Privacy and Data Protection in India

Dhiraj R. Duraiswami*

INTRODUCTION

India's recent demonetization initiative signaled a push towards digitization and a cashless economy primarily in order to eliminate corruption and black money while also improving the quality of life of the average citizen. The Indian Finance Minister in his budget speech announced an ambitious target of 25 billion digital transactions for the year 2017-18 which appears to be in line with recent growth trends.[1] Also, as a popular outsourcing destination India already sees a large volume of data cross its borders daily for processing, storage and use. Even more significant is the prevalence of cyber-attacks and cybercrime across the globe, which makes it imperative for a robust regulatory framework augmented with strict enforcement and redressal mechanisms and the adoption of good data governance practices. Risks presented by cyber-attacks know no borders; and individuals, organizations and nations are not fully protected. India is one of the top ten countries identified for cybercrime[2] and is not among the top ten countries most

* *Dhiraj Duraiswami* is an international business and technology consultant who has advised numerous clients in the United States over the last twenty years. He is a Certified Information Systems Auditor (CISA). He earned an LL.M in Intellectual Property and Information Law from the Benjamin N. Cardozo School of Law, a post graduate diploma in International Trade from IIFT, Delhi and MBA, BL, and B.Com degrees from the University of Madras, India. He is admitted to the Bar in Chennai, India. He also serves as the Digital Content Editor for the Journal of Law & Cyber Warfare.

[1] Dipti Jain, *Can India Meet the Target of 2500 crore Digital Transactions in 2017-18?*, LIVEMINT (March 30, 2017, 04:52 PM IST), http://www.livemint.com/Politics/637uTLKanriP4PbFhhCznJ/Can-India-meet-the-target-of-2500-crore-digital-transaction.html.

[2] James Cook, *The World's 10 Biggest Cybercrime Hotspots in 2016*

prepared for cyber-attacks.[3] In 2016, according to Symantec in their Norton Cyber Security Insights Report, over 689 million people in twenty-one countries experienced cybercrime and over $126 billion spent by the victims since 2015.[4]

This article provides an overview of the current privacy and data protection laws in India, the enforcement and liability provisions of those laws, and pending regulations and trends to protect privacy and enhance data governance practices.

I. REGULATORY OVERVIEW

Protection of privacy and personal data is achieved most commonly through the regulatory framework of laws, policies and procedures that minimizes the intrusion into the privacy of individuals as a result of the collection, storage and dissemination of sensitive personal data. Such personal data generally refers to the information collected by any person, organization, government or agency and is not to be confused with trade secrets or other confidential information. There is no dedicated or omnibus piece of legislation in India that protects privacy or personal data, but there are various laws pertaining to information technology,

---

Ranked, BUSINESS INSIDER (May 14, 2017, 3:01 AM), http://www.businessinsider.com/worlds-10-cybercrime-hotspots-in-2016-ranked-symantec-2017-5/.

[3] José Santiago, *Top Countries Best Prepared against Cyber-attacks*, WORLD ECON. FORUM (22 July 2015), https://www.weforum.org/agenda/2015/07/top-countries-best-prepared-against-cyberattacks/.

[4] *2016 Norton Cyber Security Insights Report*, SYMANTEC, https://us.norton.com/cyber-security-insights-2016 (last visited July 28, 2017).

contracts, intellectual property and crimes that offer protection and impose civil and criminal liability. Presently, the provisions of the Information Technology Act, 2000 ("IT Act") and the rules issued thereunder cover the concept of sensitive personal data or information and provide the legal framework for data protection and privacy in India.

In addition to the IT Act and the implied right to privacy under the Constitution upheld by the judiciary[5], the main pieces of legislation that provide data protection include the Contract Act, 1872; The Indian Copyright Act, 1957; Indian Penal Code, 1860 and the Credit Information Companies Regulation Act, 2005. The Justice Shah Report on Privacy in 2012 recommended the passing of privacy legislation, in addition to identifying 57 specific existing sectoral and policy guidelines that have privacy implications and hence would need to be amended as the new legislation is passed.[6] A draft privacy protection bill was introduced in the Indian Parliament in 2014 and is expected to be reviewed and passed as law in response to concerns regarding personal data protection in the country.[7] While the bill is pending, the focus for the purposes of this article remains on the existing laws and rules available to protect personal data.

