University of New South Wales
University of New South Wales Faculty of Law Research Series
2011

Year 2011 *Paper* 45

India's U-turns on Data Privacy

Graham Greenleaf*

*University of New South Wales, g.greenleaf@unsw.edu.au

India's U-turns on Data Privacy

Graham Greenleaf

Abstract

India sought an 'adequacy assessment' from the EU in 2009/10 (no outcome has been announced), to ease compliance burdens in relation to outsourcing. By late 2010 it had no significant data protection laws in force. The Information Technology Act 2000 covered little of significance to data privacy, and amendments to it in 2008 which could create remedies for disclosure of 'sensitive' information depended on Rules yet to be made. A year later, the situation is quite different. India has implemented an extensive data privacy regime (limited to the private sector) through Rules made under s43A of the IT Act (as amended in 2008), which deals with negligence in providing and 'maintaining reasonable security practices' (April 2011). The essence of India's data protection scheme seems to be that the Rules made under s43A comprise part of the obligations on companies to both have in place and to implement a comprehensive information security programme. Whether the whole s43A scheme is ultra vires, or even unconstitutional, may eventually be tested by the Courts, but for now it is the law. The Rules then set out a conventional set of data protection principles, provide data export limitations, and even attempt to control what use foreign recipients make of data from India when they use it in their own countries, an innovation sure to annoy those opposed to effective data protection. Enforcement of complaints is through a special system of investigation by Adjudicating Officers, with a right of appeal to the Cyber Appellate Tribunal (CAT). The whole system is as yet untested, but has the appearance of a serious data privacy regime, except for the absence of a DPA. In August 2011 the relevant Ministry seemed to panic about what it had done with these Rules, and issued a 'Press Note' which purported to 'clarify' them to the effect that they did not apply to companies in India and overseas involved in outsourcing relationships. The interpretations in the 'Press Note' attempt to defy the meaning of the words in the Rules and the legislation, and should be regarded with scepticism.

A draft Privacy Bill, 2011 (India Legislative Department, 2011) also became public, but has not been introduced into Parliament. If enacted, it will create a three person Data Protection Authority of India (DPAI). The Bill will also create a statutory right of privacy (another first for the Asia-Pacific), open-ended in its definition but including rights of confidentiality, freedom from surveillance, and protection of personal data (possibly including the specific rights under the s43A Rules system). The Bill also sets out a detailed data privacy code, somewhat different from that under the s43A Rules. The DPAI will have very extensive functions, including keeping a register of data controllers (a step out of keeping with all other Asia-Pacific laws), and strong powers to investigate the actions of any data controller and issue directions to them. Individuals will be able to lodge complaints against data controllers with the CAT, which would be empowered to make any orders it thinks fit including compensation. A bizarre aspect of the Bill, for a country seeking an EU adequacy finding, is that it limits its protection to Indian citizens. The Bill is very complex, including detailed controls on surveillance as well, but only a draft as yet, and will undoubtedly be modified very considerably before it progresses.

India is therefore one of the few countries to have enacted data privacy laws for its private sector, but not for its public sector. That may not prove to be tenable in the longer run.

India's U-turns on data privacy

Graham Greenleaf, Professor of Law & Information Systems, University of New South Wales <graham@austlii.edu.au>
8 November 2011 *This paper is a compilation of four articles published as a series throughout 2011 in* Privacy Laws & Business International Report*, Issues 110-114* <*http://www.privacylaws.com*>

Contents

Introduction – Little privacy before 2011

In a survey of India's data privacy protections to the end of 2010 I concluded that India did not provide significant protection to personal data in relation to all or most of the common privacy principles, in any sector, to meet any international standards. It was is still an open question whether India was taking steps to do so, or whether this is an illusion. I suggested that external observers needed to suspend their belief in promises even when embodied in legislation, and insist that India move from illusions or promises to verifiable reality, if it wants its data protection efforts to be acknowledged as providing an international standard of protection[1].

In twelve months, a great deal has changed, attempts have been made to pretend that it has not changed, and proposals have been made that it should change even further. But confusion, and perhaps illusion, remains and it is still difficult to identify reality in Indian data protection. The following four articles show how India's privacy U-turns evolved through 2011.

India attempts data protection by regulations (April)[2]

India does not have a comprehensive data protection law covering any sector. Its only such attempt, on credit reporting, is ignored by both the regulator (the Reserve Bank of India) and the regulated (credit reporting agencies).

The Information Technology Act 2000 ('IT Act') is India's only significant legislation with potential effect on information privacy generally, although it deals primarily with electronic transactions and digital signatures. Even after extensive amendments by the Information Technology (Amendment) Act 2008 ('ITAA') (see Greenleaf, PL&B International, June 2009, p.1)), it only covers what appears to be a small part of what is normally dealt with by information privacy legislation, through a civil law provision on data security (s43A), with compensation for data subjects. There are other minor provisions: an offence against wrongful disclosure; and identity-related offences that also give some protection against wrongful disclosures of personal information.

The key data protection provision (s43A), has not until now been effective due to lack of implementing regulations. However, proposed new Rules under s43A, which could come into force at any time, give the appearance of not only providing an implementation of the 'security principle', but also (and surprisingly) adding an extensive set of other data protection principles.

However, whether these Rules (if and when implemented) can deliver the substance of data protection, or are just an unenforceable illusion, is the subject of this article. It is not an easy question to answer.

