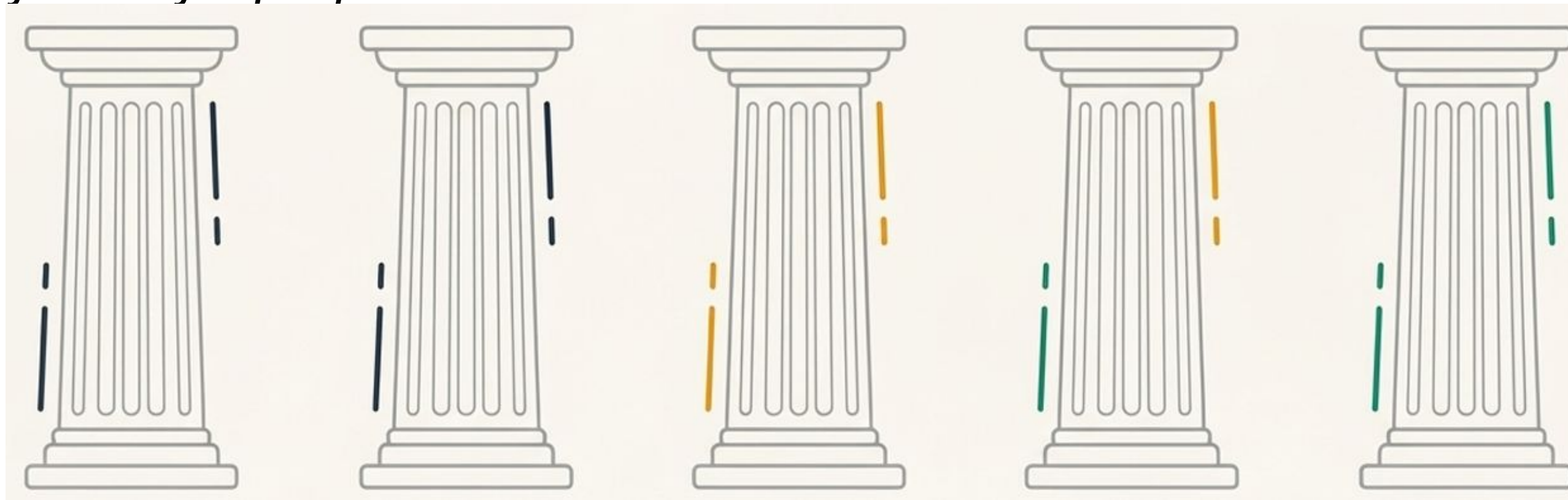


The Consequence: This historic judgment created the constitutional mandate for a comprehensive data protection law in India.

The Verdict: Privacy was declared a fundamental right, intrinsic to life and personal liberty under Article 21 of the Constitution.

A New Chapter of Digital Rights: The DPDP Act, 2023

The official purpose is: “An Act to provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and and the need to process such personal data for lawful purposes...”.



The Act creates a new balance of power between you (the individual) and the organizations that collect your data.

Who's Who in Your Digital World?



Data Principal

You. The individual to whom the personal data relates. This includes children, where parents/guardians are the principals.



Data Fiduciary

The organization that decides the 'why' and 'how' of data processing (e.g., your school, a social media app, a bank). They have the primary responsibility.



Data Processor

An entity that processes data on behalf of the Fiduciary (e.g., a cloud provider, a payroll service).