A. Constitutional Protection

Article 21 of the Constitution of India dealing with

---

[5] *Kharak Singh v. U.P*, AIR, 1963 SC 1295 (India).

[6] *Report of the Group of Experts on Privacy*, GOV'T OF INDIA PLANNING COMM'N, (16 October, 2012), http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf.

[7] Ranjani Ayyar & Rachel Chitra, *Data Privacy Back in Spotlight,* THE TIMES OF INDIA (January 19, 2017, 09:43 AM IST), http://timesofindia.indiatimes.com/trend-tracking/data-privacy-back-in-spotlight/articleshow/56658914.cms.

the fundamental freedom to life and liberty has been interpreted to include the concept of the privacy right. The constitutionally guaranteed right to free speech and expression provided under Article 19(1)(a) can have privacy read into such individual fundamental rights, which however, as with other existing fundamental rights, are only enforceable against the state and subject to reasonable restrictions that may be imposed under Article 19(2). Indian courts have given paramount importance to such a perceived, albeit limited, right of privacy which can only, in their opinion, be fettered for compelling reasons, such as national security and in the interests of the public.[8] However, the Supreme Court of India has yet to conclusively decide if such a right to privacy is a fundamental right guaranteed under the Constitution, though a challenge was allowed in 2015, with the matter pending and referred to a larger bench of the apex court for a decision.[9]

It is relevant to note that privacy has been recognized as a fundamental human right; enshrined in numerous international human rights instruments[10] including the

---

[8] *Kharak Singh v. U.P*, AIR, 1963 SC 1295 (India); *Gobind v. M.P.*, AIR, 1975 SC 1375 (India); *R. Rajagopal v. Tamil Nadu* (1994) 6 SCC 632 (India); *People's Union of Civil Liberties (PUCL) v. Union of India*, AIR, 1997 SC 568 (India); *Dist. Registrar and Collector, Hyderabad v. Canara Bank*, AIR, 2005 SC 186 (India).

[9] *Puttaswamy v. Union of India*, http://judis.nic.in/supremecourt/imgs1.aspx?filename=42841 (last visited June 18, 2017).

[10] G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948); G.A. Res. 45/158, United Nations Convention on Migrant Workers (Dec. 10, 1990); G.A. Art. 16, Convention of the Protection of the Child, 1577 U.N.T.S., 3 (Nov. 20, 1989); G.A. Art. 17, International Covenant on Civil and Political Rights, 999 U.N.T.S, 171 (Dec. 16, 1966); Organization of African Unity, *African Charter on the Rights and Welfare of the Child* art. 10, Jul.11, 1990,

International Covenant on Civil and Political Rights ("ICCPR"). Article 17 of the ICCPR provides that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation". States party to the ICCPR have a positive obligation to "adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right [privacy]"[11]. India is also party to The Universal Declaration of Human Rights, whose Article 12 provides privacy protection.

B. Information Technology Act, 2002 and Privacy Rules

The Information Technology Act ("IT Act"), read along with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("Privacy Rules"), contains specific provisions that constitute the relevant national law regulating the collection, transfer and use of

---

CAB/LEG/24.9/49 (1990); Organization of American States, *American Convention on Human Rights* art.11, Nov.21, 1969, O.A.T.S. No.36, 1144 U.N.T.S.123; African Union *Declaration of Principles on Freedom of Expression* art.4, Oct.22, 2002, available at: http://www.refworld.org/docid/4753d3a40.html [accessed 2 July 2017]; Inter-American Commission on Human Rights, *American Declaration of the Rights and Duties of Man* art.5, May.2, 1948, OEA/Ser. L./V.II.23, doc. 21, rev. 6 (1948); League of Arab States, *Arab Charter on Human Rights* art.17, Sep.15, 1994, http://www.refworld.org/docid/3ae6b38540.html [accessed 2 July 2017]; Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms* art. 8, Nov.4, 1950, E.T.S 5, 213 U.N.T.S. 221.

[11] *ICCPR*, General Comment No. 16 (1988), para. 1.

personal information. The IT Act is specifically intended to protect electronic data, which by definition includes non-electronic records or information that have been, are currently or intended to be processed electronically. Additionally, the IT Act regulates other aspects of information technology including electronic commerce and cybercrimes.

The Privacy Rules[12] require corporate entities collecting, processing and storing personal data including sensitive personal information to comply with prescribed procedures. It distinguishes between the "personal information" and "sensitive personal data or information" ("SPDI") as a subset of personal information. Personal information is defined as any information that relates to a natural person, which either directly or indirectly, in combination with other information that is available or likely to be available to a corporate entity, is capable of identifying such person.[13]

The Privacy Rules identify the following personal information as SPDI:

- passwords;
- financial information, such as bank account or credit card or debit card or other payment instrument details;
- physical, physiological and mental health condition;

[12] *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*, MINISTRY OF COMMC'N. & INFO. TECH., GOV'T OF INDIA, http://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf (last visited June 27, 2017).

[13] *Id.*, Rule 2(1) (i).

- sexual orientation;
- medical records and history;
- biometric information;
- any detail relating to the above as provided to body corporate for providing services; and
- any information received under the above by body corporate for processing, stored or processed under lawful contract or otherwise.[14]

"Biometrics" has been defined to mean the technologies that measure and analyze human body characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns, hand measurements and DNA for authentication purposes.[15] However, any information freely available in the public domain is exempt from the above definition.

1. Reasonable Security Practices and Procedures

Any corporate entity that possesses, manages or handles any SPDI in a computer resource that it owns, controls or operates, under section 43-A of the IT Act, is liable for civil liabilities. These liabilities require compensation for negligence in implementing and maintaining "reasonable security practices and procedures" in relation to such SPDI that results in wrongful loss or wrongful gain to any person. This section along with the Privacy Rules has compelled companies collecting and using

[14] *Id.*, Rule 3.
[15] *Id.*, Rule 2(1) (b).

such personal data to review their contractual arrangements in order to ensure that their data security practices and procedures are at par with those that are stipulated.[16] The Privacy Rules stipulate that "reasonable security practices and procedures" to be adopted by any corporate entity to secure sensitive personal information are procedures that comply with the IS/ISO/IEC 27001 standard on "Information Technology – Security Techniques – Information Security Management System – Requirements".[17] Any industry association or corporate entity following any other standard for data protection is required to get its pertinent codes for data protection best practices approved and notified by the Government of India.[18] Such corporate bodies which have implemented the stipulated standard or approved codes also need to get the same certified or audited by an independent auditor approved by the Central Government. Further, an audit has to be carried out by such an auditor at least once a year or whenever there is a significant upgradation of processes and computer resources.[19]

2. Collection, Processing and Transfer

The Privacy Rules require any corporate entity or any person acting on its behalf to obtain prior consent in writing from the information provider(s) regarding the purpose of usage of the SPDI.[20] The corporate entity is required to take reasonable steps to ensure that the information provider is notified, at the time of collection of the SPDI or other

[16] *Id.*, Rule 8(1).
[17] *Id.*, Rule 8(2).
[18] *Id.*, Rule 8(3).
[19] *Id.*, Rule 8(4).
[20] *Id.*, Rule 5(1).

personal information of: the collection of information, the purpose of collecting such information, the intended recipients of the information and the name and address of the agency collecting and retaining the information. Such information may only be collected for a lawful purpose connected with the functioning of the corporate entity.[21] The corporate entity must also ensure that the information is used only for the purpose collected and that it does not retain the sensitive personal information for longer than for the required purpose.[22]

