India's new Act creates civil liability for data breaches and criminal offences

Author:
Greenleaf, Graham

Publication details:
Privacy Laws and Business International Newsletter
0953-6795 (ISSN)

Publication Date:
2009

India's new Act creates civil liability for data breaches and criminal offences

Graham Greenleaf, University of New South Wales Faculty of Law

Published in *Privacy Laws & Business International Newsletter*, Issue 99, June 2009, 1-5

Extensive amendments to India's *Information Technology Act 2000* deal principally with cyber-security, and were enacted to some extent in response to the attacks in Mumbai in November 2008. They also include the most significant provisions to date in Indian statutes affecting data protection and privacy, though how extensive these turn out to be will depend to some extent on implementing regulations. Most Indian commentators have concentrated on the cyber-security aspects of the legislation, often very critically. This article focuses only on the Act's data protection and privacy implications.

The *Information Technology (Amendment) Act 2008* was passed on the last day of the legislative sitting before vacation on 22 December 2008, and received the President's assent on February 5 2009. It was published in the Official Gazette on the dame day, which brought its provisions into effect. It and eight other bills only received seventeen minutes debate in Parliament.

Civil liability for inadequate personal data security

From the perspective of data protection and privacy, the most significant aspect of the legislation is that it inserts a new s43A on 'Compensation for failure to protect data', which 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.

'Body corporate' is given a broad meaning as 'any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities'. This last clause would exclude religious and social organisations whose activities are not classified as 'commercial'.

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.

However, on closer inspection, the provision has considerable limitations which may give it a different meaning.

First, 'reasonable security practices and procedures' is defined to mean 'security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment'. This part of the definition gives it broad coverage as a data security provision. However the definition goes on to require that it only applies to those practices and procedures 'as may be specified in an agreement between the parties or as

may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit'. So it may be that a consumer who has been damaged can find no applicable standard on which to base their claim. No standard has yet been prescribed by government.

Second, the reference to 'an agreement between the parties' also opens up a possible argument that the provision, despite its wording, is only intended to benefit parties who have contracted to have data processing done for them, and not consumers/ data subjects.

Third, 'sensitive personal data or information' is defines so that it means (not 'includes') 'such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit'. So the government can prescribe however narrow a class of personal information as it deems appropriate, and unless it prescribes something s43A will not come into effect at all.

It is therefore uncertain when s43A will come into effect, if at all. Depending on what the government prescribes under the definitions of 'reasonable security practices and procedures' and 'sensitive personal data or information', and whether it interpreted to benefit all data subjects, it could have a significant effect as a personal data security provision, or it could have very little.

A disclosure offence

Another new section relevant to data protection has been added entitled 'Punishment for disclosure of information in breach of lawful contract' (s72A), but it goes further than its title suggests. It provides for an offence, subject to any other legislation in force, where 'any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person'. So the disclosure does not have to be in breach of the contract provided it is without the consent of the data subject, which would always be the case given the intent that is also required. The offence is punishable by up to three years imprisonment or a fine of up to five lakh (500,000) rupees (US$10,600), or both.

There are important limiting factors in this offence. First, the requisite intent must be present when access to the material is obtained ('secured'). Second, the relevant intent is to cause 'wrongful loss or wrongful gain', and the wrongfulness of either the loss of the gain may be difficult to prove in cases where personal information has been disclosed, for example, only so that it can be used for a commercial purpose such as direct marketing, rather than for some more obviously wrongful purpose such as credit card fraud. Third, the offence only occurs if there is disclosure of the information, as distinct from use of it for a wrongful purpose by the party securing access to it.

Other new offences relevant to data protection

The Act also creates three other more specific new offences which will strengthen data protection in India. The offences carry penalties of up to three years imprisonment or a fine of up to one lakh rupee (US$2,120), or both.

The first offence is where a person who 'dishonestly received or retains any stolen computer resource or communication device knowing or having reason to believe the same to be

stolen' (s66B). Those involved in dealing with unlawfully obtained personal data, or even data resulting from data leaks, could be prosecuted under this section.

The second offence is where a person 'fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person' (s66C). This is an 'identity misuse' provision which should have a wide ambit to deal with misuse of credit card numbers, drivers licence numbers and the like due to the breadth of 'any other unique identification feature'. It is probably broad enough to deal with the combination of a person's name and address.

The third offence covers other forms of 'identity misuse' wherever a person 'by means for any communication device or computer resource cheats by personating (s66D). Logging into a person's account by use of any information such as usernames and passwords would be covered by this, even if the information used could not be said to constitute a 'unique identification feature'.

Special protections for intermediaries

Both the civil liability for personal data security (s43A) and the offences concerning disclosure (s72A) and identity (ss66B-D) are made somewhat more complex by the protection against liability given to intermediaries in certain cases (s79). Where the section 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 it may be arguable that this limitation also applies to 'data' and 'communication'.

The protection to intermediaries only applies where one of three conditions is satisfied:

(a) 'the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hasted'; or

(b) 'the intermediary does not— (i) initiate the transmission, (ii) select the receiver of the transmission, and (iii) select or modify the information contained in the transmission';

(c) 'the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Cetral (sic) Government may prescribe in this behalf'.

The protection will also be lost if the intermediary has contributed in some way to the unlawful act, or upon receiving notice of it from a government authority fails to take steps to prevent it continuing.

Privacy offences concerning private parts

There is further new provision (s66E) that criminalises (with similar penalties as above) where a person 'intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent'. 'Private area' means 'the naked or undergarment clad genitals, public area, buttocks or female breast'. ('Public area' is presumably a misprint for 'pubic area'.)

The offence only occurs ‘under circumstances violating the privacy of that person’, which is defined to mean ‘circumstances in which a person can have a reasonable expectation that (i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or (ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place’. So a streaker at a cricket match would not be protected by this section, nor would someone walking naked down Janpath, nor would a celebrity wearing a revealing dress, but in most other circumstances the defined ‘private parts’ will be protected from being photographed, videoed or transmitted.

The technological circumstances required by the offence are further defined. Merely observing a person, by whatever means, is not covered by this offence, the image has to be recorded in some medium (‘capture’ means to videotape, photograph, film or record by any means’). So a photograph or a video image viewed only by the person taking it will be sufficient.

‘Transmit’ means ‘to electronically send a visual image with the intent that it be viewed by a person or persons’, and ‘publishes’ means ‘reproduction in the printed or electronic form and making it available for public’. These further offences could be committed either by the person who recorded the image, or a person who did not record it but receives it and then transmits or publishes it.

Data surveillance provisions

As well as with protecting privacy in various ways, the amendments also increase government surveillance capacities. These powers are too extensive to be analysed fully in this article, but need to be noted because, on-balance, this legislation is not necessarily pro-privacy.

There are open-ended powers to require ISPs and other intermediaries to preserve data: ‘Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe’ (s67C). Failure to do as required is an offence.

The government is given a general power to monitor and collect traffic data (which is defined): ‘The Central Government may, to enhance cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminant in the country, by notification in the Official Gazette, authorise any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.’ (s69B). If intermediaries or those in charge of data storages fail to cooperate with the government agency, they commit serious offences. Provided ‘traffic data or information’ is read as ‘traffic data or traffic information’, this power has a more limited scope, but if it read as applying to ‘any information’ then it is extraordinarily and unjustifiably broad.

The government seems to be given sweeping powers to determine what modes of encryption may be used: ‘The Central Government may, for secure use of the electronic medium and for promotion of e-governance and e-commerce, prescribe the modes or methods for encryption.’ (s84A).

The extent to which these powers (or the regulations which will implement them) are consistent with the protection of privacy provided by the Indian Constitution will need to be considered.

A first instalment of data protection legislation?

From a data protection perspective, this Act may provide a useful civil law provision on data security, with compensation for data subjects, depending on its implementing regulations. This is supplemented by the identity-related offences. The new offence gives some protection against wrongful disclosures of personal information, though issues of intent cloud its likely effect. The offence concerning images is minor addition, but one that could limit some Internet distribution of sexual images. In sum, this Act gives India a very small first instalment toward data protection laws, but is no substitute for legislation dealing generally with collection, use, disclosure, access and correction of personal information.