India's draft *The Right to Privacy Bill 2014* – Will Modi's BJP enact it?

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

(2014) 129 *Privacy Laws & Business International Report*, 21-24

The overwhelming victory in India's May 2014 national elections of the Bharatiya Janata Party (BJP), which now holds 283 seats in India's 543-seat lower house (Lok Sabha), may end the log-jam of legislative inactivity that characterised the last few years of the previous Congress-led government. The BJP is the first party in 30 years to hold a Lok Sabha majority without relying on coalition partners. However, it has less than one fifth of the seats in the upper house (Rajya Sabha) and must rely on support from a number of small regional parties to pass most legislation. Another possibility is that where a Bill is blocked in the upper house, the Prime Minister can ask the President of India to call a joint sitting of both houses, in which it would be somewhat easier for the BJP to obtain the necessary support from other parties to make up a majority. Prime Minister Modi therefore has fewer obstacles to enacting legislation than did the Congress-led government, if not a clear path to do so. He may be able to enact a data privacy law if that becomes a BJP priority.

From 2011-13 there there were three significant proposals for a comprehensive data privacy law in India but none gained the endorsement of the previous government.[1] In February 2014 they were joined by the draft *The Right to Privacy Bill 2014*, a redraft of its 2011 draft Bill by the Committee of Secretaries (CoS), the heads of seven of India's most powerful Ministries and Departments.[2] The Notes to the re-draft say it takes into account the 2012 recommendations of the Expert Group on Privacy chaired by former Justice A P Shah. The draft Bill is not available publicly,[3] but this article is based on it. A detailed and very valuable comparison of the differences between the 2011 and 2014 draft Bills has also been published by the Centre for Internet and Society.[4] This draft Bill represents the current thinking of India's bureaucracy, and the election of a new government capable of enacting legislation makes it timely to review its main provisions.

Scope of *The Right to Privacy Bill 2014*

The essence of this Bill is that it is a very comprehensive but otherwise conventional data privacy (or data protection) law. It also contains provisions on Interception of Communications (Ch VI) and Covert Surveillance (Ch VII), and offences relating to them, which are not further discussed here.[5] All rights created under the Bill apply to 'individuals', which means residents of India (see definition of 'individual'), not only citizens (though intelligence agencies and the Home Ministry continue to lobby for that restriction). It applies to both the private sector (including non-commercial entities and individuals), and to all levels of India's public sector. Personal data

---

[1] See 'Competing comprehensive data privacy Bills' in Graham Greenleaf 'India's data protection impasse: Conflict at all levels, no privacy' (2014) 127 *Privacy Laws & Business International Report*, 23-24.

[2] Department of Personnel and Training (DoPT, Ministry of Personnel, Public Grievances and Pensions); Home Secretary; Department of Telecommunications; Department of Electronics and Informatiion Technology (DEITY); Law Secretary, Ministry of Law and Justice; Legislative Department, Ministry of Law and Justice;

[3] Director, IR, Department of Personnel and Training 'Draft CoS Note on Right to Privacy Bill' (Office Memorandum, DoPT, 3 February 2014), including 'Note for Committee of Secretaries', January 2014 (4 pgs) and 'Draft for Consideration and Approval – The Right to Privacy Bill, 2014' (34 pgs).

[4] Elonnai Hickok 'Leaked Privacy Bill: 2014 vs. 2011' (The Centre for Internet & Society, 31 March 2014) <http://cis-india.org/internet-governance/blog/leaked-privacy-bill-2014-v-2011>.

[5] For a brief critical analysis of the current law and the provisions in the 2011 draft Bill (but not the 2014 Bill), see Bhairav Acharya 'Legislating for Privacy – Part II' (The Centre for Internet & Society, 20 May 2014) <http://cis-india.org/internet-governance/blog/the-hoot-may-20-2014-bhairav-acharya-legislating-for-privacy>.

mandatorily disclosed must be processed according to this Bill, irrespective of the provisions of other Acts, so this Bill is not subordinate to other existing laws (in contrast, for example, with Singapore's Privacy Act).