The Privacy Rules also mandate that any corporate entity or any person who on behalf of such entity collects, receives, possess, stores, deals or handles such information provide a privacy policy that discloses its practices regarding the handling and disclosure of personal information, including sensitive personal information, and ensure that the policy is available for view, including on the website of the corporate entity or the person acting on its behalf.[23] The providers of information should be allowed to review and correct the information they had so provided to ensure that no part of the information is inaccurate or deficient.[24] Further, the provider of information has to be provided a right to opt out or retract the consent earlier provided. However, in case the provider of information does not provide or subsequently withdraws consent, the corporate entity will have the option not to provide the services or goods for which the information was earlier sought.[25]

The corporate entity or the person collecting the data on its behalf must obtain the consent of the provider for any

[21] *Id.*, Rule 5(2).
[22] *Id.*, Rule 5(4).
[23] *Id.*, Rule 4(1)(i).
[24] *Id.*, Rule 5(6).
[25] *Id.*, Rule 5(7).

transfer of sensitive personal information to any other corporate entity or person in India, or in any other country provided that the transferee ensures the same level of data protection adhered to by the data collector under the Privacy Rules.[26] The transfer may be allowed only if is required for the performance of a lawful contract between the corporate entity or any person acting on its behalf and the provider of information. A corporate entity may not transfer any sensitive personal information to another person or entity that does not maintain the same level of data protection as required in the IT Act and Privacy Rules.

Contracts regulating between the data collector and the transferee should contain adequate indemnity provisions for a third-party breach, must clearly specify the end purposes of the data processing, including who would have access to such data, and clearly specify a mode of transfer that is adequately secured and safe. Such contracts are required specifically to include provisions that entitle the data collector to distinguish between "personal information" and "sensitive personal information" that it wishes to collect or process; this is to represent that the consent of the person(s) concerned has been obtained for collection and disclosure of such personal information or sensitive personal information; and to outline the liability of the third-party transferee.

3. Enforcement, Breach Notification and Redressal

The erstwhile Department of Electronics and Information Technology (upgraded to full-fledged ministry in July 2016) was the government agency empowered to

[26] *Id.*, Rule 7.

administer the IT Act. The DEITY periodically publishes rules for the regulation of data privacy and personal data protection. In this regard, DEITY notified and brought into force the Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 ("Cert-In Rules").[27] The Cert-In Rules impose mandatory notification requirements on service providers, intermediaries, data centers and corporate entities in the event of certain types of "Cyber Security Incidents" including unauthorized access of IT systems or data. The Cert-In Rules define "Cyber Security Incidents" as

> Any real or suspected adverse events, in relation to cyber security, that violate any explicitly or implicitly applicable security policy, resulting in: unauthorized access, denial or disruption of service; unauthorized use of a computer resource for processing or storage of information; or changes to data or information without authorization.[28]

Any occurrence of the following types of cyber security incidents will trigger the notification requirements under the Cert-In Rules:

- targeted scanning/probing of critical networks/systems;

---

[27] *Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013*, NOTIFICATION, MINISTRY OF ELECS. & INFO. TECH., GOV'T OF INDIA, http://meity.gov.in/writereaddata/files/G_S_R%2020%20%28E%292_0.pdf (last visited June 27, 2017).

[28] *Id.*, Rule 2(1)(h).

- compromise of critical information/systems;
- unauthorized access of IT systems/data;
- defacement of websites or intrusion into website and unauthorized changes such as inserting malicious code or links to external websites;
- malicious code attacks such as spreading virus, worms, trojans, botnets/spyware;
- attacks on servers such as database, mail, DNS and network devices such as routers;
- identity theft, spoofing and phishing attacks;
- denial of service (DoS) & distributed denial of service (DDoS) attacks;
- attacks on critical infrastructure, SCADA systems and wireless networks;
- attacks on applications such as e-governance and e-commerce etc.[29]

Upon the occurrence of any of these events, companies are required to notify the Indian Computer Emergency Response Team ("CERT-In") CERT-In is a government body established to collect, analyze and disseminate information on cyber incidents, as well as provide forecasts and alerts about cyber security incidents, provide emergency measures for handling cyber security incidents and coordinate cyber incident response activities. Such notifications are required to be made within a reasonable time, so as to leave scope for appropriate action by the authorities. It is important to follow "breach notice obligations" which would depend upon the "place of occurrence of such breaches" and on whether or not Indian customers have been targeted. The specific format and

[29] *Id.,* Annexure to the Cert-In Rules.

procedures for reporting cyber security incidents are set out by CERT-In on its official website.[30] CERT-In currently functions under the newly constituted Ministry of Electronics and Information Technology ("MEITY").

