MORRISON | FOERSTER

Morrison & Foerster Client Alert.

May 4, 2011

India's New Privacy Regulations

By Miriam H. Wugmeister and Cynthia J. Rich

Overnight, the privacy landscape in India has undergone a dramatic transformation. On April 13, 2011, India quietly issued final regulations implementing parts of the Information Technology (Amendment) Act, 2008, dealing with protection of personal information. These regulations could have a profound effect on multinational businesses that either outsource business functions to Indian service providers or maintain their own operations in India.

The new rules prescribe how personal information may be collected and used by virtually all organizations in India, including personal information collected from individuals located outside of India. Among other obligations, prior written consent will be required, without exception, to collect and use sensitive personal data. These consent requirements are far more restrictive than what is required under either the Gramm-Leach-Bliley Act or the EU Directive. As a result, U.S. and European multinational businesses that currently rely on their India-based operations or Indian outsourcing service providers to handle sales and other transaction-related calls from their U.S.- or EU-based customers (or even benefit-related calls from their U.S.- or foreign-based employees) may have to adjust their personal data collection practices to conform to Indian data protection rules, even though their current practices may comply fully with U.S. or EU privacy rules.

BACKGROUND

For years, efforts to develop omnibus privacy legislation in India have proceeded in fits and starts. Earlier this year, a draft privacy bill had been circulating informally for comment only to be withdrawn from consideration; the government indicated to industry that they would be "starting over" on the drafting process. At the same time, in February, India's Department of Information Technology quietly posted for public comment a set of draft regulations implementing parts of the Information Technology (Amendment) Act, 2008, dealing with protection of personal information, data security, due diligence observed by service providers, and guidelines for cyber cafes. On April 13, the government issued the final

Beijing

Paul D. McKenzie 86 10 5909 3366
Jingxiao Fang 86 10 5909 3382

Brussels

Karin Retzer 32 2 340 7364
Joanne Lopatowska 32 2 340 7365

Hong Kong

Gordon A. Milner 852 2585 0808
Nigel C.H. Stamp 852 2585 0888

Los Angeles

Michael C. Cohen (213) 892-5404
David F. McDowell (213) 892-5383
Russell G. Weiss (213) 892-5640

London

Ann Bevitt 44 20 7920 4041
Chris Coulter 44 20 7920 4012
Anthony Nagle 44 20 7920 4029

New York

John F. Delaney (212) 468-8040
Joan P. Warrington (212) 506-7307
Miriam Wugmeister (212) 506-7213
Sherman W. Kahn (212) 468-8023
Madhavi T. Batliboi (212) 336-5181
Suhna Pierce (212) 336-4150
Marian A. Waldmann (212) 336-4230

Northern Virginia

Daniel P. Westman (703) 760-7795
Timothy G. Verrall (703) 760-7306

Palo Alto

Christine E. Lyon (650) 813-5770
Bryan Wilson (650) 813-5603

San Francisco

Jim McCabe (415) 268-7011
James McGuire (415) 268-7013
William L. Stern (415) 268-7637
Roland E. Brandel (415) 268-7093

Tokyo

Daniel P. Levison 81 3 3214 6717
Gabriel E. Meister 81 3 3214 6748
Jay Ponazecki 81 3 3214 6562
Yukihiro Terazawa 81 3 3214 6585
Toshihiro So 81 3 3214 6568

Washington, D.C.

Richard Fischer (202) 887-1566
Reed Freeman (202) 887-6948
Andrew M. Smith (202) 887-1558
Julie O'Neill (202) 887-8764
Obrea O. Poindexter (202) 887-8741
Cynthia J. Rich (202) 778-1652
Kimberly Strawbridge Robinson (202) 887-1508
Nathan David Taylor (202) 778-1644

privacy-related rules.[1] In less than three months, the government has dramatically altered the privacy landscape for both multinational organizations with operations in India and local Indian companies engaged in outsourcing activities.

