Aadhaar 2.0 Privacy: Analyzing Data-Privacy Risks in India’s Upgraded Digital Public Infrastructure

I. Executive Summary

Aadhaar 2.0, representing a significant upgrade to India's digital public infrastructure, introduces a new era of digital identity management with the aim of enhancing user convenience and security.[1] This evolution, primarily manifested through a new mobile application, seeks to eliminate the need for physical Aadhaar cards and photocopies by leveraging facial recognition and digital verification.[1] While these advancements offer numerous benefits, they also introduce potential data privacy risks that warrant careful analysis. Key among these risks are vulnerabilities associated with centralized data storage, the intricacies of consent-based data sharing, the reliability and security of new authentication methods like facial recognition, and the amplified attack surface resulting from broader integration with various digital services.[3] The Digital Personal Data Protection Act, 2023 (DPDP Act), plays a crucial role in this evolving landscape, setting the legal framework for data protection and necessitating an alignment of the Aadhaar legal framework to ensure user-centricity, privacy, and transparency.[6] To mitigate these risks, this report proposes several recommendations focusing on strengthening data security protocols, enhancing user control over data, ensuring inclusivity, and establishing robust governance mechanisms.[4]

II. Introduction: The Evolution of Aadhaar and the Advent of Aadhaar 2.0

The Aadhaar program, initiated to provide a 12-digit unique identification number to every resident of India, has become a cornerstone of the nation's identity infrastructure.[9] Serving as a proof of identity and address, it aimed to eliminate the pervasive issue of duplicate and fake identities that plagued various government and private databases.[9] Over time, Aadhaar has grown to become the world's largest biometric ID system, with an overwhelming majority of India's adult population enrolled.[10] Initially, its primary focus was to facilitate the efficient delivery of government benefits through Direct Benefit Transfer (DBT) schemes, ensuring that subsidies and services reached the intended beneficiaries.[10]

The upgrade to Aadhaar 2.0 is driven by several factors, reflecting the rapid advancements in technology and the evolving needs of a digitally empowered society.[1] The proliferation of smartphones and the increasing reliance on digital transactions have created a demand for more convenient and secure methods of identity verification.[1] There is a growing need for enhanced security features to protect against increasingly sophisticated cyber threats, coupled with a desire for a more seamless and user-friendly experience.[1]Furthermore, the scope of digital identity is expanding beyond traditional government services, encompassing a wider array of

applications in the private sector, including e-commerce, healthcare, and financial services.[4]

Aadhaar 2.0 holds significant importance within India's broader digital public infrastructure.[1] It serves as the foundational layer for various digital services, forming a crucial component of the "India Stack," a collection of digital goods aimed at enabling presence-less, paperless, and cashless service delivery.[16] This upgrade is also seen as a vital step towards achieving digital self-reliance ("Atmanirbharta"), reinforcing the nation's capacity to build and manage its own digital infrastructure with enhanced security and privacy considerations.[4]The progression from the initial Aadhaar program to Aadhaar 2.0 signifies a transition from a basic identification tool to a more sophisticated and integrated digital identity platform, essential for India's continued digital transformation.

III. Features and Functionality of Aadhaar 2.0

The cornerstone of Aadhaar 2.0 is a new mobile application designed to revolutionize how individuals interact with their digital identity.[1] A key feature of this app is the intended elimination of the need to carry a physical Aadhaar card or provide photocopies for verification purposes.[1] Instead, the app incorporates facial recognition authentication, providing an additional layer of security when authorizing the transfer of personal information.[1] It also offers 100% digital identity verification capabilities, streamlining the process across various service points.[1]

A significant enhancement in Aadhaar 2.0 is the emphasis on consent-based sharing of data.[1] Users will have the ability to share only the necessary data required for a specific verification, and only with their explicit consent, granting them greater control over their personal information.[1] The verification process through the new app is designed to be similar to UPI payments, where users can authenticate their identity by scanning QR codes at various verification points such as hotels, shops, and airports.[1] The app also boasts a more user-friendly interface compared to its predecessor, aiming to improve accessibility and ease of use for all individuals.[1]

