Data-Privacy Risks in Aadhaar 2.0 and India's Upgraded Digital Public Infrastructure

Figure: An individual using an Aadhaar card for digital authentication. The ubiquity of Aadhaar in India's digital public infrastructure (DPI) brings significant benefits as well as data-privacy challenges.

India's **Digital Public Infrastructure (DPI)** – exemplified by the Aadhaar identity system, digital payments (UPI), and data-sharing platforms – has transformed service delivery and financial inclusion. Over **1.3 billion Indians** now have Aadhaar, enabling instant identity verification for banking, welfare, and more. This **"India Stack"** of interoperable digital services has streamlined access to welfare and reduced leakages in subsidy programs, saving the government an estimated $34 billion by 2021. However, alongside these successes, **Aadhaar's expansion has raised serious data-privacy and security concerns**, especially as India upgrades to "**Aadhaar 2.0**" and extends digital identity usage across sectors. Recent developments in **2023–2025** – including new Aadhaar authentication rules, large-scale data breaches, and India's enactment of the **Digital Personal Data Protection Act (DPDP), 2023** – highlight both progress and persistent vulnerabilities. This report provides a comprehensive analysis of data-privacy risks associated with Aadhaar 2.0 and India's evolving DPI, covering sector-specific issues (healthcare, finance, welfare, etc.), as well as legal, technical, and governance challenges. A comparison with global data protection frameworks (such as the EU's GDPR and California's CCPA) is included to assess compliance gaps, strengths, and weaknesses in India's approach.

Scope and Context: *Aadhaar* is a 12-digit unique ID linked to an individual's **biometric data** (fingerprints, iris scans) and demographic information. It serves as the foundational digital ID in India's DPI. "**Aadhaar 2.0**" refers to ongoing enhancements aimed at reinforcing this foundation – for example, exploring a **blockchain-based unified KYC platform** for 24×7 identity verification with user-controlled data sharing, introducing **face recognition authentication**, and aligning Aadhaar's operations with new privacy laws. As Aadhaar's usage broadens from public welfare into private-sector services (e-commerce, healthcare, finance, etc.), **data privacy risks multiply**. Key concerns include potential **data breaches**, **identity theft (biometric fraud)**, **profiling and surveillance**, and **misuse of personal data** by both state and private entities. Addressing these risks is crucial for protecting citizens' rights and maintaining trust in India's digital ecosystem.

The table below summarizes **key data-privacy risks** identified for Aadhaar 2.0 and related DPI, the sectors affected, and suggested mitigation measures:

Key Risk	Affected Sectors	Potential Impact	Suggested Mitigations
Data Breaches & Leaks – Large-scale exposure of personal data from Aadhaar or linked databases	*All sectors:* Welfare (government databases), Healthcare (health records), Finance (banking KYC), etc.	Sensitive personal data (Aadhaar numbers, biometrics, bank details, health info) can be **stolen and sold** on the dark web. Breaches undermine privacy and facilitate fraud (identity theft, financial scams).	• **Strong encryption & cyber security audits** for all Aadhaar databases and APIs.• **Vendor oversight:** Enforce security standards for all third-party service providers handling Aadhaar data.• **Breach notification & response:** Promptly inform users and authorities of breaches, patch vulnerabilities, and rotate credentials.
Biometric Identity Fraud – Cloning or misuse of fingerprints/iris for Aadhaar authentication	*Finance:* Banking, Digital Payments; *Welfare:* Aadhaar Enabled Payment System (AePS) for cash withdrawals; *Others:* Any biometric attendance or verification system.	**Identity theft and unauthorized transactions:** Fraudsters have **cloned fingerprints** using silicone molds to defeat Aadhaar-enabled payment systems, siphoning off money from victims' bank accounts . Lack of additional verification (PIN/OTP) in AePS exacerbates risk. Also, biometric errors can **deny services** to rightful users (authentication failure).	• **Multi-factor authentication:** Complement biometrics with PIN/OTP, especially for financial transactions, to avoid single-point failure .• **Biometric locking & liveness checks:** Encourage users to lock Aadhaar biometrics when not needed ; deploy devices with liveness detection or advanced scanners to thwart fakes .• **Periodic audits:** Check that authentication devices are certified and not compromised .
Unauthorized Data Sharing & Profiling – Function creep of Aadhaar, linking data across domains without proper consent	*All sectors:* E.g. linking Aadhaar with SIM cards, bank accounts, educational records, and other databases. *Private sector services:* E-commerce, travel,	**Privacy erosion and surveillance:** Extensive linking of datasets via Aadhaar enables profiling of individuals' finances, health, and activities **without sufficient consent or transparency** . Risks include targeted marketing	• **Purpose limitation & consent:** Enforce that Aadhaar data is used *only* for the specific service consented to, and require fresh, informed consent for any secondary use .• **Data minimization:** Limit the personal data shared in

Key Risk	Affected Sectors	Potential Impact	Suggested Mitigations
	etc., now using Aadhaar.	or government surveillance of citizens' everyday transactions. Recent rule changes allowing **private entities** to use Aadhaar authentication for "ease of living" raise concern over scope creep without clear limits .	each transaction (e.g. use tokens or digitally "masked" Aadhaar IDs instead of full ID) to prevent unnecessary aggregation.• **Independent oversight:** Establish audits by data protection authorities or independent bodies to detect and deter unlawful profiling or surveillance.
Weak User Control & Consent Mechanisms – Gaps in empowering individuals over their own data	*All sectors:* Citizens often submit Aadhaar copies to telecom providers, banks, hospitals, etc. *Welfare:* Biometrics taken for PDS ration or pension without clear consent process.	**Loss of autonomy and risk of misuse:** Users may not know which agencies hold their Aadhaar data or how it's used. For instance, offline verification (sharing photocopies or QR codes) by entities **not monitored by UIDAI** can lead to misuse of identity info . Until recently, Aadhaar-enabled services like AePS were "on" by default, sometimes used without explicit user consent for each transaction .	• **Enhanced consent framework:** Align Aadhaar processes with the DPDP Act's standards (freely given, specific, informed, *unambiguous* consent) . E.g. require user approval to activate services like AePS, rather than auto-enrollment .• **Consent management tools:** Provide simple dashboards for users to review where their Aadhaar data was used and withdraw consent if desired. Ensure withdrawing consent triggers **data erasure**, per DPDP mandates .• **Licensing of verifiers:** Only permit UIDAI-licensed entities to collect/verify Aadhaar info; penalize unauthorized use of Aadhaar copies.
Legal and Governance Gaps – Misalignment with robust privacy norms;	*All sectors (systemic)* – India's data protection regime vs. global standards (EU	**Compliance and trust issues:** The Aadhaar Act (2016) lacked many modern privacy protections (it did not even define "personal data" comprehensively) .	• **Update laws & harmonize:** Amend the Aadhaar Act to incorporate **data minimization, purpose limitation, and data deletion**

Key Risk	Affected Sectors	Potential Impact	Suggested Mitigations
enforcement weaknesses	GDPR, California CCPA). Also government use of Aadhaar data.	The new DPDP Act (2023) improves the legal landscape but **exempts government agencies broadly** on grounds like national security, allowing potential mass surveillance without oversight . Unlike GDPR, the Indian law has no dedicated category for sensitive biometric data, and enforcement is via a government-appointed Board rather than an independent regulator. These gaps can undermine public trust and international data partnerships.	requirements, bringing it in line with DPDP Act and global principles . Close loopholes (e.g., mandate deletion of Aadhaar data upon consent withdrawal).• **Independent supervision:** Empower a truly independent Data Protection Authority (as GDPR does) to oversee Aadhaar-related processing, including government use. Limit the scope of government exemptions – require judicial or parliamentary review for national-security overrides.• **Transparency & accountability:** Regular transparency reports from UIDAI on data requests, breaches, and compliance audits. Individuals should have easy avenues for grievance redressal and compensation in case of misuse.

Table: Summary of key data-privacy risks in Aadhaar 2.0 and DPI, with affected sectors and suggested mitigation strategies.

Legal and Governance Framework: Aadhaar 2.0 in the Privacy Law Context

Aadhaar Act vs Data Protection Law: Aadhaar was governed by its own law (Aadhaar Act, 2016) long before India had a general data protection statute. This meant that when Aadhaar rolled out, there was *"no appropriate data protection and privacy law"* in place. In 2018, India's Supreme Court upheld Aadhaar's validity for **limited purposes** (allowing it for welfare and

PAN-tax ID linking) but **struck down Section 57**, which had allowed unrestricted private-sector use . The Court underscored privacy as a fundamental right, pushing the government to adopt a proper data protection regime. Finally, in August 2023, India passed the **Digital Personal Data Protection Act (DPDP Act)**, which is slated to **replace the patchwork** of sectoral rules with an overarching framework . The DPDP Act introduces principles similar to the EU's GDPR – e.g. requiring consent or certain "legitimate uses" for data processing, defining rights for individuals, and prescribing penalties up to ₹250 crore for violations . However, the law is high-level and not fully operational yet (rules and a Data Protection Board are forthcoming) .

Alignment Efforts ("Aadhaar 2.0" Governance): Recognizing the need to **modernize the Aadhaar legal framework**, the government in 2025 announced plans to amend the Aadhaar Act to better align with the DPDP Act . Proposed changes aim to embed *"data minimization, data erasure, and stricter limitations"* on Aadhaar data use beyond the original purpose . Notably, one identified gap is that while the current Aadhaar system lets users **withdraw consent** for an eKYC or authentication, it **does not oblige data processors to delete previously collected data** – something the DPDP Act *does* require . Another gap is the lack of clarity in the Aadhaar law's definitions (using narrow terms like "identity information" and "authentication records" rather than a broader "personal data" definition) . Aligning terms and standards will ensure Aadhaar data enjoys the same level of protection as other personal data under the new law.

Government Exemptions and Oversight Concerns: A critical governance issue is the DPDP Act's broad **exemption for government agencies**. The law empowers the central government to exempt any of its departments or bodies from data protection obligations for reasons such as *"security of the State" or "public order."* In effect, an exempted agency could collect and use Aadhaar-linked personal data without adhering to purpose limitation, storage duration, or other safeguards . Combined with separate provisions allowing data to be retained indefinitely and enabling law-enforcement to bypass certain consent requirements, this raises fears of **unchecked surveillance**. Privacy advocates note that such carte blanche powers could facilitate **mass surveillance**, conflict with the Supreme Court's privacy mandates, and undermine citizens' trust . Strengthening oversight is thus a priority – for instance, ensuring the upcoming Data Protection Board of India is independent in practice, and instituting review mechanisms for any government exemption invoked.

UIDAI and Accountability: The Unique Identification Authority of India (UIDAI) administers Aadhaar. Past audits have flagged shortcomings in UIDAI's data security practices. A 2022 audit by the national Comptroller & Auditor General (CAG) revealed that **UIDAI had not ensured adequate safety of data in Aadhaar vaults**, and leaks were often stemming from **poor oversight of external partners** entrusted with Aadhaar data. Essentially, while UIDAI claims "Aadhaar data is fully safe and secure," evidence of recurring breaches (e.g., the infamous 2018 incident where reporters obtained access to the Aadhaar database for ₹500) suggest otherwise.

Governance improvements for Aadhaar 2.0, therefore, include tighter **vendor management**, regular security audits, and **transparency**. It also involves clear liability assignment – if a state government or bank or private company misuses Aadhaar data or suffers a breach, users need avenues for redress. The DPDP Act provides for grievance redressal officers and penalties, but these must dovetail with UIDAI's own grievance handling and the sectoral regulators (e.g., RBI for banks, NPCI for payments) to form a cohesive oversight ecosystem.

In summary, the legal backdrop for Aadhaar is in flux – moving towards stronger privacy guarantees but still with notable weaknesses. "Aadhaar 2.0" governance will hinge on **bridging the gap** between lofty privacy principles and actual practice on ground: updating laws, curbing government overreach, and making UIDAI more accountable to the public.

Technical and Data Security Risks in the Digital ID Infrastructure

1. Data Breaches and Hacks: The centralized repositories of personal data that power India's DPI have proven to be attractive targets for attackers. Aadhaar's database, seeded into numerous government and private systems, vastly increases the **attack surface**. Recent revelations underscore the scale of risk: in late 2023, a cybersecurity firm **claimed that 815 million Indians' data** – including Aadhaar and passport details – was being sold on the dark web. The leaked trove purportedly came packaged with data from the Indian Council of Medical Research, suggesting cross-breach of health and identity databases. While UIDAI officially denied any breach, the **Comptroller & Auditor General's** findings (that Aadhaar data leaks "were largely emanating from client *vendors*" lacking oversight) indicate that even if the central database isn't hacked directly, the *peripheries* (state service portals, partner agencies, etc.) often leak like a sieve. In one notorious case, personal details of **over 130 million Aadhaar holders** (and ~100 million linked bank accounts) were exposed on the web due to misconfigured government websites . Such incidents compromise not only privacy but also **financial security** – leaked Aadhaar and bank info have been used in social engineering scams and illicit withdrawals.

