# A COMPARATIVE ANALYSIS OF INDIAN PRIVACY LAW AND THE ASIA-PACIFIC ECONOMIC COOPERATION CROSS-BORDER PRIVACY RULES

—David J. Kessler,* Sue Ross** and Elonnai Hickok***

*In today's global economy, and particularly for India, the importance of strong, enforceable, and internationally interoperable data protection standards cannot be underestimated. While India has adopted various sectoral laws and policies for securing data protection, most significantly the Information Technology Act and the Rules thereunder, a holistic national legislation on privacy rights is absent. Such an attempt can be seen in the October 2012 Report of the Group of Experts on Privacy, which sets out nine National Privacy Principles. This paper examines the Report in the backdrop of the privacy principles of the APEC and the Information Technology Rules in light of the Cross-Border Privacy Rules. It concludes that if India is to become a member of APEC, while the principles in the Report reflect many of the principles central to the APEC privacy framework, it must expand a few aspects of its privacy requirements under the Rules to align them more perfectly with the Cross-Border Privacy Rules.*

## I. INTRODUCTION

In today's global economy, the importance of strong, enforceable, and internationally interoperable data protection standards cannot be underestimated. This is very true for India, as it has sought, and is seeking to position itself as an attractive destination for business and data processing.[1] To help achieve this goal, India sought 'data secure' status from the European Union in 2012 as part

* Partner, Fullbright & Jaworski LLP, Co-head E-discovery and Information Governance practice.
** Senior Counsel, Fullbright & Jaworski LLP.
*** Policy Analyst, Center for Internet and Society.

1 "In the Twelfth Five Year Plan it is proposed to sustain IT and ITeS industry's growth momentum by building an enabling policy environment, support small and medium enterprises and provide competitive edge through fiscal benefits, innovation fund and incubation, …" Report of the

of negotiations on the free trade agreement with the region.[2] According to the Data Security Council of India, if India were to receive adequacy, the Indian outsourcing sector could increase from $20 billion to $50 billion annually.[3] For many years, India has also been seeking membership to the Asia-Pacific Economic Cooperation (APEC).[4]

This paper will examine the predominant and existing legal protections in India for personal data and the recommended privacy framework laid out in the 2012 Report of the Group of Experts on Privacy (the "Report"). This paper will also compare legal protections related to privacy and the recommended regime in the Report against the APEC's Cross-Border Privacy Rules which recognize "the importance of the development of effective privacy protections that avoid barriers to information flows, ensure continued trade, and economic growth in the APEC region."[5] As India is still seeking membership in APEC and because the Cross-Border Privacy Rules (along with the E.U. Data Protection Directive) stand as one of the most respected and robust multi-national privacy paradigms, this comparison is the most apt. It provides a framework to consider the current state of India's privacy jurisprudence and where it may be heading in view of the Report. This paper will conclude by presenting suggestions as to how India could strengthen its data privacy framework to ease international transfers of information to India, but not limited to, aligning its framework with APEC.

## II. PRIVACY IN INDIA

Presently, India does not have comprehensive privacy legislation guaranteeing individuals the right to privacy and addressing the protection of personal data.

---

Working Group on Information Technology Sector Twelfth Five Year Plan (2012 – 17) *available at* http://planningcommission.gov.in/aboutus/committee/wrkgrp12/cit/wgrep_dit.pdf.

2 *Data secure status for India is vital: Anand Sharma on FTA with EU*, The Economic Times (September 3, 2013) *available at* http://articles.economictimes.indiatimes.com/2013-09-03/news/41726773_1_foreign-trade-eu-and-india-industry-minister-anand-sharma.

3 Amita Sen, *Batting for $100 billion BPO industry: India links free trade agreement with EU data secure tag*, The Economic Times (September 10, 2012) *available at* http://articles.economictimes.indiatimes.com/2012-09-10/news/33737141_1_data-secure-status-india-under-data-protection-data-security.

4 Asia Briefing, *India Appeals for APEC Membership*, (October 6, 2013) *available at* http://www.asiabriefing.com/news/2013/10/india-appeals-apec-membership/. APEC is an organization currently comprised of 21 member economies: Australia; Brunei Darussalam; Canada; Chile; People's Republic of China; Hong Kong, China; Indonesia; Japan; Republic of Korea; Malaysia; Mexico; New Zealand; Papua New Guinea; Peru; The Republic of the Philippines; The Russian Federation; Singapore; Chinese Taipei; Thailand; United States of America; and Viet Nam. See http://www.apec.org/FAQ.aspx. India is not currently a member of APEC, but has discussed membership with the current chair of APEC in October of 2013. Saroj Mohanty, "*India Eyeing APEC Membership*?" Hi India Live (October 4, 2013) *available at* http://hiindialive.com/?q=detail/business/india-eyeing-apec-membership?/14912.

5 APEC Privacy Framework, Foreword, *available at* http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx ("Privacy Framework").

Despite this, the Indian judiciary has interpreted the right to privacy to be a fundamental right, read into Articles 19(1)(a) (the right to free speech) and 21 (the right to life and personal liberty) of the Indian Constitution.[6] Since the 1960s, the Indian Judiciary has defined the right to privacy on a case-by-case basis – for example looking at privacy in the context of surveillance by the State,[7] the right to free speech,[8] and medical information.[9] Though the Indian Judiciary has never created one definition of privacy, in some cases it has interpreted the right to be what affects an individual person's life, including an individual's family, marriage, motherhood, procreation, child bearing and education,[10] and it has concluded that privacy is not an absolute right.[11] It is important to note that

---

[6] Planning Commission of India, Report of the Group of Experts on Privacy *available at* http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf.

[7] For example, the Supreme Court, in the order 18.12.1996 in Writ Petition (C) No.256/1991 by *People's Union for Civil Liberties* v. *Union of India*, recognized "Telephone - Tapping is a serious invasion of an individual's privacy. With the growth of highly sophisticated communication technology, the right to sold telephone conversation, in the privacy of one's home or office without interference, is increasingly susceptible to abuse. It is no doubt correct that every Government, howsoever democratic, exercises some degree of subrosa operation as a part of its intelligence outfit but at the same time citizen's right to privacy has to be protected from being abused by she authorities of the day."

[8] For example, in the case *R. Rajagopal* v. *State of Tamil Nadu*, (1994) 6 SCC 632, the Supreme Court held "(1) The right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. It is a 'right to be let alone'. A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child-bearing and education among other matters. None can publish anything concerning the above matters without his consent whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned and would be liable in an action for damages. Position may, however, be different, if a person voluntarily thrusts himself into controversy or voluntarily invites or raises a controversy. (2) The rule aforesaid is subject to the exception, that any publication concerning the aforesaid aspects becomes unobjectionable if such publication is based upon public records including court records. This is for the reason that once a matter becomes a matter of public record, the right to privacy no longer subsists and it becomes a legitimate subject for comment by press and media among others."

[9] For example, in the case *'X'* v. *Hospital 'Z'*, (1998) 8 SCC 296: AIR 1999 SC 495, a hospital had disclosed a blood donors HIV status without the permission of the individual. As a result, the individual's fiancée broke off the engagement. In the case, the Supreme Court held "27... In the face of these potentialities, and as already held by this Court in its various decisions referred to above, the Right of Privacy is an essential component of right to life envisaged by Article 21. The right, however, is not absolute and may be lawfully restricted for the prevention of crime, disorder or protection of health or morals or protection of rights and freedom of others. 28. Having regard to the fact that the appellant was found to be HIV(+), its disclosure would not be violative of either the rule of confidentiality or the appellant's Right of Privacy as Ms. Akali with whom the appellant was likely to be married was saved in time by such disclosure, or else, she too would have been infected with the dreadful disease if marriage had taken place and consummated."

