Information Technology Law

This column will be dedicated to discussion on areas of Information Technology and Intellectual Property Laws in association with Fox Mandal.

THE LEGAL FRAMEWORK SUPPORTING AADHAAR

Rajesh Vellakkat, Partner at Fox Mandal & Associates, Bangalore

Cite as: (2017) PL (IT) May ##

Rajesh Vellakkat, Partner

In the last couple of months, the Government has mandated the use of the Aadhaar number for availing various government services and benefits. It has been made mandatory for filing tax returns and for booking air and train tickets, etc. This move has been criticised by various sections of society primarily on grounds of citizen privacy and data security. The topic has been discussed at length in Parliament, and the Supreme Court is hearing various cases that have been filed before it on this subject. The media too has given wide coverage to the concerns, and helped to create an atmosphere of discomfort among the general public around the Government's insistence on using Aadhaar mandatorily for all dealings.

It is however clear that there is a general lack of awareness about the legal regime that supports the Aadhar programme. This article is aimed at creating awareness about the fairly comprehensive legal framework that exists to enable the Aadhaar programme.

In March 2016, the President of India gave his assent to the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (the Aadhaar Act). Introduction of this legislation as a Money Bill has been criticised and challenged in the Supreme Court. However, despite all the opposition it faced, the Government moved quickly to create a set of subordinate legislations and continued to insist on the mandatory use of Aadhaar for many services.

In order to address the concerns of privacy and security and establish an administrative mechanism, four regulations were made by the Unique Identification Authority of India (UIDAI), named as the Aadhaar (Enrolment and Update) Regulations, 2016, Aadhaar (Authentication) Regulations 2016, Aadhaar (Data Security) Regulations, 2016, Aadhaar (Sharing of Information) Regulations, 2016. The Aadhaar Act and these Regulations are collectively intended to create, for all residents of India, a robust identification mechanism that eliminates impersonation, duplication, fraud, forgery and many other unacceptable practises that are sadly rampant in our country.

It is very difficult to narrate the entire legal framework in a short write up; however, an attempt is made to summarise below the essential aspects of this legal framework.

The Aadhaar Act creates a statutory body called the Unique Identification Authority of India, which in turn creates and maintains the Central Identities Data Repository (CIDR), a centralised data repository to store data relating to all residents in India. A unique Aadhaar number is issued to every resident after collecting fingerprints and a scan of his/her iris (collectively referred to "biometric information") as well as name, gender, date of birth and address (collectively referred to "demographic information"). Any resident (defined as a person who has lived in India for more than 182 days in the previous year) can apply for an Aadhaar number, which is a 12 digit random number that bears no relation to the attributes or identity of the holder. An Aadhaar number issued to one person cannot be reassigned to any other person. The Aadhar number is primarily intended to authenticate the identity of the person before any subsidy or benefits are given by the Government. As like any other personal data collection requirement, the entity who would like to get an individual's data authenticated has to obtain the consent of the individual. An Aadhaar number will not confirm any right or proof

of citizenship or domicile to the holder.

The UIDAI is statutorily required to ensure security of every individual's identity records. The CIDR is required to be secured and protected against access, use or disclosure not permitted under this Act and against accidental loss or damage. Section 29(1) of the Act says that "No core biometric information, collected or created under this Act, shall be— (a) shared with anyone for any reason whatsoever; or (b) used for any purpose other than generation of Aadhaar numbers and authentication under this Act". Biometric information collected is sensitive personal data and information as defined in the Information Technology Act. A court not inferior to a District Judge can ask the UIDAI to disclose information; however, such orders can be passed only after hearing the UIDAI.

Chapter 7 of the Act provides an elaborate list of offences. Impersonation by providing false demographic and biometric information, collecting the identity or information of people without authority, intentionally disclosing, transmitting or copying identity information introducing virus or computer contaminants in the CIDR, etc. are all punishable offences leading to three years of imprisonment. If the offender is a company, it is specifically provided that whoever is in charge of the affairs of the Company shall also be punished. In order to strengthen the legal framework, the UIDAI has notified regulations.

Enrolment and update

The Aadhaar (Enrolment and Update) Regulations defines an elaborate procedure for collecting identity information. It specifies the kind of biometric and demographic information to be collected. Biometric information will not be collected for children below 5 years of age. Similarly, for people with deformities or for those who cannot provide biometric information, only biometric information that is available will be collected. UIDAI has appointed Registrars and enrolling agencies for collection of identity information. These Registrars and enrolling agencies are required to only use the software provided by UIDAI. Further, they are required to comply with the security features specified by UIDAI. The Registrar and Enrolling agencies are required to explain to the individuals who are providing identity information the purpose of the information being gathered as well as how any errors can be corrected. The Regulations include a list of supporting documents to be provided.The Registrar or enrolling agencies shall upload the information to the CIDR following which the UIDAI will perform checks including on duplications. The Regulations also provide for updating information. Provisions have also been made for omission and deactivation of Aadhaar numbers. The Regulations also provide for a Grievance Redressal Centre.

Authentication

The Aadhaar (Authentication) Regulations 2016 provide the mechanism for authenticating a person's identity, based on the data stored in the CIDR. This Regulation recognises Authentication Service Agencies and Authentication User Agencies.

The Regulations provide for two types of authentication — Yes/No authentication facility and e-KYC authentication.

The Regulations recognise three modes of authentication as listed below:

(*i*) Based on demographic authentication wherein the Aadhaar number and demographic information of the holder is matched with the information in the CIDR.

(*ii*) Biometric-based authentication where the biometric information of the holder is matched with the data stored in the CIDR.

(*iii*) Another mode of authentication recognised in this Regulation is based on a One-Time Pin (OTP) wherein an OTP with limited time validity is sent to the Aadhaar number-holder's mobile number or email address. The Aadhar number-holder provides this OTP for authentication.

The Regulations also recognise multi-factor authentication where two or more of the above modes of authentication are used in combination.

The entire authentication process should be carried out only after the consent of the Aadhaar number-holder. The requesting entity is required to maintain logs or records of such consent for a stipulated period of time. For biometric authentication, only certified biometric devices following the specification laid by the UIDAI can be used. All biometric data should necessarily be in encrypted form and the UIDAI may specify encryption standards and requirements from time to time. The application software used by the requesting entity shall conform to the standards and specifications laid down by UIDAI.

The data collected for authentication should be put in Personal Identity Data (PID) block before

transmission. The request will go through the authentication service agency. The authentication request should be digitally signed. On receipt, the CIDR shall validate the input parameters and shall send a digitally signed Yes/No authentication response or digitally signed e-KYC response. It is specifically mandated that the requesting entity shall ensure that encryption of PID block takes place at the time of capture of data as per the process specified by the UIDAI.

Another facility given to Aadhaar number-holders is the ability to permanently lock their biometrics and temporarily unlock the data whenever needed for biometric authentication.

Chapter 3 of this Regulation elaborates on the appointment of requesting entities and authentication service agencies. Requesting entities are classified into 3 categories:

(*i*) Category 1 includes Central and State Governments and their ministries, and authorities constituted under Central or State Acts.

(*ii*) Category 2 includes regulated service providers like public sector banks, foreign banks, payment and settlement system networks like ATM networks, prepaid payment network, instant money transfer, TRAI, etc.

(*iii*) Category 3 comprises private companies and partnership firms that satisfy certain criteria.

The eligibility criteria to be a requesting entity can be modified by UIDAI from time to time. Schedule B of the Regulations details the eligibility criteria for being an Authentication Service Agency. To be an eligible authentication user agency it is mandated that the entire backend infrastructure such as servers should be located within the territory of India. The agency should have a prescribed data privacy policy and the organisation should have adopted the data security requirements as per the Information Technology Act, 2000. Only after proper physical verification of these conditions will UIDAI recognise a requesting entity and authentication service agency.

Regulation 14 elaborates the functions and obligations of these agencies in great detail. It is specifically mentioned that the requesting entity shall not store, share or publish or keep a copy of the biometric information of the Aadhaar number-holder. PID blocks should not be buffered. Any identity information shall not be disclosed to anyone expect with the prior consent of the Aadhaar number-holder. The identity information collected shall be kept confidential, secured and protected. All data storage protection relating laws are to be followed. The requesting entity should maintain the logs of the authentication transactions processed by it for a period of 2 years. During this period Aadhaar number-holders shall have right to access the logs. After 2 years, the said logs shall be archived for a further period of 5 years. The requesting entity shall not share authentication logs with any person other than the Aadhaar number-holder.

The roles, responsibilities and code of conduct of the authentication service agencies are described in detailed in this Regulation. The authentication service agencies are also mandated to maintain the logs of the authentication transactions processed by it. UIDAI has the power to audit the requesting entities and authentication service agencies. The requesting entities and authentication service agencies should have their servers in data centres located in India. In case of any default by authentication service agency, the authority can suspend and terminate the appointment. UIDAI shall maintain such authentication transaction data for a period of 6 months and thereafter archive it for a period of 5 years. After 5 years, the said data will be deleted. Aadhaar number-holders have the right to access their authentication records from the authority during the 6 months. The UIDAI may also provide digitally signed e-KYC data to the Aadhaar holder through biometric or OTP authentication.