---

[1] Greenleaf G 'Promises and illusions of data protection in Indian law' International Data Privacy Law (2011) 1(1): 47-69 at <http://idpl.oxfordjournals.org/content/1/1/47.full>

[2] Published as Greenleaf, G 'India attempts data protection by regulations' *Privacy Laws & Business International Report*, Issue 110: 11-14, April 2011:

Section 43A – civil liability for personal data security

Section 43A of the IT Act, inserted by the ITAA in 2008, provides:

> 'Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected'.

There is no limitation imposed on the compensation that can be awarded. At first glance this looks like a useful data protection provision dealing with data security: organisations controlling personal data that fail to implement reasonable security procedures will be liable to pay compensatory damages to 'the person so affected' for resulting 'wrongful loss'. Data leaks and other data security breaches could, it seems, result in compensation to the data subjects so harmed. Foreign companies dealing with Indian outsourcing organisations could also have a statutory basis for compensation, as could Indian companies outsourcing some of their processing.

However, on closer inspection, s43A has limitations which need to be considered. The scope of s43A is limited to a 'body corporate', which 'means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities'. Its scope is therefore limited to the private sector. The last clause would also exclude religious and social organisations whose activities are not classified as 'commercial'. 'Company' will be used hereinafter, for convenience.

Section 43A's operation is also made somewhat more complex by the protection against liability given to intermediaries in certain cases (s79). Where s79 applies, 'an intermediary shall not be liable for any third party information, data, or communication link made available or hasted by him' (this should presumably say 'hosted'). 'Third party information' is defined to mean 'any information dealt with by an intermediary in his capacity as an intermediary', and this limitation may also apply to 'data' and 'communication'.

The draft Rules for data protection

The Department of Information Technology within the Ministry of Communications and Information Technology has now completed receiving submissions on Draft *Information Technology (Reasonable security practices and procedures and sensitive personal information) Rules*, *2011*, to be made under s87(2)(ob) of the IT Act (as inserted by the ITAA), allowing rules to be made concerning 'the reasonable security practices and procedures and sensitive data or information under section 43A'. Once made, the Rules will come into force on the date of their publication in the Official Gazette.

An important point is that these proposed Rules do not purport to be made under any statutory power other than that provided by s43A. Given that s43A does not purport to regulate anything other than 'negligen[ce] in implementing and maintaining reasonable security practices and procedures', it is difficult to see any legislative mandate for the Rules to impose any obligations other than those which can be described as 'reasonable

security practices and procedures'. This brings into question how the proposed Rules dealing with privacy policies, a variety of data protection principles, and disclosure of data (Rules 4-6 respectively) can be enforced (or even made *intra vires*) unless they can be related to what is defined as 'reasonable security practices and procedures'.

'Reasonable security' defined

The IT Act makes the meaning of 'reasonable security practices and procedures' depend on the existence of regulations. Before proceeding further it is therefore essential to examine Rule 7 which provides such a definition:

> 'Any person, including a body corporate shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards which shall require a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected. In the event of an information security breach, any such person, including the body corporate shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies' (Rule **7**(1)).

On its face, this requires the company to 'have implemented' such a security programme, not merely to pay lip service to one. Presumably, negligent failure to implement such a programme, if proven to cause the requisite damage, will constitute a breach of s43A. There is no reference to negligent failure to implement in Rule 7(1), the latter part of which requires companies 'to demonstrate' that they 'have implemented' the required standard. It is however, hard to see how this Rule can override the requirement of negligence stated in s43A, and the requirement 'to demonstrate' should best be considered as a separate obligation relating to security, not as a reversal of the onus of proof.

The Rule goes on to state that Rule 7(1) enshrines the Standard IS/ISO/IEC 27001 which 'has been adopted by the country' (Rule 7(2). Furthermore 'Industry associations or industry cluster who are following other … codes of best practices for data protection and fulfill the requirement of [Rule 7(1)] shall get their codes of best practices approved by the government'. Finally, those who comply with either of these approaches, 'shall be deemed to have complied with reasonable security practices and procedures' (Rule 7(4)).

Although the wording is somewhat confusing, the essence of India's data protection scheme (if the draft Rules are implemented) seems to be obligations on companies to both have in place and to implement 'a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected'.

The only way to give meaning to Rules 4-6 is to conclude that they constitute some (not necessarily all) of the requirements necessary for such a security programme, the breach of which will constitute a failure to have or implement the requirements of Rule 7. Assuming this is correct, we can now turn to what personal data is covered, and which obligations have been defined by Rule 4-6 in relation to such data.

What personal data is covered?

'Sensitive personal data or information' is defined (Rule 3) to include

> 'information collected, received, stored, transmitted or processed by body corporate or intermediary or any person, consisting of: (i) password; (ii) user details as provided at the time of registration or thereafter; (iii) information related to financial information such as Bank account / credit card / debit card / other payment instrument details of the users; (iv) Physiological and mental health condition; (v) Medical records and history; (vi) Biometric information; (vii) Information received by body corporate for processing, stored or processed under lawful contract or otherwise; [or] (viii) Call data records'.

However, this is an inclusive definition, so other data may be covered, within the ordinary meaning of **'**sensitive personal data or information', according to principles of statutory interpretation. On its face, it is a broad if unusual definition of personal data in its specific inclusions, which seem to cover most normal categories covered in other countries' laws. It is in any event is subject to expansion by the courts.

The use of 'sensitive' is not helpful for comparative purposes, because much of what is covered by this definition would simply be included in the definition of 'personal data/information' in other countries' legislation, and not in the more restricted category of 'sensitive data/information' given a higher standard of protection. Given that the Indian provision is not directed at providing a higher standard of protection than other personal data, it is better to think of this as the Indian definition of 'personal data'.

