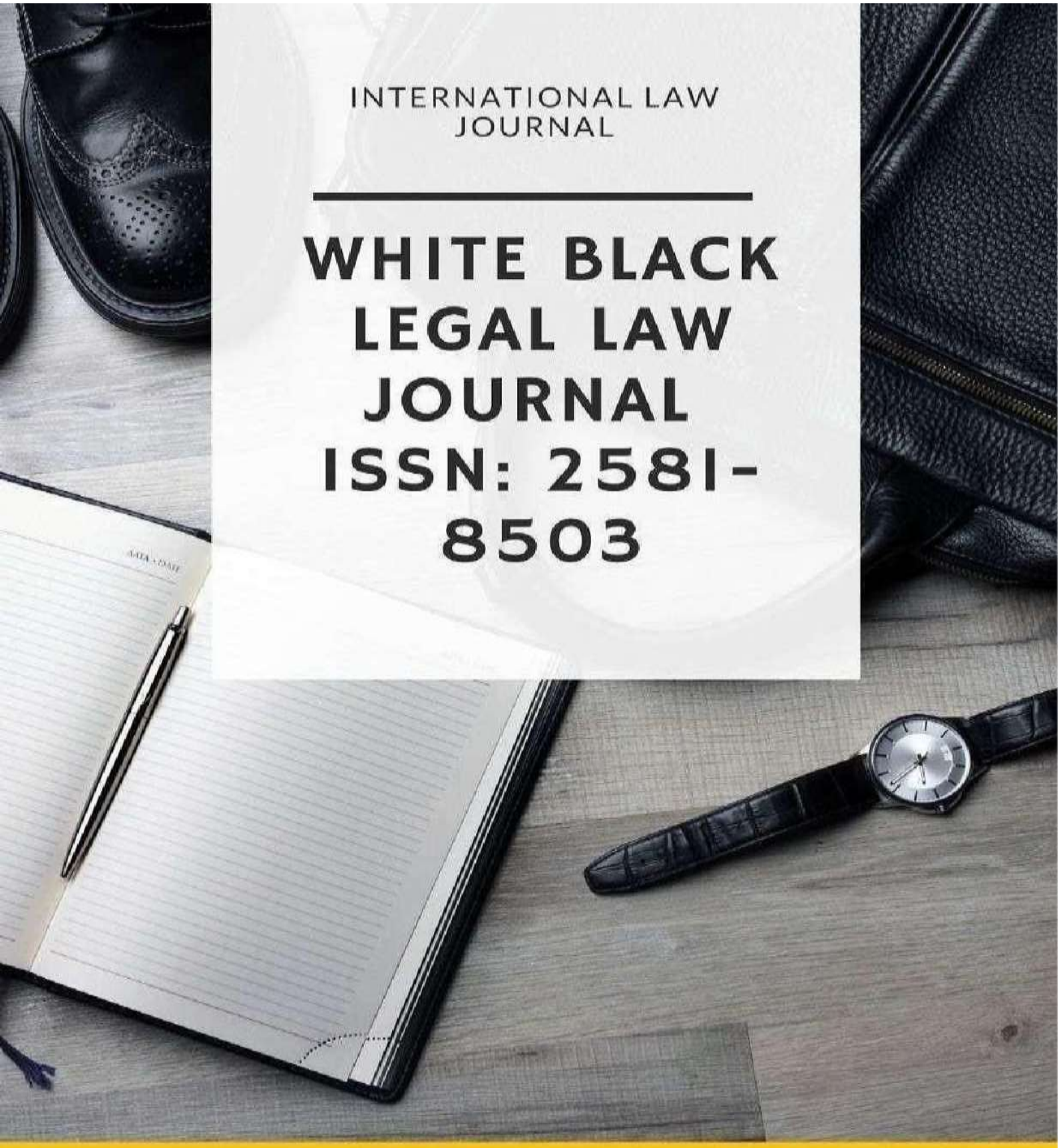

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

www.whiteblacklegal.co.in
Volume 3 Issue 4 | Feb 2026 ISSN: 2581-8503

DIGITAL PERSONAL DATA PROTECTION IN INDIA: ADDRESSING AADHAAR LEAKS THROUGH LESSONS FROM US PRIVACY LAW

AUTHORED BY - SHRISTY
Christ (Deemed To Be) University, Pune, Lavasa Campus

ABSTRACT

India's approach to digital governance has profoundly influenced delivery of public services, with others serving as a foundational element of the transformation. Aadhar has enhanced efficiency, inclusivity and transparency; persistent data breaches have exposed significant governance and security deficiency in the nation's data protection system. The Digital Personal Data Protection Act, 2023 was established to defend individual privacy rights; however, specific structural shortcomings particularly with enforcement state exclusion and regulatory independence, persistently remind safeguarding of Aadhar link personal data. This paper examines the reoccurring incident of Aadhar related breaches, assess the limitations of the DPDP Act, and offer a comparative analysis of US privacy law, with particular focus on the enforcement framework of the Federal Trade Commission. Despite differing constitutional principles, administrative framework and welfare models of India and the United States, the enforcement model reveals substantial insight regarding deterrence, liability and regulatory autonomy. The primary assertion is that India's challenge lies not in the absence of legal provision, but rather than in the deficiency of credible enforcement that holds government officials accountable. This study examines necessary reform to cultivate a responsible, transparent and resilient Aadhar ecosystem, emphasizing US enforcement principles.

KEY WORDS

Aadhar Digital Governance, Data Protection, Privacy Legislation, Digital Personal Data Protection Act 2023, Enforcement Mechanism, Regulatory Oversight, Data Breaches, Feder Trade Commission, Comparative Privacy Framework, Accountability, Institutional Vulnerabilities.

I. INTRODUCTION

India's digital transformation has redefined its governance framework, enhancing welfare distribution, regulatory mechanism and public service delivery. Central to this transition is the world's largest digital identity system, which was initially meant to streamline welfare service and prevent leakages in subsidy delivery.