

Translating India's New IT Law

Law360, New York (July 12, 2011) -- The technology law landscape in India recently underwent a dramatic change with the adoption of new administrative rules governing data security and privacy as well as website content, which may impact the way U.S. and other foreign businesses operate in India. The Privacy Rules and the Content Rules, which became effective in April 2011, have been promulgated by the Indian Ministry of Communications and Information Technology under the Indian Information Technology Act of 2000 (the "IT Act").

This article assesses the potential impact of these rules on U.S. and other foreign companies operating in India, and argues that without clarification and amendment, the rules could deter foreign companies from engaging in business activities in India.

The Privacy Rules

The Privacy Rules apply to certain types of personal information collected in, or transferred to, India, but are not limited to information relating to residents of India. The inclusion of non-Indian data in the scope of the Privacy Rules means that operations of multinational companies doing business in India may be affected, as well as U.S. companies that outsource their business processes to Indian vendors.

1) Information Covered

The Privacy Rules define two categories of information.

"Personal information" relates to a natural person, which in combination with other information available is capable of identifying such person."

"Sensitive personal data or information" is defined as personal information which consists of information relating to: (i) passwords; (ii) financial information such as bank account, credit card, debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; and (vi) biometric information.

2) Privacy Policy Requirement

The Privacy Rules require a company that collects personal information to publish a privacy policy on its website detailing how it handles personal information and sensitive personal data, regardless of whether the data has been collected online. Therefore, a company operating a call center in India that collects personal information by telephone and does not operate a website would have to develop and launch a website in order to post the required privacy policy.

3) Collection and Use of Information

The Privacy Rules impose requirements on the collection of any personal information and more stringent requirements on sensitive personal data.

When collecting personal information directly from a person, the collector must take steps as are "reasonable under the circumstances" to ensure the person has knowledge that information is being collected, the purpose and intended recipients of the information, and the name and address of the collector of the information.

Further, when disclosing any personal information to third parties, companies must obtain prior consent unless such disclosure has been previously agreed to in a contract or is requested by a government agency for the purpose of verifying identification or preventing, detecting, investigating, prosecuting or punishing offenses. This gives government agencies broad powers to request personal information or sensitive personal data from companies that collect such information, without the need to formally subpoena such information.

A company collecting sensitive personal data must obtain prior written consent (by letter, fax or email) of the provider of

Expert Analysis

Translating India's New IT Law



India recently adopted new administrative rules that govern data security and privacy as well as website content. Though an intended purpose of the rules may be to support

India's outsourcing industry by adopting a customer-friendly data security and privacy regime, without clarification and amendment, these rules could deter foreign companies from engaging in business activities in India, says Paresh Trivedi of Proskauer Rose LLP.

the information regarding the purpose of collection and usage of the information. Providers of sensitive personal data may withdraw previously provided consent. Sensitive personal data may only be collected for a lawful purpose connected with a function of the company collecting the information.

Sensitive personal data cannot be retained longer than is required for the purposes for which it was collected or used for any purpose other than for which it was originally collected. If a company seeks to use sensitive personal data for a purpose different from the purpose that collection was originally consented for, the company would have to obtain additional consent for such different use.

Conceivably, broad consent permitting use for any purpose connected with the activities or services performed by the company may satisfy the consent requirement, however, since judicial or governmental interpretations or explanations have not been proffered, it is unclear how specific the consent requirement in the Privacy Rules is intended to be.

The Privacy Rules also prohibit transfer of sensitive personal data within India or outside of India unless the transferee ensures the same level of data protection that is adhered to by the transferor and is required under the Privacy Rules. This condition means if a company has multiple affiliates or outsources operations and needs to share sensitive personal data of its customers or employees to affiliates or outsourcing vendors, it would need to ensure that such affiliates or vendors have the same level of data security protections in place as the company sharing the information.

4) Rights of the Information Provider; Grievance Officers

The Privacy Rules require a company collecting personal information to afford the provider an opportunity to review and request correction of any inaccurate or deficient information. Additionally, companies that collect any personal information in India must appoint an officer to address grievances of information providers and publish the contact information of the grievance officer on the company's website. The officers must redress grievances "expeditiously but within one month from the date of receipt of grievance."

The correction opportunity and grievance officer requirements may increase operating and compliance costs for companies that collect or transfer personal information or sensitive personal data in India. Neither of these requirements exists in the U.S. Therefore, a U.S. company subjected to the Indian Privacy Rules must modify the way it operates to comply.

5) Data Security Requirements

Companies that collect personal information are required to have a comprehensive, documented information security program and information technology policies that contain managerial, technical, operational and physical security control measures. A company is deemed compliant with the data security requirements of the Privacy Rules if it has implemented ISO 27001 standards or others approved by the government of India and has been certified or audited at least once per year by government-approved independent auditors.

