University of New South Wales Law Research Series

YOUR MONEY OR YOUR LIFE? MODI'S DECEPTIVE ENACTMENT OF INDIA'S ID LEGISLATION

GRAHAM GREENLEAF

(2016) 140 *Privacy Laws & Business International*

Report 18-20, April 2016

[2016] *UNSWLRS* 53

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: : http://www.ssrn.com/link/UNSW-LEG.html

Your money or your life?
Modi's deceptive enactment of India's ID legislation

Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia

Published in (2016) 140 *Privacy Laws & Business International Report* 18-20, April 2016 *

India's Modi government inherited from its Congress government predecessors a national ID system, the Aadhaar,[1] which has enrolled up to 800 million of India's 1.2 billion residents since 2009. Legislation to legitimise the system had been stalled in India's lower house (the Lok Sabha) since 2010, partly because of privacy concerns of legislators. Modi's government enthusiastically accepted this gift, promoting its expansion and defending it in the courts against constitutional claims that it infringed privacy.

However, the Supreme Court still presented a potential legal road-block, with a case concerning the Aadhaar's constitutionality having been referred to a 'constitution bench' (to be appointed by the Chief Justice) for determination. Lack of a majority in the upper house (Rajya Sabha) presented a political obstacle to obtaining legislative legitimacy for the system, which still depended on a 2009 Executive decision for its imprimatur. This serial has had many episodes since 2009.[2]

This article explains how the Aadhaar legislation has unexpectedly been enacted, the basic structure of the ID system it establishes, its potential private sector uses, the privacy vacuum within which it will operate, and how it is now much more dangerous as a result of this enactment. A concluding question is whether this Bill is what Indians have been led to expect for the last seven years, or whether they have been deceived?

A Money Bill or maybe not

In what has been described as a 'masterstroke'[3] – but one of dubious legality – the Modi government introduced the *Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Bill 2016* ('Aadhaar Bill')[4] into the Lok Sabha on 3 March 2016 as a 'Money Bill'. This characterisation (agreed to by a compliant Speaker) means that the Rajya Sabha can not stop the passage of the bill and may only make suggestions concerning it. Nor do Money Bills have to go before Parliamentary committees. The Bill passed the Lok Sabha on 11 March and will be considered approved on 25 March, because the government will not accept recommendations suggested by the Rajya Sabha.[5]

Article 110(1) of India's Constitution provides that 'a Bill shall be deemed to be a Money Bill if it contains only provisions dealing with all or any of the following matters, namely', and there follows a list of six types of financial matters (a)-(f) (in short, taxes, government borrowings,

* Thanks to Elonnai Hickock for providing very valuable comments on a draft. Responsibility for all content remains with the author.

[1] Aadhaar means 'foundation' or 'base'.

[2] For background, see articles cited herein.

[3] Gyanant Singh 'Aadhaar card is about privacy, not money' *Businesstoday.in*, 16 March, 2016 <http://www.businesstoday.in/current/policy/aadhaar-card-is-about-privacy-not-money/story/230292.html>

[4] Aadhaar Bill as passed by Lok Sabha 11 March 2016 <http://www.prsindia.org/uploads/media/AADHAAR/Aadhaar%20bill%20as%20passed%20by%20LS.pdf>

[5] The Wire Staff 'Three Rajya Sabha Amendments That Will Shape the Aadhaar Debate' *The Wire* 16 March 2016 <http://thewire.in/2016/03/16/three-rajya-sabha-amendments-that-will-shape-the-aadhaar-debate-24993/>

custody or appropriation of consolidated funds, charges on them, and receipt of monies for them), plus '(g) any matter incidental to any of the matters specified in sub clause (a) to (f)'.

Few, if any, of the 59 clauses of the 2016 Bill deal directly with such 'money matters', with the exception of cl. 7 'Proof of Aadhaar number necessary for receipt of certain subsidies, benefits and services, etc.' It would therefor seem questionable whether all remaining 58 clauses can be regarded as 'incidental' to cl. 7. Alternatively, perhaps the establishment of the world's most comprehensive biometric identification system, and the creation and regulation of the organisation which will run it, is in fact the substance of the Bill. The Aadhaar Bill is similar in many respects to the previous government's *The National Identification Authority of India Bill 2010*, which was not described as a 'Money Bill', but did not include an equivalent to cl. 7.

However, sub-article 10(3) of the Constitution says 'If any question arises whether a Bill is a Money Bill or not, the decision of the Speaker of the House of the People thereon shall be final'. The Speaker is reported to have taken a robust approach to this question: 'First Speaker GV Mavalankar stressed that the word "only" was not "restrictive" and if a Bill dealt with a tax, it could also have provisions necessary for administration of that tax.'[6]

The extent to which Article 110(1) can be satisfied by such fictions cannot be addressed here, but may become yet another constitutional issue before India's courts. The Congress Party, which also has a chequered history in abusing the Money Bills provision, has threated a court challenge.[7] In the meantime, the reality (even if temporary) of the soon-to-be Aadhaar Act must be addressed.

Mandatory use confirmed

Just as breathing is only mandatory if you wish to stay alive, obtaining an Aadhaar will only be mandatory for most people in India if they wish to avail themselves of government services (or many private sector services). Section 7 states that the Central Government or a State Government may 'for the purpose of establishing identity of an individual as a condition for receipt of a subsidy, benefit or service' paid from central government funds 'require that such individual undergo authentication, or furnish proof of possession of Aadhaar number'. Where an applicant does not yet have an ID number, the government may require that 'such individual makes an application for enrolment'. In the interim 'the individual shall be offered alternate and viable means of identification' that they can provide until their Aadhaar number is allocated. One of the amendments proposed by the Rajya Sabha, but rejected by the government, would have stated that an individual could choose 'not to opt for enrolment' for an ID number, but instead provide 'alternate and viable means of identification'.[8]

Section 7 is the core mechanism by which the Aadhaar is made mandatory. Attempts to achieve this without legislative authority have led to the cases now before the courts. There was no equivalent to this clause in the 2010 Bill (as discussed in the conclusion). Once governments can impose this mandatory requirement, pervasive use of the ID number follows rather easily. Governments and the private sector can accept the ID number 'as proof of identity … for any purpose' (s4(3)), and the private sector can make its provision (but not its authentication) mandatory wherever it wishes.

---

[6] Gayant Singh, above

[7] Times of India (staff report) 'Aadhaar Bill: All you need to know' *Times of India* 17 March 2016; The government refers to 'the juvenile justice bill and the workman injury compensation bill that the Congress brought as money bills when it was in power.'

[8] The Wire, above cited.

An Authority for life-long surveillance

The Act establishes the Unique Identification Authority of India (UIDAI – 'the Authority') which 'may engage one or more entities' to maintain the Central Identities Data Repository (CIDR) (s10) for which it is responsible.

The UIDAI 'may require Aadhaar number holders to update their demographic information and biometric information, from time to time, in such manner as may be specified by regulations, so as to ensure continued accuracy of their information' in the CIDR (s6). If addresses are required by regulations to be updated, perhaps this may be required every time a person has to have their identity authenticated, or perhaps on other events such as voting. Updating of photos may be periodically required. Since children will have ID numbers, CIDR data could accumulate over a person's whole life. There are no provisions for individuals to request that data be removed from the CIDR, and a proposed Rajya Sabha amendment to this effect was rejected by the government.

Time and circumstance, impossible to predict, will reveal to what extent CIDR data will be required to be updated. However, the CIDR has the potential to become a location register for India's people, a core form of surveillance in countries such as China and Vietnam, but one that has not occurred in modern India.