[1] Overtime Aadhar has got embedded in a broad range of sectors including telecommunications, banking to healthcare, education and the civic registration making it one of the most expensive identity infrastructure globally.[2] However Aadhar has bought with its tremendous risk throughout the past decade India's has witnessed multiple cases in which Aadhar related data has been exposed through insecure state websites, improperly designed databases, negligent third-party handling.[3]These breaches have not resulted from sophisticated cyberattacks, but from systematic deficiency is showing shortcomings in governance, supervision and enforcement. Sensitive details like Aadhar numbers, demographic information and welfare record have been made publicly accessible evaluating persistence institutional weaknesses.[4] The digital person data protection act 2023 was enacted in response to increase the concern regarding privacy and data governance.[5] Though portrayed as a comprehensive reform, the act leaves vast exemption for government bodies, lacks independent regulatory authority and provides limited parts for accountability.[6] Consequently, the government acts despite being liable for most Aadhar related breaches with no penalty for abusing personal data. The United States, despite lacking a unified privacy act, has established a powerful enforcement ecosystem suited in the federal trade commission, industry specific privacy loss and court recognition of privacy losses. The American model compromises harsh penalties, rigorous oversight and a culture that values accountability and deterrence. This article explores why Aadhar leaks remain ubiquitous, assesses the weakness in India's enforcement structure and compares the difficulties with US privacy enforcement measures.[7]It argues that Aadhar challenges are rooted in institutional design and weak enforcement, rather than technological limitations and proposes reforms tailored to India's welfare driven context.

[1] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, No. 18 of 2016, Statement of Objects & Reasons (India).
[2] *Justice K.S. Puttaswamy (Aadhaar) v. Union of India*, (2019) 1 SCC 1 (India).
[3] K. Rathee, *Aadhaar Data Leak: What Went Wrong?*, Indian Express (May 2018).
[4] Internet Freedom Foundation, *Aadhaar Breach Tracker* (2021), https://internetfreedom.in.
[5] Digital Personal Data Protection Act, No. 22 of 2023, Gazette of India (Aug. 11, 2023).
[6] Id. 17–18 (government exemptions); 27 (Data Protection Board).
[7] Vrinda Bhandari & Renuka Sane, *Aadhaar: Legislative and Regulatory Gaps*, NIPFP Working Paper No. 215, at 11–14 (2017).