Beyond user convenience, Aadhaar 2.0 incorporates enhanced privacy safeguards and security measures.[1]The design aims to protect against data misuse and potential leaks, ensuring that personal information remains secure.[1] The digital nature of the verification process also aids in the prevention of document forgery, adding another layer of security.[1] This upgraded system is designed to seamlessly integrate with India's existing digital public infrastructure while prioritizing strong privacy protections.[1]

To understand the advancements in Aadhaar 2.0, it is important to compare its features with those of the original Aadhaar program.[9] The initial Aadhaar focused on the principles of uniqueness, achieved through biometric and demographic de-duplication, nationwide portability for online authentication, and the generation of a random number devoid of any inherent intelligence.[12] It enabled online verification of demographic information in a cost-effective manner and provided authentication services to various

agencies.[9] The original Aadhaar also introduced the e-KYC functionality, allowing for digital verification of identity for services like banking and telecom.[16] While the original system laid a strong foundation for digital identity, Aadhaar 2.0 builds upon this by introducing more sophisticated and user-centric features, particularly in the realm of mobile-based access and enhanced privacy controls.

IV. The Data Privacy Landscape in India

The foundation for data privacy in India rests upon the fundamental right to privacy, which has been affirmed by the Supreme Court.[15] While the Information Technology Act, 2000, provided some initial framework for data protection, it had limitations in addressing the complexities of a comprehensive data privacy regime.[7] The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act), marks a significant milestone in India's efforts to establish a robust legal framework for the protection of personal data in the digital era.[6]

The DPDP Act defines key terms such as "personal data," which refers to data about an individual who is identifiable, and outlines the roles of "data fiduciary" (similar to a data controller) and "data principal" (the individual whose data is being processed).[28] The Act is built upon core principles including obtaining informed consent before processing personal data, limiting the processing to specified purposes, and collecting only the necessary data.[26] It grants several rights to data principals, such as the right to access and correct their personal data, the right to seek erasure of their data, and the right to have grievances addressed.[34]

The DPDP Act also imposes several obligations on data fiduciaries, including the implementation of reasonable security safeguards to protect personal data, the obligation to notify the Data Protection Board of India (DPB) and affected individuals in case of a data breach, and the requirement for Significant Data Fiduciaries (SDFs) to appoint a Data Protection Officer.[28] The Act regulates the cross-border transfer of personal data, allowing transfers except to countries specifically restricted by the government.[30] It establishes the Data Protection Board of India as an independent body responsible for overseeing the implementation and enforcement of the Act.[28] Non-compliance with the provisions of the DPDP Act can result in significant financial penalties.[26]

Recognizing the importance of aligning the legal framework for Aadhaar with the evolving data protection landscape, the government has stated its intention to harmonize the new Aadhaar law with the DPDP Act.[6]The focus of this alignment is to ensure that the updated Aadhaar law remains user-centric, prioritizes privacy, and operates with transparency.[6] This alignment will have a direct impact on how Aadhaar data is handled, particularly within the context of Aadhaar 2.0.[8]

The DPDP Act introduces stricter consent requirements for the collection and processing of Aadhaar data, necessitating clear and informed consent from individuals.[8] It also reinforces the need for enhanced security measures and the

adoption of data minimization principles, ensuring that only necessary data is collected and retained securely.[26] Organizations that utilize Aadhaar-based services will have obligations for breach reporting to both the DPB and the Unique Identification Authority of India (UIDAI), the governing body for Aadhaar.[8] Consequently, businesses leveraging Aadhaar for various services will likely need to update their compliance programs to align with both the DPDP Act and the revised Aadhaar regulations.[7] This alignment signifies a move towards a more privacy-conscious approach in managing India's digital identity infrastructure.

V. Analyzing Potential Data Privacy Risks in Aadhaar 2.0

The Aadhaar 2.0 ecosystem, while promising enhanced convenience and security, presents several potential data privacy risks that require careful consideration.

Data Collection and Storage: The types of data collected for Aadhaar include demographic information such as name, address, date of birth, and gender, along with biometric data encompassing fingerprints, iris scans, and now, facial images.[9] Optionally, mobile numbers and email addresses may also be collected.[44] UIDAI emphasizes the security measures in place for this data, both during transmission and when stored.[27]Enrolment data is encrypted at the source using a client application provided by UIDAI and transmitted securely to the Central Identities Data Repository (CIDR).[45] Secure file transfer protocols are used for uploading data to the CIDR, where it is stored centrally.[14] Within the CIDR, data undergoes archival and validation processes to ensure its integrity.[45]

Despite these measures, potential risks persist. Vulnerabilities in the client application used for enrolment or in the data upload process could be exploited. The centralized nature of data storage within the CIDR, while efficient for de-duplication and authentication, makes it a high-value target for cyberattacks.[3] The sheer volume of sensitive personal data stored in one location increases the potential impact of a successful breach. Furthermore, the risk of insider threats and unauthorized access to the database by malicious actors or through negligence remains a concern.[3] Aadhaar 2.0, with the addition of facial recognition data, expands the pool of sensitive biometric information, further amplifying the potential consequences of a data compromise. Past incidents, even those affecting third-party systems holding Aadhaar data, underscore the persistent need for robust security measures and continuous monitoring.

Data Sharing and Consent Mechanisms: A central tenet of Aadhaar 2.0 is the emphasis on consent-based sharing of data.[1] The new mobile application is designed to facilitate mechanisms for obtaining and managing user consent for specific data sharing requests.[1] The aim is to allow users to share only the data that is necessary for a particular verification purpose, thereby enhancing privacy.[1] However, the effectiveness of these consent mechanisms hinges on several factors. The clarity and user-friendliness of the consent requests are paramount. If users find the process confusing or cumbersome, they may grant permissions without fully understanding the implications.[40] There is also a risk of "consent fatigue," where users, faced with frequent

consent requests, may become desensitized and grant permissions indiscriminately. The potential for misuse of consent frameworks, either through deceptive practices or coercion, also needs to be addressed. Furthermore, the security of the consent management system itself is crucial; any vulnerabilities could undermine the intended privacy benefits. In the context of offline e-KYC, it is noted that hashed versions of mobile numbers and emails are shared [51], which, while providing a degree of anonymization, still represent personal information that could potentially be linked back to individuals.

Authentication and Verification Processes: Aadhaar 2.0 introduces facial recognition as a new modality for authentication.[1] This adds to the existing methods of biometric authentication (fingerprints and iris scans), OTP-based verification, and demographic matching.[13] Digital verification through QR code scanning is also a key feature, offering a convenient way to authenticate identity at various service points.[1] While these new methods offer potential benefits, they also introduce new privacy and security considerations. The accuracy and reliability of facial recognition technology, especially across diverse demographic groups and in varying environmental conditions, need to be carefully evaluated.[52] There is also the risk of spoofing or biometric cloning, where malicious actors might attempt to impersonate individuals using fabricated biometric data.[4] The security of the QR code generation and scanning process is also critical to prevent tampering or unauthorized access to information. Vulnerabilities in the authentication APIs that facilitate these processes could be exploited by attackers.[47] Additionally, there is a potential for exclusion of individuals who may be unable to use facial recognition due to disabilities or lack of access to compatible devices, highlighting the need for inclusive design and alternative authentication methods.[17]

