Aadhaar Act and its non-compliance with Data Protection Law in India

Amidst all the hue and cry, the Aadhaar Act 2016, which was introduced with the aim of providing statutory backing to the use of Aadhaar, was passed in the Lok Sabha in its original form on 16th March 2016, after rejecting the recommendations made by Rajya Sabha[1]. Though the Act has been vehemently opposed on several grounds, one of the concerns that has been voiced is regarding privacy and protection of the demographic and biometric information collected for the purpose of issuing the Aadhaar number.

In India, for the purpose of data protection, a body corporate is subject to section 43A of the Information Technology Act, 2000 ("**IT Act**") and subsequent Rules, i.e. -The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("**IT Rules**"). Section 43A of the IT Act, 2000[2] holds a body

[1] The Rajya Sabha had proposed five amendments to the Aadhaar Act 2016, which are as follows:

i. Opt-out clause : A provision to allow a person to "opt out" of the Aadhaar system, even if already enrolled.
ii. Voluntary: to ensure that if a person chooses not to be part of the Aadhaar system, he/she would be provided "alternate and viable" means of identification for purposes of delivery of government subsidy, benefit or service.
iii. Amendment restricting the use of Aadhaar numbers only for targeting of government benefits or service and not for any other purpose.
iv. Amendment seeking change of the term "national security" to "public emergency or in the interest of public safety" in the provision specifying situations in which disclosure of identity information of an individual to certain law enforcement agencies can be allowed.
v. Oversight Committee : the oversight committee , which would oversee the possible disclosure of information, should include either the Central Vigilance Commissioner or the Comptroller and Auditor-General.

Sources :

- http://indianexpress.com/article/india/india-news-india/rajya-sabha-returns-aadhar-act-to-lok-sabha-with-oppn-amendments/
- http://thewire.in/2016/03/16/three-rajya-sabha-amendments-that-will-shape-the-aadhaar-debate-24993/

[2] Section **43A :Compensation for failure to protect data.**

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Explanation.—For the purposes of this section,— (i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities; (ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

corporate, which is possessing, dealing or handling any sensitive personal data or information, and is negligent in implementing and maintaining reasonable security practices resulting in wrongful loss or wrongful gain to any person, liable to compensate the affected person and pay damages.

Rule 3 of the IT Rules enlists personal information that would amount to Sensitive personal data or information of a person and includes the biometric information. Even the Aadhaar Act states under section 30 that the biometric information collected shall be deemed as "sensitive personal data or information", which shall have the same meaning as assigned to it in clause (iii) of the Explanation to section 43A of the IT Act; this reflects that biometric data collected in the Aadhaar scheme will receive the same level of protection as is provided to other sensitive personal data under Indian law. This implies that, the agencies contracted by the UIDAI (and not the UIDAI itself) to perform functions like collection, authentication, etc. like the Registrars, Enrolling Agencies and Requesting Entities, which meet the criteria of being a 'body corporate' as defined in section 43A,[3] could be held responsible under this provision, as well as the Rules, to ensure security of the data and information of Aadhaar holder and could potentially be held liable for breach of information that results in loss to an individual if it can be proven that they failed to implement reasonable security practices and procedures.

In light of the fact that some actors in the Aadhaar scheme could be held accountable and liable under section 43A and associated Rules, this article compares the regulations regarding data security as found in section 43A and IT Rules 2011 with the provisions of Aadhaar Act 2016, and discusses the implications of the differences, if any.

1. Compensation and Penalty

Section 43A: Section 43A of the IT Act, 2000 (Amended in 2008) provides for compensation for failure to protect data. It states that a body corporate, which is possessing, dealing or

---

(iii) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.'.

[3] The term 'body corporate' has been defined under section 43A as "any company and includes a firm, sole proprietorship or other association of individuals *engaged in commercial or professional activities*"

handling any sensitive personal data or information, and is negligent in implementing and maintaining reasonable security practices resulting in wrongful loss or wrongful gain to any person, is liable to compensate the affected person and pay damages not exceeding five crore rupees.

Aadhaar Act : Chapter VII of the Act provides for offences and penalties, but does not talk about damages to the affected party.

- Section 37 states that intentional disclosure or dissemination of identity information, to any person not authorised under the Aadhaar Act, or in violation of any agreement entered into under the Act, will be punishable with imprisonment up to three years or a fine up to ten thousand rupees (in case of an individual), and fine up to one lakh rupees (in case of a company).
- Section 38 prescribes penalty with imprisonment up to three years and a fine not less than ten lakh rupees in case any of the acts listed under the provision are performed without authorisation from the UIDAI.
- Section 39 prescribes penalty with imprisonment for a term which may extend to three years and fine which may extend to ten thousand rupees for tampering with data in Central Identities Data Repository.
- Section 40 holds a requesting entity liable for penalty for use of identity information in violation of Section 8 (3) with imprisonment up to three years and/or a fine up to ten thousand rupees (in case of an individual), and fine up to one lakh rupees (in case of a company).
- Section 41 holds a requesting entity or enrolling agency liable for penalty for violation of Section 8 (3) or Section 3 (2) with imprisonment up to one year and/or a fine up to ten thousand rupees (in case of an individual), and fine up to one lakh rupees (in case of a company).
- Section 42 provides general penalty for any offence against the Act or regulations made under it, for which no specific penalty is provided, with imprisonment up to one year and/or a fine up to twenty five thousand rupees (in case of an individual), and fine up to one lakh rupees (in case of a company).