HIGHLIGHTS

Scope. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("Privacy Rules"), apply to all organizations that collect and use personal data and information in India.[2] This would appear to include service providers or intermediaries that collect and process information on behalf of other organizations. It is not entirely clear whether intermediaries are covered because of the various definitions of "intermediary" and the jurisdictional scope in the Information Technology Act, 2000 (21 of 2000) ("IT Act"), the Information Technology (Amendment) Act, 2008, and the new Privacy Rules. In addition, 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. Furthermore, the IT Act applies to any violation committed outside of 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.

That said, Section 79 [2] of the IT Act limits the liability of intermediaries (such as network providers) in certain cases, and it is unclear if this limitation of liability would apply to all service providers or just a subset of service providers. "Intermediary" is defined in the Information Technology (Amendment) Act, 2008 as "any person, who on behalf of another person receives, stores or transmits that [electronic] record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes."

General Obligations. Although these are cast as regulations to the IT Act, the Privacy Rules impose obligations that are typically found in omnibus privacy laws. The Privacy Rules include an obligation to provide notice to individuals when personal information is collected. Organizations covered by the Privacy Rules must establish and make a privacy policy available to individuals. Organizations must also grant individuals the right to access and correct personal information. In addition, organizations must secure information and establish a dispute resolution process that applies to the collection and use of all personal information.[3]

Collection and Use of Sensitive Data

In addition to the general obligations found in an omnibus data protection law, there are obligations specific to the collection, use, and disclosure of sensitive personal data. Sensitive personal data is broadly defined to include password; financial information (bank account, credit/debit card, or other payment instrument details); physical, physiological, and

[1] The Government of India issued these rules under the authority granted to it by Clause (ob) of the Sub-Section (2) of Section 87 read with Section 43A of the Information Technology Act, 2001.

[2] The provisions apply to a "body corporate," which is defined as "any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities," as well as, in many instances, "any person on its behalf."

[3] Personal information is defined as "any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person."

mental health conditions; sexual orientation; medical records and history; and biometric information. Any information that is freely available or accessible in the public domain or furnished under the Right to Information Act, 2005, is excepted from the definition.

Consent. Prior to the collection of information, the organization or any person on its behalf must obtain written consent (by letter, fax, or email) from the provider of the sensitive personal data regarding the purpose of use. There are no exceptions listed in the regulation. In addition, sensitive personal data may not be collected unless it is for a lawful purpose connected to the function or activity of the organization or any person on its behalf, and the collection is considered necessary for that purpose.

Right to Opt Out. The provider of the information[4] has the right to refuse to provide the requested information and withdraw consent previously given. The withdrawal of consent must be sent in writing to the organization. The organization does have the right to refuse to provide goods and services if the provider of the information refuses to provide consent or withdraws consent.

Third-Party Disclosures. Prior consent is required to disclose sensitive personal data to any third party unless such disclosure has been agreed to in a contract or where the disclosure is necessary for compliance with a legal obligation.[5] The organization or any person on its behalf may not publish the sensitive personal data, and the third party receiving sensitive personal data may not disclose such data further.

Transfer of Information. An organization or any person on its behalf may transfer sensitive personal data to any other organization or person in India or to another country that ensures the same level of data protection as provided by these Privacy Rules. The transfer may only be allowed if it is necessary for the performance of the contract between the organization or any person on its behalf and the provider of the information or where the person has consented to the transfer.[6]

Obligations Applicable to the Collection and Use of All Personal Information

Notice. At the time information is collected directly from the person concerned, the organization or any person on its behalf must take steps to reasonably ensure that the person is aware of the fact that information is being collected, the purpose of use, the intended recipients of the information, the name and address of the organization collecting the information, and the organization that will retain the information.