Integration with Other Digital Services: Aadhaar serves as a foundational identity layer for a wide range of digital services, including e-KYC, digital payments, and various government and private sector applications.[16]The expansion of Aadhaar authentication to private sector entities further broadens its reach.[20] This increasing integration leads to more linkages with other databases, such as those of banks and mobile service providers.[4] While this interconnectedness enhances the utility of Aadhaar, it also amplifies the potential data privacy risks. A wider integration means an increased attack surface, as more systems become potential targets for malicious actors.[4] The aggregation of data across multiple services raises concerns about the potential for profiling and surveillance, where detailed pictures of individuals' economic and social lives can be built.[47] Individuals may find it challenging to keep track of all the services their Aadhaar is linked to, increasing the risk of unauthorized or fraudulent linkages.[4] Furthermore, the data security vulnerabilities in the systems of third-party entities that integrate with Aadhaar can pose a significant risk to the privacy of Aadhaar holders.[3] If these entities do not have adequate security measures in place, Aadhaar data shared with them could be compromised.

Potential for Data Breaches and Misuse: The history of Aadhaar data leaks from both government and third-party systems serves as a stark reminder of the vulnerabilities

inherent in large-scale digital identity systems.[3]There have been instances of Aadhaar data being sold or accessed by unauthorized individuals, highlighting the potential for both internal and external threats.[3] The consequences of such data breaches can be severe, including identity theft, financial fraud, and other cybercrimes.[5] The misuse of biometric data, including the facial recognition data introduced in Aadhaar 2.0, is a growing concern, as this information is highly sensitive and can have long-lasting implications if compromised.[4] A contributing factor to these risks is the lack of widespread awareness among citizens about data security and privacy best practices, making them potentially more vulnerable to social engineering attacks and other forms of data exploitation.[5]

VI. Impact on Individual Liberties and Societal Implications

The Aadhaar system, particularly with the advancements in Aadhaar 2.0, has sparked considerable debate regarding its impact on individual liberties and broader societal implications. Concerns have been raised about the potential for mass surveillance and the erosion of privacy due to the centralized nature of the Aadhaar database, which could allow for tracking and monitoring of citizens' activities across various services.[47] There are also worries about the potential for exclusion of vulnerable populations who may face technological barriers in accessing or using Aadhaar 2.0 services, or who may experience authentication failures due to various reasons.[17]

The debate surrounding the mandatory nature of Aadhaar for accessing essential services continues, with concerns that making it compulsory could infringe upon individuals' rights and choices.[3] The Aadhaar system's impact on social equity and access to welfare schemes is also a subject of discussion, with instances reported where authentication failures or lack of Aadhaar have led to the denial of benefits to eligible individuals.[17]Furthermore, the collection and use of biometric data, especially sensitive information like iris scans and facial images, raise significant ethical considerations regarding consent, potential misuse, and the long-term implications for individuals' privacy and autonomy.[18] Balancing the benefits of a digital identity system with the need to safeguard individual liberties and ensure social equity remains a critical challenge in the ongoing evolution of Aadhaar.

VII. Proposed Security Enhancements and Mitigation Strategies

To address the potential data privacy risks associated with Aadhaar 2.0, a comprehensive set of security enhancements and mitigation strategies is necessary.

Strengthening data security within the Aadhaar 2.0 ecosystem requires implementing robust security protocols at every stage.[4] This includes the use of advanced encryption techniques to protect data both in transit and at rest, as well as the adoption of multi-factor authentication mechanisms to secure access to sensitive systems.[14] Regular security audits and thorough vulnerability assessments should be conducted to identify and address potential weaknesses in the infrastructure.[27] Implementing anomaly

detection systems and tracking suspicious usage patterns can help in identifying and preventing unauthorized access or misuse of Aadhaar data.[4]

Enhancing user control over data sharing and linkage management is crucial for building trust in the system.[1]Providing users with clear and intuitive tools within the mobile application to manage their consent preferences and track their Aadhaar linkages is essential. Promoting the use of Virtual IDs (VIDs) can further limit the exposure of the actual Aadhaar number during authentication processes.[20] The security of authentication devices and the processes they employ must also be continuously strengthened, ensuring that biometric data is captured and transmitted securely.[27] Rigorous implementation of data minimization principles, ensuring that only the necessary data is collected and retained for specific purposes, is paramount.[26] Furthermore, clear guidelines and secure practices for the storage and disposal of any paper records containing Aadhaar information are necessary to prevent data leaks.[4]

Mitigating privacy risks requires a focus on transparency and user empowerment.[4] Enhancing transparency involves providing clear and easily understandable information to users about how their data is collected, used, and shared. Raising public awareness about data security and privacy risks, and educating individuals on how to protect their information, is also crucial.[4] Establishing robust and easily accessible grievance redressal mechanisms for users to report privacy violations or data breaches is essential for accountability and building trust.[17] Exploring the potential of privacy-enhancing technologies (PETs) could offer additional layers of protection. The proposed pillars for Aadhaar 2.0, including Suspicious Usage-Pattern Tracking, Transaction Alerts, Linkage Summaries, and Novel Identity Verification methods, offer a promising framework for enhancing both security and privacy.[4]

Addressing the risks associated with the integration of Aadhaar 2.0 with other digital services necessitates establishing clear security standards and protocols that all integrating entities must adhere to.[4] Implementing strict access controls and robust data governance frameworks for all linked databases is critical to prevent unauthorized access and data breaches.[59] Regular security audits of all integrating systems should be mandated to ensure ongoing compliance with security best practices.[59]

Ensuring inclusivity and preventing exclusion requires maintaining alternative means of identification and authentication for individuals who may face challenges with digital methods, such as those without smartphones or those with disabilities.[17] Providing adequate assistance and support for vulnerable populations in enrolling for and using Aadhaar 2.0 services is essential.[11] The accessibility of the mobile application and related services for individuals with disabilities should be a key consideration in the design and development process.[64]

VIII. International Perspectives on Digital Identity and Data Privacy

Examining international experiences with digital identity systems and data privacy regulations can provide valuable insights for the ongoing development of Aadhaar 2.0.[39] Several countries have implemented robust data protection laws, such as the European Union's General Data Protection Regulation (GDPR), which sets high standards for consent, data processing, and individual rights.[15] Models for consent management and data sharing in other digital identity programs, such as Singapore's Singpass and MyInfo system, offer examples of how to streamline access to services while maintaining user control over data.[50] Different countries have adopted various approaches to balancing national security concerns with the protection of individual privacy in their digital identity systems, providing lessons on the trade-offs involved.[52] Learning from data breaches and security incidents that have occurred in other national ID systems can help India proactively address potential vulnerabilities in Aadhaar 2.0.[48] By studying these international perspectives, India can gain valuable knowledge and best practices to inform the design and governance of a secure and privacy-respecting digital identity infrastructure.

IX. Conclusion: Towards a Privacy-Centric and Secure Aadhaar 2.0

Aadhaar 2.0 represents a significant step forward in India's digital transformation, offering enhanced convenience and functionality through its upgraded digital infrastructure. However, this evolution brings with it inherent data privacy risks associated with centralized data storage, consent mechanisms, new authentication methods, broader integration with digital services, and the ever-present threat of data breaches. It is paramount that the development and implementation of Aadhaar 2.0 are closely aligned with the principles of the Digital Personal Data Protection Act, 2023, ensuring a user-centric approach that prioritizes privacy and transparency.

To mitigate these risks effectively, a multi-pronged strategy is essential. This includes the implementation of robust security enhancements, such as advanced encryption, multi-factor authentication, and regular security audits. Empowering users with greater control over their data through transparent consent management and tools to track and manage their Aadhaar linkages is crucial for building trust. Furthermore, ensuring inclusivity by maintaining alternative authentication methods and providing support for vulnerable populations is vital. The proposed pillars for Aadhaar 2.0 offer a promising direction for reinforcing security and privacy within the system.