Limitations on information sharing & use

The Aadhaar (Sharing of Information) Regulations, 2016 provides for the limited sharing of information by UIDAI. Core biometric information collected by the Authority under the Act shall not be shared with anyone for any reason whatsoever. The demographic information and photograph of an individual collected by the Authority under the Act may be shared by the Authority with a requesting entity in response to an authentication request for e-KYC data pertaining to such individual. This is subject to the requesting entity obtaining consent from the Aadhaar number-holder for the authentication process, in accordance with the provisions of the Act and the Aadhaar (Authentication) Regulations, 2016. The Authority may share demographic information and photograph, and the authentication records of an Aadhaar number-holder when required to do so in accordance with Section 33 of the Act.

What can be shared by requesting entity is narrated in the

Regulations. Accordingly, core biometric information collected or captured by a requesting entity from the Aadhaar number-holder at the time of authentication shall not be stored and shall not be shared with anyone for any reason whatsoever. The identity information available with a requesting entity shall not be used by the requesting entity for any purpose other than that specified to the Aadhaar number-holder at the time of the latter submitting identity information for authentication and shall not be disclosed further without the prior consent of the Aadhaar number-holder. A requesting entity may share the authentication logs of an Aadhaar number-holder with the Aadhaar number-holder concerned upon his request or for grievance redressal and resolution of disputes or with the Authority for audit purposes.

The responsibilities of any agency collecting Aadhaar details are explained in the Regulations and as per the same any agency which collects Aadhaar number or any document containing the Aadhaar number, shall collect, store and use the Aadhaar number only for a lawful purpose. They are required to inform the Aadhaar number-holder the purpose for which the information is collected, whether submission of Aadhaar number for such purpose is mandatory or voluntary, and if mandatory, the legal provision mandating it; alternatives to submission of Aadhaar number or the document containing Aadhaar number, if any; obtain consent of the Aadhaar number-holder to the collection, storage and use of his Aadhaar number for the specified purposes. Such agency shall not use the Aadhaar number for any purpose other than those specified to the Aadhaar number-holders at the time of obtaining their consent. Such individual, agency or entity shall not share the Aadhaar number with any person without the consent of the Aadhaar number-holder.

The Aadhaar number of an individual shall not be published, displayed or posted publicly by any person. Any individual, entity or agency, which is in possession of Aadhaar number(s) of Aadhaar number-holders, shall ensure security and confidentiality of the Aadhaar numbers and of any record or database containing the Aadhaar numbers. No entity, including a requesting entity, which is in possession of the Aadhaar number of an Aadhaar number-holder, shall make public any database or record containing the Aadhaar numbers of individuals, unless the Aadhaar numbers have been redacted or blacked out through appropriate means, both in print and electronic form. No entity shall require an individual to transmit his Aadhaar number over the Internet unless such transmission is secure and the Aadhaar number is transmitted in encrypted form except where transmission is required for correction of errors or redressal of grievances. No entity shall retain Aadhaar numbers or any document or database containing Aadhaar numbers for longer than is necessary for the purpose specified to the Aadhaar number-holder at the time of obtaining consent.

Author's views on the Regulations

Having gone through the legal framework enabling Aadhaar, it is the author's view that the Government has made a fair attempt to address the important issues of data privacy, security, confidentiality and use. A reasonably robust administrative and regulatory mechanism exists to supervise and control all users of Aadhaar data.

Looking at the benefits Aadhaar will provide to our society by way of reducing if not completely eliminating pilferage of subsidies, frauds, impersonation and other offences that is prevalent in this country and the Government should be encouraged to implement this identity authentication mechanism wherever required. The current criticisms seem to be based on lack of awareness about existing regulatory safeguards and the examples of wilful violation that have come to light.

However, it is also true that no system will always remain fully secure, and no data will always be free from the risk of theft and misuse — whether it is kept in the UIDAI repository, or in physical paper form or any other digital form. Such concerns of loss of privacy and security breach should not be a reason to prevent the use of Aadhaar; rather, the emphasis should be on upgrading regulatory requirements and technology/infrastructure capabilities used by the UIDAI and others in the ecosystem. The regulations makes it clear that Government has made conscious provisions to ensure data security and Privacy compliance by companies involved in Aadhaar data use. Of course, these companies can fail in compliance. In general, complete data privacy and security for any data shared in digital world is a fallacy; data security and privacy breach is happening even in countries where the law on these subjects are very stringent. It being so, why to oppose this unique identification facility on the fear of data and privacy breach, if it apparently gives more benefits.

Rajesh Vellakkat, Partner, specializes in IPR and Technology and has been working in these areas for more than 20 years. He may be contacted at <rajesh.vellakkat@foxmandal.com>.