Mitigation: Securing the DPI requires a **defense-in-depth** approach. This includes hardening central systems (Aadhaar data vaults) with encryption and access control, but equally, enforcing security standards among all ecosystem players (state governments, banks, telecoms, hospitals, etc.). Regular **security audits and penetration tests** should be mandated, and any data exchange with Aadhaar (e.g. via APIs) must be logged and monitored for anomalies. The DPDP Act's requirement for breach notification to a central Data Protection Board and affected individuals is a positive step, though it lacks a strict timeline. Instituting a **72-hour breach reporting rule**

(akin to GDPR) and an incident response framework will improve accountability. Additionally, UIDAI can reduce risk by minimizing the personal data it stores or shares – for example, by using **tokenization** (issuing unique tokens for Aadhaar numbers for different agencies, so breaches don't expose the universal ID) and encouraging the use of **offline Aadhaar verification** (where a cryptographically signed QR code or XML is shared by the user, limiting exposure of the core database).

2. Biometric Data Vulnerabilities: Aadhaar's promise of "one identity, one authentication" hinges on biometrics (fingerprints, iris scans, and now facial recognition) as keys to verify identity. But biometric authentication, once compromised, is difficult to reset (unlike passwords). **Cloning of fingerprints** has emerged as a potent attack method. In mid-2023, police in Hyderabad busted a gang that had used silicone casts of fingerprints to fool Aadhaar-enabled Payment System (AePS) devices and drained bank accounts. Investigations in various states found that fraudsters obtained fingerprint images from documents (like those in land registries or loan forms where people submitted Aadhaar copies), created molds, and then made transactions at banking agents or corrupt merchants by impersonating the victim's biometric identity. The AePS infrastructure was particularly vulnerable because it allowed withdrawals with just an Aadhaar number, bank name, and fingerprint – **no PIN or OTP** required as a second factor . This design, meant for rural inclusion and simplicity, unfortunately "negates the need for OTP… leaving the attacker with the task of using a silicone thumb" . Furthermore, many Aadhaar fingerprint scanners use **optical technology**, which is easier to spoof with a fake finger, unlike pricier biometric sensors that detect liveliness via capacitance or ultrasonic waves . Beyond fraud, another consequence of biometric issues is **exclusion**: aging, manual labor, or health conditions can cause fingerprint changes, leading to authentication failures. Indeed, **6% of fingerprint and 8.5% of iris authentications failed** in UIDAI's own 2017 tests . Such failures in welfare delivery (e.g., an elderly person denied rations because the system doesn't recognize their fingerprint) raise equity concerns .

Mitigation: Tackling biometric risks involves both **technical fixes and user awareness**. On the tech side, UIDAI has rolled out options like the **Virtual ID (VID)** – a revocable 16-digit alias that users can generate to mask their real Aadhaar number during authentication . This helps, but specifically for biometric misuse, **locking one's biometrics** is effective: users can lock their fingerprint/iris data via the Aadhaar system when not needed, ensuring any authentication attempt gets blocked (unless they unlock via mobile/OTP for a genuine use). Public education campaigns are needed so that more people use the "lock/unlock" feature, especially if they suspect any compromise. For services like AePS, adding a layer of PIN or mobile OTP (sent to the Aadhaar-registered phone) would drastically reduce fraud, even if it sacrifices a bit of convenience. UIDAI and RBI (for banking) might also enforce **liveness detection standards** – e.g., certifying only fingerprint devices that have anti-spoofing features for use in Aadhaar authentication going forward. Lastly, the principle of **optional alternative authentication** should be adopted widely: no one should be denied an essential service due to biometric failure

without being offered an alternative (OTP to registered mobile, or manual ID verification, etc.), as also emphasized by the Supreme Court.

3. Weak Linkages and Third-Party Applications: Aadhaar's strength – its ubiquity – is also a weakness when it comes to **data linkage**. There are hundreds of government portals and private apps interfacing with Aadhaar. Each linkage is a potential weak link. For example, the **DigiLocker** platform allows users to fetch documents (like driver's licenses or health insurance cards) using Aadhaar eKYC; numerous state scholarship and exam registration sites verify students via Aadhaar; hospitals may pull patient records tied to Aadhaar. If any of these applications implement Aadhaar integration poorly (e.g., not securing the API tokens or storing Aadhaar numbers in plaintext), they could be exploited by attackers to query or scrape personal data. There have been instances of **Aadhaar number enumeration** – insecure APIs allowing attackers to cycle through ID numbers and retrieve details. The **2018 Tribune exposé** showed how, by exploiting lax security on a utility provider's portal, one could gain access to the demographic data of any Aadhaar number. Moreover, **mobile apps** that use Aadhaar (for instance, fintech apps that do instant Aadhaar-based KYC) might cache documents on phones; if the phone or app is compromised, so is the data.

Mitigation: All agencies and developers using Aadhaar authentication must follow **UIDAI's security guidelines and best practices** (e.g., UIDAI provides a detailed authentication **API "playbook" and SOPs**). Implementing **rate-limiting, encryption of data at rest and in transit, and secure coding practices** is essential. The concept of an **"Aadhaar Data Vault"** – isolating and encrypting Aadhaar numbers separately from other personal data in an organization's database – should be enforced so that even if other info is breached, the Aadhaar number (as a key identifier) isn't easily exposed. Additionally, UIDAI could expand the use of **tokenized Aadhaar identifiers** for different sectors (UIDAI already supports a reference ID for the banking sector that isn't usable elsewhere). On the user side, vigilance is key: people should avoid sharing Aadhaar PDFs or photocopies freely, and use the **masked Aadhaar** option (which hides the first 8 digits) whenever a physical copy is needed. Applications like mAadhaar (official app) enable secure QR code sharing of eKYC data, which is preferable to handing over photocopies that can be later misused.

4. Potential Misuse of Authentication Logs and Metadata: Every Aadhaar authentication (whether biometric or OTP-based) generates a log entry – recording transaction details like the Aadhaar used, time, requesting entity, and a yes/no result. Over time, these logs could paint a detailed picture of an individual's activities: e.g., authentication at a hospital, then at a bank, then at a liquor store (if age verification by Aadhaar was used), etc. While UIDAI by law is supposed to retain logs only for a limited period (currently **6 months** as per Aadhaar Act amendments post-2018 ruling) and use them only for grievance handling or legal compliance, there is a **privacy risk if this metadata is misused**. If law enforcement or intelligence gain unfettered

access to Aadhaar authentication logs, they could track persons of interest without judicial oversight, essentially creating a **surveillance trail**. There have been **concerns about government agencies leveraging Aadhaar** for policing – for example, using the Aadhaar database to match fingerprints found at crime scenes, or deploying facial recognition on CCTV feeds against the Aadhaar photo database. The law strictly forbids sharing the core biometric database for such purposes (it can be done only in rare national security cases with high-level approval), but **technological temptation** to repurpose Aadhaar data for security is high. Without robust checks, what begins as an identity system could morph into a tool for **Big Brother**.

Mitigation: The foremost safeguard here is **legal prohibition and oversight**. The current law (post-Supreme Court ruling) disallows using Aadhaar authentication logs or biometric data for anything other than intended purposes, and any national security exception requires a committee approval. These provisions must be enforced in spirit – any agency request for Aadhaar data should require a court warrant or oversight committee nod, and blanket analytics or data mining of authentication records should be off-limits. Technically, UIDAI should ensure logs are **anonymized for analysis** (e.g., for system improvement or fraud monitoring) and automatically deleted after the retention period. An independent audit of UIDAI's handling of metadata could assure citizens that their trail of authentications isn't being misused. In addition, exploring more **decentralized identity models** (as Moody's report in 2023 suggested) could alleviate this risk: e.g., if in the future Aadhaar 2.0 allows offline verification or verifiable credentials that do not "phone home" every time to a central server, then the metadata generated centrally would be minimal . India's push for **self-sovereign identity (SSI)** solutions or a federated identity (as hinted in decentralised ID discussions) might be a way to combine convenience with privacy, though that's a longer-term evolution.

Sectoral Applications: Privacy Risks and Impacts

A. Finance and Banking: The finance sector was one of the earliest adopters of Aadhaar for e-KYC (Know Your Customer) verification. Banks and fintech firms leveraged Aadhaar to instantly authenticate customers for opening accounts, loans, and mobile wallets. This dramatically reduced onboarding time and costs, boosting inclusion. But it also introduced **privacy and security issues**:

- *KYC Data Misuse:* When you complete KYC with Aadhaar, the bank or broker gets a lot of personal information (name, address, date of birth, etc., and in earlier days, even a copy of the biometric or XML data). There is a risk that this data could be **misused or insufficiently protected** by the firm. In 2019, it was revealed that thousands of Aadhaar eKYC packets (which include demographics and often photo) were floating on the internet due to unscrupulous agents re-selling them for identity fraud. Aadhaar 2.0's blockchain KYC proposal explicitly tries to tackle this by giving users more control on

what data is shared. The idea is that instead of handing over all details, a user could consent to share just the necessary fields. Until such user-controlled frameworks are in place, the risk remains that personal financial details obtained via Aadhaar KYC could leak or be sold.

- *Aadhaar–Bank Account Linking:* Over 1 billion bank accounts are now reportedly linked with Aadhaar for direct benefit transfers and such. If Aadhaar numbers are leaked, it potentially links to one's financial accounts. Attackers have exploited this by phishing: e.g., calling people pretending to be from a bank or UIDAI, citing the victim's Aadhaar number and partial data (from a leak) to gain trust, and then extracting OTPs or passwords. Also, as noted earlier, the AePS system allowed for **card-less withdrawals** using Aadhaar data; while great for financial inclusion, it created a new attack vector for fraud.
- *Credit and Insurance Profiling:* With a unified ID, there's a temptation for financial institutions to consolidate profiles. For instance, if all loan records, tax filings, and subsidy receipts are keyed to Aadhaar, a lender might infer creditworthiness or an insurer might infer risk (e.g., noticing someone is receiving health subsidies might signal illness). Such **profiling without consent** would violate privacy and potentially fairness norms. Currently, credit bureaus in India use PAN (tax ID) more than Aadhaar, but as Aadhaar seeding grows, these concerns could become real. Financial data is highly sensitive; misuse could lead to discrimination (denial of services) or predatory targeting.

Mitigations in Finance: Regulatory guidelines by RBI now require that Aadhaar eKYC data be stored securely and not be shared onward without consent. The use of the **'Offline KYC' (XML/QR code)** is promoted, where the user downloads an encrypted XML of their data from UIDAI and gives it to the bank, thereby **eliminating live queries** to the Aadhaar system and limiting data to what's needed. Banks also have started using **masked Aadhaar copies** (showing only last 4 digits) for documentation. Going forward, the **Account Aggregator** framework – part of India's DPI – allows sharing of financial data in an encrypted, consented manner; integrating Aadhaar verification into that with proper consent flows will help. On fraud, NPCI has introduced certain limits and velocity checks on AePS transactions to catch unusual activity, and users are repeatedly cautioned to **never share OTPs or personal info**. Biometric fraud incidents have led to advice that individuals should *lock their Aadhaar when not in use* and unlock only when needed for a transaction . Ultimately, robust implementation of the DPDP Act (which mandates purpose limitation and consent) in the financial sector – and heavy penalties for breaches – will push banks and fintechs to tighten privacy.