Learning from international experiences in digital identity management and data protection can provide valuable insights and best practices for India. Ongoing vigilance, continuous adaptation to emerging threats, and active public engagement are necessary to ensure the long-term privacy and security of India's upgraded digital public infrastructure. By prioritizing these considerations, India can strive towards an Aadhaar 2.0 that serves as a secure and trustworthy digital identity platform, fostering both innovation and the fundamental rights of its citizens in the digital age.

Key Valuable Tables:

1. Comparison of Aadhaar and Aadhaar 2.0 Features

Feature	Aadhaar	Aadhaar 2.0
Physical Card Requirement	Primarily relied on physical card	Aims to eliminate the need for physical cards
Facial Recognition	Not a primary authentication method	Incorporated for enhanced security and authentication
Digital Verification	Online verification of demographic information	100% digital identity verification capabilities
Consent-Based Sharing	Limited control over data sharing	Users can share only necessary data with explicit consent
Verification Method	Biometric (fingerprint, iris), OTP, demographic matching	Biometric (fingerprint, iris, facial), OTP, demographic matching, QR code scan
Interface	Primarily physical card-based with some online portal functionalities	Primarily mobile app-based with user-friendly interface
Primary Focus	Proof of identity and address, enabling service delivery	Enhanced user convenience, security, and granular control over data sharing

2. Key Provisions of the Digital Personal Data Protection Act, 2023 Relevant to Aadhaar

Provision	Description	Relevance to Aadhaar
Definition of Personal Data	Data about an individual who is identifiable	Aadhaar data, including demographic and biometric information, falls under this definition
Consent Requirements	Processing of personal data requires free, specific, informed, unconditional, and unambiguous consent	Collection and processing of Aadhaar data, especially for new integrations, will require explicit user consent
Data Principal Rights	Rights to access, correction, erasure, and grievance redressal	Aadhaar holders will have enhanced rights over their Aadhaar data
Data Fiduciary Obligations	Obligations for data security, breach notification, and appointment of DPO for SDFs	UIDAI and entities using Aadhaar data will have obligations to secure the data and report breaches
Data Breach Notification	Mandatory notification of data breaches to the DPB and affected data principals	Any breach involving Aadhaar data will need to be reported to both UIDAI and the DPB

Cross-Border Data Transfer	Transfers allowed except to restricted countries	Regulations on cross-border transfers will apply to any potential international use of Aadhaar data

3. Potential Data Privacy Risks in Aadhaar 2.0 and Proposed Mitigation Strategies

Risk Area	Specific Risk	Proposed Mitigation Strategy
Data Collection & Storage	Centralized Storage makes it a high-value target	Implement advanced encryption, robust access controls, and regular security audits
Data Collection & Storage	Insider Threats and unauthorized access	Strict background checks, role-based access control, and continuous monitoring
Data Sharing & Consent	Consent Fatigue leading to users granting permissions without understanding	Design user-friendly consent interfaces with clear information and options for managing preferences
Data Sharing & Consent	Misuse of Consent frameworks or coercion	Establish clear guidelines and oversight mechanisms for consent collection and management
Authentication & Verification	Facial Recognition Accuracy issues across diverse demographics	Continuous improvement of algorithms, thorough testing, and provision of alternative authentication methods
Authentication & Verification	Biometric Cloning and spoofing	Implement liveness detection and other anti-spoofing measures
Integration with Other Services	Increased Attack Surface due to wider integration	Establish strict security standards for integrating entities and conduct regular audits
Integration with Other Services	Profiling and surveillance through data aggregation	Enforce data minimization principles and provide users with transparency over data linkages
Data Breaches & Misuse	Identity Theft and financial fraud	Implement strong security measures, provide user awareness training, and establish robust incident response plans
Data Breaches & Misuse	Lack of Awareness among citizens about data security	Conduct public awareness campaigns on data privacy and security best practices