ALSTON+BIRD LLP

Outsourcing and Privacy & Security ADVISORY

June 21, 2011

Questions Answered, More Questions Raised:

Exploring the Outsourcing Implications of India's Recently Released Privacy Rules

If you outsource any of your operations to India or otherwise have operations in India, new rules issued by India's Central Government on April 11, 2011, could have serious consequences for these operations. These consequences, however, are not limited to just the customer of outsourcing services; the service provider is also subject to these rules and may well share in the burden of complying with them.

The rules are officially known as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the "Privacy Rules"). They were issued by India's Central Government in accordance with statutory authority granted under The Information Technology Act, 2000 (the "Act"),[1] as amended by The Information Technology (Amendment) Act, 2008 (the "ITAA").[2] The Privacy Rules were supposed to clarify two terms of a key privacy compliance provision in the Act,[3] however, they go much further. The Privacy Rules put in place significant new obligations that cover the collection, use, disclosure or transfer of information. Information qualifying as "sensitive personal data or information" (e.g., passwords, financial information, and medical records) is subject to tighter regulation, above that applying to information.

If not changed, the Privacy Rules will force companies to re-examine their information practices in India, including outsourcing arrangements. It is difficult, however, to imagine that these rules will be meaningfully implemented in their present form due to the significant requirements they impose on the outsourcing industry and its customers. Based on our conversations with industry insiders, we understand that India's outsourcing trade association, the National Association of Software and Services Companies ("NASSCOM"), will take steps to influence changes to the Privacy Rules to make them more accommodating to the outsourcing industry. Of course, it is still possible that the Privacy Rules will remain in place without change.

Our goal with this Advisory is to inform you of obligations under the Privacy Rules that could have a material impact on the way you manage your information practices in India. We caution, however, that there is still much that is unknown about the Privacy Rules, including whether they will remain in effect for very long and whether they will be enforced.[4] Despite the potentially transformative nature of the Privacy Rules and their wide ranging impact if enforced, much is uncertain regarding their final implementation.

Information, Personal Information, and Sensitive Personal Data or Information

The Privacy Rules establish a new, almost EU-like data privacy regime with rules covering collection, use, disclosure, and transfer of information, and privacy policy requirements. The Privacy Rules also establish requirements for the security of information.

This advisory is published by Alston & Bird LLP to provide a summary of significant developments to our clients and friends. It is intended to be informational and does not constitute legal advice regarding any specific situation. This material may also be considered attorney advertising under court rules of certain jurisdictions.

This new regime is divided among three categories of information: (i) information; (ii) personal information; and (iii) sensitive personal data or information. "Information," the broadest term, is defined in the Act to include "data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche."[5] The term "Personal Information" is defined in the Privacy Rules as a subset of Information and includes "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,[6] is capable of identifying such person."[7] Finally, "Sensitive Personal Data or Information" is a subset of Personal Information and is defined as: "such personal information which consists of information relating to: (i) password; (ii) financial information such as Bank account or credit card 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 body corporate for providing service; and (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract: provided that, any information that is freely available or accessible in public domain or furnished 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 the purposes of these rules."[8]

Requirements Under the Privacy Rules

The Privacy Rules lay out a comprehensive list of requirements that apply to combinations of these information categories. We explore many of these requirements below[9] and include just a few of the many issues with these requirements that U.S. companies and their service providers should consider. More issues will likely surface as the outsourcing industry and its customers digest the rules further.

Privacy Policy

Any company or any person who on behalf of a company collects, receives, possesses, stores, deals or handles *information*,[10] must provide a privacy policy for handling of or dealing in *personal information*, including *sensitive personal data or information* and ensure that the privacy policy is available for view by those who provide the *information*.[11] The requirement to maintain a privacy policy therefore attaches to anyone who collects, receives, possesses, stores, deals or handles any type of information, while the privacy policy must specifically address personal information and sensitive personal data or information. This requirement does not distinguish between an outsourcing customer (the "Controller" as typically encountered in countries adopting an EU Data Directive type law) or a service provider (the "Processor" as typically encountered in countries adopting an EU Data Directive type law).

Required Disclosures to Data Provider

When a company is collecting *information* directly from an individual, a company must take such steps as are, under the circumstances, reasonable to ensure that the person concerned has knowledge of: (i) the fact that the information is being collected; (ii) the purpose for which the information is being collected; (iii) the intended recipients of the information; and (iv) the name and address of the agency collecting the information and the agency that will retain the information.[12] As with the privacy policy, this requirement attaches to any company that collects any type of information. Obviously, this requirement presents a number of challenges for data collected in and/or from the United States that is stored and processed by service providers in India.

Similarly, service providers operating customer care centers and many other customer focused processes will also have to implement new, extensive and probably costly procedures to comply with this requirement.

Access

A company or any person on its behalf shall permit the provider of *information*, as and when requested by them, to review the information they provide and ensure that any *personal information or sensitive personal data or information* found to be inaccurate or deficient shall be corrected or amended as feasible.[13] A company is not responsible for the authenticity of the personal information or sensitive personal data or information supplied by the provider of the information.[14] The right of access has long been present in the EU Data Directive and similar laws,[15] but presents a potentially significant implementation burden where it has not been required previously.