There is a proviso to Rule 3 that 'any information that is freely available or accessible in public domain or accessible under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for purposes of these rules'. Such provisions are not unusual in other countries' laws.

Other definitions

The IT Act does not deal specifically with data protection, so core concepts such as 'personal data/information', 'processing', 'disclosure', and 'consent' are not defined in that Act. There is a very broad definition of 'data' in the IT Act (s2(1)(o)), which covers data 'in any form' 'which is intended to be processed, is being processed or has been processed in a computer system or computer network'. Data in entirely non-automated systems would therefore not be covered by the Act, but data in non-electronic form which had previously been the subject of processing could be. 'Information' has a broad definition in terms of media, and is not restricted to personal information.

The draft Rules, on the other hand, provide a number of significant definitions in Rule 2. "Password", "Biometrics" and "Call data record" are all given broad definitions which should

not unduly limit the scope of the Rules. "Data", "Information", and "Intermediary" are given the same meaning as in the Act.

Privacy policies required

A company or person acting on its behalf who 'collects, receives, possess, stores, deals or handle ['personal information' (these words are missing in the draft)] shall provide a privacy policy for handling of or dealing in user information including sensitive personal information and ensure that the same are available for view by such providers of information who has provided such information under lawful contract'. 'Such policy shall provide for: (i) Type of personal or sensitive information collected under sub-rule (ii) of rule 3; (ii) Purpose, means and modes of usage of such information; (iii) Disclosure of information as provided in rule 6' (Rule 4).

Data protection principles

Rule 5 sets out briefly quite a comprehensive set of data protection principles, covering collection (consent, lawful use etc), notice, retention, internal use, access, correction, security, and handling of grievances. Each is paraphrased briefly below. Given that s43A only deals with 'sensitive personal data or information' and the Rules also imply such a limitation in their title, it can be assumed that they only relate to sensitive personal data as defined. The paraphrases below simply refer to 'personal data', for better comparative understanding. Where 'information' is used in quotations, it means the same thing.

Collection: Companies must obtain, before collection, consent from the provider of the personal data 'regarding purpose, means and modes of uses'.

Lawful purpose and minimal collection: The collector must ensure that 'the information is collected for a lawful purpose connected with a function or activity of the agency'; and 'the collection of the information is necessary for that purpose'.

Notice: Companies 'collecting information directly from the individual concerned' (but not otherwise), 'shall take such steps as are, in the circumstances, reasonable to ensure that the individual concerned is aware of' the fact of collection, the purpose, the intended recipients, and the contact information for the collector and the party that will hold the data (Rule 5(3)).

Retention: Companies may not retain personal data beyond when it may lawfully be used.

Use limitation: Personal data must be used for the purpose for which it has been collected.

Subject access and correction: Companies must permit the users to review the personal data they had provided and modify the same, wherever necessary.

Opt-out: Companies must provide 'an option to the provider of the information to opt-in or opt-out'. This is not an option necessarily provided to the data subject.

Security: Companies must 'keep the information secure'.

Complaints regime: Companies must 'address any discrepancies and grievances of their users with respect to processing of information in a time bound manner'.

Disclosure limitations and exceptions

Companies disclosing personal data to any third party require prior permission from the provider of the personal data, who has provided such information under lawful contract or otherwise (Rule 6(1)). Where companies have received 'sensitive personal information' from a third party rather than from the data subject, this provision will not require them to obtain permission from the data subject for disclosure. This significantly weakens the data protection value of this key provision.

A proviso to Rule 6(1) provides an exception for disclosure where 'the information shall be provided to government agencies for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, and punishment of offences'. Government agencies must provide written requests to companies holding sensitive information 'stating clearly the purpose of seeking such information'. The government agency shall also state that the information thus obtained will not be published or shared with any other person. While breaches of this undertaking could result in an action for breach of confidence, a direct prohibition would be more useful (but perhaps *ultra vires*). Information may also be disclosed by an order under any law in force. These exceptions are no worse than found in many data protection laws, and are not accompanied by a host of other exceptions.

Companies must not publish sensitive personal information. Third parties receiving personal data under this Rule 'shall not disclose it further'.

Enforcement – the uncertain ingredient

The IT Act establishes special procedures for civil actions coming under it which operate through specialist tribunals outside the normal civil courts. Any contraventions of the Act coming under Chapter IX (Penalties and Adjudication), which includes s43A, are to be heard by an adjudicating officer (AO) appointed by the Central Government, who is to hold an inquiry (s46(1)). AOs must have 'experience in the field of Information Technology and legal or judicial experience' (s46(2). The Secretaries of the Departments of Information Technology in each State or Territory have been so appointed. Anyone aggrieved by an order of an AO may appeal to a Cyber Appellate Tribunal (CAT) with jurisdiction in the matter (s57(1)).

Cyber Appellate Tribunals (CATs) may be appointed by notification by the Central Government, with jurisdiction over specified matters and places (s48). As yet there is only one CAT, in Delhi, but there is press discussion of the need for another CAT for South India to be established in Bangalore. They comprise a Chairperson (with qualifications as a High Court judge) and other Members (with ICT and legal qualifications) (ss49-50). Tribunals are not to be bound by civil procedure laws 'but shall be guided by the principles of natural justice' (s58(1)), and with the same enumerated powers as a civil court (s58(2)). AOs have the same powers as a civil court conferred on the Cyber Appellate Tribunal. This would seem to give both bodies independence from government instructions in carrying out their duties.

To date, the CAT has delivered decisions in a few matters, but none relevant to data protection. As yet no appeals from a CAT have been heard by a High Court. This aspect of India's data protection structure is newly established, and it is premature to assess how well it will work, including its independence.