II. LITERATURE REVIEW

The research on the system of digital identity and privacy governance in India has gained widespread scholarly rooted interests within the last few years. Early academic work is mostly concerned with the legal and constitutional aspects of Aadhar, especially following the acknowledgement by the Supreme Court of the privacy as a fundamental right[8] of the subject, much of this writing discusses the issue of surveillance, data centralization, and the possibility of exclusion in service provision.[9] Scholars also had doubts over the sufficiency of the act 2016 of the Aadhar in protecting the personal data and expressed question marks on the regulation capability of the UIDAI.[10] Much Indian research explores the Aadhar operational risk of insecure welfare data, vulnerabilities and authentication systems and distribution of Aadhar photocopies and in the enrolment and verification process via the use of third-party vendors. Numerous authors are in agreement with the fact that Aadhar has its greatest weaknesses not in the central biometric database itself but in the ecosystem[11] around it. The main issue of concern has been brought to the decentralized nature of the welfare platforms and unequivocality of data protection practices across states. Scholarships, especially the US international one, have adopted an extremely different dimension. Instead of even constitutional questions, American writers tend to explore how these agencies are enforced, the regulatory components of the agencies such as the FTC and the place of sector-specific privacy laws. Research findings reinforce the importance of such enforcement with penalties and compliance orders along with long-term consent decrease in molding the organizational behavior and developing the cultures of safeguarding the data in the public and in the private spectrums. A typical benefit of a comparative study between India and international standards like GDPR is that India has no autonomous data regulation, the government exemption is discretionary, and no effective breach liability policies. Scholars also pointed out that the Aadhar system in India is a welfare project that needs a new regulatory paradigm as compared to the western paradigm which places an individual autonomy over the administrative effectiveness. In spite of this abundance of scholarship, there are a number of gaps. The failure of enforcement[12] has not been directly associated with recurring Aadhar leak and much of the Indian literature. Reason being that, few studies determine the extent to which exemptions that

[8] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (India).
[9] Usha Ramanathan, *Aadhaar: Surveillance, Profiling and Identity*, 52 Econ. & Pol. Weekly 38 (2017).
[10] Reetika Khera, *The UID Project and Its Limitations*, 45 Econ. & Pol. Weekly 38 (2011).
[11] Vrinda Bhandari & Renuka Sane, *Aadhaar: Legislative and Regulatory Gaps*, NIPFP Working Paper No. 215, at 9–14 (2017).
[12] Amber Sinha, *The Identity Trap: Aadhaar and Other Identity Technologies* 76–82 (2020).

are enjoyed by government acts directly lead to outgoing weaknesses.Furthermore, how the potential of the US enforcement mechanisms, in particular, FTC veteran based model can be ascertained in the Aadhar governance context is yet to be explored. This paper aims at addressing these gaps by focusing on the area of enforcement and accountability as the main harm of the long-term data protection capability of Aadhar.

III. THEORETICAL AND CONCEPTUAL FRAMEWORK

The present paper concentrates attention on three interrelated article structures to assess the regulatory and institutional issues of the Aadhaar system and the data protection level in India in general.