Written Consent

Before a company or any person on its behalf may collect *sensitive personal data or information*, the company must obtain consent in writing through letter, fax or email from the provider of the sensitive personal data or information.[16] This requirement presents numerous questions as to its practicality and how it can be implemented, particularly in the context of an outsourcing arrangement where the customer is in the United States and the service provider is located in India. This provision might require, for example, any company that requires provision of a bank account number to an Indian call center to have previously received written consent from the individual to collect that information. Note though that this requirement only applies to sensitive personal data or information, not to the broader terms information or personal information. Nonetheless, the definition of sensitive personal data or information is quite wide, encompassing many categories of information frequently collected in India-based operations.

Disclosures

Any disclosure of *sensitive personal data or information* from a company to a third party requires prior permission from the provider of such information, who has provided such information under a lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the company and the provider of information, or where the disclosure is necessary for compliance with a legal obligation.[17] The third party that receives the sensitive personal data or information from the company or any person on its behalf is prohibited from disclosing it further.[18] These requirements are subject to exceptions for disclosure to government entities.[19]

This requirement has potentially huge implications for the outsourcing industry. If the company collecting the information is the service provider, and the third party is the customer of the service provider, this clause would appear to require prior permission from the information provider for the service provider to disclose the information to the service provider's customer. Moreover, the customer would appear to be prohibited from any further disclosure of the information. This situation might arise, for example, in an HR transaction where the Indian service provider receives benefits related information directly from an individual (who is the employee of the outsourcing customer). It would also appear that where the customer receives the sensitive personal data or information directly from the individual, consent from each individual would need to be obtained to disclose that information to the service provider, unless the contract between the individual and the customer permits such disclosure.

Transfer

A company or any person on its behalf may transfer *sensitive personal data or information* including any *information* to another company or person in India, or located in another country, that ensures the same level of data protection that is adhered to by the company as provided for under the Privacy Rules.[20] This transfer is allowed only if it is necessary for the performance of a lawful contract between the company or any person on its behalf and the provider of the information or where consent to the transfer was obtained from the data provider.[21] There is an ambiguity in this provision in that the clause "that ensures the same level of data protection" could apply either to the company or person in India, or it might apply to the country. If the clause is construed to apply to the country, then this clause takes on an EU-like "adequate level of protection" requirement,[22] requiring countries receiving data from India to have equally protective laws. The second half of this requirement is particularly burdensome, unless consent has been provided, since it will be necessary to establish that the transfer is necessary for contractual performance.

Data Security Requirements

In addition to defining sensitive personal data or information in the Privacy Rules, the Indian Central Government also defined reasonable security practices and procedures:

> A [company] or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have 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 with the nature of business.[23]

The Privacy Rules provide that a company that implements the ISO 27001 standards, or other codes of best practices of industry associations that have received approval by the Central Government, is deemed to have complied with reasonable security practices and procedures provided that such standards or codes of best practices have been certified or audited on a regular basis by entities through an independent auditor, duly approved by the Central Government.[24]

The definition of reasonable security practices and procedures in Section 8 of the Privacy Rules is intended for purposes of further defining the private right of action in Section 43A of the Act.[25] Section 5(8) of the Privacy Rules, however, provides that a company or any person on its behalf shall keep information secure as provided in Section 8 of the Privacy Rules.[26] Thus, Section 5(8) of the Privacy Rules purports to create a direct statutory breach if a company fails to implement the reasonable security practices and procedures defined in Section 8 of the Privacy Rules.

Another key aspect of the Privacy Rules is a requirement that in the event of a security breach, a company is required to demonstrate, as and when called upon to do so by a designated government agency, that it has implemented security control measures as per its documented information security program and information security policies.[27] Thus, when and to the extent the Central Government enforces these rules, a company that collects and stores information in India must anticipate the possibility that in the event of a breach the Indian government may elect to verify that the company was complying with its information security policies.

Conclusions

The Privacy Rules raise many questions for U.S. companies with operations in India. If the Privacy Rules were to be enforced today, industry insiders in India have suggested that the majority of outsourcing operations that involve personal information would be found to violate the Privacy Rules and it would take a considerable amount of time and effort to get the industry in compliance.

We are working with prominent Indian counsel to explore these and other issues raised by the Privacy Rules. As a part of our effort, we are assembling a list of concerns for NASSCOM and our other contacts in India to share with the Indian government and invite you to share with us any particular concerns you might have.

We will provide updates as we learn more.

This advisory was written by James A. Harvey and Todd S. McClelland.

(Endnotes)

1 The Information Technology Act, 2000, No. 21, §§ 43A, 87, India Code (2000).

2 The Information Technology (Amendment) Act, 2008, No. 10, §§ 22, 46, India Code (2009).

3 The Act, as amended by the ITAA, was in part intended to hold companies accountable for the protection of personal data by providing a private cause of action to individuals against companies that are negligent with the individual's personal information. This cause of action was codified in amendments to Section 43A of the Act by the ITAA:

> 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.

The Information Technology (Amendment) Act, 2008, No. 10, §22, India Code (2009) (amending Section 43A of the Act) (*emphasis added*). Importantly, two key terms in Section 43A – "sensitive personal data or information" and "reasonable security practices and procedures" – were left undefined by the ITAA's amendments. The ITAA's amendments permit the Indian Central Government to define these terms. *Id*. at §§22, 46 (amending Section 87 of the Act – the provision granting specific rule making authority to the Central Government – to permit the Indian Central Government to define these terms). Indeed, the introduction to the Privacy Rules references Sections 43A and 87 of the Act as the basis of its authority to make the Privacy Rules. See Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Gazette of India, Part II, Section 3(i) (Apr. 11, 2011).

4 Industry counsel has informed us that there is no Indian agency currently tasked with enforcing the Privacy Rules.

5 The Information Technology Act, 2000, No. 21, §2(1)(v), India Code (2000).

6 "Body corporate" is a common term in the Privacy Rules and means "any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities." The Information Technology (Amendment) Act, 2008, No. 10, §22, India Code (2009).

7 Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, §2(i), Gazette of India, Part II, Section 3(i) (Apr. 11, 2011).

8 Id. at §3.

9 We do not address all of the implications of the Privacy Rules, but have focused on those with the most likely material impact on U.S. companies and their service providers.

[10] In some instances we have italicized *information, personal information*, or *sensitive personal data or information* to emphasize the placement of these terms. The requirements become particularly burdensome where they apply to the broader terms.

[11] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, §4(1), Gazette of India, Part II, Section 3(i) (Apr. 11, 2011).

[12] *Id*. at §5(3).

[13] *Id.* at §5(6).

[14] *Id*.

[15] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995, O.J. (L 281) 31.

[16] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, §5(1), Gazette of India, Part II, Section 3(i) (Apr. 11, 2011).

[17] *Id*. at §6(1).

[18] *Id*. at §6(4).

[19] *Id.* at §6(1).

[20] *Id.* at §7.

[21] *Id*.

[22] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, art. 25(6), 1995 O.J. (L 281) 31.

[23] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, §8(1), Gazette of India, Part 2, Section 3(i) (Apr. 11, 2011). The ITAA included an incomplete definition of reasonable security practices and procedures: "security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment . . . ." The Information Technology (Amendment) Act, 2008, No. 10, §22, India Code (2009) (amending §43A of the Act). As noted above, the Act, as amended by the ITAA, permitted the Indian Central Government to define this term.

[24] *Id*. at §8(4).

[25] *Supra* note 3.

[26] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, §5(8), Gazette of India, Part 2, Section 3(i) (Apr. 11, 2011).

[27] *Id*. at 8(1).

ALSTON+BIRD LLP

If you would like to receive future *Outsourcing and Privacy & Security Advisories* electronically, please forward your contact information including e-mail address to **privacy.advisory@alston.com**. Be sure to put "**subscribe**" in the subject line.

James A. Harvey
404.881.7328
jim.harvey@alston.com

Todd S. McClelland
404.881.4789
todd.mcclelland@alston.com

Jonathan M. Gordon
213.576.1165
jonathan.gordon@alston.com

Britton T. Richardson
214.922.3417
britt.richardson@alston.com

Darren C. Hauck
214.922.3401
darren.hauck@alston.com

George M. Taulbee
704.444.1023
george.taulbee@alston.com

William J. Helmstetter, III
404.881.7942
bill.helmstetter@alston.com

David S. Teske
404.881.7935
david.teske@alston.com

David C. Keating
404.881.7355
david.keating@alston.com

Katherine M. Wallace
404.881.4706
katherine.wallace@alston.com

Paul G. Martino
202.239.3439
paul.martino@alston.com

ATLANTA
One Atlantic Center
1201 West Peachtree Street
Atlanta, GA 30309-3424
404.881.7000

CHARLOTTE
Bank of America Plaza
Suite 4000
101 South Tryon Street
Charlotte, NC 28280-4000
704.444.1000

DALLAS
Chase Tower
Suite 3601
2200 Ross Avenue
Dallas, TX 75201
214.922.3400

LOS ANGELES
333 South Hope Street
16th Floor
Los Angeles, CA 90071-3004
213.576.1000

NEW YORK
90 Park Avenue
New York, NY 10016-1387
212.210.9400

RESEARCH TRIANGLE
4721 Emperor Blvd.
Suite 400
Durham, NC 27703-8580
919.862.2200

SILICON VALLEY
275 Middlefield Road
Suite 200
Menlo Park, CA 94025-4004
650.838.2000

VENTURA COUNTY
Suite 215
2801 Townsgate Road
Westlake Village, CA 91361
805.497.9474

WASHINGTON, D.C.
The Atlantic Building
950 F Street, NW
Washington, DC 20004-1404
202.239.3300

www.alston.com

© Alston & Bird LLP 2011