Compensation

If the interpretation of the role of Rules 4-6 taken in this article is correct, then it may be that the CAT or a court could consider that a breach of any of the conventional set of data protection principles contained in them was also a breach of s43A, at least if it resulted from negligence (or an intentional act). If so, the negligent company will 'be liable to pay damages by way of compensation'. But the CAT cannot award any other remedies, and it is not clear that the 'wrongful loss' caused can include damage to reputation or emotional distress, as is common in other data protection laws. Although 'wrongful loss' and 'wrongful gain' are defined by Section 23 of the Indian Penal Code, s43A is a civil compensation provision and its meaning is not necessarily the same, particularly as those definitions require use of 'property', and information by itself is not usually regarded as property.

Conclusions

There are also many other questionable matters of interpretation concerning both s43A and the proposed Rules. The failure of the Rules to clearly distinguish between the rights of data subjects and the rights of third party providers of personal information is a confusing matter.

The effectiveness of enforcement through the CAT is also uncertain. The right of action before the CAT certainly appears to be a useful remedy, in the nature of a right of action before an independent, and informal, tribunal. Complaints can also be resolved before they get to the CAT by a decision by an adjudicating officer (AO). However, it does not seem that either an AO or the CAT would have the resources (or jurisdiction) to independently investigate a complaint, so that aspect of a data protection authority's role is still missing. Other tribunals in India are coming under constitutional challenges because of such deficiencies, and such a challenge could also not be ruled out in relation to the CAT and the AOs. India's data protection may therefore be on shaky foundations.

The proposed IT Act Rules are a novel way to introduce a data protection regime into a country. In a short review such as this, even before they are finalised, it would be unwise to draw any final conclusions, other than that this appears to be a potentially significant step in the evolution of data protection in India.

References

Decisions of the Cyber Appellate Tribunal are available at <http://www.mit.gov.in/content/judgment-cat>

The draft Rules are on the DIT Cyber Laws & Security page at http://www.mit.gov.in/content/cyber-laws

Outsourcing: No cause for panic (June)[3]

India's new privacy law is now operational, with the coming into force by gazettal on 11 April 2011 of the *Information Technology (Reasonable security practices and procedures and sensitive personal information) Rules, 2011*, made under s87(2)(ob) of the *Information Technology Act 2000* (IT Act).

The Rules are the same as the draft analysed in the previous issue (*Privacy Laws & Business International Report* Issue 110, April 2011, pgs 11-14), with the very important difference of addition of a new Rule 7 ('Transfer of information') which limits personal data exports rather strictly.

All overseas organisations using data processing or data collection facilities based in India will now have to consider the need to adjust their practices in light of the new regulations, which are an extensive set of data protection principles, even though they are technically only an implementation of a data security requirement. This may present problems of whether they are *ultra vires*, but until then businesses can only safely assume they are valid.

The regulations are already causing some commentators to issue dire warnings to outsourcers. MH Wugmeister and CJ Rich of Morison & Foerster, for example, warn of 'a profound effect on multinational businesses that either outsource business functions to Indian service providers or maintain their own operations in India'. Halpert et al from DLA Piper express concern that the rules might 'strangle' the Indian outsourcing industry 'by the application of highly restrictive and burdensome data transfer regulations'. The implications are serious, but not quite as sweeping as these warning suggest.

Wugmeister and Rich sum up the broad application of the Rules to information about non-Indians as follows: 'neither the IT Act nor the Privacy Rules limit the application of these rules to the collection and use of personal data from or about Indian citizens or residents, nor do they limit the application just to situations where the Indian entity is acting as the "data controller" or "principal." As a result, these Privacy Rules appear to apply to any personal information that is collected from within India, regardless of whether the organization is collecting information from individuals who reside outside of India, and no matter what role the entity in India plays'. The IT Act s79 limitation of liability for intermediaries that they think may have some effect is in fact not relevant.

Collection of data in India

The main reason for concern is that Regulation 5(1) states that 'Body corporate or any person on its behalf shall obtain consent in writing through letter or fax or email from the provider of the sensitive personal data or information regarding purpose of usage before collection of such information'.

It should first be noted that this refers to obtaining written consent from the 'provider' of the personal data, rather than from the subject of the personal data (or as rule 5(3)

[3] Published as Greenleaf G 'Outsourcing and India's new privacy law: No cause for panic' *Privacy Laws & Business International Report*, Issue 111: 16-17, June 2011; The assistance of Prof Shamnad Basheer of NUJS Kolkota, and Prashant Iyengar of the Centre for Internet and Society, Bangalore, is acknowledged with thanks.

puts it 'the person concerned', distinguishing it from 'provider'). So, where company A in Europe or the USA transfers personal data to company B in India for processing, company B only needs to obtain the written consent of company A. Transcription of medical notes, transfer of HR records etc will be unaffected by this.

The problem arises when Indian company B deals directly with the European or American clients of European or US company A, and obtains personal data 'directly from the person concerned'. Then, that person is the 'provider', and so their written consent to obtain the information must be obtained ('through letter or fax or email'). However, this written consent can be obtained by company A in Europe or the USA, which would make the provision more practical. This is clear from the reference to 'or any person on its behalf' (rule 5(1)). The DLA Piper authors regard this as uncertain, and look for clarification from the Ministry. While the rules could be changed, unless this happens any 'clarifications' must come from the Cyber Appellate Tribunal or the Courts.

