Comparing provisions in Aadhaar Bill with Principles of A.P. Shah Committee Report

Principle in A.P. Shah Report	Description of Principle	Corresponding provision in Aadhaar Bill		Comments/Concerns
		Enrolling Agency (EA)	Requesting Entity (RE)	
Notice (During collection & Other notices) *Both, EAs & REs 'collect' information for their specific purposes of enrollment & authentication respectively.*	What information is being collected	No mention	Section 8(2)(a): Obtain consent for the purposes of authentication	No itemized declaration of contents and nature of information being collected is provided to the individual. This is crucial considering the Authority retains the right to include other biological attributes as biometric information through regulations.
	Purposes of collecting	No mention	Section 8(2)(a): obtain consent for the purposes of authentication	Proper counseling needs to be given of where Aadhaar can be used, and if alternative measures are also in place.
	Uses of such information	Section 3(2)(a): Inform the data subject about the manner in which information shall be used	Section 8(3)(b): Inform the individual about the uses to which information received during authentication may be put to.	
	Security safeguard established by Data Controller	No mention	No mention	No notice of the security standards followed at the CIDR, or the measures used by the EA & RE to safeguard the data
	Ability of Data subjects to access & correct information	Partially. Section 3(2)(c) only provides a notice	N/A (information given at enrollment)	Correction of information and its procedure is provided under Section 31. But, no notice is given regarding such information at the time of

		for the means to access their information.		enrollment.
	Contact details of privacy officers & ombudsmen to file complaints.	No mention	No mention	There is no mention of a complaint mechanism against the EA& RE, or any medium to approach in case of misuse/breach of data held by the Authority. It is clearly stated that the court can only take cognizance when the complaint is filed by the Authority.
	Notification of data breaches to data subject and commissioner	No mention	No mention	Data subject should be aware for the sake of his safety and securing other social and economic connections linked with his Aadhaar number.
	Notification to data subject of any legal access to their information	No mention	No mention	Highlights the need for a privacy legislation that lays down the groundwork for accountability of the Government and its agencies as well as enumerates the privacy rights of citizens.
	Notification of changes in Data controller's privacy policy	No mention	No mention	Linking/using of Aadhaar is not limited to solely the welfare schemes. Section 57 allows other body corporate or person to use the Aadhaar number for the purposes of establishing identity of an individual after following provisions in Section 8 (Procedure for authentication by requesting entity), and Chapter VI (Security & Protection of Data) of the Bill. It is important that changes in the privacy policies of such body corporates/ anybody else also be notified.

	Any other information deemed necessary	Section 3(2)(b): Nature of recipients with whom the information is intended to be shared during authentication	N/A	
Choice & Consent	Choice to Opt in/Opt out of providing PI	Not mandatory to get an Aadhaar, but under Section 7, the State/Central Government is allowed to make Aadhaar a condition for availing benefits of welfare schemes.		Effectively, if one wants to avail those benefits that have a mandatory Aadhaar requirement, there is no choice to opt in/opt out.
	Consent only after providing information practices	EA: Section 3(2) provides the information practices for an enrolling agency.	RE: Section 8(3) states Provisions where RE informs the individual about purposes and use of the data	
	After consent has been taken will the data controller collect, process, use, or disclose such information to third parties, except in case of authorized agencies	Section 8(2)(a): Take consent of individual before collecting his identity information for the purposes of authentication.		
	An option to withdraw his/her consent given to the data controller	No mention		There should be an option to have the information deleted from the CIDR respecting a person's right to choice, and that Aadhaar is an entitlement and not a compulsion.
	Information collected	Section 29(4): No Aadhaar number, or		