B. Healthcare: The healthcare sector handles extremely sensitive personal data, from medical histories to genetic information. India's public health programs have begun integrating with Aadhaar for identification and record-keeping. For example, **Ayushman Bharat Digital Mission (ABDM)** assigns a Health ID (now called ABHA ID) which patients can link with Aadhaar to pull their hospital records. Many states require Aadhaar for benefits like free COVID vaccinations or maternity scheme payments. This raises multiple privacy issues:

- *Health Data Breaches:* A breach of a health database linked with Aadhaar can reveal a patient's identity along with their medical conditions. In one incident, as part of the large dark web leak claimed in 2023, data from ICMR (possibly COVID-19 test data or health research data) was part of the package. If, say, HIV or tuberculosis patient registries are tied to Aadhaar and get leaked, named individuals could face stigma or discrimination. Unlike financial data, health data leakage impacts dignity and can cause social harm.
- *Privacy vs Public Health:* There's tension in linking Aadhaar to health programs. On one hand, **targeted health interventions** (like ensuring a TB patient follows up) become easier if the system knows exactly who the person is and can track compliance. On the other hand, it may **deter people from seeking care** for stigmatized conditions if they know it's all being logged under their ID. Studies noted **patients halting treatment for TB or HIV due to fears of privacy breaches** when Aadhaar linkage was introduced. This chilling effect is a serious ethical concern – privacy lapses could literally cost lives if patients drop out of treatment.
- *Data Sharing with Insurers/Employers:* There is also fear that health data might be shared (or demanded) beyond its initial purpose. For example, an insurance company could request access to a person's unified health record (if ABHA and Aadhaar make it easy) before issuing a policy – this might be *with* consent, but is it truly free consent if refusing means denial of service? Similarly, employers might ask for medical details for insurance or fitness-for-job checks. Without a strong privacy law classifying health info as *sensitive* (GDPR does this, but India's DPDP does not explicitly), there's ambiguity on how such scenarios are handled.

Mitigations in Healthcare: The key is to **segregate health identities** from general identities where possible. ABDM provides an optional Health ID that can be created using Aadhaar or other IDs – users could opt to use a mobile number or a random ID instead of Aadhaar to avoid linking everything back to the central ID. Where Aadhaar is used (for example to verify eligibility for a government health subsidy), systems should store a *tokenized reference* rather than the raw Aadhaar number. Access controls must be stringent – only the patient and authorized healthcare providers should retrieve records, and every access should be logged. The forthcoming Health Data Management Policy under ABDM has rules for consent and data sharing – these need enforcement teeth. *Consent management* could be made very granular: e.g., a patient can consent to share their prescription history with a new doctor for better treatment, but decline sharing of mental health records if not necessary. Technologically, this is being built via consent artifacts in the health stack. Additionally, an independent ethics or privacy board for health data (including patient representatives) could oversee large government health databases to ensure they are used only for public good and not misused for profiling. Finally, awareness is vital: patients should be informed that they have a choice in linking Aadhaar, and that treatment will not be denied if they choose not to provide it (as per Supreme Court, no one can be denied essential services for not having Aadhaar).

C. Welfare and Social Services: Aadhaar was originally justified as a tool to ensure subsidies and welfare benefits reach the right people (eliminating ghosts and duplicates). It is extensively used in programs like PDS (ration distribution), MGNREGA (rural employment payments), LPG gas subsidies, pensions, and scholarships. **Privacy risks in the welfare context** often translate to risks of exclusion and surveillance:

- *Public Exposure of Beneficiary Data:* To promote transparency, many welfare departments published beneficiary lists and payment details online – inadvertently exposing personal data. The 2017 study by CIS in India found **over 13 crore (130 million) Aadhaar numbers and 10 crore bank account numbers** publicly accessible on government websites, as part of PDS and NREGA data dumps . This not only violated privacy but also opened poor villagers to fraud (there were cases of scammers using these lists to call people, posing as officials). Even if such data is later removed, the archives persist. Privacy-by-design calls for aggregate transparency (total numbers, amounts) rather than personal details on public portals.
- *Surveillance and Behavior Modification:* When every welfare service usage is authenticated, it becomes possible for the state to build a **social profile** – knowing if person X is availing food rations, health check-ups, school lunches for kids, etc. In a positive light, this helps ensure multi-dimensional benefits reach those in need. But critics worry it could be used punitively – for example, threatening to cut off one benefit if someone is found using another "undesirable" service, or simply creating a stigma profile (e.g., identifying individuals who take certain disease treatments or welfare aid). There's also a concern of **political misuse**: data could be mined to target voters (for instance, knowing who got housing aid and sending them tailored messages during elections). While there's no public evidence of Aadhaar data being used this way so far, the potential exists if data governance is weak.
- *Mandatory Use and Exclusion:* Despite the Supreme Court's ruling, some local authorities continued insisting on Aadhaar for welfare, and if authentication fails or the person doesn't have Aadhaar, benefits may be denied. This is a violation of rights and also a privacy issue because it forces individuals to use a system and give up data under duress (else lose essential needs). There were reported cases of hunger deaths allegedly linked to Aadhaar authentication failures in ration shops, which show the grave consequences of not having robust fallback processes.

Mitigations in Welfare: **Delink identity from entitlements** to the extent possible – adopt a principle that no one will be denied benefits due to identification issues; instead, they can be verified through alternate means or later verification. This reduces the pressure that might lead to privacy being ignored. Government sites must remove or redact personal identifiers from public reports – use codes or aggregate info only. The DPDP Act's provisions (once effective) would consider publishing someone's personal data without consent as a violation; thus, authorities need to audit their data sharing practices. For surveillance concerns, India could enact policies like **data trust scores or impact assessments** before linking databases – basically analyzing the proportionality and necessity of linking Aadhaar with each welfare scheme, and storing only minimal data (e.g., just store Aadhaar and that subsidy was given, not details of individual's

other programs). Also, community oversight via civil society can help – social audits that include checking privacy compliance (not just financial compliance) in welfare delivery. The **Aadhaar 2.0 idea of "suspicious usage pattern tracking"** could be double-edged – it might catch fraud, but might also track individuals – so it should be implemented with privacy safeguards (flag anomalous activity of cards in aggregate, not personal profiling).