The obligations under the Bill apply to a 'data controller', defined as anyone who controls, at any point in time, the personal data of a data subject (except by provision of communications or storage only). Processors are not defined separately, unlike in the 2011 draft Bill.

Extra-territoriality, non-residents and data transfers

The international dimensions of the Bill's scope are complex. Its extra-territorial scope is unclear, because it simply states that it applies to any person who 'shall collect, process or otherwise deal with personal data of any individual' (i.e. resident of India). On its face, this extends to any overseas data controller who collects or processes such data, without need for any 'Indian link' other than the residence of the data subject. The intended extra-territorial operation of the Bill is clear from the requirement that any data controller who does not have a place of business in India, but who collects, processes or otherwise deals with personal data of any resident of India, must nominate a representative resident in India who will be responsible for compliance (and therefore subject to any penalties). This provision seems similar to the position under EU law concerning extra-territoriality (an 'establishment') and the proposed requirements for a representative resident in the EU.

Data controllers may not export personal data outside India unless the recipient is 'subject to a law, code of conduct, or contract which binds such recipient to adhere to principles of data protection substantially similar to the provisions of this Act', or where the data subject consents, or where necessary for completion of a contract to which the data subject and data controller are both parties (thereby avoiding problems of privity of contract under Indian law). This is a strict data export restriction, given that the principles in the Bill (discussed below) mean that 'substantially similar' is a high benchmark. Furthermore, data controllers will remain liable for compliance by the overseas recipient, a vicarious liability provision which is unusual in any data privacy law.

These are strong provisions, protecting Indian residents no matter where or by whom their personal data is processed. However, because the Bill's protections only apply to residents of India, no protection is afforded to non-residents if their personal data is processed in India. In most cases this means that any personal data imported into India will be exempt, for example data imported from Europe for outsourced processing (a 'data imports exemption' or 'outsourcing exemption'). Such 'outsourcing exemptions' exist to some extent in the data privacy laws of Singapore, Malaysia, the Philippines, and Hong Kong.[6] The relevance of the Bill to questions of EU adequacy is therefore limited, and by itself it could not be the basis of a finding of adequacy. Such an exemption may suit US outsourcers, but not those in the EU. The existing 2011 data privacy 'Rules' under s43A of the Information Technology Act do have some application to outsourced processing (although limited relevance to domestic protection in India), but fail to provide adequate protection in themselves.[7] If were also left in place even though this Bill was enacted, this might assist on questions of adequacy, but it would be extremely confusing, particularly due to overlapping inconsistent provisions.

Privacy principles

Nine National Privacy Principles (NPPs)[8] are set out in very brief form in the Schedule, in language similar to the 1980 OECD privacy Guidelines but with a strong interpretation (for example,

[6] G Greenleaf *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP, forthcoming 2014), Ch 17.

[7] See 'Failed 2011 Data Privacy Rules' in Greenleaf 'India's data protection impasse: Conflict at all levels, no privacy'.

[8] Notice; Choice and Consent; Collection Limitation; Purpose Limitation; Access and Correction; Disclosure of Information; Security; and Accountability.

collection limited to that 'necessary for the identified purpose'). However, sections 7-28 (Ch IV) of the Bill elaborate the NPPs in ways which strengthen them to an extent which goes considerably beyond the OECD Guidelines and is in fact much closer to the EU data protection Directive and in some cases stronger than current European principles. These stronger aspects include (in brief):

- Collection directly from the individual, with limited exceptions;
- No collection of data about minors without consent of their guardian;
- Notice of the identity of intended third party recipients (including processors), and justifications for disclosures to any overseas third parties;
- Retrospective revocation of consent to collection of personal data, and resulting deletion;
- Deletion of personal data after the purpose of collection is completed;
- Data breach notifications to the DPA and the data subject;
- Where personal data is required to be in a public register, access must be limited to the extent 'strictly necessary to fulfil the purpose' of the register;
- Sensitive personal data (which has a different meaning – both broader and narrower than in the EU[9]) is not to be collected or processed without authorisation by the DPA, with ten specified exceptions, of with further consent by the data subject;
- Specific restrictions on 'collection and use of personal identifiers';
- Restrictions on the installation and use of video recording equipment in public places; and
- Mandatory Privacy Officers as identified contacts, and with compliance responsibilities, for each data controller.