Besides the civil liabilities prescribed under section 43-A, section 72-A of the IT Act imposes punishment for disclosure of "personal information" by any service provider, without the consent of the data subject or in breach of an agreement with such subject, and with the intent to, or knowing that it is likely to cause wrongful gain or wrongful loss. The IT Act provides for criminal sanctions of up to three years in prison and/or a fine of up to INR 500,000 in respect of intentional or negligent disclosure of an individual's personal information, obtained under a contract, where such disclosure is made without the consent of the concerned individual or in breach of the concerned contract.

The Privacy Rules provide that a corporate entity must address grievances of the information provider within a specified time. The corporate entity should appoint a Grievance Officer to address such grievances within one month from receipt of the grievance. There is no specific requirement that the Grievance Officer must be a citizen of or resident of India, nor are there any specific enforcement actions or penalties associated with not appointing a data protection officer correctly. However, appointment of such an officer is part of the statutory due diligence process and it thus becomes imperative to appoint one.

In August of 2011, India's Ministry of Communications and Information issued a Press Note[31] to

---

[30] *Indian – Computer Emergency Response Team*, MINISTRY OF ELECS. & INFO. TECH., GOV'T OF INDIA, http://www.cert-in.org.in/ (last visited June 18, 2017).

[31] *Clarification on Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information)*

make some clarifications on the Privacy Rules, which included one that exempted any Indian outsourcing service provider organization that provides services relating to collection, storage, dealing or handling of sensitive personal information or personal information under contractual obligation with any legal entity located within or outside India from the collection and disclosure of information requirements, including the consent requirements discussed above, provided that they do not have direct contact with the data subjects (providers of information) when providing their services.

C. Indian Contract Act, 1872

Given the limitations of enforceability and incomprehensive nature of the IT Act and Privacy Rules in India, which is a popular off-shoring destination, redressal for violation of personal data and privacy rights can be sought within the framework of the law of contracts as provided under the Indian Contract Act, 1872. Companies generally enter into contractual agreements with other companies who may be clients, suppliers or partners and, where personal sensitive information needs to be kept secure, the agreements usually contain confidentiality and privacy clauses in addition to arbitration clauses for the purpose of resolving any foreseeable disputes. Remedies in the nature of damages or compensation can be sought for violation of any terms of the contract or for non-performance of the obligations imposed, including those specifically

---

Rules, 2011 Under Section 43A of the Information Technology ACT, 2000, PRESS NOTE, MINISTRY OF COMMC'N & INFO. TECH., PRESS INFORMATION BUREAU, GOV'T OF INDIA, http://pib.nic.in/newsite/erelcontent.aspx?relid=74990 (last visited June 18, 2017).

relating to data protection or any breach of contractual obligations in general, are provided under the Contract Act.

When US companies enter into contracts with off-shore or third party vendors in India, it is customary to include terms and specific conditions in their contracts for data protection to comply with the Graham-Leach Bliley Act, Health Insurance Portability and Accountability Act, Fair and Accurate Credit Transactions Act, etc. Typically, these vendor agreements also prescribe how the information can be disclosed and provide for implementation of necessary safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the data provided to the vendors. Since personal data collection itself is not being done in India in such cases, the process of seeking consent to collect, process, use, store or otherwise transfer such personal data will be done outside of India by the customer company, and obligations for their protection would be imposed on the Indian vendor entities.

D. Criminal Laws & Procedure – Indian Penal Code, 1860

As the Indian criminal law does not specifically address privacy or data privacy under the Indian Penal Code ("IPC"), liability for such breaches must be inferred from related crimes. Where there is a theft of data, prosecution can follow for the offenses of theft[32], misappropriation of property[33] or criminal breach of trust.[34] For example, section 403 of the IPC imposes a criminal penalty for dishonest misappropriation or conversion of "movable property" of

[32] PEN. CODE, Sections 378, 379.
[33] *Id.*, Section 403.
[34] *Id.*, Sections 405, 408, 409.

another for one's own use. Movable property has been defined as property which is not attached to anything and is not land, and can also be construed to include private personal data, which is stored in a tangible medium. The punishment for such criminal offences, as in the case of a breach of trust, is stringent by way of imprisonment which may extend to three years, a fine or both.

E. Intellectual Property Laws – Copyright Act, 1957

India's Copyright Act, 1957 governs intellectual property rights in literary, dramatic, musical, artistic and cinematographic works. Indian Courts have recognized copyright in computer databases[35] and granted them the status of "literary work" under this Act. Compilations of client or customer lists developed by a person by devoting time, money, labor and skill have been interpreted to amount to "literary work" wherein the author has a copyright under the Copyright Act. Any infringement that occurs with respect to such protected databases leads to a cause of action under the Copyright Act for the outsourcing parent entity. Copying the computer database, or copying and distributing the database without legal authorization, would amount to infringement of copyright as such and give rise to the remedies of injunction and damages for the plaintiff. Any person who knows of such infringement and conceals or abets it is also liable to pay a fine up to INR 200,000, faces imprisonment up to three years or both.

The Indian Copyright Act prescribes mandatory punishment for piracy of copyrighted matter depending on

[35] *Burlington Home Shopping Pvt. Ltd. v. Rajnish Chibber* 61 (1995) DLT 6; (1996) 113 PLR 31.

the gravity of the offence. Section 63B of the Indian Copyright Act provides that knowingly using a computer to create an infringing copy of a computer program shall be punishable for a minimum period of six months and a maximum of three years in prison. Fines in the minimum amount of INR 50,000 up to a maximum of INR 200,000 may be levied for second or subsequent convictions.

F. Credit Information Companies Regulation Act, 2005

Based on the Fair Credit Reporting Act and Graham Leach Bliley Act, the Credit Information Companies Regulation Act ("CICRA") has created a strict framework for protecting information regarding credit and finances of the individuals and companies in India. The CICRA requires that the credit information of individuals in India has to be collected as per privacy norms enunciated in the CICRA regulation. The Reserve Bank of India has notified Regulations[36] under CICRA which provide for strict data privacy principles. Entities collecting the data and maintaining the same have been made liable for any possible leak or alteration of this data. The Regulations specify the following entities as "specified users"[37] within the purview of the CICRA and authorized to collect credit information:

> (a) an insurance company as defined under the Insurance Act, 1938 and registered with Insurance

[36] *Credit Information Companies Regulations, 2006 Under Section 37 of the Credit Information Companies (Regulation) Act, 2005,* MINISTRY OF FINANCE, DEPT. OF ECONOMIC AFFAIRS, BANKING DIVISION, GOV'T OF INDIA, https://rbidocs.rbi.org.in/rdocs/Content/PDFs/69700.pdf (last viewed June 27, 2017).
[37] *Id.,* Rule 3.

Regulatory and Development Authority;
(b) a company providing cellular/phone services and registered with Telecom Regulatory Authority of India;
(c) a rating agency registered with Securities and Exchange Board of India.
(d) a broker registered with Securities and Exchange Board of India;
(e) a trading member registered with a recognized Commodity Exchange;
(f) Securities Exchange Board of India; and
(g) Insurance Regulatory and Development Authority.

II. RECENT TRENDS AND INDUSTRY INITIATIVE

A. Proposed New Legislation

Of particular interest is the petition filed recently in the Supreme Court of India challenging WhatsApp's privacy policy change allowing sharing of data with Facebook. The policy was first challenged in the Delhi High Court by petitioners who claimed violation of users' privacy.[38] In September last year the Delhi High Court had ruled that WhatsApp had to delete user account information of all those who deleted the application and that the company could not share such information with its parent company Facebook up to the date of the order. The petition specifically points out the government's responsibility to

[38] *WhatsApp Privacy Policy Case: Here's what it says and Why it Matters*, THE INDIAN EXPRESS (updated April 29, 2017 8:57 am) http://indianexpress.com/article/technology/tech-news-technology/whatsapp-facebook-privacy-case-supreme-court-everything-you-need-to-know-4631853/ (last visited June 18, 2017).

guarantee and ensure the protection of the personal and private data when using such modes of communication whereby private and confidential data and information is exchanged.[39]

In response to this case and already in earlier hearings, the Government Counsel indicated that a regulatory regime on data protection for consumers in India is expected soon,[40] while the Department of Telecommunications informed the court that over the top ("OTT") players such as WhatsApp, Facebook and Skype were sought to be covered by new regulations that are being explored. This marks the significance of the new privacy legislations that are sought to be introduced soon in addition to the available current legal framework provided by the IT Act and complemented by the other available general laws. Earlier concerns relating to the review and passage of the new Privacy Bill, due to reservations from various quarters, are sought to be addressed soon.[41]

B. Industry Initiative

Given the lack of comprehensive legislation for privacy and data protection, the private sector rather than the government has taken the initiative and made efforts to comply with the demands of privacy principles and self-regulation. The National Association of Service & Software

---

[39] *WhatsApp Case, supra* quotes from original petition.

[40] Priyanka, *Indian Govt is Working on Data Protection Law*, PIXR8, http://pixr8.com/indian-govt-is-working-on-data-protection-law (last visited June 18, 2017).

[41] Yatish Yadav, *Privacy Bill held up due to Intel Agency Reservations*, THE NEW INDIAN EXPRESS (updated 07 March 2017 03:30 AM), http://www.newindianexpress.com/nation/2017/mar/07/privacy-bill-held-up-due-to-intel-agency-reservations-1578461.html.

Companies ("NASSCOM") is India's national information technology business group and has taken various steps to drive private sector efforts to improve data security.[42] Recognizing the need to provide assurances of privacy protection of nonpublic personal information to foreign clients, many BPO service providers in India have engaged in self-regulation after recognizing the potential damage that could be inflicted on the Indian BPO industry resulting from major security abuses. Through the efforts of NASSCOM, stringent security measures have been developed and recommended to BPO service providers, such as the following:

- armed guards posted outside offices;
- entry restricted by requiring microchip-embedded swipe cards;
- bags and briefcases prohibited in the work area;
- key information, such as passwords, encrypted and unseen by employees;
- employees monitored via closed-circuit television.[43]

NASSCOM has also created a National Skills Registry as a centralized database of employees of IT vendor services and business process outsourcing ("BPO") companies.[44] This repository provides information about all

[42] Barbara Crutchfield George & Deborah Roach Gaut, *Offshore Outsourcing to India by U.S. and E.U. Companies*, 6 U.C. DAVIS BUS. L.J. 13 (2006).
[43] *Id.*, at 15.
[44] NATIONAL SKILLS REGISTRY, https://nationalskillsregistry.com/aboutus.htm (last visited June 27, 2017).

registered professionals including background check reports of the workforce employed within the IT/BPO industry. Additionally, a self-regulatory organization has been launched which will establish, monitor and enforce privacy and data protection standards for India's business process outsourcing industry supported by extensive industry membership.

III. CONCLUSION

Given the current dynamic and constantly expanding scenario in India, which is replete with challenges, increasing foreign investments and economic growth in an ever-expanding digital era, there is an unprecedented need to update privacy and data protection laws and standards in line with global initiatives which are tested and already in place. The lack of comprehensive legislation, while a matter of concern, has been offset by recent initiatives by the industry, the public and the government. These initiatives seek to bring in the needed legal framework while complementing the existing regulations and the proactive opinions and to stand by the judiciary to ensure defaulting entities are held accountable for not adequately protecting personal data. It behooves companies seeking to establish business in India to adhere to the local laws especially in the context of the increasing sensitivity of the Indian legal system towards data protection and privacy concerns.