D. Other Sectors (Telecom, Education, etc.): Aadhaar has permeated into obtaining mobile SIM cards (e-KYC for SIM activation), education (scholarship applications, exam registrations, even attendance monitoring in some schools), travel and hospitality (some hotels allow Aadhaar-based check-in, and the government had proposed Aadhaar-based airport entry). Each of these applications carries familiar privacy risks:

- *Telecom:* SIM card registration via Aadhaar was very common until the 2018 court judgment forbade mandating it. During that time, there were reports of **agents storing fingerprint scans** and later using them to issue fake SIMs or even link to bank accounts. One high-profile case saw a person's Aadhaar used to procure dozens of SIM cards by criminals, leading to police knocking on the innocent person's door when those SIMs were misused . Now SIM verification can be done through alternate IDs or a voluntary Aadhaar OTP. The lesson is that whenever a private business uses Aadhaar, there must be strict controls to prevent **data reuse** beyond the transaction.
- *Education:* Students have had to give Aadhaar for board exam registration, which raised concerns when databases like the National Scholarship Portal were breached. Students are minors, so parental consent issues arise too (the DPDP Act mandates **verifiable parental consent for under-18 data**, which Aadhaar systems must incorporate). Privacy in education also intersects with surveillance if Aadhaar is used to track attendance or performance of students across schools.
- *Travel and Other Services:* As Aadhaar-based authentication becomes available "anytime, anywhere" for private companies , one could envision routine activities like checking into a hotel or boarding a train via Aadhaar scan. While convenient, it means more entities collecting identity data and possibly **location and activity data**. Without robust data protection obligations, a hotel could potentially share Aadhaar-based check-in info with data aggregators or law enforcement without guest knowledge, infringing on the right to privacy of movement and anonymity in public.

Mitigations in Other Sectors: For telecom, the regulator (TRAI) and DoT have issued guidelines that **no Aadhaar biometric data is to be stored** by operators and that they should use the UIDAI's licensed devices/SDKs which don't expose the raw biometrics. Compliance needs to be audited. In education, perhaps use **alternate IDs for children** or limit Aadhaar use only to certain necessary areas (like one-time verification for exam registration, not continuous tracking). Any data collected for educational purposes should not be repurposed (e.g., to profile students) without consent. For new private-sector uses, the government's move to provide SOPs and a portal for onboarding is good – it means those who want to use Aadhaar auth must register

and agree to terms. **Data minimization** should be a condition – e.g., if a hotel only needs to verify age and name, the Aadhaar authentication should ideally return just a yes/no or those two fields, not the person's entire identity record. Technology like **UIDAI's eKYC "yes/no" authentication** (which simply confirms if a person's name and Aadhaar match, for instance) can serve such needs. Finally, there is a need for **privacy awareness training** in all organizations using Aadhaar: employees handling customer Aadhaar info (be it a telco store clerk or a college administrator) should be sensitized that this data must be handled carefully and lawfully.

Emerging Developments: Aadhaar 2.0 and New Mitigation Technologies

As India upgrades its digital identity infrastructure, several new initiatives are underway to address past weaknesses and future demands:

- **Aadhaar on Blockchain (Self-sovereign Identity):** A research consortium (IDRBT, IIIT Hyderabad, IIT Bhilai) is working on a blockchain-based platform for a unified digital identity, often dubbed *"Aadhaar 2.0"*. The goal is to enable citizens to **store and share their identity attributes in a tamper-evident ledger** and give granular consent for each sharing. This could enhance security (blockchain's immutability and distributed trust) and user control (no central silo holding all data, and the user decides what to expose). It might also allow continuous availability (your data is on a decentralized network, accessible 24/7). However, privacy experts will watch for how the system handles the **right to erasure** and modification – blockchain's strength (immutability) can conflict with the need to delete or correct personal data. One must ensure that personal data is not written irreversibly to the ledger; instead, perhaps pointers or encrypted blobs that can be turned off. Additionally, **key management** becomes crucial: if the user truly "owns" their digital identity (like a private key controlling access), losing it could be catastrophic, and theft of it could allow impersonation. Thus, Aadhaar 2.0 blockchain designs should incorporate key recovery mechanisms and robust authentication to use one's keys. As this is still exploratory, no sensitive deployment is live yet.
- **Face Authentication and Multi-modal Biometrics:** UIDAI has introduced **face recognition** as an additional mode of authentication, useful for those with worn fingerprints or aged irises. In 2022–2023 it was used in conjunction with fingerprint/iris for verifying pensioners and others. By 2025, **face authentication was opened to private entities** as well . While multi-modal biometrics can improve success rates and user convenience, face data introduces new privacy concerns. Face recognition can be done passively (without active consent) if one has access to cameras, raising specter of mass surveillance. If private apps start using face auth via Aadhaar, one must ensure the **live photo captured isn't stored or misused** beyond the immediate authentication. UIDAI has a "registered device" protocol to secure capture devices – that needs to extend to phone cameras capturing faces. Also, India lacks a specific law regulating facial

recognition use (unlike some jurisdictions). It would be wise for UIDAI to issue guidelines: e.g., prohibiting analysis of face images for anything other than one-to-one authentication (no emotion detection or profiling), and disallowing law enforcement from grabbing those face images from private authentications. Technically, **liveness detection** (to ensure it's not a photo or mask) and encryption of face data in transit are implemented, but ongoing oversight is needed.

- **Offline Verification and mAadhaar:** To reduce the need for sharing Aadhaar numbers or biometrics widely, UIDAI has boosted offline verification tools. The **QR code on Aadhaar cards** now contains most demographic info plus photo in signed form – agencies can scan it to verify authenticity without hitting the UIDAI server (thus not generating a traceable log at UIDAI side). The **mAadhaar mobile app** lets users generate time-bound OTPs and share e-copies with a "masked" ID. These are privacy-friendly moves because they localize the verification and give the user more agency. The risk, however, is if relying parties do not honor the limited data principle – e.g., after scanning a QR code, an unscrupulous entity could still save the data or the image. That's why the earlier point of licensing and audit of all entities comes in: even offline, if you misuse data, there should be penalties.
- **Data Empowerment & Protection Architecture (DEPA):** This is India's broader framework for consent-based data sharing through "consent managers." It is being applied in banking (via Account Aggregators) and potentially upcoming in health and other sectors. Aadhaar 2.0 will likely plug into DEPA, meaning **users can seamlessly but safely share their data** (like bank statements, or educational certificates) for a specific purpose. DEPA ensures data is encrypted end-to-end and the consent is fine-grained and logged. This is a positive development for privacy *if* done right, as it moves away from blanket consent to each transaction having a scope. The mitigation need here is to avoid **consent fatigue** – if users blindly click "Yes" to share data via consent managers, it's no better than not having consent. Usability research and perhaps adaptive defaults (like reputable purposes being pre-approved in some way) will be key so that it doesn't become too burdensome and thereby ignored by users.

In conclusion, the technological upgrades in Aadhaar 2.0 show promise in **bolstering security and giving users more control**, but they must be coupled with strong policy and oversight to truly reduce privacy risks. India's DPI is at a crossroads where it can set a global example of how to balance scale and convenience with individual privacy rights.