6) Impact of Privacy Rules

As international competition for outsourcing business processes has increased over the years, Indian outsourcing vendors and industry groups have been keen to see the Indian government adopt a privacy and data security regulatory regime that would give outsourcing customers comfort in outsourcing sensitive functions to Indian vendors. However, the breadth and scope of the Privacy Rules adopted by the Indian government may make choosing Indian vendors less desirable from a compliance, operational and cost perspective.

Under a literal interpretation of the Privacy Rules, if a U.S. participant in a health insurance plan called the insurance company's outsourced call center in India with a question regarding a claim, and if assisting the caller would require the operator to collect personal data defined as "sensitive," the call center operator would be unable to assist the caller until the caller provided written consent by letter, fax or email. In addition to delaying the insurance company's ability to address the caller's issue, this could also highlight the fact that the company has outsourced its call center operations — something that companies often prefer not to emphasize.

Another potential problem concerns the data review and correction right, and whether it extends to persons outside India. Such an interpretation of the Privacy Rules would afford U.S. residents whose data is outsourced to India a right of review and correction that they do not have under U.S. law, and consequently would have the potential to exponentially raise the compliance costs of outsourcing providers in India.

The requirement that companies implement information security standards and undergo annual compliance audits would likely result in significant cost increases to companies with operations in India as well as companies that engage Indian

outsourcing vendors who would attempt to pass the impact of such costs to customers in the form the higher fees. The increased cost of compliance may also deter smaller Indian startups from entering certain types of outsourcing businesses and potentially stunt the growth of the Indian outsourcing industry.

The Content Rules

The new Content Rules impose obligations and potential liabilities on website operators in connection with third-party content such as user-generated content appearing on its websites. The extremely broad substantive provisions of these Rules may also restrict free speech on the Internet.

Under the Content Rules, no provider of a service involving the receipt, storage or transmission of a third party's electronic content (an "Intermediary") may host, publish or transmit any information that either violates the proprietary rights of another person or that otherwise falls into a very broadly defined category of "prohibited content," which includes, but is not limited to, content that is grossly harmful, harassing, blasphemous, defamatory, hateful, obscene, harms minors, is deceptive, is unlawful, threatens national security, contains software viruses or threatens unity, integrity, defense, security or sovereignty of India's friendly relationships with foreign states. Significantly, these broad terms are not further defined.

An Intermediary, which may, given the breadth of the definition, be a website operator, online social network, video sharing site or other "Web 2.0" service, must publish terms and conditions restricting users of its service from hosting, displaying, uploading, modifying, publishing, transmitting, updating or sharing prohibited content. Further, an Intermediary must act to remove prohibited content within 36 hours of discovery or notice and retain the prohibited content and associated records for 90 days for investigative purposes.

The Content Rules do not clarify what such vague and broad descriptions as disparaging, harassing, grossly harmful, hateful or blasphemous content means and the potential for a liberal interpretation of what constitutes prohibited content could result in Intermediaries requiring full-time teams of personnel to promptly respond to reports of such content. Absent strict compliance, social networks could face liability for what users write on another user's "wall," video and photo sharing sites could be liable for videos or photos posted by users and even e-commerce sites could face liability for prohibited content in product reviews posted by customers.

Internet companies and free speech advocates have argued that the Content Rules may restrict the flow of information online and freedom of speech on the Internet. Though Article 19 of the Indian Constitution guarantees freedom of speech, it also permits the making of laws that impose reasonable restrictions on such freedom of speech and the government of India, and various Indian state governments have a history of engaging in censorship for often subjective or politically motivated reasons.

Accordingly, such fears may be justified. India's Minister of Communications and Information Technology appears to have heeded some of these concerns. His recent comment that the ministry is trying to see if the Content Rules "can be made more rational" seems to suggest that even the ministry that has promulgated these rules is questioning the rationality of them.

Conclusion

How the Privacy Rules and Content Rules will be enforced and interpreted remains to be seen. If an intended purpose of the Privacy Rules was to support India's outsourcing industry by adopting a customer-friendly data security and privacy regime, the stringency and impracticality of the Privacy Rules may frustrate this purpose. Further, the vague and seemingly overbroad categories of content to which the Content Rules apply may complicate how Internet services that accept user-generated content operate in India.

Further, there is uncertainty around what the penalties for violations would be. Since neither of the rules specify penalties, the IT Act's residuary penalty clause would seem to suggest that a violation would give rise to liability of up to 25,000 rupees to an affected person or as a penalty.

However, additional penalties — particularly with respect to certain violations of the Content Rules — specified under the Indian Penal Code may also apply. Section 1(2) of the IT Act, which states that the IT Act applies to offenses or contraventions committed outside of India by any person, compounds the uncertainty around the potential liability for U.S. companies operating or outsourcing to India.

--By Paresh Trivedi, [Proskauer Rose LLP](#)