Indian company B will also have to take reasonable steps to ensure that that person is aware of '(a) the fact that the information is being collected; (b) the purpose for which the information is being collected; (c) the intended recipients of the information; and (d) the name and address of — (i) the agency that is collecting the information; and (ii) the agency that will retain the information' (rule 5(3)). Once again, company A could inform all its customers that its data collection etc operations will be outsourced to company B in India, and then provide evidence of this informing to company B.

These requirements will no doubt annoy European and US companies who like to hide the fact that they are outsourcing data processing to India, but what a good result for data subjects: they will actually be told when their personal data is going overseas, and to whom. And if European or US companies chop and change their overseas outsourcers, their customers will have to be told again. It is called 'transparency', and is one of the things lacking from so-called 'accountability'.

Wugmeister and Rich complain that US and European companies may have to 'adjust their practices' at home even though they 'comply fully with US or EU privacy rules'. What irony, in light of US and European attempts to force tougher intellectual property laws on developing countries.

Disclosure by the Indian outsourcing agent

Once Indian company B has collected, or processed, personal data can it disclose the personal data to its client, outsourcing US or European company A? Such disclosure 'to any third party' requires 'prior permission' from the 'provider' of the personal data, no matter how the personal data has been provided (Rule 6(1)). There is an exception to the requirement of permission where 'such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation'. This would include a contractual obligation (particularly since rule 6(4) covers statutory obligations).

As discussed above, where the 'provider' is not the data subject (eg in HR record processing or medical transcriptions), this disclosure restriction will have no effect, because company A can provide the consent. But where the personal data has been collected by the Indian company directly from the data subjects (no matter where located), permission for disclosure must be obtained from the data subject. Rule 6 does not say the permission must be given to the Indian collector, so it could be given in advance to the US or European client. Nor does it

say that it must be in writing, so it could be collected verbally and recorded by the Indian company. Compliance will require adjustments, but is not unduly onerous, given the privacy interests at stake.

Also, where Indian company B has received the personal data from a third party rather than from the data subject, rule 6 will not require them to obtain permission from the data subject for disclosure. This significantly weakens the data protection value of Rule 6, but makes compliance much easier.

Extra-territorial reach?

Rule 6(4) provides that the third party (US or EU company A) receiving the personal data from Indian company B or any person on its behalf under rule 6(1) 'shall not disclose it further'. Once it is 'tainted' by Indian processing, US companies would be prevented from doing whatever they liked with personal data.

With this and other provisions in mind, Wugmeister and Rich assert that 'the IT Act applies to any violation committed outside India by any person (Section 1) therefore, personal information that is collected in India from individuals located outside of India and then transferred outside of India should be collected, used, and protected in accordance with the Privacy Rules'. However, they neglect to note that this unlimited territorial jurisdiction is subject to anything otherwise provided in the Act (s2(1)). The substance of s1 is repeated in s75(1), but it is subject to s75(2) which provides that the section only applies 'if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India'. Given the proviso in s2(1), it seems likely that s75(2) also limits the scope of s1. While interpretation is possible that s2(1) deals with the person liable and s75(2) deals with the cause of action arising in India, local commentators such as Duggal (2004, p16) thought it 'implausible' that the extra-territoriality of s1(2) would be implemented.

While it would be extremely unlikely that criminal provisions would apply to actions which occur outside India and are unconnected with Indian computer networks, there is nothing very surprising about the civil provisions of data protection statutes having extra-territorial effect where there is a connection between the jurisdiction and the processing of the personal data. For example, Australian law has such provisions. Here, the data has been collected or processed in India, so it does seem rule 6(4) could apply to data legitimately transferred to the USA. The surprising things is that rule 6(4) is so blunt, simply stating that the US company 'shall not disclose it further', rather than require the US company to comply with Rule 6(1) and get permission for further disclosure.

Data export restrictions – an additional hurdle

The new rule 7 imposes two conditions for a transfer of personal data by a company in India to any person 'located in any other country':

(i) The recipient 'ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules'; and

(ii) The transfer (a) 'is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information'

or (b) 'such person has consented to data transfer' (presumably 'the person concerned' or data subject).

It seems that, as in most data protection legislation, the exporter has to comply with both the disclosure principle (rule 6) and the data export principle (new rule 7). This does mean that there cannot be any exports of personal data from India (not only in the outsourcing situation, but generally) except to countries that ensure 'the same level' of data protection as India now does. How high a standard India now has is still an open question, but no longer a trivial one.

References

GSR 313(E) Dated 11 April 2011: Information Technology (Resonable Security Practices and procedures and sensitive personal data or information) Rules, 2011 is available at <http://www.mit.gov.in/content/notifications>

Draft Privacy Bill 2011: Novel and complex (September)[4]

Unofficial copies have became available of a draft *Privacy Bill, 2011*, dated 19 April 201 and marked as a 'Third Working Draft (For Discussion and Correction)' from India's Legislative Department. The Bill would, if enacted, create a Data Protection Authority of India (DPAI), plus a statutory right of privacy (a first for the Asia-Pacific), a complex regime controlling surveillance activities, and a data privacy code. This Bill is only a draft with no official status as yet, and many of its provisions are inconsistent and poorly drafted, so it is unlikely to be the final form of the Bill.

However, it is important for organisations involved in outsourcing to India, and for those interested in India's development of data privacy, to understand how this Bill would interact with the data privacy Rules already in force under s43A of the *Information Technology Act 2000* (see Greenleaf, PLBIR 111 and 112). This article focuses on that interaction, and does not attempt to cover wider matters such as the surveillance provisions.