If enacted, these would be one of the strongest sets of privacy principles in any data privacy law in Asia.[10] But they would be subject to broad exemptions and exceptions, and of little value until the effectiveness of the enforcement mechanisms is demonstrated.

In addition, direct marketing can only be carried out with the consent of the data subject, who can also require a data controller to cease using his or her data at any time for direct marketing (sections 37-38, Ch VIII).

Extensive exemptions and exceptions

It is not surprising that a Bill with as broad a scope and such strong principles also has extensive exemptions and exceptions, too numerous and complex to explain in an overview. Intelligence agencies have obtained extensive exemptions from the Bill for actions in the interests of the sovereignty, integrity and security of India, but are continuing to lobby for a blanket exemption. Intelligence and law enforcement agencies are exempt from most DPA complaint or other investigations, but it seems that courts have power to investigate complaints against them.

There are exemptions from most, but not all, of the privacy principles for collection and processing in these situations: by persons bound by codes of professional ethics requiring disbarment for misuse of personal data; and for purposes of national security, crime prevention or detection, apprehension or prosecution of offenders, revenue collection, historical research, statistical purposes, legal proceedings, or publications for of journalistic, literary or artistic materials. None of these exemptions are unprecedented in other countries, though they are extensive here. Other broad exemptions apply to government use of personal identifiers, which is largely unrestricted; and to individual uses for personal or household purposes (an exemption found in all data privacy laws).

---

[9] 'Sensitive personal data' is defined as 'personal data relating to: (a) physical and mental health including medical history, (b) biometric, bodily or genetic information, (c) criminal convictions (d) password, (e) banking credit and financial data (f) narco analysis or polygraph test data, (g) sexual orientation'. There is a proviso 'that any information that is freely available or accessible in public domain or to be furnished under the Right to Information Act 2005 or any other law for time being in force shall not be regarded as sensitive personal data for the purposes of this Act'.

[10] Graham Greenleaf *Asian Data Privacy Laws: Trade and Human Rights Perspectives*, Ch 17 (OUP, forthcoming October 2014).

Choice of enforcement mechanisms

The Bill creates a Data Protection Authority of India (DPA) consisting of a Chair and up to two other Members, as a statutory authority, and with some protections of independence (but perhaps not sufficient). It has a broad range of functions concerning both individual and systemic privacy issues, and strong powers to investigate the actions of data controllers and related parties, plus powers to issue directions to data controllers in relation to the discharge of any of its functions.

Data subjects may complain directly to the DPA about a breach of the NPPs, and it can make such orders as it considers necessary. It can be assumed that complaints may also be made about the NPP-related provisions in Chapter IV and elsewhere, which the DPA clearly has powers to investigate, but the Bill should clarify this. Complaints by data subjects can also first be made to the Privacy Officer of the data controller, or to the industry ombudsman of the relevant industry association. If the data subject is not satisfied with the resolution by them, he or she can still complain to the DPA of a breach of the NPPs. The DPA may appoint on of its Members, or one of its senior Officers, as an adjudicating officer for any complaint or other enquiry. Such adjudicating officers can not only give directions in relation to complaints, but can also impose penalties under the Bill's penalty provisions (discussed below). Appeals against DPA decisions may be made within 30 days to the Cyber Appellate Tribunal (CAT) established under the IT Act, and from there to the High Court of the State in which the data subject resides. Civil courts may not intervene in matters in which the CAT has jurisdiction. Unfortunately, the CAT has not been functioning for three years,[11] so this vital element of the Bill's enforcement scheme is paralysed.

A data subject can also seek compensation (and litigation costs) from a court for any breaches of the Bill which cause loss or damage to the data subject, including for adverse determinations made as a result of records which have not been corrected or updated despite requests.

Civil penalties may be issued by an adjudicating officer, up to 1 million rupees (US$17,000), or up to 2 million rupees for each subsequent offence (US$34,000). These penalties apply to any breaches of Chapter IV (in effect, any breaches of the NPPs), for contravention of directions of the DPA, and for intentional unauthorised access to personal data ('data theft'). Higher penalties of 5 million rupees (US$85,000) apply to obtaining personal data on false pretences, and for unauthorised disclosure of personal data by an officer or employee of a telecommunications provider or a government agency.

Any breaches of the Bill's provisions may also constitute a criminal offence. Where the breach is by a government department, individual officers are only liable for prosecution if the contravention has been committed with their consent or connivance, or due to their neglect. Where a breach is by a company (or firm or other corporate body) the person responsible for the company's business will also be liable for prosecution unless they can show they had no knowledge and had exercised due diligence.

The 2011 draft Bill required registration of data controllers, but that has now been dropped. In Asia, only Malaysia requires registration, primarily for revenue-raising purposes.

Industry standards and ombudsmen

The Bill has very general provisions encouraging 'industry associations' to develop 'privacy standards' consistent with the NPPs and the Bill, and to appoint an industry specific ombudsman as part of this. The DPA may make regulations based on such standards, and may make such standards by regulations where an industry fails to do so. However, such standards do not supplant the provisions of the NPPs or the Bill, or the compliant processes, so they seem to be self-regulation measures which are additional to the provisions of the Bill.

---

[11] See 'Failed 2011 Data Privacy Rules' in Greenleaf 'India's data protection impasse: Conflict at all levels, no privacy'.

Tentative conclusions concerning the 2014 Bill

For residents of India (but not persons overseas), this Bill would, if enacted, provide significant protections of international standards, if they were enforced. That is a significant 'if', because the enforcement mechanisms in the current 'Rules', particularly the CAT which this Bill also relies upon, have not functioned for three years. India has no track record whatsoever of enforcing data privacy laws. It would be up to the DPA to change that before *The Right to Privacy Act* would be credible. This brief assessment is not a detailed critical appraisal of the Bill, which would no doubt reveal many points of detail on which it could be improved, but the overall structure of the Bill is sound in theory, and compares well with most data privacy laws in Asia.

The related fate of India's ID system

The BJP did not have any specific election policy in relation to India's universal ID numbering system (UID), and so is not committed to scrapping it. India's new Home Minister, Rajnath Singh, 'has hinted at the possibility of looking at the merger of the National Population Register (NPR)' being developed by the Registrar General of India (RGI) and the UID. Both NPR and UID involve the collection of biometrics from the whole of India's population. There are various options under consideration involving some types of merger of the NPR with the UID,[12] some of which might avoid the need for separate legislation to authorised development of the UID,[13] without which the Supreme Court has said its use cannot be made compulsory, and it cannot be issued to non-citizens.[14] The Home Ministry may also push its own multi-purpose national identity card (MPNIC) scheme based on the NPR,[15] which already has legislative authority, but only applies to citizens.

A 2012 report on proposed UID legislation by a parliamentary committee headed by BJP leader Yashwant Sinha, was severely critical of the UID on many grounds, including its registration of non-citizens, its duplication with the NPR, the security and integrity of its enrolment processes, and the lack of any corresponding data privacy legislation. Expanded use of personal identifiers such as the UID are one reason the Notes to the draft 2014 Bill say 'a need has been felt' for data privacy legislation. It remains a strong possibility that these two issues will be dealt with together.

---

[12] Bharti Jain 'Rajnath hints at merger of NPR and Aadhaar' (*Times of India*, 30 May 2014) <http://timesofindia.indiatimes.com/india/Rajnath-hints-at-merger-of-NPR-and-Aadhaar/articleshow/35740480.cms>

[13] Jain, 'Rajnath hints at merger of NPR and Aadhaar'.

[14] Greenleaf 'India's data protection impasse: Conflict at all levels, no privacy'

[15] Manan Kumar 'Future of Nandan Nilekani's UIDAI hangs precariously as home ministry prepares for a kill' (DNA India, 22 May 2014) <http://www.dnaindia.com>.