Comparison with Global Data Protection Frameworks (GDPR and CCPA)

To put India's data-privacy landscape in perspective, we compare key aspects of India's approach (especially regarding Aadhaar 2.0 and DPDP Act) with the **European Union's GDPR** and **California's CCPA/CPRA** frameworks.

Legal Basis and Scope: The EU's GDPR is often seen as the gold standard for data protection. It applies broadly to *all* personal data (whether digital or physical) of individuals in the EU, and has extraterritorial reach. India's DPDP Act is narrower in scope – it covers only **"digital personal data"**, i.e. data that is collected or processed in digital form . This means, for instance, a physical paper record not intended for digitization might not be protected (though in practice most data is digitized now). Both laws assert that they apply to foreign companies dealing with their residents' data . CCPA (California Consumer Privacy Act), by contrast, is limited to for-profit businesses meeting certain thresholds and concerns data of California residents. CCPA doesn't cover government entities or nonprofits, whereas GDPR and DPDP apply to any "data fiduciary" including government departments (unless exempted). In the Aadhaar context, this means GDPR would *in theory* regulate something like UIDAI if it processed EU persons' data, whereas DPDP has clauses letting Indian government bodies be exempt – a divergence in accountability .

Consent and Lawful Processing: GDPR offers multiple bases for processing (consent, contract necessity, legal obligation, vital interest, public task, legitimate interests), but it places strict conditions on consent (must be freely given, specific, informed, unambiguous, and revocable). India's DPDP Act is actually **more consent-centric** in a way – it requires consent for most processing, with a few "legitimate use" exceptions like government functions, court orders, medical emergencies, or employment purposes . Notably, DPDP **does not include "legitimate interests" or "contract" as broad bases** – so companies can't just skip consent by claiming it's required for a contract, which is a stricter stance in theory. For Aadhaar, originally the system worked on a form of consent (you had to willingly provide your biometric/OTP), but it was often bundled (try getting a SIM card without Aadhaar in 2017 – practically impossible). Going forward, aligning with GDPR/DPDP means **making consent real and retrievable** – no coercion (alternatives must exist for those who refuse), and records of consent. The Aadhaar Act amendments aim to solidify this: e.g., **purpose-specific consent** for each authentication, and easier withdrawal . California's CCPA, interestingly, doesn't always require consent except for children's data or sale of data – it instead gives a right to opt-out of sale of data and mandates notices. So CCPA is less stringent on upfront consent than GDPR/DPDP; it's more about transparency and control. In practice, Aadhaar's use by private firms would likely satisfy CCPA by just disclosing in a privacy policy, whereas GDPR would require more active justification (probably seeking consent due to lack of other bases after the Supreme Court ruling against using Aadhaar data freely in private sector).

Individual Rights: GDPR grants a suite of rights – access, rectification, erasure ("right to be forgotten"), restriction of processing, data portability, and objection to processing (especially for marketing or when based on legitimate interests), plus rights around automated decision-making. DPDP Act has some similar rights: **access** (or essentially the right to know what data is held and to get summary information), **correction and erasure**, and the right to **grievance redressal** . However, there are differences: DPDP doesn't explicitly mention data portability or the right to object/opt-out (since it doesn't have a concept of processing on "legitimate interest" basis that one would object to). Also, GDPR's right to erasure is broad (can include search engines delisting results, etc.), whereas India's DPDP is more narrow – you can ask for deletion of your data from a data fiduciary if it's no longer needed or if you withdraw consent. For Aadhaar, even before DPDP, there was a provision to lock your biometrics and to revoke consent for eKYC (which would make the KYC data stored by service providers invalid for reuse). But users could not easily get their Aadhaar number or biometric data *deleted* from a service provider's database. Under DPDP, once enforced, if you withdraw consent, the bank or telco should delete your eKYC data (unless required by law to keep). Comparing to CCPA/CPRA: Californians have the right to know what categories of data are collected and to delete personal data (with some exceptions), and as of CPRA (2023) they can correct data and limit use of sensitive personal data. Biometric data in CCPA is considered sensitive, giving the right to limit its use. India's law doesn't differentiate sensitive data – all personal data is more or less treated the same, which **could be seen as a weakness** because things like biometrics, health, or financial info arguably merit stricter handling. The Aadhaar system internally treats biometrics carefully (e.g., encrypted transmission, not sharing them except for matching), but the legal framing doesn't give additional rights to individuals over biometric data versus other data.

Data Security and Breach Accountability: GDPR requires organizations to implement appropriate security and mandates **breach notification within 72 hours** to authorities (and to individuals if high risk). DPDP Act requires entities to **notify the Data Protection Board of India of breaches** and possibly the affected users, but it does *not specify a timeline*. This open-ended timeline is a weakness – it might be defined in rules, but currently there's flexibility that could delay letting people know. CCPA doesn't have a breach notification clause within it (California has other laws for breach notification), but it does allow consumers to sue for data breaches under certain conditions (statutory damages if a business's lack of security leads to a leak of certain ID info). India's DPDP Act *does not provide for individual private lawsuits* for breaches; enforcement is solely through the Data Protection Board's fines. So if Aadhaar data leaks, under GDPR an EU citizen could complain to a DPA and possibly get compensation; under CCPA a Californian could sue in court if certain data (including biometric or ID numbers) were leaked due to negligence; an Indian citizen under DPDP would rely on the Board to investigate and fine, with maybe some indirect remedy. This **difference in enforcement and remedy** is important.

Regulatory Oversight: GDPR is enforced by independent Data Protection Authorities in each member state, coordinated by a European board. CCPA initially by California's Attorney

General, now also a dedicated California Privacy Protection Agency (CPPA) – an independent state agency. India's model is a **Data Protection Board** appointed by the central government, which has raised questions about independence. There is no independent "commissioner" akin to Europe. The Board can impose fines and issue directions but is structurally within the executive's purview. For something as politically sensitive as Aadhaar, an independent regulator might have been better to build credibility (for example, ordering UIDAI to pause some service if risky, or auditing government programs impartially). The current setup might face constraints if, say, a breach involves a government agency – can the Board freely penalize a ministry? That remains to be tested.

Government Access and Surveillance Safeguards: GDPR allows exceptions for national security, etc., but those are meant to be used narrowly. It also has the concept of Data Protection Impact Assessments and prior consultation if a project poses high risk (imagine if Europe were to roll out an "Aadhaar"; GDPR would likely require a thorough privacy impact assessment and mitigations in design). India's DPDP Act has a concept of classifying some data fiduciaries as "significant" and requiring them to do audits and maybe DPIAs, but details are pending. Importantly, as noted, the Indian law explicitly allows the government to exempt itself and its agencies wholesale . CCPA doesn't regulate government at all (only businesses), but residents are protected from government overreach by other laws (and public pressure). In India, aside from the constitutional right to privacy, there isn't a dedicated privacy oversight for government surveillance (no equivalent of, say, a Privacy and Civil Liberties Oversight Board). This is an area of weakness if we benchmark globally. The Aadhaar database by law cannot be accessed for criminal investigation except in national security with high approval, which is *some* check, but broader data intelligence using Aadhaar seeding is still a grey zone.

Strengths and Weaknesses Summary: India's strengths with DPDP (as it relates to Aadhaar) include a **clear emphasis on consent**, hefty fines to push compliance, and modern concepts like data principals' rights and data audits for large entities – all influenced by GDPR principles. Aadhaar-specific laws add additional security mandates (encryption, secure devices) that align with protecting biometric data. India's push for **DPI with privacy (DEPA consent managers, etc.)** is somewhat pioneering on a global scale. However, gaps remain: the **broad government exemptions, lack of sensitive-data categorization, and a not-fully-independent regulator** are often cited as points where India's framework is weaker than GDPR . Compared to CCPA, India's law is actually more stringent on paper (CCPA is more limited in scope and doesn't mandate many practices beyond transparency and honor opt-outs). But in practice, a law like GDPR is backed by strong enforcement and a culture of privacy in organizations – India will need to cultivate similar seriousness. Aadhaar 2.0 will succeed privacy-wise if it not only follows the letters of DPDP Act but also the spirit of global privacy norms – data minimization, user empowerment, and accountability at every step.

Conclusion and Recommendations

Aadhaar and India's expanded digital public infrastructure stand at a pivotal juncture. They have undeniably **revolutionized service delivery**, making transactions cashless, presence-less, and paperless across the country. Yet, the very centralization and pervasiveness that give DPI its power also amplify the **risks to data privacy**. As detailed in this report, sectors from finance to healthcare to welfare each face specific vulnerabilities – from cloned fingerprints enabling bank fraud, to health records potentially leaking and harming patients, to welfare data being misused for profiling. The legal landscape is catching up (with the DPDP Act 2023 bringing a long-awaited privacy regime), but effective implementation is the key. India must strive to enforce **privacy by design** in all new digital initiatives, especially Aadhaar 2.0, treating personal data as a sacred trust.

Recommendations Summary: Going forward, India should **institutionalize strong governance** for Aadhaar – perhaps an independent watchdog or parliamentary committee specifically reviewing its operations, given its critical importance. It should push pending **Aadhaar Act amendments** that introduce data deletion, purpose limitation, and hefty penalties for misuse, as promised . Technical upgrades must continue – e.g., improving biometric accuracy and security, offering easy-to-use features for citizens to control their data (lock, unlock, virtual IDs, etc.). Crucially, a cultural shift towards **data ethics** is needed among both government agencies and private partners: collecting only what is necessary, securing what is collected, and respecting user consent at all times. Lessons can be drawn from GDPR on empowering individuals – for instance, consider adding a right to data portability (so users could extract and port their verified identity data to a different system if needed) and a stronger right to erasure that might even allow one to disengage from Aadhaar if they choose (within reason, given it's used for subsidies).

On comparing with global frameworks, India's approach can be seen as an attempt to balance innovation and protection. Aadhaar's scale is unprecedented, so the world is watching how India addresses the privacy concerns that come with it. By plugging the gaps – such as narrowing government exceptions and ensuring truly independent oversight – India can move closer to GDPR-level robustness. Meanwhile, it can also serve as a model for many developing nations (as seen by countries adopting aspects of India's DPI) by demonstrating that **digital public infrastructure can be privacy-respecting and secure**. The next few years (2023–2025 and beyond) will be crucial: as the DPDP Act comes into force and Aadhaar 2.0 initiatives roll out, effective enforcement and constant vigilance against misuse must be prioritized.

In sum, **Aadhaar 2.0's success will not just be measured in how many services it powers or how many seconds an authentication takes, but in how well it safeguards the rights of the 1.4 billion individuals it represents**. Ensuring data privacy is protected across all sectors of India's digital ecosystem isn't just a legal mandate – it is essential for sustaining public trust in the technology-driven transformation of governance and society.

Sources:

1. Pandey, P. & Shukla, A. *Approaches to Digital Public Infrastructure in the Global South – Case Study: India* (CSIS, 2023) – India's DPI layers and challenges.
2. Jagmeet Singh. *"India expands Aadhaar authentication for businesses, raising privacy concerns."* – TechCrunch (Feb 2025).
3. *Editorial: "Aadhaar data bust raises fresh safety and privacy concerns."* – New Indian Express (Nov 2023).
4. Barkha Kumari. *"Lock Aadhaar biometrics to prevent fraud: Experts."* – Deccan Herald (Dec 2023) .
5. Dipti Yadav. *"Cloning fingerprints, Fake shell entities: Is your Aadhaar as safe as you may think."* – India Today (Jun 2023) .
6. Amlegals. *"Data Privacy in the Context of Aadhaar and India's Digital Identity Systems."* (2023) .
7. ET Legal. *"Govt plans amendment to Aadhaar Act for enhanced privacy and consent controls."* – Economic Times Legal (Apr 2025) .
8. Mimansa. *"Govt Allows Private Entities to Use Aadhaar for Face Authentication, Raising Privacy Concerns."* – Medianama (Mar 2025) .
9. Sarasvati T. *"Moody's Review of Aadhaar Project Irks the Government… Are concerns unfounded?"* – Medianama (Sep 2023) .
10. Sinha, A. & Kodali, S. *"Information Security Practices of Aadhaar (or lack thereof)"* – CIS Report (2017) . (Historical context on leaks)
11. Latham & Watkins LLP. *"India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison."* (Dec 2023) .
12. Medianama. *"Fifteen major concerns with India's Data Protection Bill, 2023."* (Aug 2023) .