Though the Aadhaar Act prescribes penalty in case of unauthorised access, use or any other act contravening the Regulations, it fails to guarantee protection to the information and does not provide for compensation in case of violation of the provisions.

2. Privacy Policy

IT Rules: Rule 4 requires a body corporate to provide a privacy policy on their website, which is easily accessible, provides for the type and purpose of personal, sensitive personal information collected and used, and Reasonable security practices and procedures.

Aadhaar Act: Though in practise the contracting agencies (the body corporates under the Aadhaar ecosystem) may maintain a privacy policy on their website, the Aadhaar Act does not require a privacy policy for the UIDAI or other actors.

Implications: Because contracting agencies will be covered by the IT Rules if they are 'body corporates', the requirement to maintain a privacy policy will be applicable to them.

3. Consent

IT Rules: Rule 5 requires that prior to the collection of sensitive personal data, the body corporate must obtain consent, either in writing or through fax regarding the purpose of usage before collection of such information.

Aadhaar Act: The Act is silent regarding consent being acquired in case of the enrolling agency or registrars. However, section 8 provides that any requesting entity will take consent from the individual before collecting his/her Aadhaar information for authentication purposes, though it does not specify the nature (written/through fax).

Implications: If the enrolling agency is a body corporate, they will also be required to take consent prior to collecting and processing biometrics. It is possible that since the Aadhaar Act envisages a scheme which is quasi-compulsory in nature, a consent provision was deliberately left out. This circumstance would give the enrolling agencies an argument against taking consent, by saying that the Aadhaar Act is a specific legislation which is also later in point of time than the IT Rules, and a deliberate omission of consent coupled with the

compulsory nature of the Aadhaar scheme would mean that they are not required to take consent of the individuals before enrolment.

4. Collection Limitation

Rules: Rule 5 (2) requires that a body corporate should only collect sensitive personal data if it is connected to a lawful purpose and is considered necessary for that purpose.

Aadhaar Act: Section 3(1) of the Act states that every resident shall be entitled to obtain an aadhaar number by submitting his demographic information and biometric information by undergoing the process of enrolment.

5. Notice

Rules: Rule 5(3) requires that while collecting information directly from an individual, the body corporate must provide the following information:

- The fact that information is being collected
- The purpose for which the information is being collected
- The intended recipients of the information
- The name and address of the agency that is collecting the information
- The name and address of the agency that will retain the information

Aadhaar Act: Section 3 of the Act states that at the time of enrolment and collection of information, the enrolling agency shall notify the individual as to how their information will be used; what type of entities the information will be shared with; and that they have a right to see their information and also tell them how they can see their information. However, the Act is silent regarding notice of name and address of the agency collecting and retaining the information.

6. Retention Limitation

Rules: Rule 5(4) requires that body corporate must retain sensitive personal data only for as long as it takes to fulfil the stated purpose or otherwise required under law.

Aadhaar Act: The Act is silent regarding this and does not mention the duration for which the personal information of an individual shall be retained by the bodies/organisations contracted by UIDAI.

7. Purpose Limitation

IT Rules: Rule 5(5) requires that information must be used for the purpose that it was collected for.

Aadhaar Act: Section 57 contravenes this and states that the Act will not prevent use of Aadhaar number for other purposes under law by the State or other bodies. Section 8 of the Act states that for the purpose of authentication, a requesting entity is required to take consent before collection of Aadhaar information and use it only for authentication with the CIDR. Section 29 of the Act states that the core biometric information collected will not be shared with anyone for any reason, and must not be used for any purpose other than generation of Aadhaar numbers and authentication. Also, the Identity information available with a requesting entity will not be used for any purpose other than what is specified to the individual, nor will it be shared further without the individual's consent.

Section 57 contravenes the above and states that the Act will not prevent use of Aadhaar number for other purposes under law by the State or other bodies.

8. Right to Access and Correct

Rules : Rule 5(6) requires a body corporate to provide individuals with the ability to review the information they have provided and access and correct their personal or sensitive personal information.

Aadhaar Act : The Act provides under section 3 that at the time of enrolment, the individual needs to be informed about the existence of a right to access information, the procedure for making requests for such access, and details of the person or department in-charge to whom such requests can be made. Section 28 of the Act provides that every aadhaar number holder may access his identity information except core biometric information. Section 32 provides that every Aadhaar number holder may obtain his authentication record. Also, if the demographic or biometric information about any Aadhaar number holder changes, is lost or is

found to be incorrect, they may request the UIDAI to make changes to their record in the CIDR.