1. Regulatory enforcement theory emphasises that good governance lies not on the roots but on effective enforcement as follows, under this theory both the private and the public players play their roles to respond to expected meaningful punishment of a rule violation. Deterrence thus entails the fact that responsibility is clearly assigned to people, that punitive measures are commensurable and regularly instituted and that compliance is monitored by independent auditors. Failure of consistency or selectivity in enforcement also gives minimal motivation to actors to comply with the loss, creating systematic failures. As a matter of fact, the governance challenges of Aadhar point directly to the confusion of legislation on paper and implementation in practice.[13]
2. The accountability-oriented system of data protection emphasizes proactive risk management, rather than a check box attitude toward compliance. It argues that any business operating with personal data must have firm protection measures which include proactive risk reduction measures, periodic in-house audits, well-defined governance strategies, and a powerful breach control system. But accountability on the Aadhar system is not well spread. Most of the government organizations that are the biggest custodians of Aadhar have exemptions under accountability requirements.[14] Consequently, the system has been left open and susceptible to a series of database intrusions.
3. Study staff an associated legal approach, by examining how other jurisdictions at practice privacy and data protection laws to shape India approach in this specific instance, the emphasis is on the enforcement context of the United States, where

[13] *Justice K.S. Puttaswamy (Aadhaar) v. Union of India*, (2019) 1 SCC 1, 447–52 (India).
[14] Digital Personal Data Protection Act, No. 22 of 2023,17–18 (India).

organizations such as the Federal Trade Commission[15] resolve the notion of privacy infrastructure, as well as penalties, compliance audits, and lawsuits to address instances of violations of privacy law.This comparative framework does not imply wholesale importation of the practices in the United States but to extrapolate pieces of the enforcement model that can be translation to India retributive welfare ethos.

IV. RESEARCH METHODOLOGY

The article adopts a combination of doctrinal and comparative methods of evaluating the legal and institutional processes that govern Aadhar and data protection in India. The doctrinal part involves the thorough examination of fundamental documents on the law, such as the Aadhar Act, 2016, the Digital Personal Data Protection Act, 2023, major judicial rulings, and policy guidelines that have been announced by UIDAI, along with publicly published instances of Aadhar related violations.[16]

These resources contribute to making the regulatory framework clear, clarifying the burden imposed on various actors, and revealing the common governance vices. This is supplemented by the comparative dimension that examines the applicable US law most significantly the Federal Trade Commission Act and many industry specific privacy laws to come up with enforcement provisions that can be adapted to the Indian context.[17] The study is qualitative in nature and addresses more general structural issues as design of regulation, institutional responsibility, enforcement mechanisms and systematic weaknesses. One of the main limitations of this systematic approach is that there will be no access to sensitive internal audit or proprietary government databases which limits the investigation to the material that will be available in the publicly accessible sources.[18] However, recurring patterns to be gained through statutory interpretation, documented violations and regulatory operations furnish a rigorous enough framework on appraising the breaches of the existing data protection landscape in India.

[15] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583, 600–12 (2014).
[16] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, No. 18 of 2016 (India); Digital Personal Data Protection Act, No. 22 of 2023 (India); Unique Identification Authority of India (UIDAI), Circulars & Notifications, https://uidai.gov.in; Internet Freedom Foundation, *Aadhaar Breach Tracker* (2021), https://internetfreedom.in.
[17] Federal Trade Commission Act, 15 U.S.C. § 45(a); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583, 600–12 (2014).
[18] Vrinda Bhandari & Renuka Sane, *Aadhaar: Legislative and Regulatory Gaps*, NIPFP Working Paper No. 215, at 12–15 (2017).

V.AADHAR'S STRUCTURAL AND ADMINISTRATIVE VULNERABILITIES

The basic technology backbone of Aadhar has generally been viewed to be secure but the most critical weaknesses of the system were the general institutional ecosystem that governs Aadhar related information. Such risks are caused by incoherent administrative bodies, absence of uniform security measures, and ineffective controlled systems. Although biometric data are sorted at a central repository, Aadhar numbers and demographic data are regularly handled by a multitude of disparate actors in such a way that they have highly unequal technical capacity and security maturity, leading to extremely uneven approaches to data protection as well as offering several areas of vulnerability. These vulnerabilities are magnified by the fact that security protocols are not standard and binding across states. UIDAI[19] can provide guidelines on how to protect the data of Aadhar, but these measures are usually more of a suggestion and are not well implemented, which leads to the recurrent issues, like publicly available lists of beneficiaries, unprotected authentication trail, unencrypted data transfer, and use of outdated digital infrastructure. Since the Aadhar authentication has been integrated with hundreds of benefit systems, sensitive personal information is stored, transmitted and circulated on multiple platforms, increasing the attack surface, instead of reducing it. The level of oversight is also sufficient because the governance system of Aadhar does not add to frequent, independent audits of state level databases. The monitoring by UIDAI is more oriented on the side of the private actors that enable the governmental systems wherein most of the leaks exist to go unscrutinized.[20] Consequently, the violations tend to be left unnoticed over a long time, the administrators have minimal motivation to alter their security policies and the correction procedures, and even the failures are frequently uninitiated. Even the lack of personal or institutional responsibility to carelessness is near complete and adds to this difficult situation. When government departments and officials are not liable to legal consequences[21] or even monetary fines in the event of Aadhar-linked data mishandling, the occurrence of security breaches is regularly attributed to a minor administrative issue as opposed to a serious offense. With time, this non-conformity has inculcated lax behavior of handling sensitive information, which has made it easy to perpetuate other instances of attack on the Aadhar ecosystem.

[19] Unique Identification Authority of India (UIDAI), *Security Guidelines for Aadhaar Ecosystem* (2017), https://uidai.gov.in.
[20] Internet Freedom Foundation, *Aadhaar Breach Tracker* (2021), https://internetfreedom.in.
[21] Vrinda Bhandari & Renuka Sane, *Aadhaar: Legislative and Regulatory Gaps*, NIPFP Working Paper No. 215, at 13–17 (2017).

Therefore, the main biometric repository can be resistant; however, the administrative ecosystem around it is heterogeneous, weekly governed, and suffers from systemic failures.

VI. Restrictions of the Digital Person Data Protection Act, 2023

It is the first effort to create an encompassing legal system of protecting personal data in India, but the Digital Personal Data Protection Act, 2023 is gravely flawed in the form of structural loopholes that outweigh any meaningful responsibility in favor of administrative convenience. Among the most urgent problems of the extremely broad authority bestowed on the central government to absolve any of its agencies of the principal requirements of this act, even such as compliance obligations, penalties against contravention, the limitation of the methods in which personal data may be handled, and even the very rights that are naturally pertinent to data principles.[22]

The fact that most of the data breaches associated with Aadhar were the result of government run websites and welfare schemes makes this set of exceptions a complete undermining of the whole idea of data protection regulation since it gives the government a free pass to its own failures.[23] The other major weakness is that the act does not require companies to report to these individuals at once in case their personal information has been compromised. They only have to inform the Data Protection Board that it means that individuals will never know that their number or personal connection has been violated without being able to take their proactive measure towards protection. It also prevents scrutiny and pressures on the authorized authorities by the general population to improve the security standards. Moreover, the act introduced a data protection board which is not really independent since the members are appointed and regulated by the central government and it lacks the power to independently investigate itself. An independent regulator who is relying on the government cannot possibly be able to hold the government departments accountable, particularly when the ministries are the ones committing the majority of the Aadhaar beaches. The act also aims at making it very clear who is responsible in case there is a leakage of Aadhaar data by a system that includes multiple parties. What we should do with the responsibility is not advised either should it be UIDAI, the state government, or the third party service provider and there is no clear outline of how this can be achieved through sanctions or restitution. Consequently, violations will tend

[22] Digital Personal Data Protection Act, No. 22 of 2023, 17–18 (India).
[23] Internet Freedom Foundation, *Aadhaar Breach Tracker* (2021), https://internetfreedom.in.

to go through the cracks of bureaucracies, and nobody will be charged. Although the act provides huge monetary fines, the fines are not applicable in government agencies that are exempted and, therefore, do not contribute much in deterring incompetence within the government institutions. Lastly, other provisions of the act are increased privacy troubles as it justifies legalizing extensive data sharing between government departments, data retention longer than warranted and processing without specification, weekly defined causes of the public interest. Though this paper mostly dwells on the enforcement in adequacies, these aspects point to the fact that the DPDP act could inadvertently overreach and undermine individual privacy defence. Finally, despite the impression that the act is introducing a contemporary data protection system, its weak enforcement system and massive government exemption exclude it as an appropriate measure of maintaining Aadhar associated personal information and reducing instances of recurrent violations.

VII. U.S. PRIVACY LAW: ENFORCEMENT AND ACCOUNTABILITY

The United States does not have a single and comprehensive privacy law such as the GDPR, but has instead created a strong and multi-tiered enforcement system established by a mixture of federal regulatory, industry-specific, and state level mandates[24]. The Federal Trade Commission, which serves as the main regulator of unfair or deceptive data practices,[25] tries to do so with the assistance of the ecosystem of enforcement. The FTC possesses substantial enforcement authority through carrying out investigation of privacy violations that impose heavy financial fines and require corporations to implement comprehensive corrective measures which often cause the corporation to break-in long-term consent decrees, which mandate the company to overhaul their security framework, have their systems audited on numerous occasions after which they are obliged to report to the regulator on their compliance actions. The mere threat of drawing regulatory attention, coupled with the reputational damage that our companies and the FTC action will incur, provides strong incentive that Enterprises should use strict data privacy controls[26]. In addition to the authority that the FTC has, a variety of federal laws and regulations create increased limitations on specific categories or sensitive information. The HIPAA creates specific regulations and sanctions of health data; the Gramm-Leach-Bliley[27] Act enforces inscription and routine evaluation of risky activities and the

[24] Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. Rev. 1814, 1820–22 (2011).
[25] Federal Trade Commission Act, 15 U.S.C.45(a).
[26] Federal Trade Commission, *Privacy and Data Security Enforcement Actions* (2023).
[27] Gramm-Leach-Bliley Act (GLBA), Pub. L. No. 106-102, 113 Stat. 1338 (1999).

preservation of robust security; and the COPPA creates strict conditions of child personal data gathering and utilization with the obligatory parental approval. These sectoral guidelines are a risk based approach whereby industries that handle some sensitive information are subjected to more rigorous oversight processes. The state level breach reporting requirements further strengthen the concept of transparency as they require enterprises to disclose personal data breaches to both the individuals who are affected as well as the regulators[28]. These notices should contain the type of the breach, the type of data involved as well as the action individuals can take in order to secure themselves. Besides enhancing the trust of the people, this openness also puts a pressure on organizations to prevent breach in the first place. The US mechanism is also a combination of civil and criminal redress, where individuals harmed in an accident can resort to class action lawsuits, statutory damages, and an injunction of the court, and that any ill abuse of information can generate criminal liability. This enforcement paradigm is supported by the institutional autonomy of the FTC since the commissioners have term limits and are not directly politically bound, which makes the agency able to act both against a public firm and a private firm. All these aspects add to an overall culture of deterrence, the active implementation of the said is anticipated, in portions are to be taken seriously and corporations face prompt repercussions in case of non-compliance. The accountability and regulating aspect highlights important lessons to be learned by India, especially as it struggles to face recurring governance and enforcement challenges within the Aadhar ecosystem[29].

VIII. COMPARATIVE ANALYSIS: UNDERSTANDING AADHAR'S PERSISTENT AND VULNERABILITIES

Comparison of the data protection system in India and the US privacy enforcement model reveals significant structure differences that elucidate byAadhar related breach are still persisting even though legislation exists[30]. Though India gradually developed a legal system to state that privacy is a right and established clear standards, they do not always have any significant enforcement tools. Most of the requirements that are imposed on government departments are not supported with significant sanctions and this lowers the compliance with a cosmetic administrative exercise as opposed to a type of legal necessity. Comparatively, the US system is founded upon: the threat of an investigation by the Federal Trade Commission serves as a permanent reminder that misusing personal data can incur significant financial fines,

[28] National Conference of State Legislatures, *Security Breach Notification Laws* (2024).
[29] Centre for Internet & Society, *Learning from U.S. Privacy Enforcement for Aadhaar Governance* (2023).
[30] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

a lengthy investigation through relentless downsizing, and a significant loss of reputation. This is a current threat that causes organisations to lay more emphasis on data protection. Even in India, however, even serious Aadhar breaches rarely create punitive action creating institutional inefficiency and obliterating trust in the government[31]. The various exemptions that the government actors are allowed to enjoy under the DPDP Act are also a hindrance to accountability. The India system grants the state the protection it needs against the compliance requirements, unlike in the US where the privacy standards tend to apply to both commercial firms, thus permitting the government departments to continue their operations without the fear of punishment and the primary handlers of the other information. Such exceptions have a serious negative impact on any effort to guarantee security to the system. The independent oversight is also an advantage of the US approach: the FTC is an independent institution, which enables it to execute enforcement action free of any political interventions. Contrary to UIDAI is also both the implementer and regulator of Aadhar infrastructure at the same time, creating a clear conflict of interest and reducing regulatory trust. Lastly the enforcement situation in India can be described as decentralized with obligations spread all over UIDAI, state authorities, data protection board, and the many third-party operators. This separation of power brings some guarantee, the passing of the blame of bureaucracy, and, in most cases, ends in hit and run violations[32]. All these weaknesses of its structures go to show that India does not have the cohesive, nonpartisan, and retaliatory enforcement mechanism to protect such an extensive and sensitive digital identity system as Aadhar[33].

IX. RECOMMENDATIONS

Even though India cannot implement the US privacy enforcement model directly due to its varied welfare encompassing governance system, some of the essential tenets of the US approach specifically those that pertain to the strength of regulations, accountability of the organisation, and systematic transparency can be modified to enhance the Aadhar data protection system to a significant level[34]. The first step of forming an independent Aadhar monitoring body, which is structurally independent of UIDAI, and which clearly has the mandate to review compliance, conduct security audits, supervise the enforcement efforts, and find emerging systematic violations would be critical. The distinction between operational and

[31] Centre for Internet & Society, *Aadhaar Data Breaches and Institutional Accountability* (2022).
[32] Comptroller and Auditor General of India, *Audit Report on Aadhaar Ecosystem* (2022).
[33] World Bank, *Digital ID Systems: Enforcement, Trust and Accountability* 44–47 (2021).
[34] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583, 586–90 (2014).

regulatory norms is essential to avoid the conflict of interests and achieve objective supervision. It is also vital that the sweeping state exemptions under the DPDP statute are removed, such that government outfits managing Aadhar information can face significant fines in case of carelessness, be required to disclose this information publicly and have their compliance audited on a regular basis[35]. Unless the state actors are held accountable, there will be little likelihood of correcting the persistent deficiencies of Aadhar. Mandatory breach notification procedures must also be included in the law, whereby persons are quickly informed in case related information has been leaked and information explaining the nature of the breach and preventative measures taken should be included. This transparency does not just serve to generate trust among the populace but also compel the corporations to devise more robust security measures that are imposed on the population as well as non-governmental actors and be reminded of the character of breach and the way to prevent irresponsible conduct. Severe system of penalties, akin to FTC enforcement method, would strengthen the idea of compliance. The enhancement of security also involves frequent, independent audits, such as annual audits, security certifications, and vulnerability analysis of all agencies and platforms accessing the Adha data[36]. Publication of a synopsis of these audits would go a long way to enhance institutional accountability. Also, the Aadhar ecosystem should be highly data minimalistic, with Aadhar numbers only being collected when absolutely essential, the use of tokenized identifiers or virtual IDs and withholding other related data on the public facing systems. India should also have explicit liability provisions with third-party vendors to ensure that they have end-to-end accountability, which include contractual fines, mandatory security practices, and damage compensation mechanisms in case of any breach of the rules committed by external services providers. Lastly, the system needs to empower the citizens by allowing them to seek personal redress through compensation on the breach of their privacy, redress collectively as a group through the class action and statutory damages in severe circumstances. Not only would these enhancements bring India in line with the global standards of privacy, but a more robust, accountable policy of data protection would be founded in respect to the scale and sensitivity of Aadhar[37].

