India's data protection impasse: Conflict at all levels, privacy absent

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

(2014) 127 *Privacy Laws & Business International Report*, 23-24

The development of data protection in India has been stalled for at least two years. The principal reason is the degree of conflict over data privacy issues at every level, with no early solutions in sight. The result is that India's national Parliament, Supreme Court and Executive (Congress government, and Ministries alike) are all in conflict over privacy issues, and this is heighted by further conflicts with some State governments (often non-Congress governments) and some State High Courts. This article gives a brief explanation of these privacy conflicts, and their interconnections, as at the end of 2013. With national elections to be held in April or May 2014, there is little likelihood of resolutions before a new government is in office.

Failed 2011 data privacy Rules

India did not have any general data protection legislation until 2011, when a set of Rules (delegated legislation) made under s43A of the *Information Technology Act 2000* (IT Act) purported to create a whole data privacy regime. These Rules superficially resemble a data protection law, but they have crippling deficiencies and ambiguities, only some of which can be mentioned here: they may be *ultra vires*; half of the Rules only apply to a very restrictive definition of 'sensitive personal data', and not to other personal data; half of them do not impose obligations in relation to data subjects per se, but only to 'the provider of the information'; and it is questionable whether and when consumers (data subjects) are given a right of civil action. No consumer has exercised any rights under these Rules, and after two and a half years they have had no visible effect.

The data privacy Rules, along with other aspects of the IT Act, are supposed to be enforced by a system involving an 'Adjudicating Officer' (AO) in each of 35 State governments, plus a right of appeal to the Cyber Appellate Tribunal (CAT). After nearly a decade of operation, the 35 Adjudicating Officers have produced an average of about 13 decisions per year across the whole of India (a total of 125) by, and only four of these decisions are readily available (none on privacy issues). The CAT is also in practice defunct, and has not delivered any decisions, or heard any new matters, since 30 June 2011[1] the date on which the CAT last had a Chairman. A bench of the CAT cannot hear a matter without the Chairman as part of it.[2] It is claimed that there has been no appointment because the Chief Justice refuses to consent to the Union Law Minister's nominee for Chairman, and the Minister refuses to nominate an alternative candidate.[3] This AO/CAT complaint system appears on paper as if it could be made to work, but is currently almost completely lacking in either effect or transparency. In terms of either legal principles or enforcement India therefore does not yet have a privacy law in reality.

[1] There are no published decisions of the Tribunal on its website since June 30, 2011: Cyber Appellate Tribunal at <http://www.catindia.gov.in/>

[2] Vijayashankar Na "Cyber Appellate Tribunal Chairman-Status' (Naavi blog, 5 June 2013) <http://www.naavi.org/wp/?p=1474>

[3] Vijayashankar Na '13th Anniversary of the Indian "Digital Society Day"' (Naavi blog, 17 October 2013) <http://www.naavi.org/wp/?cat=34>

Trade and adequacy

India's outsourcing industry is of considerable national economic importance, but is facing strong economic challenge from countries such as the Philippines. It also faces legal impediments, because of the European Union's restrictions on exports of personal data from EU Member States to countries which have not been held to provide 'adequate' data protection the 1995 EU DP Directive. India's laws were not found to be 'adequate' in a previous EU study in 2010.[4] A further expert report was obtained by the EU in 2013, and according to the Data Security Council of India:[5]

> India and EU have appointed an Expert Group comprising experts from both the sides to discuss the findings of the EU Data Adequacy report on Indian data protection regime. With representation from DSCI and NASSCOM, the group will also review the periodic progress made by EU and India on the implementing the recommendations of the Expert Group with the ultimate objective of exploring the possibility of provisional adequacy and specific arrangements for IT/BPM sector. First meeting is proposed in Feb 2014 in Brussels.

India has tried to link what it calls 'data secure status' to its negotiations for a proposed EU-India Free Trade Agreement (FTA), but EU representatives have stated that adequacy status is not a matter that can be included in trade negotiations,[6] which seems to be clear from the Directive. The FTA negotiations are reported to be 'in suspended animation' at least until the 2014 Indian elections are held.[7]

The conflicts around the ID system

Since 2009, India's Congress party national government has aggressively pursued the development of an ID system, the Unique Identification Number (UID number or aadhaar), with the ostensible aim of increasing social inclusion by providing a verifiable means of identification to the large proportion of India's population that lacks it. The Unique Identification Authority of India (UIDAI) was established by Executive Order in 2009. The UIDAI aims to issue a biometric-based unique ID number to all of India's estimated 1.2BN population, and claims to have issued about 450M UIDs. The UIDAI claimed from the outset that obtaining a UID number was not compulsory, that it did not involve the issue of a card, and that it was not an indication of 'citizenship' because it was available to any resident of India. However, by a variety of means, possession of a UID (or at least one of a variety of 'official' documents stating it) has become compulsory, in some States in India, for people to obtain various essential services such as LPG gas allocations. This is very contentious, e.g. because of the delays and difficulties that many people have in obtaining UIDs, because of privacy concerns, and because some governments in States which are not Congress-led, such as West Bengal, see no reason to promote a key Congress party political initiative which is of dubious legality.[8]

---

[4] Nayanima Basu 'Data adequacy grant to India non-negotiable, says EU envoy' (Business Standard (India), 17 May 2013) <http://www.business-standard.com/article/economy-policy/data-adequacy-grant-to-india-non-negotiable-says-eu-envoy-113051700013_1.html>

[5] (2013) 4(7) *DSCI News*, p.2 (Nov/Dec 2013)

[6] Basu, ibid.