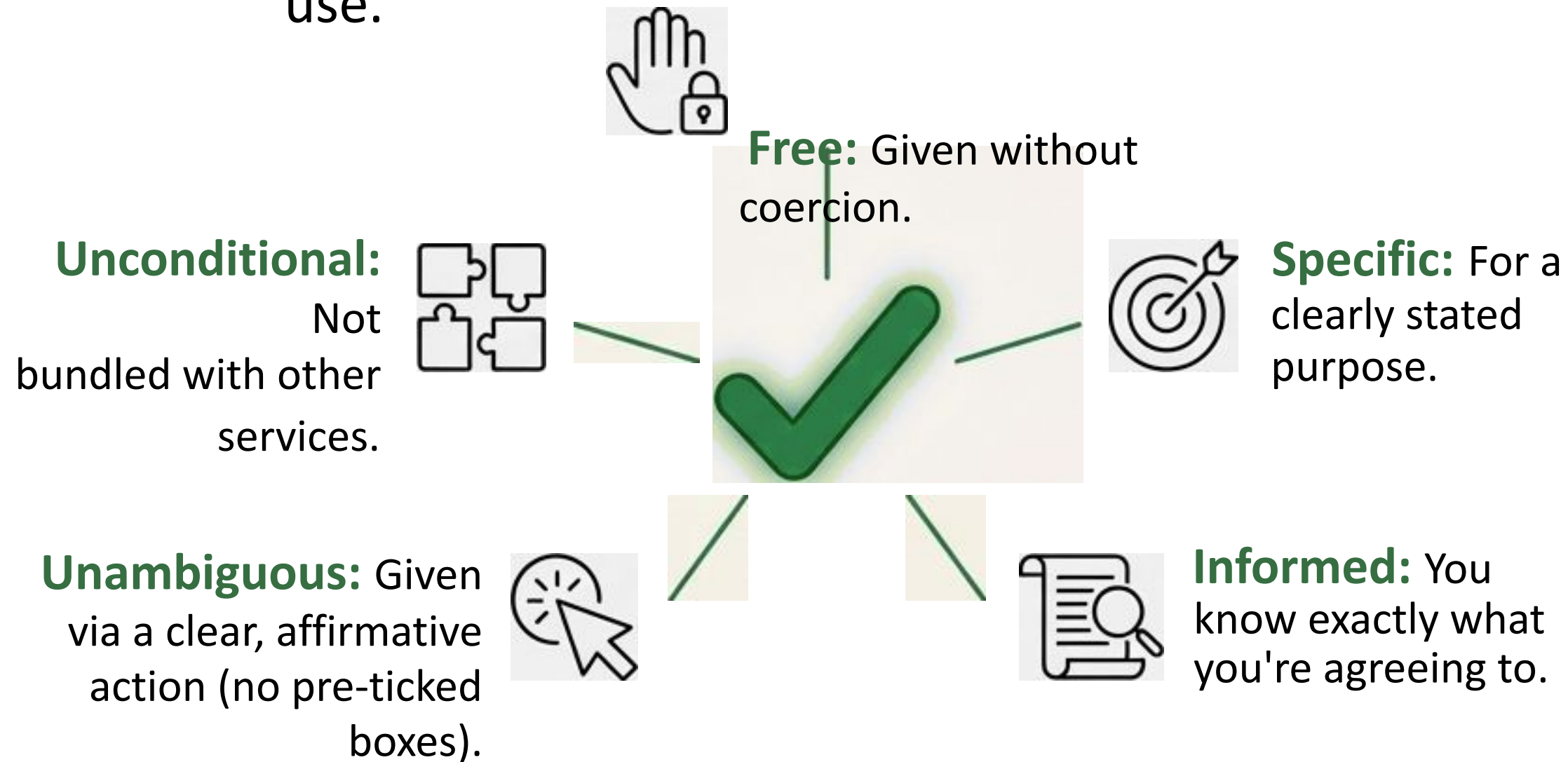


Data Protection Board of India

The new independent authority to enforce the law and protect your rights.

The New Gold Standard for Your "Yes"

All data processing must be based on either your explicit consent or a "certain legitimate use."



The right to withdraw your consent must be as easy as the act of giving it.

Your New Digital Rights as a Citizen



Right to Access

Information

You can demand a summary of your data being processed and who it has been shared with.



Right to Correction & Erasure

You can request to correct inaccurate data or erase data that is no longer necessary for its original purpose.



Right of Grievance

Redressal

You have the right to have grievances addressed by the company first, and then by the Data Protection Board.



Right to Nominate

You can nominate another person to exercise your rights in the event of your death or incapacity.

Protecting the Next Generation: Special Rules for Children's Data



Definition

A "child" is any individual under the age of 18.

The Golden Rule for Fiduciaries

Must obtain verifiable consent from a parent or lawful guardian before processing a child's data.

Strict Prohibitions

- ✗ Process data in a way that is likely to cause any detrimental effect on a child's well-being.
- ✗ Conduct tracking or behavioral monitoring of children.
- ✗ Direct targeted advertising at children.

The Ethical Dilemma in Our Schools: Safety vs. Surveillance



Scenario 1: The WhatsApp Classroom

- Teachers' personal numbers are exposed to all parents and students.
- Students' numbers and profile pictures are visible to strangers in large groups.
- This blurs the line between personal and professional life.



Scenario 2: The "Smart" Classroom

- CCTVs monitor every action in a classroom.
- EdTech apps track student performance to market “fear of failure” products to parents.

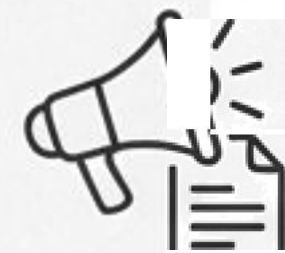
Does constant monitoring create better, safer students, or does it create anxious students who are afraid to make mistakes?