Unprecedented broad scope

The starting point is that the scope of the proposed Bill appears at first sight to be broader than any other data protection legislation known. This can be seen from its Table of Contents: Ch. I (ss1-2) Preliminary; Ch. II (s3) Right to Privacy; Ch. III (ss4-13) Privacy of Communication and Prohibition from its Interception [sic]; Ch. IV (ss14-23) Procedure for Interception of Communication; Ch. V (s24) Prohibition of Surveillance and its Regulation; Ch. VI (ss25-26) Use of Photographs, Fingerprints, Body samples of persons, DNA samples, and other samples taken at Police Station; Ch. VII (ss27-28) Health Information Privacy; Ch. VIII (ss29-31) Privacy relating to Data; Ch. IX (ss32-42) Obligation and Procedure for collecting or processing or using or disclosing data; Ch. X (ss43-48) Residuary; Ch. XI (ss49-62) The Data Protection Authority of India; Ch. XII (ss63-66) Grants, Funds, Accounts and Audit and Annual Report; Ch. XIII (s67) Settlement of Disputes; Ch. XIV (ss68-84) Offences and Penalties; and Ch. XV (ss85-94) Miscellaneous.

[4] Published as Greenleaf, G 'India's draft Privacy Bill 2011: Novel and complex' in *Privacy Laws & Business International Report*, Issue 112, September 2011; 21-24; *Valuable comments on this article were received from Ruchi Gupta*

Right of privacy

Section 3 states simply that 'Every individual shall, subject to any law for the time being in force or order of court, have a right to his privacy'. It then goes on to list eleven matters that are included in (but do not exhaust) this right of privacy. They include rights of confidentiality of various types of communications, information, affairs and transactions, protection against searches, freedom from surveillance, protection against identity theft, protection of bodily samples and in s3(2)(l) 'protection of data relating to individual'. The enumerated inclusions are so broad that they place no obvious constraints on the interpretation of what is meant by 'privacy'.

Data privacy code

Chapter VIII ('Privacy relating to data'), Chapter IX ('Obligation and Procedure for collecting or processing or using or disclosing data') and Chapter X ('Residuary'), taken together (ie ss29-48), can be considered as the general 'data privacy code' contained in the Bill. Ignoring the restrictions on their scope for the moment (discussed in the next two sections), they are a comprehensive set of data protection principles, with some novel elements. A set of legitimating conditions for processing are given (s30(1)) and s32. Data previously collected is covered (s31). There are few exceptions to consent and authorisation by law for collection of personal data. Where personal data is collected directly from the individual the notice requirements are extensive, including notice of the details of overseas transfers (s33). Data cannot be required beyond what is 'absolutely necessary' for a documented purpose in a transaction (s34(2)). Standard rights are provided for fair processing, maintaining data quality, sensitive data, opting out of direct marketing, data retention, and data security (ss34-40) and access and correction (s42). Vicarious liability for sub-contractors is required. There is a very strong provision for data breach notification to both the individual and the DPAI (s41). Transfer outside India is only allowed to places ensuring 'an adequate level of protection' (otherwise undefined) (s47(5)). These add up to a set of reasonably strong data protection principles not dissimilar to those in other EU or OECD-influenced Acts.

Limitations of these rights in relation to outsourcing

There are two very significant limits on both the right of privacy and the data privacy code which are of particular importance to overseas outsourcing to India, but also of more general importance in relation to India's private sector.

First, both s3(1) and s3(2)(l) refer to an 'individual', and s2(h) says 'individual' 'means a citizen of India', so the right of privacy does not apply to anyone who is not a citizen of India. It is therefore substantially irrelevant to overseas outsourcing operations. Similarly, all of the provisions of the 'data privacy code' (Chs VIII-X) apply only to 'individuals', with some important exceptions in Ch IX (s30, s34(1) and (2), s38, s40) where 'individual' has not been used. In general, therefore, both the Ch II right of privacy and much of the data privacy code are irrelevant to overseas outsourcing operations, unless by coincidence the person concerned is an Indian citizen. However, the application to Indian citizens is itself enough to cause complications in outsourcing, as well as the few provisions that will on the face of it apply to data about non-citizens.

These problems might, however, be resolved by the second limitation. The s3 right of privacy is 'subject to any law for the time being in force', which will include the current s43A Rules under the *Information Technology Act* (assuming they are *intra vires*). So the

right of privacy cannot be inconsistent with the s43A Rules, although it can otherwise provide rights which go beyond those in the Rules. In similar fashion, Chs VIII-IX are unlikely to apply where s43A applies. Section 29 provides that to 'collect or process or use or disclose' data 'in accordance with the provision of … any other law for the time being in force' is an alternative to obtaining consent. So compliance with the s43A Rules seems to make it unnecessary to comply separately with Ch VIII, because the other provisions in that Chapter all state that they are 'without prejudice to the provisions contained in s29'. Since all of Ch IX deals with obligations and procedures affecting how to collect or process or use or disclose data, all of its provisions are likely to be subject to s29. Ch X only applies to matters 'not specifically covered' under earlier sections, and most matters relating to outsourcing will have been dealt with by such sections, so Ch X will probably not apply either.

The result, then, is that for most purposes the s43A Rules will be the applicable law affecting the private sector, including those involved in outsourced data processing, and will exclude the Privacy Bill's operation where they apply.

Different public sector coverage

Much of the Bill applies to Indian governments, with 'government' defined to include the Central, State and local authorities (s2). The right of privacy (Ch II) is not restricted in its application. Other provisions are explicitly stated to apply to government as well as to other persons (Ch III and Ch IV on interception, Ch VI on samples, and Ch VII on health information). However, the general provisions on surveillance (Ch V) only apply to 'persons' (individuals, companies and associations: s2), and not to governments.

The 'data privacy code' also only applies to 'persons' for most of Ch VIII and Ch IX. But there is inconsistency in drafting, and the sections concerning data security, access and correction (ss38-42) refer to 'data controllers' (which is not defined) rather than persons. Whether the context of Ch IX implies that a 'data controller' must also be a person (and therefore excludes government data controllers) would be a question of interpretation if this ambiguity survives redrafting.

The residuary part of the data privacy code (Ch X) applies to 'any matter relating to privacy of an individual which is not specifically covered under sections 4 to 42 (inclusive)' (s43). The general privacy rights in Ch X (ss44-48) simply refer to 'personal information' and are not restricted to actions by 'persons'. They therefore apply to governments. They provide a briefly stated version of a basic set of data protection principles (collection, accuracy, deletion, use and disclosure, and data exports). As mentioned, access, correction and security are covered by ss38-42, and their omission from Ch X perhaps implies that they do apply to governments, otherwise Ch X would be an incomplete set of rights.

Since the s43A Rules do not apply to government, if this Bill was enacted India would have in Ch X (and parts of Ch IX) a different data privacy code for its public sector than applies to its private sector. It would also have a statutory right of privacy applying against the public sector (in additional to constitutional rights of uncertain scope).

The provisions in Ch X only apply to 'individuals', so only Indian citizens will gain protection against the use of their personal information by Indian governments.

Data Protection Authority of India

The Bill will create a Data Protection Authority of India (DPAI) of up to three persons (Ch XI), with protections against removal from office except for proper cause (s58). The DPAI will have very extensive functions (s57), including monitoring laws and government policies for consistency with the Act, making recommendations to government, monitoring technology and education, and making recommendations concerning adherence to international agreements.

Surprisingly, it is proposed that the DPAI will keep a National Data Controller Registry, a step out of keeping with all other Asia-Pacific laws. Companies processing data using equipment located in India, but which do not have a place of business in India, will also have to nominate a representative to the DPAI (s29(2)).

Dispute resolution

Breaches of provisions of the Bill could result in actions commencing before the DPAI, the Cyber Appellate Tribunal or the Courts.

The DPAI's functions include 'to monitor and enforce compliance of all the provisions of (sic) relating to data by all persons to whom it applies', but it is not clear whether the reference to 'persons' means this does not apply to governments. The DPAI is to have the function of receiving and investigating data protection complaints under specified Chapters of the Bill, but which Chapters is left blank in the draft Bill (and will determine whether it includes complaints against government), and 'to issue appropriate orders and directions'.

Individuals will be able to lodge complaints against data controllers (only) with the Cyber Appellate Tribunal (established under the Information Technology Act) (s67), which would be empowered to make any orders it thinks fit including compensation (s76) and also to hear appeals against any decision of the DPAI. There is a separate provision by which individuals may take civil actions against a person (ie not the government) for contravening a provision of the Act in a way that affects them adversely (s84), but not in respect of any matter that can be brought before the Cyber Appellate Tribunal (s86).

There are also numerous offences which can result in fines or imprisonment (Ch XIV), including for contravening orders by the DPAI. The Bill clearly adds a very wide variety of enforcement mechanisms to the current limited options under the s43A Rules.

Conclusion: Still no cause for panic (or euphoria)

The Bill is very complex, including detailed controls on surveillance as well as the data privacy aspects emphasised in this article, But it is only a draft as yet, and will undoubtedly be modified very considerably before it progresses.

From the perspective of organisations outsourcing data processing to India, the impact of the Bill will probably be limited because most of the data privacy provisions will not apply. But there are enough uncertainties about what might apply, and before which enforcement body actions might be commenced, that outsourcing organisations will have concerns if the Bill is not made more precise.

Because most of the Bill's protections only apply for the benefit of Indian citizens, its contributions to any assessment of the strength of Indian privacy protections will be more limited than would otherwise be the case. However, its addition of a data protection authority, and a right of actions before the courts, would certainly be strong new positive factors.

Nevertheless, Indian commentators stress that the exclusion of the Indian government from the scope of the Bill is a very severe weakness, particularly because there are so many privacy-invasive public sector projects going forward in India at present, including the national ID number, and NATGRID (see Greenleaf, 2010). Some of this surveillance legislation also empowers private organisations to act as agents of the government in collecting data, probably outside this Bill. Another avenue of criticism is that the widely-respected Information Commission, established under the Right to Information Act, would be a more appropriate and independent source of adjudication than the proposed system of departmental adjudicating officers and right of appeal to the Cyber-Appellate Tribunal.

If anything like this Bill proceeds, India may get one of the stronger Asia-Pacific privacy regimes, but it will be one of considerable complexity and overlapping rights and remedies.

References

India, Legislative Department (2011) Draft *Privacy Bill 2011* (Third Working Draft, Legislative Department, 19 April 2011), available at <http://bourgeoisinspirations.files.wordpress.com/2010/03/draft_right-to-privacy.pdf>

Greenleaf, G 'India attempts data protection by regulations' Privacy Laws & Business International Report, Issue 110, April 2011

Greenleaf, G 'The Illusion of Personal Data Protection in Indian Law' (2011) 1 (1): 47-69 *International Data Privacy Law*, Oxford University Press, available at <http://idpl.oxfordjournals.org/content/1/1/47.full>

Greenleaf, G 'Outsourcing and India's new privacy law: No cause for panic' *Privacy Laws & Business International Report*, Issue 111, 16-17, July, 2011

Greenleaf, G 'Data surveillance in India: Multiple accelerating paths' Privacy Laws & Business International Newsletter, Issue 105, June 2010