	on a mandatory basis should be anonymized, if published in public databases	information collected under this number shall be disclosed, published publicly.	
Collection Limitation	Only collect PI from data subjects as is necessary for the purposes identified for such collection, regarding which notice has been provided and consent of the individual taken	N/A	Aadhaar is only valid with **all** the components of the Personal Information that include, photograph, demographic information, fingerprints, iris scans, or other biological attributes as may be specified.
Purpose Limitation	PI collected should be adequate and relevant to the purposes for which they are processed	The caption of the bill provides an insight into its purpose states that it for 'efficient, transparent, and targeted delivery of subsidies, benefits and services, the expenditure for which is incurred from the Consolidated Fund of India...'	Contrary to the said purpose, as per Section 57, Aadhaar can be used to establish identity of a person by State or any body corporate or person, by following the obligations in Section 8 (procedures for authentication by Requesting Entity) and Chapter VI (protection & sharing of data). Therefore, the bill is not limiting itself to the delivery of benefits, for which expenditure is incurred from Consolidated Fund of India.
	Data controller shall collect, process, disclose, make available, or otherwise use PI only for the purposes stated in the notice after taking consent. If there is a	Section 8(2)(b): Requesting Entity ensures information is used only for the purposes of authentication Section 29(1)(b): Core biometrics only to be for the purpose of generation of Aadhaar numbers and authentication under this Act Section 29(3) (a): Identity information	

	change in purpose, must notify the data subject.	with Requesting entity only to be used for the purpose specified to the individual at the time of submitting his information for authentication Section 29(3)(b): Requesting entity shall not disclose Identity information further without prior consent of the individual	
	After PI has been used in accordance with the identified purpose, it should be destroyed as per the identified procedures	No mention	-PI stored for perpetuity -No mention if any data is retained by RE & EA or if it gets transferred directly to the CIDR servers. -Section 32(1) provides that UIDAI will keep a record of all authentication records, but does not specify retention time of these records. It is important to note that such records make it easy for tracking activities of the person concerned, and with no notification given to the data subject of when their information was accessed by law enforcement, this would be an easy means of surveillance by the Government. It has also been mentioned that this would be a violation against the right guaranteed in Article 20(3). This article includes the right against compulsory extraction of information from a person. Having enough information to profile and track a person would be a serious infringement of this right. (*Usha Ramanathan's comment on P22 of the Standing Committee's*

			Report)
	Data retention mandates by Government should be in compliance with the National Privacy Principles	N/A	Not in compliance with the National Privacy Principles No option for deletion of data even at the choice of the data subject, personal data as well as the authentication record do not specify time limit for retention
Access & Correction	Data subject shall have access, be able to seek correction, amendments, or deletion of such information where it is inaccurate	Section 28(5) proviso: Data subjects can request access to identity information, but not core biometrics Section 32(2): Data subject entitled to obtain authentication record in such manner as specified in Regulations. Section 6: Authority may require the data subject to update their demographic and biometric information as may be specified in further regulations. Section 31(2): In case any biometric info is lost or ***changes***, the data subject should ask the authority to make necessary alterations	In Section 31(2), there is an option to update the biometric information if it has 'changed'. This is an acceptance of a possibility that biometric information is vulnerable to change and hence not an infallible identity proof as has been claimed in the Supreme Court by many.
	Be able to confirm that a data controller holds	Section 32(2): Data subject entitled to obtain authentication record in such	

	or is processing information about them	manner as specified in Regulations.	
	Be able to obtain from the data controller a copy of the personal data	Partially. As per Section 28(5), cannot get a copy of their core biometrics. i.e. fingerprints, iris scans, any other biological attribute as may be specified.	
	Access and correction to any PI may not be given by the Data controller if it is not possible to do so without affecting the privacy rights of another person, unless the person has explicitly consented to disclosure.	No mention	This principle is not possible without initially demarcating what are the privacy rights granted to a person by the Indian legislature
Disclosure of Information	Data controller shall not disclose PI to third parties, except after providing notice and seeking informed consent from the individual for such disclosure	Section 29(1) (a): No sharing of core biometrics Section 29(2): Identity information shared as per the rules provided Section 29(3)(b): Requesting entity shall not disclose Identity information further without prior consent of the individual	Clarification required on sharing of data amongst government departments, and sharing of data between third parties, not government departments.
	Third parties are bound to adhere to relevant and applicable privacy principles	Section 28(4)(c): the Authority shall ensure that arrangements entered into with any third parties enforce equivalent security obligations on data protection.	

	Disclosure for law enforcement purposes must be in accordance with the laws in force	Section 33(1): By way of order of nothing lower than a District Judge, identity information or authentication records can be disclosed. This does not apply to core biometric information. Section 33(2): Any disclosure of information , including core biometrics can be done in the interest of National Security in pursuance of a direction of an officer not below the rank of Join Secretary to the Government of India, specially authorised in this behalf by an order of the Central Government. Every such direction will be reviewed before it takes effect by an Oversight Committee consisting of Cabinet Secretary and the Secretaries to the GOI, Department of Legal Affairs and the DEITY. Direction valid for 3 months, extend for another 3 months after a review.	The procedure established for disclosure for national security purposes is not reasonable, just, or fair. Where even core biometrics can be shared and disclosed, the term 'national security' is vague and has a wide scope of misuse. Huge differences when compared with Section 69 of IT Act and Rules for Interception. Section 69 (1) criteria for interception is similar to that of article 19(2) reasonable restrictions, and not simply national security. Also, Section 69(1) states that the act be necessary, and reasons be recorded in writing. The rules provide that such direction be issued after considering the option of acquiring such data by alternative means, and the destruction of such records of interception. Comparing it with the Telegraph Act, which has a provision for interception of telecommunication, but is limited to situations of public emergency and public safety and not simply national security. It is also interesting to note, that under the Telegraph Act, the direction for such interception can be given by a Home Secretary and only in urgent situations can a Joint Secretary issue such order. Both these Acts that include provisions for interception have reasonable safeguards in place with narrowly tailored criteria for interception.
	Data controllers shall not publish or in any	Section 29(4): No Aadhaar number or other information will be displayed,	

	other way make public PI, including personal sensitive information	published, or posted publicly, except for the purposes specified in regulations.	
Security	Secure PI that they have either collected or have in their custody, by reasonable security safeguards against loss, unauthorized access, destruction, use, processing, storage, modification, de-anonymisation, unauthorized disclosure (either accidental or incidental) or other reasonably foreseeable risks.	Section 28(3): The Authority shall take necessary measures to ensure that information in possession or control of the Authority, including information stored in the CIDR, is secured and protected against access, use or disclosure not permitted under this Act or regulations made thereunder, and against accidental or intentional destruction, loss or damage.	
Openness	Take all necessary steps to implement practices, procedures, policies, and systems in a manner proportional to the scale, scope, and sensitivity to the data they collect, in order to ensure compliance with the privacy principles, information	Not satisfactory	Lack of transparency and openness in the following areas: - Criteria for entities and agencies to qualify for the purposes of management of CIDR or enrollment in Aadhaar is crucial information that should not be delegated for regulations made by the UIDAI. - Clarification on retention/storage policies of these entities, or if they would be storing any data whatsoever in relation to Aadhaar

	regarding which shall be made in an intelligible form, using clear and plain language, available to all individuals.		enrollment or authentication. - Clarity on if data sharing between government departments would also qualify as third party disclosures. - When sensitive information is handed to law enforcement agencies without a legislation on privacy and data protection, such an action can be dangerous with no boundaries set for law enforcement to use this data. It is pertinent that the use of such sensitive data be limited by certain safeguards.
Accountability	Data Controller shall be accountable for complying with measures which give effect to the privacy principles		In the process of Aadhaar, there are different data controllers at various steps. At the time of enrollment, it is the enrollment agency, the time of using the Aadhaar card for certain service, the requesting agency uses the Aadhaar identity information for the purposes of authentication; and the UIDAI is the data controller when the data is stored in the CIDR and during the process of authentication for a Requesting entity. In this bill, there is no provision for complaining against any data controller, the EA, RE or UIDAI. It creates a conflict of interest where the Authority is the custodian of this data and Section 47 states that the Courts will only take cognizance of complaints that have been made by the UIDAI or any officer authorized on its behalf. Does this mean that a person cannot approach

			the police if they find that their PI has been stolen or misused?
	Such measures should include mechanisms to implement privacy policies; including tools, training, and education, external and internal audits, and requiring organization or overseeing bodies extend all necessary support to Privacy commissioner and comply with the specific and general orders of the Privacy Commissioner	No Mention	No mention of capacity building or trainings for entities that may be authorized for enrollment or authentication.