[10] In the case *R. Rajagopal* v. *State of Tamil Nadu*, (1994) 6 SCC 632 ¶ 26(1), the Supreme Court held "the right to privacy is implicit in the right to life and liberty and guaranteed to the citizens of this country by Article 21. It is a 'right to be let alone'. A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child-bearing and education among other matters."

[11] In the case *Gobind* v. *State of Madhya Pradesh*, (1975) 2 SCC 148: (1975) 3 SCR 946, it was noted "...Too broad a definition of privacy will raise serious questions about the propriety of judicial reliance on a right that is not explicit in the Constitution. The right to privacy will, therefore,

the Indian judiciary has never granted private citizens a right of action against another private citizen for a violation of privacy.[12]

## III. CURRENT PRIVACY STATUTES AND REGULATIONS

Instead of national holistic privacy law, India has over 50 sectoral laws, policies, regulations, and proposed legislation that have provisions relevant to privacy. These include, but are not limited to, legislation applicable to the financial,[13] health,[14] and IT sectors.[15] Of these, the Information Technology Act 2000 (ITA) is understood by many to define a data protection regime for the handling of digital information in India.[16]

The ITA was ratified by the Indian Parliament in 2000 and was enacted following the adoption of the UNCITRAL Model Law on E-Commerce 1996[17] and the passing of a resolution by the United Nations General Assembly supporting member states to consider and incorporate the Model Law on E-Commerce when enacting or amending national laws.[18] The ITA applies to the whole of

necessarily, have to go through a process of case by case development. Hence, assuming that the right to personal liberty. the right to move freely throughout India and the freedom of speech create an independent fundamental right of privacy as an emanation from them it could not he absolute. It must be subject to restriction on the basis of compelling public interest."

12 This was noted in the Approach Paper for a Legislation on Privacy published in 2010. The paper is discussed in more detail later in this article *available at* http://ccis.nic.in/WriteReadData/CircularPortal/D2/D02rti/aproach_paper.pdf.

13 For example, under the Credit Information Companies (Regulation) Act, 2005 the Reserve Bank of Indian published Regulations related to data protection standards that must be followed by Credit Information Companies. *available at* http://www.equifax.com/international/india/pdfs/CIC_Rules_and_Regulations.pdf.

14 For example, the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002 establishes standards and practices relating to patient confidentiality, retention of medical records, access to medical records, and informed consent *available at* http://www.mciindia.org/RulesandRegulations/CodeofMedicalEthicsRegulations2002.aspx.

15 For example, the Information Technology Act 2000, as amended in 2008, contains provisions that address hacking, identity theft, protection of sensitive personal information, data retention, interception, monitoring, and decryption, collection and monitoring of traffic data and child pornography. The Information Technology Act, 2000 and The Information Technology (Amendment) Act, 2008.

16 CRID-University of Namur, *First Analysis of the Personal Data Protection Law in India* Final Report. Pg. 30. *available at* http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_india_en.pdf.

17 UNCITRAL Model Law on Electronic Commerce, (1996) *available at* http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html.

18 General Assembly, Model Law on Electronic Commerce Adopted by the United Nations Commission on International Trade Law, 51/162 *available at* http://daccessddsny.un.org/doc/UNDOC/GEN/N97/763/57/PDF/N9776357.pdf?OpenElement and as noted in the introduction to the Information Technology Act 2000: "...Whereas the General Assembly of the United Nations by resolution A/RES/1/162, dated the 30th January, 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law. And Whereas the said resolution recommends inter alia that all States give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper–cased methods of communication and

India and to any offense or contravention of the Act committed by an individual in or outside of India.[19] Broadly, the ITA provides legal recognition of electronic commerce and electronic documents.[20] The ITA has been amended through the Information Technology (Amendment) Act 2008, which received assent from the President of India in 2009. The 2008 amendment to the Act has been controversial, as it was passed by Parliament without debate.[21] Many of the sections added to the ITA through the Amendment Act have been criticized as lacking critical safeguards to prevent against abuse, and a number of cases have been filed in the Supreme Court of India asking for sections of the ITA to be struck down and declared *ultra vires* under the Indian Constitution.[22]

The section in the Act that is most relevant to data privacy can be found under section 43A, "Compensation for failure to protect data," added in the 2008 amendment. This section requires any Body Corporate *possessing, dealing, or handling any sensitive personal data or information in a computer resource* to implement and maintain reasonable security practices and procedures.[23] The section further holds that any wrongful loss or gain to any person caused by negligence on the part of the Body Corporate must be compensated by the Body Corporate. The section clarifies the terms "*Body Corporate,"*[24] *"reasonable*

---

storage of information; and Whereas it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records..."

19 Section 1(2), Information Technology Act, 2000.

20 As stated in the Information Technology Act, 2000 "An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communications, commonly referred to as "electronic commerce," which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies, and further to amend the Indian Penal code, the Indian Evidence Act, 1872, the Banker's Books Evidence Act, 1892, and the Reserve Bank of India Act, 1934."

21 M. Kaul, *India has an internet problem*, Open Democracy (March 13, 2013) *available at* http://www.opendemocracy.net/openindia/mahima-kaul/india-has-internet-problem.

22 For example, in the case *Shreya Singhal* v. *Union of India*, the petitioned asked the Supreme Court to strike down section 66A of the Information Technology Act, 2000. In the case *Mouthshut.com* v. *Union of India* the petitioner challenged the Information Technology (Intermediaries Guidelines) Rules, 2011 and argued that the Rules are unconstitutional and go beyond the scope of the Information Technology Act 2000. For summaries of cases challenging the Information Technology Act *see* http://ccgnludelhi.wordpress.com/2013/09/19/cases-in-which-indias-supreme-court-will-define-contours-of-free-speech-online/.

23 Insertion 22, Information Technology (Amendment) Act, 2008.

24 Section 43A(i), Information Technology (Amendment) Act, 2008. 'Body Corporate' means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities." As it stands, this definition would exclude from its ambit entities like trusts, state bodies, and governmental authorities.

*security practices and procedures,"*[25] and *"sensitive personal data or information"*[26] and gives the Central Government the responsibility of prescribing reasonable security practices and procedures and designating types of sensitive personal information.[27]

As provided for under section 43A of the ITA, through powers conferred by section 87(2), on April 13, 2011, the Government of India's Department of Information Technology issued through a gazette notification the *Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules* (Rules).[28] The Rules define security practices and procedures that a Body Corporate - or any person on behalf of the Body Corporate – possessing, dealing, or handling any sensitive personal data or information must implement when possessing, dealing, or handling any sensitive personal data or information.[29] Under the Rules, 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."*[30] Additionally, the Rules lay out eight types of sensitive personal data including:

(*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;*

---

[25] Section 43A(ii), Information Technology (Amendment) Act, 2008. "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure, or impairment, 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."

[26] Section 43-A(iii), Information Technology (Amendment) Act, 2008. "Sensitive personal data or information" means "such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit."

[27] As stated in Section 43-A(ii) of the Information Technology (Amendment) Act, 2008 "…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." And 43A (iii) "…sensitive persona data or information" means "such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit."

[28] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

[29] As provided for under section 43A of the Information Technology (Amendment) Act, 2008 "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…"

[30] Rule 2(1)(i), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

(*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 service; and*

(*viii*) *any of the information received under the above clauses by a Body Corporate for processing, stored or processed under lawful contract or otherwise.*[31]

The Rules make an exception for any information that is freely available in the public domain; furnished under the Right to Information Act 2005; or under any other law in force.[32] The types of sensitive personal information defined in the Rules appear to be limited as compared to other definitions around the world because information, often regarded as sensitive personal information, such as information relating to political viewpoints, ethnicity, or religious or philosophical beliefs, are not included in the definition.[33]

The Rules lay out a number of requirements that a Body Corporate must implement and comply with. These include:

- **Policy for privacy and disclosure of information:** The Body Corporate or anyone on behalf of the Body Corporate that collects, receives, possesses, stores, deals, or handles information must provide a privacy policy on its website. The privacy policy must include five components, namely: (1) statements of the Body Corporate practices and policies; (2) types of personal or sensitive personal information collected; (3) purpose of collection and use of the information; (4) disclosure of information; and (5) the reasonable security practices and procedures that are in place to protect the information.[34]

---

[31] Rule 3, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[32] Rule 3, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[33] For example, under Article 8 of the EU 95/46/EC Data Protection Directive, the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life is prohibited except in defined circumstances. *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[34] Rule 4(1), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

The Rules are silent as to whether Body Corporate needs to provide notice of changes in its privacy policy.

- **Obtaining consent:** Before collecting sensitive personal data or information, a Body Corporate must obtain consent in writing through letter or fax or email from the provider of the sensitive personal data or information regarding the purpose of the usage.[35]

- **Collection limitation:** A Body Corporate may collect information only if the collection is for a lawful purpose and connected to a function or activity of the Body Corporate, or the collection is necessary for that purpose.[36]

- **Direct collection:** When collecting information directly from the individual the Body Corporate must provide four types of notice: (1) the fact that information is being collected; (2) the purpose of the collection; (3) the intended recipients of the information; and (4) the name and address of the agency collecting the information, as well as the agency that will retain the information.[37]

As a side note, the Rules do not clarify when the provision of a privacy policy[38] applies and when notice is to be provided for direct collection,[39] which is an undefined term.

- **Retention limitation:** A Body Corporate holding sensitive personal data or information cannot retain the information for longer than necessary to fulfill the purposes for which the information may lawfully be used or otherwise required by a law in force.[40]

- **Use limitation:** The information can be used only for the purposes for which it has been collected.[41] However, the Rules do not address the situation where the original purpose and use changes or if the

[35] Rule 5(1), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[36] Rule 5(2), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[37] Rule 5(3), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[38] As required under Rule 4, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[39] As required under Rule 5(3), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[40] Rule 5(4), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[41] Rule 5(5), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

information will be used for another purpose after the information has already been collected.[42]

- **Access and correction:** A Body Corporate, when requested by the individual who provided the information, must provide an opportunity for that person to review the information and ensure that any incorrect personal information or sensitive personal information, is corrected and amended. Though the Rule allows for correction by individuals, it specifically excludes Body Corporate from being responsible for the authenticity of the personal information or sensitive personal information provided.[43]

- **Option to withdraw consent:** Prior to collection, a Body Corporate must provide the individual with the option of not disclosing information, including sensitive personal data or information. The individual also has a right to withdraw consent.[44] It is not clear, however, if the Body Corporate has an obligation to delete information if consent is withdrawn.[45]

- **Provision of grievance officer:** Body Corporates must designate a Grievance Officer and publish its name and contact details on the website. The Grievance Officer is responsible for addressing any discrepancies and grievances with respect to the processing of information in

---

[42] Rule 5(5), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 states "The information collected shall be used for the purpose for which it has been collected." An issue that many consumers are potentially faced with is the use of provided information for purposes beyond what was initially consented to. This can be seen in the case of Facebook, when in 2011 the Federal Trade Commission charged Facebook with, among other things, in 2009 changing the Facebook website so certain types of information that may have been made private by a user were made public without providing notice or collecting consent from the user. For more information *see* http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[43] Rule 5(6), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[44] Rule 5(7), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[45] An issue that many consumer's potentially face is the retention (and potential use) of personal information by companies even after consent has been withdrawn and accounts closed. For example, though Facebook had claimed that after a user deactivates their account, access to photos and other information would be inaccessible, in 2011 the Federal Trade Commission found that Facebook was still allowing access to user content even after account deletion and deactivation. For more information *see* http://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

a timely manner. The Grievance Officer is required to address grievances expeditiously, *i.e.*, within one month of receipt.[46]

Even though this Rule provides for a Grievance Officer, the mechanism is weakened by the fact that the scope of the Grievance Officer's duties is limited to addressing grievances relating to how quickly the Body Corporate processed information.[47]

- **Disclosure of information:** A Body Corporate must obtain consent before disclosing sensitive personal data or information to third parties.[48] Circumstances of when explicit consent for disclosure is not needed include:

  a. if the disclosure has been agreed to by contract;[49]

  b. if the disclosure is necessary for compliance of a legal obligation;[50]

  c. if required by government agencies mandated under the law to obtain the information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation, including cyber incidents, prosecution, and punishment of offences. To obtain the information, the Government agency must submit to the Body Corporate a request in writing that states the purpose for access and that the information will not be published or shared;[51]

  d. if required by an order under the law for the time being in force.[52]

As a strength, the Rules prohibit a Body Corporate from publishing sensitive personal data or information,[53] prohibit third parties receiving sensitive personal

---

[46] Rule 5(9), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[47] Rule 5(9), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[48] Rule 6(1), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[49] Rule 6(1), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[50] Rule 6(1), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[51] Rule 6(1), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[52] Rule 6(2), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[53] Rule 6(3), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

data or information from disclosing that information further,[54] and prohibit Government agencies seeking sensitive personal data or information from publishing or sharing it further.[55]

- **Transfer of information:** A Body Corporate may only transfer sensitive personal data or information, including any information to another Body Corporate or person in or outside of India, if the same level of data protection is upheld that is defined under the Rules and if the transfer is necessary for the performance of a lawful contract, or if the transfer has been consented to.[56]

- **Reasonable security practices and procedures:** A Body Corporate must have a comprehensive and documented information security programme and information security policies in place. These must include managerial, technical, operational, and physical security control measures that are commensurate with the information being protected and the nature of the business. If a breach occurs, Body Corporate must be able to demonstrate that they have implemented the measures as documented.[57] The Rules provide the international standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques – Information Security Management System – Requirements" as a possible standard that can be adopted.[58] Any codes of best practices that are developed by an industry association must have the codes approved and notified by the Central Government.[59] The Body Corporate will be deemed to have complied with reasonable security practices and procedures if the standards have been certified or audited by an independent auditor at least once a year, and when the Body Corporate undertakes a significant upgrade of its processes and computer resources.[60]

---

[54] Rule 6(4), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[55] Rule 6(1), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[56] Rule 7, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[57] Rule 8(1), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[58] Rule 8(2), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[59] Rule 8(3), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[60] Rule 8(4), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

Though the Rules apply to both personal and sensitive personal information, the scope of the Rules is divided: "sensitive personal information" is the only term referred to in standards laid out for the collection,[61] retention,[62] disclosure,[63] and transfer[64] of information. In contrast, the Rules refer to "personal and sensitive personal information" for standards addressing the implementation of a privacy policy by the Body Corporate[65] and the right of access and correction.[66] Additionally, the Rules refer to "information including sensitive personal information" for the standard providing the individual the right to opt out of providing information,[67] and refer only to "information" for the standards requiring notice during direct collection,[68] security standards,[69] and a limitation on use.[70]

In August 2011, in response to concerns raised about the applicability and scope of the Rules, a press release was issued by the Ministry of Communications and Information Technology in the Department of Information

---

[61] Rule 5(2), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 "Body Corporate or any person on its behalf shall not collect sensitive personal data or information unless…"

[62] Rule 5(4), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 "Body Corporate or any person on its behalf holding sensitive personal data or information shall not retain that information for longer than is required…"

[63] Rule 6(1), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 "Disclosure of sensitive personal data or information by Body Corporate to any third party …"

[64] Rule 7, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 "A Body Corporate or any person on its behalf may transfer sensitive personal data or information or information including any information…"

[65] Rule 4(1), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 "The Body Corporate or any person who on behalf of Body Corporate collects, receives, possess, stores, deals, or handle information of provider of information, shall provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information."

[66] Rule 5(6), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011. "Body Corporate or any person on its behalf permit the providers of information, as and when requested by them, to review the information they had provided 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."

[67] Rule 5(7), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 "Body Corporate or any person on its behalf shall, prior to the collection of information including sensitive personal data or information, provide an option to the provider of the information to not to provide the data or information…"

[68] Rule 5(3), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 " While collecting information directly from the person concerned, the Body Corporate or any person on its behalf shall take such steps…"

[69] Rule 5(8), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 "Body Corporate or any person on its behalf shall keep the information secure as provided in rule 8"

[70] Rule 5(5), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011. The information collected shall be used for the purpose for which it has been collected."

Technology interpreting and "clarifying" a number of aspects of the Rules.[71] It is unclear what authority the press release has to define or clarify the Rules, and the validity of the press release and its ability to amend the Rules has been critiqued by international[72] and domestic commentators.[73] It does not appear that the Indian judiciary has incorporated the standards clarified by the press release in any rulings.[74] Three aspects of the press release deserve special attention:

1. Although Bodies Corporate that collect data are bound by Rules 5 (collection of information) and 6 (disclosure of information), an entity, including those located outside of India, that receives and stores the data pursuant to a contract with the Body Corporate is not separately bound by Rules 5 and 6.

2. The requirement for a privacy policy found in Rule 4 is only for the Body Corporate, and does not pertain to any obligation that might be found under a contract.

3. Consent as defined in Rule 5(1) includes consent given by any mode of electronic communication.[75]

Under the ITA there are three ways in which a remedy/penalty can be sought for a breach of personal data. 1.) Wrongful loss or wrongful gain to any person caused by negligence of a Body Corporate to implement reasonable security practices and procedures under section 43A can result in compensation to the affected person.[76] 2.) Section 45 of the Act provides for a residuary penalty or compensation of up to 25,000 rupees (approximately USD $500) for non-compliance with provisions of the Act where no specific penalty has already been defined.[77] 3.) Section 72A of the Act holds any person, including an intermediary, criminally liable with imprisonment up to three years and/or fined up to five

[71] Ministry of Communications and Information, *Clarification on Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal data or Information Rules, 2011 Under Section 43A of the Information Technology Act 2000*, *available at* http://pib.nic.in/newsite/erelease.aspx?relid=74990.

[72] Graham Greenleaf, *India's U-Turns on Data Privacy*, 110-114 Privacy Laws & Business International Report (2011).

[73] Bhairav Acharya, *Comments on the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011* (March 1, 2013) *available at* http://cis-india.org/internet-governance/blog/comments-on-the-it-reasonable-security-practices-and-procedures-and-sensitive-personal-data-or-information-rules-2011.

[74] To date, Rulings citing the press release have not been found by the authors in judgments available to the public, or media reports covering such a judgment.

[75] *Ibid*. Press Information Bureau, Government of India, Ministry of Communications & Information Technology, *Clarification on Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 under section 43A of the Information Technology Act, 2000* (August 24, 2011) *available at* http://deity.gov.in/sites/upload_files/dit/files/PressNote_25811.pdf.

[76] Section 43-A, Information Technology (Amendment) Act, 2008.

[77] Section 45, Information Technology Act, 2000.

lakh rupees (approximately USD $10,000). The penalty is applicable if, while providing services under the terms of a lawful contract, the person, including an intermediary, secures access to personal information with the intent of causing wrongful loss or wrongful gain or with the knowledge that such wrongful loss or gain is likely, and it discloses that information without consent or in breach of a contract.[78]

## IV. PATH TO THE 2012 REPORT OF THE GROUP OF EXPERTS ON PRIVACY

Despite the lack of privacy legislation in India, there have been several steps towards the realization of a comprehensive privacy law. Interestingly, at some points these steps have seemed to suggest that India needs only a strong data protection legislation, while at other points, there has appeared to be need for a broader legislation recognizing the right to privacy. For example, in 2006 the "*Personal Data Protection Bill*" was introduced in Parliament. The scope of the Bill was limited to the protection of personal data and its use and disclosure.[79] The Bill had been prompted by concerns over the misuse of personal data, particularly the selling and use of personal data for direct marketing purposes.[80] The Bill, however, lapsed in Parliament.[81]

In 2010, the Department of Personnel and Training (DoPT) published on its website an "Approach Paper for a Legislation on Privacy," which was drafted by a group of officers for the purpose of developing a *"conceptual framework that could serve the country's balance of interests and concern on privacy, data protection, and security..."*[82] The Paper reviewed privacy laws in thirteen different jurisdictions and set forth recommendations for a privacy regime in India. These recommendations focused on data protection, defining privacy for the purposes of the paper as *"the expectation that confidential personal information disclosed by any individual to Government or non-Government entity should not be disclosed to third parties without consent of the person and sufficient safeguards need to be adopted while processing and storing the information."*[83] The Paper also recognized that in many ways India does not have a culture of privacy[84] – for exam-

---

78 Section 72-A, Information Technology (Amendment) Act, 2008.

79 The Personal Data Protection Bill, 2006.

80 The Personal Data Protection Bill, 2006. Statement of Objects and Reasons. "...In our country, at present, there is no law on protection of personal information and data of an individual collected by various organizations. As a result many a time, personal information of an individual collected for a particular purpose is misused for other purposes also, primarily for direct marketing without the consent of the individual..."

81 Raghunath Ananthapur, *India's New Data Protection Legislation*, 8(2) Scripted 192 (2011).

82 Government of India. Ministry of Personnel, PG & Pensions, Department of Personnel Training, *Approach Paper for a Legislation on Privacy*, (18th October 2010) *available at* http://ccis.nic.in/WriteReadData/CircularPortal/D2/D02rti/aproach_paper.pdf.

83 *Id*.

84 *Supra* note 82.

ple, the Government often discloses personal information of citizens as part of its transparency efforts.[85] Another factor cited as a driving force for a privacy legislation in India was the trend towards centralization of governmental databases. In this regard, the paper highlighted the privacy concerns posed by the Unique Identification Project.[86] Finally, the paper pointed out the increased collection of personal data by private sector organizations. The paper recommended that India approach privacy regulation with a hybrid approach, with a privacy statute defining broad principles for the processing of collected personal information, and industry bodies defining detailed and sector specific guidelines to be adhered to by member organizations.[87]

In 2011, there were three significant privacy events in India. First, there was a Press Information Bureau release from the Ministry of Personnel and Public Grievances stating that "The Government proposes to bring out a legislation that will provide protection to individuals in case their privacy is breached through unlawful means…."[88] Second, news reports at the time indicated that in light of Niira Radia Tapes[89] scandal, the Government drafted a "Right to Privacy Bill 2011" which sought to create a statutory right to privacy.[90] The bill, however, has yet to be introduced to Parliament, and according to news reports, in 2013 the Department of Personnel and Training has drafted another version of the "Right to Privacy Bill," which was scheduled to be considered in the 2013 winter session of Parliament, but which, according to media sources, is pending with the

---

[85] For example: A news article on January 3, 2013 describes how gas agencies list their customers' numbers, addresses, and in many cases mobile numbers. The Election Commission places voter rolls online: the Voter Roll contains address, age, and gender of individuals. *K. Sruthijith, Indian government websites: Gold mine for cybercriminals*, The Times of India (January 3, 2013) *available at* http://timesofindia.indiatimes.com/tech/tech-news/internet/Indian-government-websites-Gold-mine-for-cybercriminals/articleshow/28320517.cms.

[86] The Unique Identification Project is an identity scheme that is currently being rolled out in India. The scheme provides individuals with a unique number based off of their biometrics. The unique number can be adopted by any platform for authentication purposes. The project has been controversial and heavily critiqued for missing critical privacy safeguards. For more information see http://164.100.47.134/lsscommittee/Finance/42%20Report.pdf.

[87] *Supra* note 82.

[88] Press Information Bureau, Government of India, Ministry of Personnel, Public Grievances and Pensions, *Right to Privacy Bill*, (August 18, 2011) *available at* http://pib.nic.in/newsite/erelease.aspx?relid=74743.

[89] In 2010, portions of recorded conversations through a phone tap by the Indian Income Tax Department between corporate lobbyist, Niira Radia, and Tata Group Chairman, Ratan Tata, were leaked to the public. The tapes exposed a number of illegal actions. In response, Ratan Tata has filed a petition in the Supreme Court seeking action against the individuals who leaked the tapes and claiming that the leak was an invasion of his privacy. For more information *see Niira Radia tapes not restricted to 2G spectrum alone: Supreme Court*, The Asian Age (October 5, 2013) *available at* http://www.asianage.com/india/niira-radia-tapes-not-restricted-2g-spectrum-alone-supreme-court-556.

[90] J. Venkatesan, *Bill on "right to privacy" in monsoon session: Moily*, The Hindu (June 7, 2011) *available at* http://www.thehindu.com/news/national/article2082643.ece.

Ministry of Home and Law, at least as of December 2013, due to differences between the two Departments.[91]

Third, at the end of December, the Planning Commission of the Government of India constituted a Group of Experts on Privacy to study privacy regimes from different jurisdictions, to analyse current programmes and projects being implemented in India from a privacy perspective, and to formulate recommendations for the Department of Personnel and Training for incorporation in the proposed draft Bill on Privacy.[92] The Committee was chaired by Justice AP Shah, former Delhi High Court Judge and present Law Commission Chairman, and consisted of members from government such as CERT-in, the Department of Personnel and Training, the Planning Commission, and the Unique Identification Authority of India; industry bodies such as NASSCOM and DSCI; civil society such as the Centre for Internet and Society, and independent researchers; and media such as NDTV.

In October 2012, the Committee published the Report of the Group of Experts on Privacy (the "Report"). Though not officially accepted by the Government of India, news items indicate that the Department of Personnel and Training has incorporated in the upcoming draft of the Privacy Bill recommendations found in the Report.[93]

- Both the *"Approach Paper for a Legislation on Privacy"* and *"The Report of the Group of Experts on Privacy"* contain analysis of the privacy protections found under the Information Technology Act and the *Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011.* The Approach Paper notes that even though the Information Technology Act protects personal data to some extent, the provisions are not comprehensive enough as they speak only to digital data. The Report of the Group of Experts on Privacy notes that the Rules fall short of meeting the standards defined by the National Privacy Principles in the Report as the Rules do not address or require anonymization of data when appropriate, do not require Body Corporate to provide notice of changes in purpose of collection or use, do not address the destruction of data, require Body Corporate to provide notice of breach of information to affected individuals, require Body Corporate to provide notice to changes in its privacy policy, and require Body Corporate

[91] http://www.indianexpress.com/news/ministries-differ-privacy-bill-gathers-dust/1202051/=.

[92] *Supra* note 6.

[93] Aman Sharma, *Privacy Bill: Draft Legislation is yet to be approved by the law ministry*, The Economic Times (December 2, 2013) *available at* http://articles.economictimes.indiatimes.com/20131202/news/44657689_1_privacy-bill-law-ministry-draft-bill.

to conduct an external audit on *all* policies and practices to ensure accountability.[94]

## V. THE REPORT OF THE GROUP OF EXPERTS ON PRIVACY

The Report of the Group of Experts on Privacy recommends both a regulatory framework for privacy in India and lays out nine National Privacy Principles that would be applied across sectors to harmonize legislation, policy, and practice.[95] The Report recommends that a privacy legislation in India apply to both the private and the public sectors.[96] In a move that could significantly impact international companies transferring data into India, the Report clarifies that the scope of the privacy legislation should apply to all data processed in India, including data that originated in India and then is subsequently transferred to another jurisdiction.[97] The regulatory framework envisioned in the Report entails the establishment of one national Privacy Commissioner and four regional Privacy Commissioners, Self Regulatory Organizations ("SRO") at the industry level for the purpose of developing sector specific privacy standards to be approved and enforced by the appropriate Privacy Commissioner, and Data Controllers and, as well as Privacy Officers at the organizational level responsible for processing data in accordance with sectoral privacy standards or the nine National Privacy Principles addressing and resolving complaints.[98]

Furthermore, the validity of any exception to the Right to Privacy must be measured against the principles of proportionality, legality, and necessity in a democratic state.[99] The Group of Experts on Privacy advocates a system of complaints that includes alternative dispute resolution mechanisms at the level of the SRO in the relevant industry sector. Complaints can also be taken to the Privacy Commissioners at the regional or central levels. Privacy Commissioners have the ability to fine organizations and take cases to court. Finally, individuals can take complaints to the courts where compensation and other actions can be sanctioned.[100] The Report specifically notes that any person who suffers damages caused by non-compliance with the privacy principles is entitled to remedy.[101] Actors that can be held liable for damages include data controllers, organization directors, agency directors, and heads of governmental departments.[102] Importantly, unlike the Rules found under section 43A of the ITA, the Report

[94] *Supra* note 6, at 52 – 55.
[95] *Supra* note 6, at 21.
[96] *Supra* note 6, at 4.
[97] *Supra* note 6, at 56.
[98] *Supra* note 6, at 56 – 57, ¶ 5.1.
[99] *Supra* note 6, at 57, ¶ 5.3.
[100] *Supra* note 6, at 58, ¶ 5.5.
[101] *Supra* note 6, at 58, ¶ 5.5.
[102] *Supra* note 6, at 58, ¶ 5.5.

recommends that a definition of personal information should be at a high level and not perspective in order to account for the contextual dependency of information. The Report explains this position by providing the example of how a license plate number held by an insurance company can be considered personal information, but the same number on a security tape in a gas station will not be personal information.[103] The Report further recommends that a privacy legislation in India should harmonize the different definitions of information currently found across various laws in force including, but not limited to, sensitive personal information, personally identifying information, and indirectly identifiable information.[104]

Among other things, the Report recommends the adoption of nine National Principles and explains the rationale and objective for each principle, along with issues and developments driving need for the principle:

1. **Notice:** This principle responds to issues arising from organizations using lengthy and complex privacy policies that are difficult for consumers to read and comprehend, from the acceptance/reading of notices being used as consent, and from notices being used to transfer the obligation of protecting privacy to the individual.[105] The principle requires data controllers to provide clear and concise notice of their information practices before collecting personal information from individuals.[106]

According to the principle, the data controller should provide a notice with seven elements before and during collection of personal information including: 1) what personal information is being collected, 2) the purposes for the collection, 3) the uses of collected personal information, 4) whether or not personal information may/will be disclosed to third persons, 5) security safeguards in place to protect the personal information, 6) methods available for subjects to access and correct their own personal information, and 7) contact details of the privacy officers for filing complaints.

Additionally, the principle recommends that when a data breach occurs, notice should be given to affected individuals and the privacy commissioner when applicable; individuals should be notified of any legal access to their personal information after the purposes for the access have been met; changes to a data controller's privacy policy must be communicated to the individual, and any other information deemed necessary and in the interest of the individual's privacy should be provided through notice.[107]

---

[103] *Supra* note 6, at 67, ¶ 7.4.
[104] *Supra* note 6, at 67, ¶ 7.5.
[105] *Supra* note 6, at 21, ¶ 3.2.
[106] *Supra* note 6, at 21, ¶ 3.2.
[107] *Supra* note 6, at 21, ¶ 3.2.

2. **Choice and Consent:** This principle evolved from a number of issues, including the difficulty individuals face in controlling the use of their personal information once it has been collected by an organization.[108] The principle seeks to empower individuals with the ability to approve and authorise the use of their personal information for defined and understood purposes.[109]

According to the principle, data controllers must provide individuals with a choice to share personal information and to obtain consent from the individual only after providing notice of the data controller's information practices. The data controller can collect, process, use, or disclose information only after consent has been provided. An exception to this standard is in the case of authorized agencies. The principle also maintains that a person will have the option to withdraw consent, except in the case of authorized agencies. Furthermore, when the provision of information is mandated by law, the data controller must still comply with the other eight National Privacy Principles, and, if the information is published in public databases, it should be anonymized within a reasonable timeframe. The principle clarifies that additional transactions completed within the purpose limitation do not require fresh consent to be given. Lastly, when it is not possible for a service to be provided in accordance with the standards defined in this principle, such as in a medical emergency, the principle recommends that choice and consent should not be required. [110]

3. **Collection Limitation:** This principle addresses issues arising from rapidly changing and evolving technology that allows for vast amounts of data to be collected and used without the individual's knowledge.[111] The principle seeks to ensure that data controllers collect personal information only to the extent it is needed for a stated objective and that it is collected through lawful and fair means, and after proper notice.[112]

According to the principle, data controllers should only collect personal information when necessary and for purposes that have been identified. Notice for these purposes must be provided to the individual and consent taken. All collection must be through lawful and fair means.[113]

4. **Purpose Limitation:** This principle arose because of the risk associated with the ability of personal information to be collected, used, and

[108] *Supra* note 6, at 22 – 23, ¶ 3.2.
[109] *Supra* note 6, at 22 – 23, ¶ 3.2.
[110] *Supra* note 6, at 22-23, ¶ 3.2.
[111] *Supra* note 6, at 24, ¶ 3.2.
[112] *Supra* note 6, at 24, ¶ 3.2.
[113] *Supra* note 6, at 24, ¶ 3.2.

retained for multiple purposes by multiple organizations.[114] The principle seeks to ensure that personal information is used only in compliance with the National Privacy Principles and only for intended and agreed upon purposes.[115]

According to the principle, personal data collected and processed by data controllers must be adequate and relevant to the purposes for which they are processed. Data should only be collected, processed, disclosed, made available and otherwise used for the purposes that have been stated in the notice and that have been consented to by the individual. If there is a change of purpose, the individual must be notified. Personal information should not be retained longer than is necessary to fulfill the stated purposes, and should be destroyed after it has been used for the identified purposes, as per identified procedures.[116]

5. **Access and Correction:** This principle seeks to address the limited ability that individuals often have to assert control over the use of their personal information.[117] The principle seeks to ensure that data controllers provide access mechanisms to data subjects if the data controller is holding his/her information and that he/she allow the individual to view, change, or delete his/her personal information.[118]

The principle requires data controllers to provide individuals with the ability to seek corrections, amendments, or deletion of information when it is inaccurate. Individuals also have the right to confirm if the data controller holds or is processing information about them, and to obtain a copy of the same. The exception to this principle is if the data controller cannot provide access without affecting the privacy rights of another person; unless that person has explicitly consented to the disclosure, access should not be given.[119]

6. **Disclosure of Information:** This principle seeks to address the issue of controlling the use of personal information by third parties by ensuring that individuals are informed and consent has been procured for the transfer of information to third parties.[120] The principle seeks to ensure that all disclosures and transfers, including to authorized agencies, are in compliance with the National Privacy Principles.[121] According to the principle, a data controller must not disclose personal

[114] *Supra* note 6, at 24, ¶ 3.2.
[115] *Supra* note 6, at 24, ¶ 3.2.
[116] *Supra* note 6, at 24, ¶ 3.2.
[117] *Supra* note 6, at 25, ¶ 3.2.
[118] *Supra* note 6, at 25, ¶ 3.2.
[119] *Supra* note 6, at 25, ¶ 3.2.
[120] *Supra* note 6, at 26, ¶ 3.2.
[121] *Supra* note 6, at 26, ¶ 3.2.

information to third parties except after providing notice and collecting informed consent from the individual for the disclosure. Third parties to whom information is disclosed must comply with applicable privacy principles. When disclosure is required for law enforcement purposes all disclosures must be in accordance with the laws in force. Data controllers are also prohibited from publishing or in any other way making public personal information, including personal sensitive information.[122]

7. **Security:** This principle seeks to address the issue that arises when organizations put in place security procedures that are reactive, compliance-driven, and process focused.[123] The principle seeks to ensure that data controllers have in place technical, administrative, and physical safeguards for protecting personal information from unauthorized use, destruction, modification, access, and retention.[124]

The principle requires data controllers to employ reasonable security safeguards to secure personal information against loss, unauthorized access, destruction, use, processing, storage, modification, de-anonymization, unauthorized disclosure (both accidental or intentional) or other reasonably foreseeable risks.[125]

8. **Openness:** This principle seeks to address the fact that often organizations do not fully disclose information regarding data practices on an ongoing basis.[126] This principle seeks to ensure that data controllers make their privacy policies, practices, systems, and related developments open, transparent, and accessible to individuals.[127]

The principle requires data controllers to take all necessary steps to implement practices, procedures, policies, and systems in a manner that is proportional to the scale, scope, and sensitivity of the data they collect in order to ensure compliance with the privacy principles. Information regarding such practices, procedures, policies, and systems must be set forth using clear and plain language, and it must be available to all individuals.[128]

9. **Accountability:** This principle seeks to address the dilemma arising from a 'one size fits all' regulation.[129] The principle seeks to ensure that data controllers are accountable to the individual, the privacy

[122] *Supra* note 6, at 26, ¶ 3.2.
[123] *Supra* note 6, at 26, ¶ 3.2.
[124] *Supra* note 6, at 26, ¶ 3.2.
[125] *Supra* note 6, at 26, ¶ 3.2.
[126] *Supra* note 6, at 26, ¶ 3.2.
[127] *Supra* note 6, at 26, ¶ 3.2.
[128] *Supra* note 6, at 26, ¶ 3.2.
[129] *Supra* note 6, at 27, ¶ 3.2.

commissioner, and other stakeholders to ensure compliance with the National Privacy Principles.[130]

The principle requires data controllers to take measures for effecting the National Privacy Principles. This includes implementing privacy policies, relevant training and education, internal and external audits, extending support to the Privacy Commissioner, and compliance with orders from the Privacy Commissioner.[131]

## VI. APEC

APEC is an economic forum that promotes sustainable economic growth through promotion of free and open trade and investment, regional economic integration and cooperation, and creating sustainable business environments.[132] APEC recognizes the importance of protected information flows to business and the impeding effect that the inability to carry out private interactions can have on business.[133] With this understanding, APEC has developed a privacy framework that seeks to balance the two interests of protecting privacy and ensuring an uninhibited flow of information.[134] The APEC privacy framework consists of Cross-Border Privacy Rules and a common set of privacy principles. Additionally, the framework seeks to improve data sharing between governments, and ensure the safe transfer of information across borders.[135] To date, India has not been granted membership. Reasons cited for this have included a lack of political clout, governmental instability, and a lack of strong support for membership from within APEC.[136]

Although the focus of APEC relates to economic growth, APEC has adopted the Cross-Border Privacy Rules ("CBPR"[137]) based upon nine principles:

1. Preventing harm

---

[130] *Supra* note 6, at 27, ¶ 3.2.

[131] *Supra* note 6, at 27, ¶ 3.2.

[132] Asia-Pacific Economic Cooperation, *Mission Statement*, *available at* http://www.apec.org/About-Us/About-APEC/Mission-Statement.aspx.

[133] Asia-Pacific Economic Cooperation Fact Sheets, *APEC Data Privacy Pathfinder*, *available at* http://www.apec.org/About-Us/About-APEC/Fact-Sheets/APEC-Privacy-Framework.aspx.

[134] *Id*.

[135] *Supra* note 133.

[136] Tridib Chakraborti and Mohor Chakraborti, *India and the Asia-Pacific Region: Dilemma of a Changing APEC Mindset*, Special Issue 1 Asia Pacific Journal of Social Sciences 1 (2010).

[137] APEC provides for accountability through a unique mechanism: a third-party "accountability agent." The accountability agent would certify the data transfer practices of a corporation under the APEC principles, as well as monitor and enforce ongoing compliance and help resolve disputes. The United States became the first formal participant in the APEC privacy framework, and the Federal Trade Commission became the first enforcement authority. The first approved accountability agent is TRUSTe, and, to date, there are two corporations that have been APEC privacy certified, IBM in August of 2013, and Merck & Co., Inc. in November of 2013.

2. Notice
3. Collection limitation
4. Uses of personal information
5. Choice
6. Integrity of personal information
7. Security safeguards
8. Access and correction
9. Accountability

APEC's CBPR define *personal information* very broadly: "any information about an identified or identifiable individual."[138] The official commentary clarifies that this definition is intended to apply only to natural persons, not to corporations or other legal persons.[139] The comments also emphasize the breadth of the definition, stating that it "includes information that would not meet this criterion alone, but when put together with other information would identify an individual."[140]

Although some of the APEC privacy principles may seem self-explanatory, others may not be so obvious, including the first principle: Preventing harm.

## A. Preventing Harm

APEC describes this principle as a recognition of the individual's legitimate expectations of privacy and prevention of misuse of personal information.[141] This principle recognizes that some information is more sensitive than other information, and may cause more harm to the individual if the information is disclosed (e.g., disclosing someone's HIV+ status could be more harmful than disclosing the fact that they had a dental checkup on Saturday). The requirements state that "specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use, and transfer of personal information."[142] Anyone interested in outsourcing should note that, unlike most American laws, the APEC privacy principles recognize restrictions on data *transfers*. The official commentary clarifies that privacy protections may take a variety of forms: "self-regulatory

[138] *Id*. at 5.
[139] *Supra* note 137.
[140] *Supra* note 137.
[141] *Supra* note 137, at 11.
[142] *Supra* note 137.

efforts, education and awareness campaigns, laws, regulations, and enforcement mechanisms."[143]

Neither current India privacy law or the Report have an analogous provision or principle though both do recognize different categories of private information that appear to be roughly based on the potential harm in its disclosures.

## B. Notice

Much like India's requirements and the Report's recommendation of "clear and concise notice," APEC provides for "clear and easily accessible" privacy statements. The APEC notice requirements contain five elements:

a. the fact that personal information is being collected;

b. the purposes for which the personal information is being collected;

c. the types of persons/organizations to which the personal information "might be disclosed";

d. the identity, location, and contact information of "a person or organization who controls the collection, holding, processing or use of personal information," which APEC calls a "personal information controller;" and

e. the "choices and means" the personal information controller offers to individuals for "limiting the use and disclosure of, and for accessing and correcting, their personal information."[144]

In contrast to the Report's recommendation of prior notice, APEC provides that, with respect to the timing of the notices, the personal information controller shall take all "reasonable practicable steps" to provide the notices "either before or at the time of collection."[145] "Otherwise, such notice should be provided as soon after as is practicable."[146] The commentary states that a "common method of compliance" is to post notices on web sites—and notices on intranets or in employee handbooks may also be appropriate.[147] The commentary also provides three categories of exceptions to the notice requirements:

---

[143] *Supra* note 137.

[144] *Supra* note 137, at 12. The Report also recommends that the notice include provisions relating to security safeguards and uses of personal information, which APEC addresses in separate sections.

[145] Privacy Framework, at 12.

[146] *Supra* note 137, at 13.

[147] *Supra* note 137.

i. If "electronic technology automatically collects information when a prospective customer initiates contact, as is often the case with the use of cookie" it may not be practicable to give notice at or before the time of collection of the employees' personal information.

ii. Where personal information "is not obtained directly from the individual, but from a third party." "For example, when an insurance company collects employees' information from an employer in order to provide medical services, it may not be practicable for the insurance company to give notice at or before the time of collection of the employees' personal information."

iii. There is no need to provide notice with respect to publicly available information, or "business contact information and other professional information that identifies an individual in his or her professional capacity in a business context."[148]

Unlike the Report's recommendations, APEC does not address notices relating to security breaches. APEC also does not have a provision similar to the Report's "openness" recommendation relating to disclosure of the personal information controller's practices, procedures, policies, and systems.

## C. Collection Limitations

Similar to the Report's recommendations, APEC uses a relevancy standard for personal information collection: "The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, with notice to, or consent of, the individual concerned."[149] Also similar to the Report, the commentary calls for "proportionality to the fulfillment of such purposes," which may be "a factor in determining relevancy."[150] The commentary also stresses that collection must be fair, so that even if local law does not prevent obtaining personal information under false or deceptive pretenses, "they may be considered an unfair means of collection."[151]

---

[148] *Supra* note 137, at 13-14.

[149] Privacy Framework, at 15. Readers familiar with the U.S. health privacy law known as the Health Insurance Portability and Accountability Act of 1996, and the regulations will see a similarity to HIPAA's "minimum necessary" standard found in the Privacy Rule, 45 CFR § 164.502(b)(1): "When using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

[150] *Supra* note 137.

[151] *Supra* note 137.

## D. Uses of Personal Information

Similar to India's rules, APEC restricts the uses of personal information to fulfillment of the purposes of collection, with the following three exceptions:

a. consent of the individual;

b. where necessary to provide the product or service requested by the individual;

c. "by the authority of law and other legal instruments, proclamations, and pronouncements of legal effect."[152]

In addition, and of particular note to anyone who outsources personal information, the commentary clarifies that *use* of personal information includes "transfer or disclosure." The commentary also states that the "fundamental criterion in determining whether a purpose is compatible with or related to the stated purposes is whether the extended usage stems from or is in furtherance of such purposes."[153]

## E. Choice

Similar to the Reports principle on Choice and Consent, the APEC principles advise that, where appropriate, "individuals should be provided with clear, prominent, easily understandable, accessible, and affordable mechanisms to exercise choice in relation to the collection, use, and disclosure of their personal information."[154] Of interest to anyone with a globally-accessible web site, the commentary provides an exception to the "easily understandable" requirement: if the personal information controller's "communication is not directed to any particular economy or national group other than the one where the organization is located, this requirement will not apply."[155] This guidance is important because multinationals with operations in only one APEC economy will need to be concerned that the language used must be "easily understandable" only in that one APEC economy—there is no need for multiple translations. Importantly to companies that are centralizing their human resources data, the commentary states: "if an organization has decided to centralize human resources information, that organization should not be required to provide a mechanism to exercise choice to its employees before engaging in such an activity."[156]

---

[152] *Supra* note 137, at 16-17. This requirement is somewhat similar to the Report's "authorized agencies" exception, although APEC does not include the anonymization recommendation for public databases.

[153] *Supra* note 137.

[154] *Supra* note 137, at 17.

[155] *Supra* note 137, at 18.

[156] *Supra* note 13, at 20.

## F. Integrity of Personal Information

APEC is also concerned that personal information be accurate, in Principle 6: "Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use."[157] The commentary places this burden on the personal information controller, not the individual, but limits the burden to the purpose of the use. Thus, if the controller obtained an individual's mailing address in order to fulfill a single purchase, the requirement that the information be kept up-to-date would be minimal; in contrast, if the controller obtained an individual's mailing address in order to fulfill a monthly subscription, then the controller would have the ongoing obligation to ensure that the mailing address information was accurate.

In contrast to this principle, the Rules specify that Bodies Corporate are not responsible for the authenticity of the information provided, and the principles found in the Report are silent on the responsibility of a data controller to ensure that information is accurate.

## G. Security Safeguards

Similar to India's existing security requirements found in the Rules and recommended principle on security found in the Report, APEC requires "appropriate safeguards against risks" to personal information. APEC provides a flexible standard: "safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held, and should be subject to periodic review and reassessment."[158]

## H. Access and Correction

Another principle that APEC shares with India's requirements under the Rules and the Report, though not comprehensively, is that an individual has a right of access to, and correction of, his/her personal information. This section is the longest of the APEC principles, and contains several elements. It begins with three general principles:

a. Individuals should be able to receive confirmation as to whether a company holds personal information about them. This is present in the recommended principles, but not in the Rules.

b. After providing "sufficient proof of their identity," individuals should be able to obtain personal information about themselves "within a

[157] *Supra* note 137.

[158] *Supra* note 137, at 21. The Report, in contrast, lists the risks to be protected against, such as unauthorized access, destruction, and de-anonymization.

reasonable time," for a charge that is "not excessive," "in a reasonable manner" and "in a form that is generally understandable."[159]

c. Individuals can challenge the accuracy of the information and "if possible and as appropriate" have that information "rectified, completed, amended or deleted."[160]

A related portion of the principle provides that if the request or challenge is denied, "the individual should be provided with reasons why and be able to challenge such denial"[161] except "in cases where such disclosure would violate a law or judicial order."[162] The commentary emphasizes that an individual's right of access is not absolute,[163] and the principle provides three general exceptions:

i. where the "burden or expense" of providing access and opportunity for correction "would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question";

ii. disclosure should be prevented "due to legal or security reasons or to protect confidential commercial information"[164]; or

iii. "the information privacy of persons other than the individual would be violated."[165] Note that only this third exception is consistent with the Report's recommendations, while the Rules are silent on all three exceptions.

The commentary states that "organizations should always make good faith efforts to provide access,"[166] but lists several conditions where denials would be "acceptable," including: situations where claims would constitute an unreasonable expense or burden on the personal information controller, such as when claims for access are repetitious or vexatious by nature, cases where providing the information would constitute a violation of laws or would compromise security; or, incidences where it would be necessary in order to protect commercial confidential information that an organization has taken steps to protect from disclosure

[159] *Supra* note 137, at 22.
[160] *Supra* note 137.
[161] *Supra* note 137, at 24.
[162] *Supra* note 137, at 28.
[163] *Supra* note 137, at 22.
[164] APEC defines *confidential commercial information* to be "information that an organization has taken steps to protect from disclosure, where such disclosure would facilitate a competitor in the market to use or exploit the information against the business interest of the organization causing significant financial loss." *Supra* note 137, at 26.
[165] *Supra* note 137, at 23.
[166] *Supra* note 137, at 25.

where disclosure would benefit a competitor in the marketplace, such as a particular computer or modeling program.[167]

## I. Accountability

The final APEC principle states that the personal information controller "should be accountable for complying with measures that give effect to the Principles stated above."[168] Similar to the Report's recommendations, this principle states that:

When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles.[169]

Also similar to the Report, the commentary notes that "in cases where disclosures are required by domestic law, the personal information controller would be relieved of any due diligence or consent obligations."[170]

# VII. CONCLUSION

As demonstrated in the analysis above, the nine recommended National Privacy Principles as laid out in the Report of the Group of Experts on Privacy, though not an exact fit, reflect many of the principles central to the APEC privacy framework. As the principles presently only reflect recommendations, based off of the standards laid out, as summarized in the table below, the nine principles of APEC are similar to the ten requirements found in the Rules.

| **India Rules** | **APEC** |
|---|---|
| Privacy Policy | Notice |
| Collection of Information | Notice and Uses of Personal Information |
| Retention of Information | Not expressly addressed |
| Purpose Limitation | Collection Limitation and Uses of Personal Information |
| Access and Correction | Access and Correction |
| Opt Out | Choice |
| Redress Mechanism | Accountability |
| Disclosure of Information | Uses of Personal Information |

[167] *Supra* note 137, at 25-26.
[168] *Supra* note 137, at 28.
[169] *Supra* note 137.
[170] *Supra* note 137, at 29.

| **India Rules** | **APEC** |
|---|---|
| Transfer of Information | Accountability |
| Security | Security Safeguards |

India's privacy requirements as found under section 43A of the ITA and subsequent Rules are a close fit with the APEC Cross-Border Privacy Rules, but they are not perfectly aligned. To more closely match the APEC privacy framework, India would generally need to expand a few aspects of its privacy requirements, specifically:

- With respect to the *Collection* requirement, the protections would need to include all personal information, rather than be limited to sensitive personal information. This requirement should also address requirements relating to electronic information collection, such as cookies, as well as collection of information from third parties.
- It would also be helpful to provide examples of what is not considered personal information, such as business contact information.
- The *Purpose* requirement could be expanded from limiting use of collected information, to include both data transfers and disclosures.
- Because it is the longest section of the APEC requirements, the Access and Correction Principles would likely require the largest number of modifications. This expanded section could contain descriptions of processes for individuals to confirm that a Body Corporate has possession or control of an individual's personal information, a description of how and under what circumstances the individual can obtain a copy of the information from the Body Corporate, as how and under what circumstances an individual can request changes to that information. It would be helpful to provide examples of instances when such access and correction is appropriate, and when it is not.
- With respect to the *Opt Out* right, where individuals can choose not to provide information and can withdraw consent, it would be helpful to provide examples of when such a right applies and does not apply, such as APEC's example of a company that is centralizing its human resources data and does not need to provide an opt-out right.
- With respect to the *Redress Mechanism* that India requires, this expansion would need to include the third party accountability agent to assist in the redress of discrepancies and grievances.

- Finally, with respect to *Disclosure of Information*, as with the *Collection* requirement, the protections would need to include all personal information, rather than be limited to sensitive personal information.

Of course, APEC is involved with far more than privacy matters. But if India were to become a member of APEC, compliance with APEC's privacy requirements seems relatively straightforward. This would also hold true if India were to adopt the nine National Privacy Principles as laid out in the Report of the Group of Experts on Privacy.