A further aspect of this continuous record of surveillance is that, although the CIDR will not record the reason for an authentication enquiry, it will record 'the identity of the requesting entity' (s2(d)). The identify of some requesting entities may be very revealing, either from the public sector (eg police) or private sector (eg a clinic). The dangers of misuse are obvious.

Authentication, uses, and 'sharing'

Any government agency, or a business or person (corporate or individual) may be a 'requesting entity' (s2(u)) entitled to obtain authentication from the Authority of the 'biometric information or demographic information' of an ID number holder (s8). The requesting entity must obtain the person's consent to collect this 'identity information' for the purpose of authentication (according to regulations), and only use it to submit it to the Central Identities Data Repository (CIDR).

The CIDR can reply with a simple 'yes' or 'no' response, or with 'any other appropriate response sharing such identity information, excluding any core biometric information' (ie fingerprints and iris scans). The CIDR may therefore provide a 'requesting entity' with any demographic information it holds (eg address, age) and any other biometric information (ie photographs). Regulations will specify the circumstances under which the CIDR can share identity information with requesting entities (s29(2)). The 2010 Bill was fundamentally different, only allowing (in cl. 5(2)) 'any other appropriate response excluding any demographic information and biometric information.' This did not allow CIDR to 'share' addresses, age or photographs.

In the 2016 Bill, individuals must be told by the requesting entity what information may be 'shared' after authentication, and to what uses they will put the information they receive. The requesting entity must tell individuals the uses to which it will put authenticated identity information, and obtain their consent before disclosing it further (s29(3)), or they will be subject to penalties. While they must be told 'alternative of submission to identity information', if over 90% of Indian adults already have Aadhaar numbers (as the government claims), then alternatives will be illusory.

ID numbers, and 'core biometrics' (fingerprints and iris scans) cannot be published or otherwise displayed, except if allowed by regulations (s29(4)). This implies that other

authenticated ID information, including photos, can be so used (subject to notice to individuals).

Private sector implications

Despite its administration within the public sector, the Aadhaar will have profound long-term implications for the operation of all aspects of the private sector operating in India, whether in relation to the customers, their employees, or any other individuals with whom they deal. This purpose is stated clearly: 'An Aadhaar number, in physical or electronic form … may be accepted as proof of identity … for any purpose' (s4(2)., and reiterated in both s57 and in s4(3) in differing words. There is no prohibition on private sector entities make provision of an ID number mandatory for any transactions they wish

It is clear from the above details that it is expected to be routine for any business in India that finds it useful to collect ID numbers, the obtain and/or authenticate further 'identity information' from the CIDR, and make extensive uses, including disclosures, of that information. While the uses of identity information in any social setting are difficult to predict,[9] there is clearly no intention by the Indian government to keep much control over the private sector uses of this ID system. The ramifications of this deserve more detailed exploration.

Built-in disclosures – Court orders and national security

'Core biometric information' (fingerprints, iris scans, and any other biometrics specified by regulations) cannot be 'shared with anyone for any reason whatsoever' or used (including by CIDR) other than for authentication or to generate ID numbers (s29(1)). This information is therefore exempt from the following disclosures, but can be used to authenticate supposed identities (eg against a fingerprint provided by a court or a security agency).

Any court (District Court or above) may order the CIDR, or any 'requesting entity' (public or private sector bodies) to disclose any identity information (eg addresses and photographs) it holds (s33(1)). There are no limitations imposed, so this could apply to orders in both criminal and civil matters, and may apply to judicial warrants.

Any specially authorised official 'not below the rank of Joint Secretary' may issue directions 'in the interest of national security', for disclosures by the CIDR, or any 'requesting entity', of any identity information or 'authentication records' (s33(2)). Any such direction must be reviewed 'before it takes effect' by an Oversight Committee.

India's privacy law vacuum continues

Other than the minimal limits on use of Aadhaar information referred to above, India has no significant privacy protections:

- Although biometric information collected under the *Aadhaar Act* is deemed by s30 to be 'sensitive personal data or information' for the purposes of s43A of the *Information Technology Act 2000* (under which India's rudimentary data privacy 'Rules' were made), this will be of little benefit. Section 30 will not prevent government abuses, because s43A and the 'Rules' only apply to companies or bodies 'engaged in commercial or professional activities'. While the UIDAI ('Authority') is created as a 'body corporate', it is not a company, and it is engaged in public administration, not commerce or a profession. Where private companies collect biometrics in the course of

[9] 'U Rao and G Greenleaf 'Subverting ID from Above and Below: The Uncertain Shaping of India's New Instrument of E-Governance' *Surveillance & Society* (2013) < http://ssrn.com/abstract=2350631>

ID creation or authentication, s30 may have some application but the whole system of s43A protections is flawed.[10]

- The Aadhaar Act does not in itself include any set of data privacy provisions, beyond a few basics of access and correction rights, protection of CIDR security, and the integrity of the enrolment/authentication processes. It does not provide remedies for individuals, and only the Authority can initiate any of its penal provisions (s47(1)).
- No comprehensive data privacy legislation has been enacted in India, though it has been proposed on numerous occasions at high levels of government.[11]
- The Modi government is arguing in the ongoing *Puttaswamy Case* that India's constitution does not provide any protection to privacy (despite long-held assumptions that case-law showed otherwise).[12]

India's lack of privacy protections will now be much more dangerous with the enactment of the Aadhaar Act. The CIDR is dangerous in itself. Records in both public sector and private sector systems will become more consistent because of Aadhaar authentication, and data matching between them will therefore be facilitated, while remaining unregulated.

Conclusion: Function creep by legislative deception

Seven years ago the Aadhaar (or UID as it was then called) was introduced as a voluntary ID number, and governments and the UIDAI constantly stressed that was so, even though this was difficult to believe.[13] The 2010 Bill did not make use of the number mandatory for any government services. Throughout the challenges in the Supreme Court to government attempts to make the use of the ID number mandatory during 2014-15, governments continued to insist that its use was voluntary. Now, after almost all of India's population has obtained an Aadhaar, the 2016 legislation includes s7 which allows governments to make its use mandatory for key government benefits. In addition, while the 2010 Bill did not allow the CIDR to 'share' address, age or photograph data, the 2016 legislation does allow this.

There are also many loopholes in the Bill where expansion by regulations is allowed,[14] and the regulation are made by the Authority itself. These include the definitions of the data that is the essence of the system ('biometric data', 'core biometric data' and 'demographic data'), and the requirements to update the CIDR, not only administrative matters concerning registration and authentication. The Aadhaar system is therefore unstable and deceptive at its core.

ID systems are prone to 'function creep', the incremental expansion of their functions, often contrary to promises made by politicians when the systems are introduced. There are few examples as blatant, even though they were predicted, as the Aadhaar's final admission of legislative compulsion, and its conversion of the CIDR from a uni-directional to a bi-directional flow of information. Much more needs to be said about the Aadhaar Act, but these are its essential deceptions.

---

[10] G Greenleaf 'India's Data Protection Impasse: Conflict at All Levels, Privacy Absent' *(2014) 127 Privacy Laws & Business International Report, 23-24*;

[11] G Greenleaf 'India's Draft the Right to Privacy Bill 2014 – Will Modi's BJP Enact it?' *(2014) 129 Privacy Laws & Business International Report, 21-24;*

[12] G Greenleaf 'Confusion as Indian Supreme Court Compromises on Data Privacy and ID Number' *(2015) 137 Privacy Laws & Business International Report, 24-26, September 2015*.

[13] G Greenleaf 'India's National ID System: Danger Grows in a Privacy Vacuum' *Computer Law & Security Review*, Vol. 26, No. 5, pp. 479-491, 2010

[14] See in particular s2(g), s2(j), s2(k), s2(m), s4(3), s5, s6, s8, s10, s23 (various ss.), s28(5), s29(4), s31, s32, s54 and s55.