The Cost of Non-Compliance: The Act Has Teeth



”Up to ₹ 250 Crore

For failure to implement reasonable security safeguards to prevent a data breach.



Up to ₹ 200 Crore

For failure to notify the Board or affected individuals of a data breach.



Up to ₹ 200 Crore

For breach of obligations related to children's data.



Up to ₹ 150 Crore

For failure of a Significant Data Fiduciary to meet its additional obligations.

Your Digital Self-Defense Kit: 4 Steps to Take Today



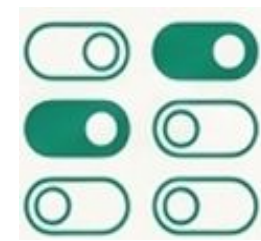
1. Stop the Spam

Register on the TRAI Do Not Disturb (DND) registry. A simple step to reduce unsolicited commercial calls and messages.



3. Use Masked Aadhaar

When you need to provide your Aadhaar, download the 'Masked Aadhaar' version from the UIDAI website. It hides the first 8 digits, preventing its misuse.



Check Your Permissions

Go into your phone's settings and review which apps have access to your camera, microphone, contacts, and location. Ask: Does a flashlight app **really** need your location? (Deny it).



4. Choose Your Browser Wisely

Consider using browsers like Brave that have stronger built-in tracking protection than default options.

The Most Important Lock You Can Set: Your Biometrics

The 'Why'

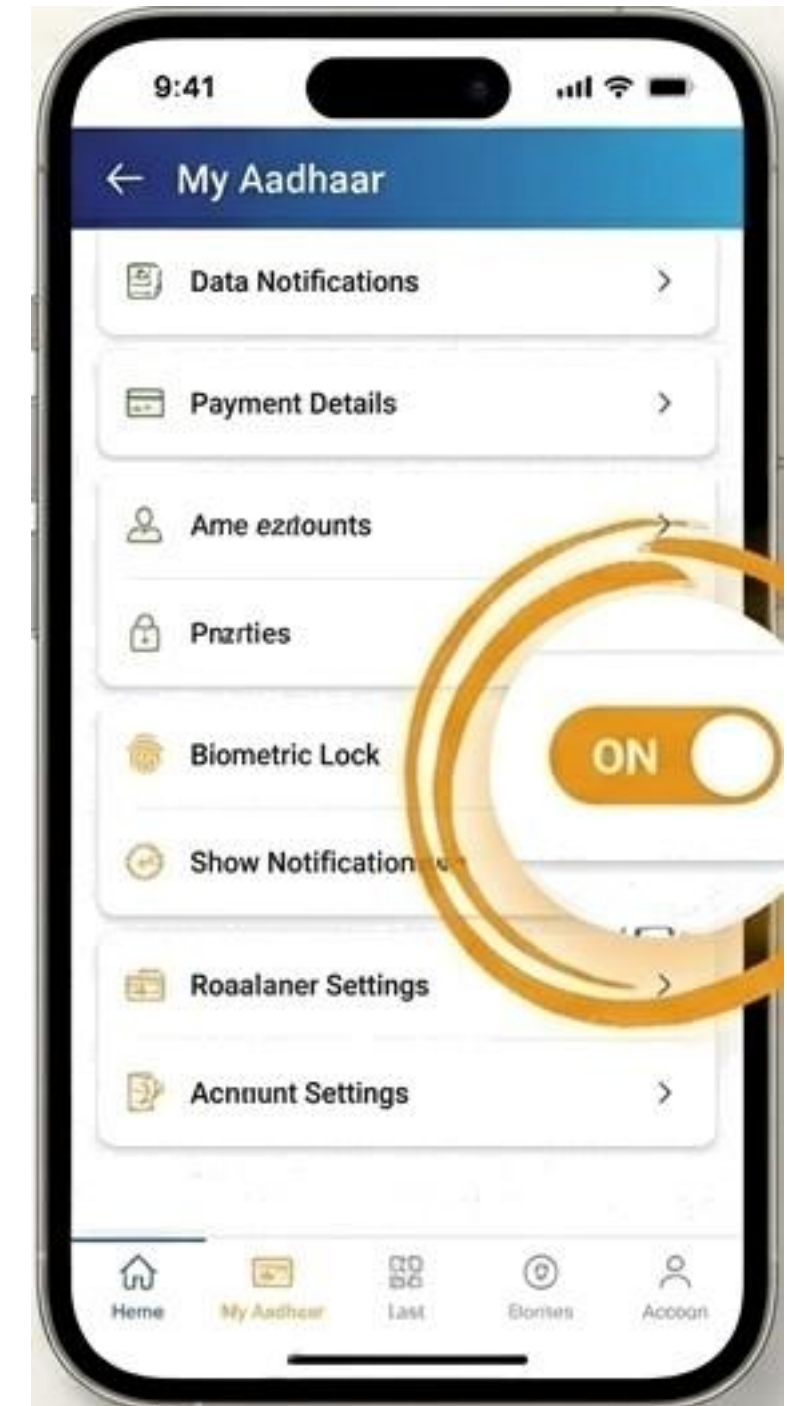
To prevent AePS (Aadhaar Enabled Payment System) fraud where criminals can drain bank accounts using stolen or duplicated fingerprints.