Privacy Policy. The organization or any person on its behalf who collects, receives, possesses, stores, deals with, or handles information from a provider of information must make a privacy policy detailing their handling of personal information, including sensitive personal data or information, available. The policy must be published on a website of the organization or any person on its behalf and contain the following information:

[4] The term "Provider of Information" has not been defined in either the IT Act or the Privacy Rules; however, it appears that, in most instances, the term likely refers to the individual who provides the information (i.e., the data subject). Nonetheless, until the term is interpreted by the courts, it is conceivable that the term could be more broadly interpreted to apply in some cases to third-party providers of information, including service providers.

[5] Information may be shared with government agencies without prior consent where the provision of sensitive personal data is mandated by law for the purpose of identity verification or for the prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences.

[6] The use of the term "person" is undefined in the Privacy Rules. In certain places the Privacy Rules refer to a "Provider of Information" and in other places the term "person" is used.

Clear and easily accessible statements of its practices and policies;

Type of personal or sensitive personal data or information collected;

Disclosure of information including sensitive personal data or information; and

Reasonable security practices and procedures.

Use. Personal information collected must be used for the purpose for which it has been collected.

Access. Providers of information must be given access to their information upon request and ensure that any personal information or sensitive personal data found to be inaccurate or deficient is corrected or amended as feasible. The organization is not responsible for the authenticity of the personal information or sensitive personal data supplied to it or any person on its behalf by the provider of information.

Disputes. Any discrepancies or grievances must be addressed in a timely manner by the organization. A Grievance Officer must be designated and his or her name and contact details must be published on the organization's website. The Grievance Officer must redress the grievances expeditiously but within one month from the date of receipt of the grievance.

Security. An organization or any person on its behalf is considered to have complied with reasonable security practices and procedures if it has implemented such security practices and standards and has a comprehensive, documented information security program and information security policies that contain managerial, technical, operational, and physical security control measures that are commensurate with the information assets being protected and the nature of the business. If there is an information security breach, the organization or any person on its behalf will be required, upon request from the authorized government agency, to demonstrate that they have implemented security control measures as per their documented information security program and policies.

The IS/ISO/IEC 27001 on Information Technology – Security Techniques – Information Security Management System – Requirements is cited as one (but not the only) such standard. Any industry association or entity formed by an industry association whose members are self-regulating by following data protection codes of practice other than IS/ISO/IEC codes must get their codes approved by the Central Government.

An organization or a person on its behalf who has implemented either the IS/ISO/IEC 27001 standard or an approved code of best practices is deemed to have complied with reasonable security practices and procedures, provided that such standard or codes have been certified or audited on a regular basis by independent auditors approved by the Central Government. The audit must be carried out at least once per year or as and when the organization or a person on its behalf undertakes a significant upgrade of its processes and computer resources.

Penalties. The penalties for breach of confidentiality and privacy provided for in the IT Act (Section 72 and 72A) or the implementing rules or regulations include up to two years' imprisonment or a fine up to one lakh rupees (approximately US$2,250) or both. Company directors are also liable unless they can prove the violation was done without their knowledge, or that they acted to prevent the violation. Service providers who disclose information in breach of a lawful contract are subject to penalties that include up to three years imprisonment or a fine of up to two lakh rupees (approximately US$4,500) or both.

IMPLICATIONS FOR BUSINESS

India is an important outsourcing hub for U.S. and European multinational organizations. Many have established extensive IT and back-office centers in India or they rely heavily on third-party outsourcing providers in India to perform those services.

The implications of these new regulations for the outsourcing industry in India are not yet clear. Unless clarification is forthcoming, outsourcing providers in India may be required to insist that they provide notice and obtain consent from every individual who calls a helpdesk or customer service. IT outsourcing vendors may seek to impose data security obligations on their customers to ensure that the customer complies with Indian law.

Given the wide scope of these Privacy Rules, including their extraterritorial application, multinational organizations that have operations in India or simply rely on Indian service providers to collect personal information on their behalf should immediately assess their current data privacy practices to determine if they comply with these new Privacy Rules.

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials in many areas. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for seven straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our free online Privacy Library, please visit: http://www.mofo.com/privacy--data-security-services/.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations.