COMPLIANCE WEEK
THE LEADING INFORMATION SERVICE ON CORPORATE GOVERNANCE, RISK AND COMPLIANCE

India Privacy Rules Raise Alarms

By Arielle Bikard – June 14 2011

Companies that outsource data processing or other back-end operations to India should be aware of a sweeping change in the country's data privacy rules that, in the worst case, could put notice-and-consent burdens on businesses so onerous that they might prod companies to reconsider why they're outsourcing to India in the first place.


Sussman

"This is a major development, particularly for companies that outsource to India where the business involves sensitive personal data as defined by this law," says Heather Egan Sussman, a partner in the law firm of McDermott Will & Emery. "There are some provisions in this law that may make it difficult to proceed with business as usual."

India's Department of Information Technology passed a set of rules in April titled "Reasonable security practices and procedures and sensitive personal data or information," requiring new standards in how corporations collect, maintain, and disclose personal data. As a result, if outsourcing involves "sensitive" personal data, then consent must be obtained from the individuals to use, transfer, and process the data without violating the rules.

In the law, India puts "its own spin" on the concepts of notice, consent, opt-in, and data security, Sussman says. As a result, even though the Indian subsidiary or outsourcing partner usually shoulders the compliance burden, multinational firms that send sensitive personal data to India may still need to make changes to existing business processes to minimize disruption.

Trouble particularly lurks around the rules'expansive definition of "sensitive" data. That includes passwords, financial information, health conditions, sexual orientation, medical records and biological information. Including passwords in the definition, for example, means that if a call center in India requires a password from an American or European caller, the center now needs to implement a mechanism for consent to comply with the rules, Sussman says.


Singh

As of now, Indian regulators have no concept of indirect consent—that is words, consent obtained at some stage from the data subject which "passes on" to the Indian service provider, says Sajai Singh, a partnerat J. Sagar Associates in India, who also works with Sussman. "We are hoping that this concept is accepted by the Indian Government soon," he says.


Pathak

"The very reason for outsourcing to India may lose relevance," since the law's compliance burdens on multinational firms may be too expansive, say Jai Pathak,partner at the law firm Gibson, Dunn & Crutcher's Singapore office. "The rules will impose a new requirement on multinationals that outsource to India to take prior consent from their customers, which may need such multinationals to designate an appropriate compliance team, review current data practices, prepare compliant data transfer strategies, designate a compliance officer,etc."

Companies that have operations processing data in India, or that rely on offshore service providers to collect personal information on their behalf, should re-assess their current data privacy practices to ensure they comply with the new law, Pathak says.

"If you are invested in outsourcing to India, then you just have to try to take advantage of the most favorable interpretation for business and be prepared for the worst." —John Neiditz, Partner, Nelson Mullins Riley & Scarborough


Neiditz

The extent to which Indian authorities will enforce these rules is also unclear. India'sNational Association of Software and Services Companies and other business organizations have called for the Indian government to issue a clarification around how the rules will be interpreted. Still, whether relief will arrive any time soon remains unclear, says Jon Neiditz, a partner at the law firm Nelson Mullins Riley & Scarborough.

"This may create an environment of uncertainty for some companies in thinking about whether or not to outsource to India,"he says. "If you are invested in outsourcing to India, then you just have to try to take advantage of the most favorable interpretation for business and be prepared for the worst—and that would be through the combination of very clear contractual language and an opinion from Indian legal counsel."

The best-case scenario for firms is that they will have the ability to spell out their own security and privacy rules contractually, and that the government's version will only apply as a default if firms don't do that, Neiditz says. Another favorable outcome would be that the rules are interpreted so that they don't apply to personal information of foreign citizens, which would work in favor of many outsourcing companies.

DATA PRIVACY IN INDIA

J. Sagar Associates Sajai Singh on India's new data privacy regime:

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("Privacy Rules") notified under section 43-A of the Information Technology Act, 2000 ("IT Act") form the backbone of the data privacy regime available in India. These rules provide guidance and procedure that the law provided under Section 43-A. Here it is mandated that a body corporate possessing, handling or dealing with sensitive personal information adopts reasonable security practices. The law and the corresponding Privacy Rules apply to all body corporates which collect and use personal data and information, including to intermediaries.

Definition of Sensitive Personal Data

The primary issue with the implementation of Section 43-A of the IT Act lay in the fact that it did not define 'sensitive personal information'. The Privacy Rules clearly defines 'sensitive personal data'. It includes the following information relating to: (i) password; (ii) financial information e.g. bank account/credit or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) biometric information; (vii) any detail relating to the above clauses as provided to a body corporate for providing services; and (viii) any of the information received under the above clauses for storing or processing under lawful contract or otherwise. However, any information that is freely available in the public domain is exempted from the above definition.

Maintenance of Privacy Policy

An obligation is cast on the body corporate or any other person collecting, receiving, possessing, storing, dealing with or handling information from a data subject on behalf of a body corporate, to provide a privacy policy for handling of or dealing in personal information, including sensitive personal data or information. The body corporate is required to ensure that the privacy policy is available for viewing by the data subject who has provided such information under a lawful contract. The policy is to be published on the website of the body corporate or any person who handles the information on its behalf and should, inter alia, clearly state the purpose of collection of information, the type of data being collected, the security measures undertaken to protect the information, details of practices and policies adopted for handling such information and the purported disclosure of such information to third parties.

Collection of information and consent

Prior to collection of sensitive personal information, the body corporate is mandatorily required to obtain consent in writing through letter or fax or email from the provider of the sensitive personal data or information. Thus, the common corporate practice of obtaining consent through a tick box or an 'I Agree" tab will not suffice. While collecting information directly from the data subject it must, inter alia, be ascertained that the data subject is aware of the purpose for which the information is being collected, that the information so collected may be transferred, the intended recipient of the information and names/addresses of the agency collecting and retaining this information.

Moreover, a body corporate or any person on its behalf is precluded from collecting sensitive personal data or information unless the information is collected for a lawful purpose connected with an integral activity of the body corporate or any person on its behalf and the collection of the sensitive personal data or information is necessary for successfully carrying out that integral activity.

An ambiguity remains regarding the issue on whether the Privacy Rules will apply to any personal data collected in India through a Website hosted abroad. The Privacy Rules are not clear on the same and limits itself to stating that it will apply to any body corporate which "collects and uses personal data and information." However, the IT Act applies to any offense committed outside India. Further, it states that the offense should involve a computer, computer system or computer network located in India wherein the definition of computer network includes the inter connection of one or more computer/computer systems/communication device. Given the above, it would appear that the Privacy Rules will apply to websites hosted abroad but collecting information in India, as the collection of data would occur via a computer network in India.

Source: J Sagar Associates, Sajai Singh.

Furthermore, some outsourcing arrangements have less risk than others. Call centers, for example, might deal extensively with personal information—or they might deal more with information of a technical nature, "where there really isn't much personal information flowing and those shouldn't be too much impacted," says Neiditz. The same goes for transaction processing: "It depends on what kinds of transactions; they can have a lot of personal information or none."

And the worst-case scenario? A government-initiated enforcement case, since there likely wouldn't be plaintiffs from other countries, Neiditz says. And under the rules right now, Indian citizens could also file private claims of action. "Clarification is really necessary: a large part of the U.S.-Indian economy is impacted," he says.


Khanapurkar

Others view the new rules as a step in the right direction given their aim to protect personal data. They may even helpmultinational companies that outsource to India, since the regulations "have added support to prosecute against unauthorized access or disclosure of data that is classified as confidential," says Nitin Khanapurkar,executive director of performance and technology services at KPMG India.

The law does not change across different functions that the company outsources."Companies need to have data classification and labeling implemented, have a privacy framework detailing the controls they intend to implement, and have a monitoring process," Khanapurkar says. Still, firms may still put different controls in place or collect different evidence in the event of prosecution, depending on the function they outsource. For example, call centers require voice-data to be preserved, she says.

To ensure full compliance with the new legislation, Khanapurkar recommends that organizations have a defined disclosure policy, conduct awareness training for employees, and ensure controls are implemented to preserve evidence that might end up in litigation.

Companies that outsource to India shouldalso check their contracts to make sure thatthe contracts include some language allowing modifications based on the new rules, Neiditz says. "If you don't have something that you would rely on if a claim were raised under those rules, then you should consider modifying them quickly," he says.


Rappa

The new data privacy rules might help businesses in other ways, too. "Regulatory frameworks can look bad on the front end, but overtime benefit industry if only because everyone is clear on the ground rules," says Michael Rappa, professor in the Department of Computer Science at North Carolina State University and founding director of the Institute for Advanced Analytics. "Rules place burdens on industry, but also protections. When bad things happens—and they do—it helps to be able to say that your business was operating in full compliance with existing rules."

Finally, "a rule is nothing until it's enforced," Rappa says. "Once the first companies are found in violation and are fined, then we'll have a better indication of what exactly the rule will mean and how companies may change their behavior as a result."