# Analysis of Aadhar Card:

# Cybersecurity Issues with India's Biometric Experiment

Ritesh Kumar

2024SP_MS_DSP_485-DL_SEC61: Data Governance, Ethics, and Law

Module 4

Data Governance Case Study 1

Candice Bradley and Pushkar Shah

July 8, 2024

Table of Contents

**The Data**

The primary source of data for this case study is the Aadhaar system, managed by the Unique Identification Authority of India (UIDAI). This database contains biometric information of approximately 1.2 billion Indian residents, including fingerprints, iris scans, and photographs, linked to a unique 12-digit identity number. The authors [1,2,3] explain how data were collected through various official channels and analyzed through reported breaches, security lapses, and subsequent reactions from the UIDAI. While the data provided offer a comprehensive view of the systemic issues within the Aadhaar system, the analysis of the data may not be entirely adequate. The data collection appears fragmented and reactive, relying heavily on reported incidents and media coverage, rather than a structured, methodical approach to identifying and addressing vulnerabilities.

**Relevance to Data Governance**

The issues surrounding Aadhaar fit within a broader data governance framework that encompasses management, legal, and ethical dimensions. From a management perspective, the UIDAI's handling of data breaches and the security of the database are critical concerns. Legally, the implications of data privacy and protection, as highlighted by the Supreme Court of India, underscore the need for robust legislation. Ethically, the unauthorized access and potential misuse of biometric data raise serious questions about individual privacy and state surveillance. The case study illustrates the complexities of managing a vast biometric database while ensuring compliance with legal standards and maintaining ethical integrity in data handling.

**Relevant Legislation**

The case study references several legislative aspects relevant to Aadhaar. Key legislation includes the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits, and Services) Act, 2016, which provides a legal framework for the biometric database. The Supreme Court of India's ruling in 2017 affirmed the right to privacy as a fundamental right under Article 21 of the Indian Constitution, impacting how Aadhaar data is managed and protected. The ruling emphasized the need for a comprehensive data protection law, which aligns with the principles outlined in Justice B.N. Srikrishna's white paper on data protection. This document advocates for a technology-agnostic, all-encompassing data protection law applicable to both private and public sectors, with stringent measures for informed consent and accountability.

The absence of a robust data protection law at the time of the breaches highlights the necessity for such legislation. The authors suggest that the legislative framework needs to be strengthened to address privacy concerns, enforce stricter penalties for data breaches, and ensure that Aadhaar operates within a secure and legally compliant environment. The proposed data protection law should include specific provisions for biometric data, given its sensitive nature and the potential for misuse.

**Data Governance Solution**

The key takeaway from this case study is the urgent need for a comprehensive and enforceable data governance framework for Aadhaar. The authors highlight several solutions, including the establishment of a strong data protection law based on the principles outlined in Justice Srikrishna's white paper. While the existing legislative measures, such as the Aadhaar Act and Supreme Court rulings, provide a foundation, they are insufficient in addressing all vulnerabilities and ensuring robust data protection.

The proposed solutions include making the data protection law technology-agnostic, applying it to both government and private entities, ensuring informed consent, and holding data controllers accountable. These measures are essential but need to be complemented with practical steps such as improving the security infrastructure of the Aadhaar database, conducting regular security audits, and fostering transparency in the UIDAI's operations.

Additional solutions could involve implementing advanced encryption techniques for storing biometric data, establishing a decentralized data verification system to reduce dependency on a central database, and educating citizens on data privacy and security practices. Moreover, the government should consider forming an independent oversight body with the authority to investigate and respond to data breaches, ensuring swift and transparent action.

In conclusion, the Aadhaar case study underscores the critical intersection of technology, law, and ethics in data governance. Strengthening the legislative framework, enhancing security measures, and fostering an ethical approach to data management are imperative for safeguarding the privacy and rights of Indian citizens.

**References**


1. [1]Jain, Mardav. “The Aadhaar Card: Cybersecurity Issues With India’s Biometric Experiment.” The Henry M. Jackson School of International Studies, May 9, 2019. https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/.
2. [2]Chikermane, Gautam. “Aadhaar Breach Is Serious, but Bigger Challenge Is a Data and Privacy Protection Law.” Observer Research Foundation, January 5, 2018. https://www.orfonline.org/expert-speak/aadhaar-breach-serious-bigger-challenge-data-privacy-protection-law.
3. [3]Economic Laws Practice. “Justice BN Srikrishna Committee - White Paper on Data Protection,” 2017. https://elplaw.in/wp-content/uploads/2023/09/ELP-Discussion-Paper-Justice-BN-Srikrishna-Committee-Data-Protection-2.pdf.
4. Sikri, A.K. “Writ Petition (Civil) No. 247 Of 2017 & Others. Versus Union Of India & Others. Judgment.” Judgment. In The Supreme Court Of India, July 1, 2017. https://www.uidai.gov.in/images/Pan-Aadhaar_Linking.pdf.
5. Ministry Of Law And Justice. “The Aadhaar (Targeted Delivery Of Financial And Other Subsidies, Benefits And Services) Act, 2016.” *The Gazette Of India Extraordinary*, March 26, 2016. https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf.