Winter January 24, 2016

Data Protection.pdf

Praveen Paliwal, *New law College, Bharti Vidyapeeth Deemed University*

DATA PROTECTION IN INDIA

INTRODUCTION

The Data Protection Act 1998 (DPA) is an Act of Parliament of the United Kingdom of Great Britain and Northern Ireland which defines UK law on the processing of data on identifiable living people. It is the main piece of legislation that governs the protection of personal data in the UK.

The protection of data finds its roots in the individual's right to privacy doctrine.[2] The right to privacy has been explicitly contained in or has inferentially been found to exist in the constitutions of most developed nations and the jurisprudential parameters of privacy rights explored in various forums.[3] However, the specific privacy issue related to protection of personal data became an issue of growing concern in progressive nations in the 1970s with the advent of computerized systems which could store and disseminate large amounts of information with relative ease via automated processes.[4]

"Data protection refers to the set of privacy-motivated laws, policies and procedures that aim to minimize intrusion into respondents' privacy caused by the collection, storage and dissemination of personal data."[5] It is the legal safeguard used to prevent misuse of information stored in computers - particularly information about individual people. Data protection encompasses control and management of the data creation and creation of basic rights and obligations and also stipulates penalties and remedies in case of misuse of the data.

In the United Kingdom, the Younger Committee on Privacy was instituted in the early 1970‘s to make recommendations regarding the manipulation of computerized personal data.[6] Similarly, in the United States, the Data Privacy Act of 1974 was enacted.[7] Subsequent protection of the privacy of personal information was accomplished in the United Kingdom and the United States through various legislative enactments.[8] However, the gold standard for data protection was established by the European Union in 1995 with the passage of E.U. Directive 95/46/EC.[9] The Directive established comprehensive legislation for data protection, setting a high standard for non-E.U. Member States to meet. The European Union's regime impacted non-

---

[2] Peter Carey, Data Protection: A Practical Guide to UK and EU Law 23 (2d ed. 2004)

[3] Ryan Moshell, Comment, _The Outlook for a Self-Regulatory United States Amidst a Global Trend Towards Comprehensive Data Protection‘, 37 Tex. Tech L. Rev. 357, 373 (2005)

[4] Carey, supra note 1, at 1-3.

[5] Organisation for Economic Co-Operation and Development, Data Protection, Glossary of Statistical Terms, http://stats.oecd.org/glossary/detail.asp?ID= 6903

[6] Ibid.

[7] 5 U.S.C. §552a.

[8] The Data Protection Act of 1984; Also see Carey, supra note 10, at 3.
[9] Council Directive 95/46/EC, 1995 O.J. (L281) (EC), available at http://europa.eu.int/comm/justice_home/fsj/privacy/law/index_en.htm

E.U. member nations directly because under the Directive data could not be transferred to states which did not provide adequate standards for protection.

The term "data" has been defined under section 2(o) of the IT Act of 2000. Data is the "physical representation of information in a manner suitable for communication, interpretation, or processing by human beings or by automatic means." The definition of "data" and its protection in the Indian context, does not give a comprehensive understanding of the term.

1.1 Research scheme

The researcher, in the course of developing a model law for data protection in India based on the European directive and other related foreign legislations, would examine India‘s recent baby steps taken in direction of data protection. These would include the proposed amendments to the IT Act, the formation of the Data Security Council of India under Nasscom, maintaining of the National Do-not-Call Register and the to-be introduced National Customer Preference Registry under TRAI. Also examined would be the challenges with respect to data protection in the upcoming cloud based computing networks in India with special emphasis on the viability in terms of security of data in the Indian government‘s ambitious Unique Identification Authority of India (UIDAI) project.

CURRENT DATA PROTECTION LAWS IN INDIA

In India, the protection of privacy, a basic human right recognized by the Universal Declaration of Human Rights of 1948[48], was derived from common law torts and constitutional law.[49] A person may be held tortiously liable for unlawful invasion of privacy of another[50], whereas under constitutional law, this right has been implicitly recognized[51], but is subject to reasonable State-imposed restrictions. However, the IT Act of 2000 is considered to be the most widely recognized legislation that covers data protection.[52] In order to cover the shortcoming in the IT Act of 2000, contractual clauses that the Indian companies have agreed to come into play in the trade with overseas clients.[53]

4.1 Constitutional Law

The protection of data finds its roots in the individual's right to privacy.[54] In a number of decisions, the Supreme Court of India has upheld the right to privacy[55] as a fundamental right.[56] Moreover, Article 300A of the Constitution of India, provides for the right to property as a constitutional right.[57] This makes intellectual property in the data a subject of this right.[58]

To adhere to the international human rights instruments (International Covenant on Civil and Political Rights,[59] International Covenant on Economic Social Cultural Rights,[60] and

[48] Universal Declaration of Human Rights, G.A. Res. 217 A (III), U.N. Doc. A/RES/217 (III), Article 12 (Dec. 10 1948), available at http://www.ohchr.org/EN/UDHR/Documents/UDHR Translations/eng.pdf.
[49] Madhavi Divan, The Right to Privacy in the Age of Information and Communications, 4 SCC (Jour) (2002), available at http://www.ebc-india.com/lawyer/articles/2002v4a3.
[50] R. Rajagopal v. State of Tamil Nadu, (1994) 6 S.C.C. 632, 639.
[51] Constitution of India,.Art. 21.
[52] NASSCOM Announces Milestones for Its 'Trusted Sourcing' Initiative, NASSCOM
[53] Vakul Sharma, Legal Issues for Data Protection: Myths and Realities.
[54] Supra note 1.
[55] U.S. Dep't of Commerce, Privacy and the NII: Safeguarding Telecommunication-related Personal Information 5 (1995), available at http://www.ntia.doc.gov/ntiahome/provwhitepaper.html.
[56] Kharak Singh v. State of Uttar Pradesh, A.I.R. 1963 S.C. 1295.
[57] Constitution of India, Art. 300A.
[58] Carpenter v. United States, 484 U.S. 19, 26-27 (1987).
[59] International Covenant on Civil and Political Rights, G.A. Res. 2200A (XXI), 21 U.N. GAOR, 23 March, 1976.
[60] International Covenant on Economic, Social and Cultural Rights, G.A. Res. 2200A (XXI), 21 U.N.GAOR.

Universal Declaration of Human Rights[61]), the Indian Parliament has enacted a variety of legislation to safeguard recognized human rights. For example, the **Protection** for Human Rights Act of 1993 provides for the constitution of a National and State Human Rights Commission and Human Rights Courts for better **protection** of Human Rights and for connected or incidental matters.[62]

4.2 Information Technology Act of 2000

The IT Act of 2000 is considered to be the law that governs data and its protection.[63] When the IT Act of 2000 was passed, the concept of "data protection" was not envisaged. The only safeguard that the IT Act of 2000 provides to data is with respect to the penalty in a case of breach or unlawful activity. The provision under the IT Act of 2000 that deals with unauthorized access and damage to data is Section 43.[64] Section 43(b) affords cursory safeguards against breaches in data protection. The scope of Section 43(b) is limited to the unauthorized access, downloading, copying, extraction, or damage of data from a computer system.[65] However, the Information Technology (Amendment) Act of 2008[66] has removed any cap on the amount of damages.[67] The damages under Section 43 were quantified at Rupees one crore, but the IT Act of 2008 has removed this limit of one crore and made the damages unliquidated; thus, the damages that one can suffer under these instances can be well above Rupees one crore.[68]

Section 43-A of the IT Act of 2008 deals with compensation for failure to protect data by a corporation involved in "possessing, dealing, or handling any sensitive personal **data** or information in a computer resource which it owns, controls, or operates" and "causes wrongful loss or wrongful gain to any person."[69] In order to ensure that a corporation is liable under this section, it has to be proved that the corporation was negligent in implementing "reasonable security practices and procedures."[70] This section places liability on an intermediary as well.[71]

---

[61] Universal Declaration of Human Rights, G.A. Res. 217 A (III), U.N. Doc. A/RES/217 (III), Article 12 (Dec. 10 1948), available at http://www.ohchr.org/EN/UDHR/Documents/UDHR Translations/eng.pdf.
[62] Protection for Human Rights Act, No. 10 of 1993.
[63] Information Technology Act, No. 21 of 2000
[64] Information Technology Act, No. 21 of 2000, Section 43.
[65] Ibid.
[66] Information Technology Act, No. 21 of 2000, Section 43A.
[67] Ibid.
[68] Ibid.
[69] Ibid.
[70] Ibid.

However, the liability of an intermediary sued under section 43-A is diluted in section 79 of the Act, which inserts both "knowledge" and "best efforts" as qualifiers prior to assessing penalties.[72] Moreover, section 85 of the IT Act of 2008 also invokes entity liability, limited to the specified illegal acts of persons for intentional or negligent acts that result in a breach of the specific violations under the IT Act of 2000.

4.3 Intellectual Property Rights Laws

Computer software (including computer programs[73], databases, computer files, preparatory design material, and associated printed documentation, such as users' manuals) receives copyright protection under Indian laws.[74] The Indian Copyright Act of 1957 "prescribes mandatory punishment for piracy of copyrighted matter commensurate with the gravity of the offense."[75] Computer programs are not per se patentable, being patentable only in combination with hardware.[76] Thus in India, by past practice and under current laws, copyright is the preferred mode of protection for computer software.

4.4 Criminal Laws

Under the Indian Penal Code of 1860 ("IPC"), there is no express criminal punishment for breaching data privacy, thus "liability for data-related breaches must be inferred from tangentially related crimes."[77] For example, "Section 403 of the Indian Penal Code imposes criminal penalty for dishonest misappropriation or conversion of 'movable property' for one's own use."[78] Therefore, "although no jurisprudence has been developed on this interpretation, arguably, movable property encompasses computer-related data and intellectual property."[79] There is an element of trust involved when a person discloses his or her personal information to

---

[71] Ibid.
[72] Information Technology Act, No. 21 of 2000, Section 79.
[73] Section 63B of the Indian Copyright Act of 1957.
[74] Section 2(o) of the Indian Copyright Act of 1957.
[75] Umesh Pandit, Intellectual Property Rights in India, knol Beta, http://knol.google. com/k/umesh-pandit/intellectual-property-rights-in-india/r0tyv5xaaisc/45#
[76] Manisha Singh, India's Patent law - is it TRIPs compliant?, Managing Intell. Prop., (2005) available at http://www.managingip.com/article/1321451/Indias-patent-lawis-it-TRIPs-compliant.html.
[77] Vinita Bali, Data Privacy, Data Piracy: Can India Provide Adequate Protection for Electronically Transferred Data? (Legal Studies Research Papers Series, Social Science Research Electronic Paper Collection, Santa Clara University School of Law, Working Paper No. 06-10, Oct. 2006).
[78] India Penal Code, Section 403.
[79] Supra note 76.

another. In the case where this information is disclosed to a third party, it could result in criminal penalties for the criminal breach of trust.[80] Further, the IPC imposes criminal liability for dishonest or fraudulent concealment or removal of property[81], and also for when a person "cheats and thereby dishonestly induces the person" in possession of the property to deliver the said property.[82] Furthermore, section 425 imposes liability on a third party who intends to cause wrongful loss or damage to the property of another person, whether or not the person is the owner of the property.[83]

4.5 Contractual Obligations

Non-E.U. states where data protection has not been found to be "adequate,"[84] such as in India[85], rely on an alternative avenue and ad hoc solutions to procure and continue business transactions. The European Commission and the Data Protection Commissioner have the power to endorse "model contracts" specific to the transferring countries' circumstances, as well as the power to approve particular contracts or other arrangements that provide satisfactory safeguards.[86] Data Exporters in other countries enter into a contract with an Indian BPO detailing the specific duties and obligations of both parties involved. Therefore, in the absence of legislation that offers sufficient and adequate legal protection for personal data, any uncertainty regarding doing business with an Indian BPO is a matter of negotiation of the relevant contract using appropriate legal expertise and advice. Apart from contractual obligations with the Data Exporters, the employment contracts between the BPO and its employees also specify that the employees have to maintain confidentiality regarding all such information that they may process.[87]

---

[80] Indian Penal Code, Section 405.
[81] Indian Penal Code, Section 424.
[82] Indian Penal Code, Section 420.
[83] Indian Penal Code, Section 425.
[84] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.
[85] Ibid.
[86] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.
[87] Ibid.

4.6 The Credit Information Companies (Regulation) Act of 2005

The Credit Information Companies (Regulation) Act of 2005 "imposes duties on credit information companies, credit institutions, and specified users while processing credit data."[88] Additionally, the Reserve Bank of India has the authority to penalize any credit information company, credit institution, or specified user, for violating this Act.[89] On this ground, the "Reserve Bank of India could be considered as a specific data protection authority in the field of credit information."[90]

[88] Rodney D. Ryder & Ashwin Madhavan, Data Protection, Privacy and Corporate Compliance: The Law and Emerging Trends in India, Scriboard.
[89] Ibid.
[90] Ibid.

INDIAN LAWS ON DATA PROTECTION

Although India has been proactive in making provisions for the protection of data, it has a long way to go in order to reach the heights of protection afforded by international provisions for data protection in foreign countries. The protection of data in India needs to be critically examined and the lacuna must be spotted. Only then can a measure for its elimination be taken. The shortcomings in the national data protection laws may be examined as follows

5.1 Information Technology Act of 2000

The major shortcoming in the IT Act of 2000, as amended by the IT Act of 2008, is that none of the three objectives detailed in the preamble[91] recognize the protection and preservation of data. The very fact that data protection is outside the scope and purpose of the IT Act weakens the relevance of its provisions. Moreover, "data" under the IT Act of 2000 is restricted to data stored and processed in the electronic form.[92] Considering that India still employs conventional methods of data storage, transfer, and process, all forms of data other than electronic data are susceptible to unauthorized use that might adversely affect the subjects of such data. Therefore, this legislation does not provide protection to data stored in the non-electronic medium.

Section 43 penalizes any unauthorized access to a computer, computer system or computer network and any unauthorized download, copying or extraction of any data.[93] An interpretation of section 43 shows that it provides for protection of data in a very limited sense - it is only a punitive provision.[94] The IT Act of 2000 penalizes any individual who misuses electronic data, without the permission of the owner or any other person in charge of such data. This penalty is inadequate because it does not address the concern of misuse of data by the person responsible for such data. Section 43 does not address data protection. Rather, it is merely

[91] Information Technology Act, No. 21 of 2000,
[92] Information Technology Act, No. 21 of 2000, S. 2(o).
[93] Information Technology Act, No. 21 of 2000, S.43.
[94] Ibid.

recourse to compensate the individual for any damage resulting from unauthorized access or damage to data.

"Data protection" in its entirety means the collection, retention, protection and proper disposal of the data collected.[95] Therefore, section 43 of the IT Act of 2000 is very limited because it only provides a remedy for unauthorized access or damage to stored data. It does not address many of the principles provided in the Data Protection Act of 1998 (DPA).

In the provisions under the DPA in the U.K., personal information and sensitive personal information have different levels of protection, where loss, unauthorized access or disclosure of sensitive personal information is considered to have a deeper impact on the data subject.[96] In contrast to the DPA, the IT Act of 2000 does not assign a higher level of care or protection to sensitive personal information. In essence, there is no difference between personal information and sensitive personal information in relation to data protection. Indeed, "personal information" is not defined in judicial precedent or the IT Act of 2008. Because this term has not been defined, it is difficult to give an exact interpretation of the provisions.

Section 43-A of the IT Act of 2008 places liability on a corporate body only if it has been negligent in implementing its security practices and procedures in relation to the **data** possessed, controlled or handled by it.[97] There is a significant difference between "negligence to implement" and "failure to implement." The former requires the test of reasonableness to be satisfied before there can be any claim of negligence, while the latter requires only non-performance of the required action. Therefore, there is no liability for the corporate body in cases of failure to implement its security practices and procedures, thereby widening their scope for escaping liability.

The terms "wrongful gain" and "wrongful loss" are used under section 43-A of the IT Act of 2008.[98] However, these terms have not been clearly defined with relevance to data protection, either under statutes or any judicial precedents. It is unclear whether these terms derive their meaning from their definition under the substantive penal law of India, the Indian Penal Code of

---

[95] Ibid.
[96] Data Protection Act, 1998 (Eng.)
[97] Information Technology (Amendment) Act, 2008, Section 43-A.
[98] Ibid.

1860. Therefore, it is difficult to comprehend the true meaning and application of this section in light of these undefined terms.

The section also makes a reference to "reasonable security practices and procedures," which has been defined under the IT Act of 2008.[99] The three methods by which reasonable security practices and procedures can be determined are: 1) by agreement; 2) by law; and 3) by prescription by the Central Government.[100] However, there is no law in India that defines this term and it will be some time before the Central Government promulgates the necessary regulations to give meaning to this term. Until these regulations are created, a corporation is not liable if the corporation does not agree with the person providing the information to define reasonable security practices and procedures, and then proceeds to disclose that information, even if the corporation causes loss or gain to that person. Thus, the protections are meaningless.

Under the IT Act of 2008, section 43-A places liability on an intermediary as well. However, an intermediary sued under section 43-A, can claim immunity under section 79, if the intermediary satisfies the test laid down under section 79.[101] Therefore, although the law creates personal liability for illegal or unauthorized acts, little effort is made to ensure that Internet service providers or network service providers, as well as entities handling data, are responsible for the safe distribution or processing of the data.[102]

Section 72-A clearly requires that a person who discloses personal information, thereby causing wrongful loss or gain, to have done so willfully.[103] Hence, in order to make a person liable it has to be proved that the person disclosing the personal information did so with an intention to cause wrongful loss or gain.[104] Mere proof of the damage is insufficient.[105] Moreover, section 72-A does not help individuals monetarily. It imposes penal consequences on such persons by way of a fine,[106] which is insufficient to compensate the injured party.

---

[99] Ibid.
[100] Ibid.
[101] Information Technology (Amendment) Act, 2008, Section 79.
[102] Supra note 76.
[103] Supra note. 100.
[104] Ibid.
[105] Ibid.
[106] Ibid.

Further, section 72-A is restricted to information about individuals and relates only to personal information obtained under service contracts.[107] This section also makes it evident that disclosure of personal information with intent to cause wrongful loss or gain has to be done without the consent of the person, whose personal information is being disclosed.[108] It may be stated that this provision has not been drafted to cover all situations. In many cases, corporations and individuals when entering into service contracts, ensure that they obtain consent of the individuals for any future disclosures. There are also standard form contracts where the clauses cannot be negotiated - the parties must accept all clauses. Hence, if disclosure of information is one of the clauses in such contracts, then any disclosure is deemed to be with the consent of the person concerned. Therefore, if such a corporation obtains the individual's consent at the time of entering into service contracts, the protection provided for under this section does not apply. The "consent" referred to in section 72-A can be easily circumvented by corporations and individuals by means of clever drafting when entering into service contracts.

Section 72 is insufficient because the section only applies if the breach is committed by a person who has been conferred certain powers under the Act, rules, or regulations.[109]

The Indian laws do not specify conditions under which data can be collected and used, and its limited scope fails to meet the breadth and depth of protection that the E.U. Directive mandates.[110] The Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data, 1980 promulgated by the OECD are also instructive, demonstrating that a large void exists in India's IT Act of 2000.[111]

5.2 Criminal Laws

The protection provided by criminal laws is not sufficient in the context of data protection. At the time of enactment of the IPC, it was not envisioned that the provisions would be used to provide data protection. Although the IT Act of 2000 and IT Act of 2008 have made amendments to the IPC, there has been no change with regard to the application of the IPC to data protection. The meaning of "movable property" is unclear as to whether it extends to include

---

[107] Ibid.
[108] Ibid.
[109] Ibid.
[110] Supra note 76.
[111] Ibid.

intellectual property. Moreover, the adequacy of the remedies under India's criminal laws is questionable in a trans-national context. As correctly pointed out, "the cost, delay and inconvenience associated with foreign nationals bringing actions in Indian courts offsets the availability of the recourse."

5.3 Intellectual Property Rights Laws

On perusal of the Indian Copyright Act of 1956, it is evident that the Act does not afford complete protection to data. The penalties under this Act are inadequate in a trans-national context. Moreover, the backlog of cases in the Indian criminal courts is not only detrimental to the enforcement of copyright laws on the national and international front,[112] but it also prolongs litigation. Further, there would be the question of conflicting rights and jurisdictions, thereby duplicating litigation.[113]

5.4 Contractual Obligations

It is pertinent to note that although the gap in the laws is sought to be filled through contractual recourse, it may not be very effective in the absence of strict laws backing it up. The major drawback in use of model contracts is that the Indian BPO is subject to the jurisdiction of an E.U. Member State and the data protection authority, and any departure from the standard clauses runs the risk of disapproval of the contract by the data protection authority.

In contracts for the transfer of data, a number of third parties may be involved: first, the data subjects; second, the third parties to whom the data is to be re-exported by the importer; and last, the data protection authorities. However, in the case of breach of contract, the injured party may only seek a remedy against the contracting party.[114] The injured third party may not have proper recourse against the actual wrong-doer. Moreover, in relations with third parties, dispute resolution clauses in the contract between the BPO and the Data Exporter are likely to be of very limited effect. The determination as to the governing law or the competent adjudicating authority will, therefore, be difficult to impose on the third parties in the event of a dispute.

---

[112] Priti H. Doshi, Copyright Problems in India Affecting Hollywood and Bollywood, 26.2 Suffolk Transnat'l L. Rev. 295 (2003)
[113] Section 62 of the Indian Copyright Act of 1957.
[114] TweddleTweedle v. Atkinson, (1861) 123 E.R. 762.

Moreover, the clause indemnifying any loss caused by a third party could prove to be detrimental to the party indemnifying the loss. The third party causing the loss could escape liability and the party to the contract, dealing with that third party, would be responsible instead. Another shortcoming in the application of contractual laws for protection of data is that some outsourcing agreements include a clause limiting the liability of the party. It contains a cap on the amount or extent of damages for which a party may be liable.[115] While this clause, detailing the liquidated damages, makes assessment of the same easier and excludes interference by the courts, it also requires an accurate pre-estimate of the possible damage, which, if not properly calculated, could result in loss to the injured party.

5.5 Researcher's suggestions towards a reform in the protection codes

The Indian system of data protection can be best described as a web, i.e. many protections are offered through various sources and the web traps some violations, but gaps and holes remain through which others slide through. In order to address the inadequacies of the IT Act of 2000 and the miscellaneous laws providing protection of data, Indian businesses and the Indian government drafted amendments which would fill the voids. Although passage of the amended law covering data protection was anticipated in 2004, the proposed legislation was shelved due to a change in government in 2004.[116] Whether the IT Act is amended, or alternative legislation enacted to protect the sanctity of transferred data, the new laws must offer effective enforcement in order to conform to the "adequacy" norms of the Directive and the Safe Harbor privacy principles of the U.S. After the new rules are in force, India will enter discussions with the E.U. to get recognition as a country that offers an adequate level of protection for personal data.

Enactment of law that facially provides protection is but one step in the fight to maintain the sanctity of data. Even if satisfactory data protection laws are in place in India, the real question in assessing the adequacy of the law is whether these laws will be effective in deterring wrongful data piracy. Two issues are examined in this context. The first general issue is whether punishment deters crime. If it is concluded that appropriate sanctions do prevent and deter crime, the second issue is whether wrongful appropriation of data will be prosecuted in India

[115] Bharath Vagadia, Outsourcing to India: A Legal Handbook 57 (Verlag Berlin Heidelberg: Springer, 2007).
[116] An amendment to the IT Act of 2000.

sufficiently so as to be a deterrent. If the Indian enforcement system is found inadequate, alternative enforcement processes must be established to prosecute violations of data privacy. A system of specialized courts instituted in India to prosecute cyber infringement cases, including data privacy violations, is essential for this purpose.

Once the data protection laws in India are strengthened, the general legal system must be tweaked in order to address data protection enforcement. Proposed remedies to fix the enforcement void include establishment of a national centralized enforcement body dedicated to, and trained in, electronic data piracy and enforcement. This national body must be given jurisdictional authority to enforce across state borders. In addition, it is essential to have specialized local police enforcement units which are specifically trained and maintained to recognize instances of, and enforce actions against, data piracy crimes. Finally, it is vital to adopt meaningful court reform to decrease burdens, costs and delays, and ensure that cases are concluded promptly with deterrent penalties and damages.

CONCLUSION

Data protection is an issue that is gaining increasing importance as our transnational exchange of private information grows. While the E.U. has adopted stringent legislation to protect data, and the U.S. has reached agreement with the E.U. to offer protection, the Indian laws remain unsatisfactory. It is anticipated that India will soon enact legislation which will provide acceptable protection to private data. The issue that remains to be dealt with in the Indian context is, unfortunately, far larger than the enactment of strong protectionist laws. Laws act as a deterrent to wrongful conduct if they are applied with certainty and speed: both sadly deficient in the Indian judicial system. Unless addressed, the systemic problems of enforcement in India, and specifically, of unresolved cases due to court delays, will continue to render India's data protection laws inadequate.