[35] Digital Personal Data Protection Act, No. 22 of 2023 (India).
[36] National Institute of Standards & Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (NIST CSF 2.0) (2024).
[37] Bimal N. Patel et al., *Governing India's Digital Future*, 18 Indian J.L. & Tech. 1, 37–39 (2023).

X. DISCUSSION: BUILDING A MODEL SUITABLE FOR INDIA'S CONTEXT

The welfare inspired model of digital governance adopted in India requires a regulation system that is efficient and private at the same time[38]. Aadhar is not easily curtailable since it is providing essential social services to millions of people[39]. The trust that facilitates effective digital governance cannot however be maintained when data leaks continue to recur as is the case. There should be a shift towards systematic enforcement. The structural weakness can not be cured on symbolic compliance or ad hoc measures. Rather, India needs to invest in autonomous bodies, transparency of process and uniform results of negligence[40]. Tighter controls will not hinder the delivery of welfare; on the contrary, it will facilitate a sense of reliability as well as strengthen confidence among the masses. Privacy that safeguards its citizens, in particular, the most vulnerable ones, must ensure accountability at each level of data processing.

XI. CONCLUSION

Aadhar is considered one of the most ambitious elements of the digital governance system in India, as it allows massive welfare provision, identity checking, and administration effectiveness[41]. However, the continuous leakage of Aadhar-related personal information demonstrates inherent weaknesses not in the technology, but in the institution and legal framework in which it is used. The multiple violation reviewed in the context of this paper indicates that major problems in the area are the effective enforcement mechanisms, the split of responsibilities, and broad statutory exemptions that protect the government departments, the principal repositories of Aadhar data, and do not hold them accountable[42]. These institutional failures have created an environment in which shoddy data handling is now the new norm, and privacy risk is accumulating without any mitigation measures. The Digital Personal Data Protection Act, 2023 was hoped to address these gaps but the planned act falls short of providing the sort of enforcement force that would protect the digital identity ecosystem as a large and delicate as Aadhar so long as the state has the option to bypass compliances and because of the order of challenges inherent in influencing Aadhar security,

[38] Ministry of Electronics & Information Technology, *National Digital Governance Framework* (2023).
[39] Unique Identification Authority of India, *Aadhaar and Welfare Service Delivery* (2024).
[40] OECD, *Independent Regulatory Authorities and Accountability Mechanisms* 22–26 (2020).
[41] Unique Identification Authority of India, *Aadhaar Dashboard & Statistics* (2024).
[42] Centre for Internet & Society, *Aadhaar Data Breaches and Accountability Gaps* (2022).

the issue of structurelessness will persist. The comparative analysis of the US privacy legislation, particularly the procedure of the Federal Trade Commission enforcement, has shown a different paradigm, with deterrence, transparency and institutional independence being the main pillars of efficient data protection. The example of the United States shows that it is not obligatory to implement any one comprehensive privacy act, but rather depends on the presence of capable regulators, plausible fines, openness, and the ability of the individuals to visualize the solutions. These ideals provide important revelations to India. They suggest that accountability can be administrative efficiency and that welfare distribution does not have to be constrained by keeping personal data. To become a credible sustainable national identity system, India needs to change its compliance based approach to a more enforcement based model of governance. The change involves making sure that misconduct on the part of any citizen or non-governmental entity has serious consequences; making the regulatory authorities more independent; making the breach notification mandatory and establishing clear liability lines[43]. It is also very important to build an atmosphere of transparency and accountability within government agencies, such that data protection is the key to administration and not a secondary concern. There is a need to preserve Aadhar not only as a technical challenge but also as a government concern. The existence of a firm, objective, deterrence-based enforcement framework is pertinent to India to uphold the personal information of its residence as it proceeds to increase its digital service delivery. It is only through the remedial of these institutional failures that Aadhar can become a secure, rights-protective and future ready digital identity system that can facilitate the developmental and governance goals of India in the long term.

[43] Law Commission of India, *Data Protection and Government Accountability* 7.4–7.9 (2024).