The 'How'

1. Download the official mAadhaar App.
2. Navigate to 'My Aadhaar'.
3. Find and activate the 'Biometric Lock' feature.

How it Works

Your biometrics are now locked. You can temporarily unlock them for 10 minutes whenever you need to use us them (e.g., for a new SIM card or property registration).



A New Ally is Coming: The Consent Manager



What is it?:

A "Consent Manager" is a new type of entity, registered with the Data Protection Board, that will act on your behalf.

What will it do?:

It will provide a single, accessible platform where you can:

Give, **Manage**, **Review**, and **Withdraw** your consent with a single click.

The Big Idea:

To put you back in the driver's seat of your own data.

Rights and Responsibilities: Your Duties as a Data Principal

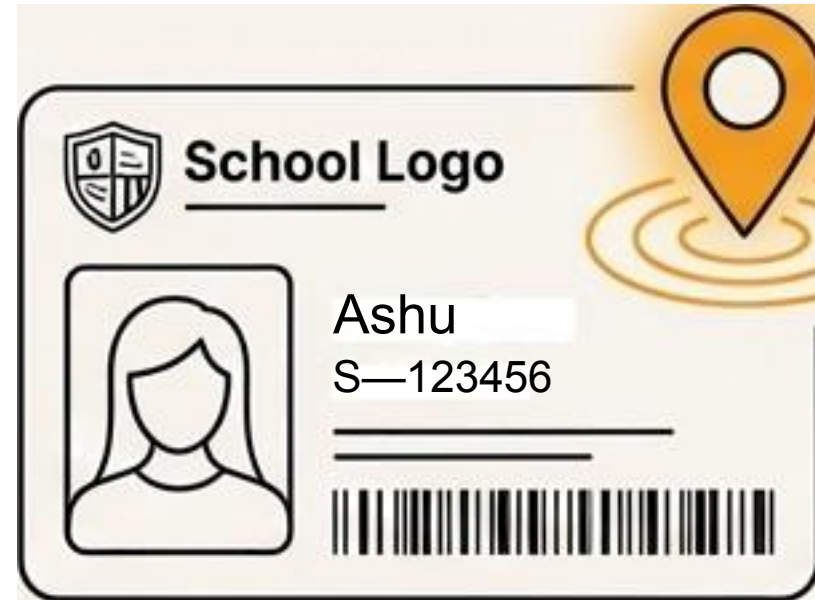


The Act creates a two-way street. You also have duties:

- Do not impersonate another person when providing personal data.
- Do not suppress material information when providing data for official documents.
- Do not file false or frivolous grievances or complaints.
- Furnish only verifiably authentic information when exercising your right to correction or erasure.

Penalty A breach of these duties can result in a penalty of up to ₹10,000.


An Ethical Challenge: The ‘Smart School’ ID Card




The Scenario:

A school proposes to introduce GPS-enabled ID cards for all students. The card will send real-time location alerts to parents' phones (e.g., “Student has entered the library,” “Student has left the school gate”).

Apply the DPDP Principles:

 **Data Minimization:** Is collecting real-time GPS data "necessary" to ensure student safety, or is a simpler gate check-in/check-out system sufficient?

 **Purpose Limitation:** Could this location data, collected for “safety,” be used for other purposes, like tracking which students visit the canteen most often to sell that data to vendors?

Where do we draw the line between caring for students and controlling them?

The Future is Built on Trust

Complying with the DPDP Act is more than a legal obligation - it is an opportunity to build deeper, more meaningful trust with students, parents, and the community.

In India's digital economy, trust is the ultimate currency.



Your Voice in a Silent World



“Arguing that you don’t care about the right to privacy because you have nothing to hide is no different than saying you don’t care about free speech because you have nothing to say.”

- Edward Snowden

Go home today. Open your phone’s setting. And check your permissions.



Thank You!