[7] Rajat Pandit 'Free Trade Agreement with EU in suspended animation till new govt takes over' (Times of India, 8 December 2013) <http://timesofindia.indiatimes.com/business/india-business/Free-Trade-Agreement-with-EU-in-suspended-animation-till-new-govt-takes-over/articleshow/27043726.cms>

[8] Ursula Rao and Graham Greenleaf 'Subverting ID from above and below: The uncertain shaping of India's new instrument of e-governance', (2013) 11(3) *Surveillance & Society* <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2350631>; Graham Greenleaf 'India's National ID System: Danger Grows in a Privacy Vacuum' (2010) 26(5) *Computer Law & Security Review*, pp. 479-491, <http://ssrn.com/abstract=1964046>

The government introduced the UIDAI Bill 2010 into Parliament in 2010 to give the UID a legislative basis, but its passage has been blocked, including on the grounds of its privacy deficiencies, and that it is not accompanied by a national data privacy Bill. It announced it would re-introduce an amended UIDAI Bill when Parliament resumed in December 2012, but has not yet tabled it. The Parliamentary committee that previously opposed it says the revised Bill does not address its concerns.

The need for enabling legislation became acute on 22 September 2013, when a two judge bench of India's Supreme Court issued an interim ruling in *Puttaswamy* v *Union of India*,[9] an action commenced by a retired High Court judge, holding that (in the absence of enabling legislation) it was unconstitutional for possession of a UID to be made compulsory for any person to obtain essential services from the government, such as LPG gas allocations. It was also unconstitutional, in the absence of enabling legislation, for UIDs to be issued to persons who were not Indian citizens, as evidence suggested had been the practice. In October, a full Supreme Court bench continued the previous prohibitive orders, but has not yet issued its final judgment on unconstitutionality. Since then, conflict continues, with some government agencies continuing to ignore the Supreme Court orders and require UIDs as a condition of service, while on the other hand the Madras High Court has directed public sector oil companies to await the Supreme Court's final decision before requiring an Aadhaar-linked bank accounts before remitting LPG subsidies.[10]

Competing comprehensive data privacy Bills

The most direct solution to India's problems with the EU, and one means of addressing privacy concerns about the UID, as well as the step which would deliver the most benefits to consumers and citizens in India, would be if India enacted an international standard data privacy law. This is not a far-fetched possibility, because since 2011 there have been three significant steps toward such legislation: (i) a draft *The Right to Privacy Bill, 2011* drafted by the Department of Personnel and Training and considered (largely favourably) by the Committee of Secretaries (2011); (ii) recommendations for a Bill from a report by a government-appointed 'Group of Experts' chaired by former Justice A P Shah (2012)[11], and (iii) a non-official Bill jointly developed in 2013 by a business group (the Data Security Council of India) and a civil society organisation (the Centre for Internet & Society, Bangalore).[12] While all three Bills have their differences, their many similarities include coverage of both public and private sectors, a data protection authority, a conventional definition of 'personal information', and privacy principles generally up to OECD standards. They differ somewhat on the range of enforcement methods and whether individuals would have court actions available. Modest improvements could bring any of them to an international standard. None of these draft Bills have yet been adopted as government proposals.

Business certainty, consumer protection

From a business perspective, where ID cards and constitutional issues and usually of secondary concern, the significance of these conflicts is that one of the most plausible solutions to these impasses (other than a complete change of the political landscape) would be political compromises resulting in a 'package' of legislation to legitimate the ID system, accompanied by something like a

---

[9] *Justice KS Puttaswamy (Retd.) v. Union of India & Ors.*, WP (c) 494/2012. The Court's order is available, but no written judgment was provided.

[10] 'Await SC Verdict on Linking Aadhaar Card, Bank account' (New Indian Express, 24 January 2014) <http://www.newindianexpress.com/states/tamil_nadu/Await-SC-Verdict-on-Linking-Aadhaar-Card-Bank-account/2014/01/24/article2016973.ece>

[11] Report of the Group of Experts on Privacy, Planning Commission< Delhi, 16 October 2012, at <http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf>

[12] For the background to this Bill, see CIS 'The National Privacy Roundtable Meetings' (CIS, 19 September 2013) <http://cis-india.org/internet-governance/blog/national-privacy-roundtable-meetings#fn13>.

'normal' data privacy law. This might also assist India to secure the trade benefits of an 'adequacy' determination by the EU. No one in India is yet proposing such a package, but it is not uncommon for privacy laws to be the trade-off for laws increasing surveillance. Potential trade benefits would increase the attraction to some business and political groups. Whether consumers would benefit overall would depend on the details of the compromise.