Apar Gupta 'Analysis of the Privacy Bill, 2011' India Law and Technology Blog, June 27, 2011 at <http://www.iltb.net/2011/06/analysis-of-the-privacy-bill-2011/>

Iyenagar, P 'The new Right to Privacy Bill 2011 – a blind man's view of the Elephunt' Privacy India blog, June 8 201, at <http://privacyindia.org/2011/06/08/the-new-right-to-privacy-bill-2011/>

Privacy Law Unreform by Press Release (December)[5]

In August 2011 India's Ministry of Communications & Information Technology issued what it called a 'Press Note' headed 'Clarification on Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or

[5] For publication as Greenleaf, G 'India – Privacy Law Unreform by Press Release' in Privacy Laws & Business International Report, Issue 114, December 2011 (in press); Valuable comments on a draft of this article were received from Peter Church, Linklaters, and Shamnad Basheer, NUJS Kolkota

Information) Rules, 2011 Under Section 43A of the Information Technology Act, 2000'. It is worth setting it out in full because it is so extraordinary:

> These rules are regarding sensitive personal data or information and are applicable to the body corporate or any person located within India. Any such body corporate providing services relating to collection, storage, dealing or handling of sensitive personal data or information under contractual obligation with any legal entity located within or outside India is not subject to the requirement of Rules 5 & 6. Body corporate, providing services to the provider of information under a contractual obligation directly with them, as the case may be, however, is subject to Rules 5 & 6. Providers of information, as referred to in these Rules, are those natural persons who provide sensitive personal data or information to a body corporate. It is also clarified that privacy policy, as prescribed in Rule 4, relates to the body corporate and is not with respect to any particular obligation under any contract. Further, in Rule 5(1) consent includes consent given by any mode of electronic communication.

Before attempting to interpret this document, it must be questioned whether it has any legal status whatsoever. Since when does Indian delegated legislation appear in the form of press releases? The *Information Technology Act 2000* (as amended in 2008) says that the 'Central Government may, by notification in the Official Gazette and in the Electronic Gazette make rules to carry out the provisions of this Act' (s87(1)). Perhaps the Ministry is pining for the return of s86(1), which provides that 'If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as appear to it to be necessary or expedient for removing the difficulty'. Unfortunately, no order can be made under that section more than two years after the commencement of the Act (ie since 2002).

Examining the four propositions

The 'Press Note' should only therefore be considered as a potentially useful guide to the Rules, but only to the extent that the Cyber Appeals Tribunal, or a court on appeal from its decisions, would interpret the Rules in the same way, uninfluenced by the Ministry's views expressed in its Press Note. Each of its four propositions is now examined:

(i) 'Any such body corporate providing services relating to collection, storage, dealing or handling of sensitive personal data or information under contractual obligation with any legal entity located within or outside India is not subject to the requirement of Rules 5 & 6.' No explanation is given for this assertion. There is no basis for it in the Rules or the Act. It should be ignored. Rules 5 and 6 apply to a '[b]ody corporate or any person on its behalf'.

(ii) 'Body corporate, providing services to the provider of information under a contractual obligation directly with them, as the case may be, however, is subject to Rules 5 & 6. Providers of information, as referred to in these Rules,

are those natural persons who provide sensitive personal data or information to a body corporate.' The second proposition is incorrect: Rule 5(3) distinguishes 'the person concerned' (the data subject) from the 'provider', making it clear that 'provider' is not limited to natural persons. The first proposition is correct, but is here as a corollary of incorrect proposition (i).

(iii) 'It is also clarified that privacy policy, as prescribed in Rule 4, relates to the body corporate and is not with respect to any particular obligation under any contract.' This is hard to understand, but may be intended (ineffectively) to negate what is otherwise the meaning of Rule 4: that the 'providers' of personal information (often overseas outsourcers) are entitled to obtain a copy of the privacy policies of their Indian agents.

(iv) 'Further, in Rule 5(1) consent includes consent given by any mode of electronic communication.' This interpretation at least has the virtue of seeming like a good idea, and may well be correct. However, 'consent' is not defined in the ITA 2000 or the 2008 amending Act or in the Rules, so the meaning of 'consent' must be determined under normal principles of statutory interpretation in Indian law (a question beyond the scope of this article), and cannot be settled by a press release.

If Indian or foreign corporations follow the advice of the Ministry, they may be in for an unpleasant surprise if and when the Rules are interpreted by a Court. The defence of 'We followed a blatantly incorrect interpretation by the Ministry' is not a defence well-known in Indian law. The better course is to treat the Press Note with extreme scepticism and interpret the words of the Rules.

Postscript: Whither data privacy in India?

The August 'clarification' clarified nothing, and as at the date of writing, there have been no further developments by way of amendments to the Rules, or judicial interpretations. Indian data privacy law in relation to the private sector is in a strange limbo. Some law firm and Internet commentators assume that a 'clarification' by press release is effective, whereas others express the same scepticism as I have stated above.

Nor have there been further public developments in relation to the draft Privacy Bill. India is therefore one of the few countries to have enacted data privacy laws for its private sector, but not for its public sector (Vietnam and Malaysia are two others, and Singapore is proposing to do likewise). The energetic nature of Indian democracy, exemplified by its Right to Information Acts, suggests that this is not likely to be a tenable position in the longer run.

India sought an 'adequacy assessment' from the EU in 2009/10 (no outcome has been announced), so it is clearly desirous of a favourable view from Europe, to ease compliance burdens in relation to outsourcing. The current state of India's privacy protections makes that a more complex question than it was a year ago.