9. Right to 'Opt Out' and Withdraw Consent

Rules: Rule 5(7) requires that the individual must be provided with the option of 'opting out' of providing data or information sought by the body corporate. Also, they must have the right to withdraw consent at any point of time.

Aadhaar Act: The Aadhaar Act does not provide an opt- out provision and also does not provide an option to withdraw consent at any point of time. Section 7 of the Aadhaar Act actually implies that once the Central or State government makes aadhaar authentication mandatory for receiving a benefit then the individual has no other option but to apply for an Aadhaar number. The only concession that is made is that if an Aadhaar number is not assigned to an individual then s/he would be offered some alternative viable means of identification for receiving the benefit.

10. Grievance Officer

Rules: Rule 5(9) requires that body corporate must designate a grievance officer for redressal of grievances, details of which must be posted on the body corporate's website and grievances must be addressed within a month of receipt.

Aadhaar Act: The Aadhaar Act does not provide for any such mechanism for grievance redressal by the registrars, enrolling agencies or the requesting entities. However, since the contracting agencies will also get covered by the IT Rules if they are 'body corporates', the requirement to designate a grievance officer would be applicable to them as well due to the IT Rules.

11. Disclosure with Consent, Prohibition on Publishing and Further Disclosure

Rules: Rule 6 requires that body corporate must have consent before disclosing sensitive personal data to any third person or party, except in the case with Government agencies for the purpose of verification of identity, prevention, detection, investigation, on receipt of a

written request. Also, the body corporate or any person on its behalf shall not publish the sensitive personal information and the third party receiving the sensitive personal information from body corporate or any person on its behalf shall not disclose it further.

Aadhaar Act: Regarding the requesting entities, the Act provides that they shall not disclose the identity information except with the prior consent of the individual to whom the information relates. The Act also states that the Authority shall take necessary measures to ensure confidentiality of information against disclosures. However, as an exception under section 33, the UIDAI may reveal identity information, authentication records or any information in the CIDR following a court order by a District Judge or higher. The Act also allows disclosure made in the interest of national security following directions by a Joint Secretary to the Government of India, or an officer of a higher rank, authorised for this purpose. The Act is silent on the issue of obtaining consent of the individual under these exceptions. Additionally, the Act also states that the Aadhaar number or any core biometric information collected or created regarding an individual under the Act shall not be published, displayed or posted publicly, except for the purposes specified by regulations.

12. Requirements for Transfer of Sensitive Personal Data

Rules : Rule 7 requires that body corporate may transfer sensitive personal data into another jurisdiction only if the country ensures the same level of protection and may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer.

Aadhaar Act : The Act is silent regarding transfer of personal data into another jurisdiction by the any of the contracting bodies like the Registrar, Enrolling agencies or the requesting entities. However, if these agencies satisfy the requirement of being “body corporates” as defined under section 43A, then the above requirement regarding transfer of data to another jurisdiction under IT Rules would be applicable to them. However, considering the sensitive nature of the data involved, the lack of a prohibition of transferring data to another jurisdiction under the Aadhaar Act appears to be a serious lacuna.

13. Security of Information

Rules : Rule 8 requires that the body corporate must secure information in accordance with the ISO 27001 standard or any other best practices notified by Central Government. These practices must be audited annually or when the body corporate undertakes a significant up gradation of its process and computer resource.

Aadhaar Act : Section 28 of the Act states that the UIDAI must ensure the security and confidentiality of identity information and authentication records. It also states that the Authority shall adopt and implement appropriate technical and organisational security measures, and ensure the same are imposed through agreements/arrangements with its agents, consultants, advisors or other persons. However, it does not mention which standards/measures have to be adopted by all the actors in Aadhaar ecosystem for ensuring the security of information, though it can be argued that if the contractors employed by the UIDAI are body corporate then the standards prescribed under the IT Rules would be applicable to them.

Implications of the differences for body corporates in Aadhaar ecosystem

An analysis of the Rules in comparison to the data protection measures under the Aadhaar Act shows that the requirements regarding protection of personal or sensitive personal information differ and are not completely in line with each other.

Though the Aadhaar Act takes into account the provisions regarding consent of the individual, notice, restriction on sharing, etc., the Act is silent regarding many core measures like sharing of information across jurisdictions, taking consent before collection of information, adoption of security measures for protection of information, etc. which a body corporate in the Aadhaar ecosystem must adopt to be in compliance with section 43A of the IT Act. It is therefore important that the bodies collecting, handling, sharing the personal information and are governed by the Aadhaar Act, must adhere to section 43A and the IT Rules 2011. However, applicability of Aadhaar Act as well as section 43A and IT Rules 2011 would lead to ambiguity regarding interpretation and implementation of the Law. The differences must be duly taken into account and more clarity is required to make all the bodies under this Legislation like the enrolling agencies, Registrars and the Requesting Entities accountable under the correct provisions of Law. However, having two separate

legislations governing the data protection standards in the Aadhaar scheme seems to have been overlooked. A harmonized and overarching privacy legislation is critical to avoid unclarity in the applicability of data protection standards and would also address many privacy concerns associated to the scheme.