Data Security and Cybercrime in India

Global, India | October 29 2018

Jurisdiction snapshot

Trends and climate

Would you consider your national data protection laws to be ahead or behind of the international curve?

Indian data protection law is behind the international curve. The country's data protection laws largely consist of:

- a statutory provision for payment of compensation for failure to protect sensitive personal information; and
- a criminal provision for disclosure of personal information without the data subject's consent or in breach of a contract.

However, both provisions apply only if a wrongful gain or loss results from the disclosure or breach. Government-prescribed rules on privacy apply only if the parties have not agreed to their own security standards and, even if they do apply, the only consequence of non-compliance would be payment of compensation if the breach results in wrongful gain or loss.

Are any changes to existing data protection legislation proposed or expected in the near future?

There have been two recent major changes to the privacy framework. First, on August 24 2017 the Supreme Court of India held that the right to privacy is a fundamental right guaranteed under the Constitution of India. This is a right available to the residents of India against the state and government. Second, the Information Technology Ministry has appointed a panel of experts to study India's data protection framework and suggest a draft data protection law that will be taken up for consideration by Parliament. Therefore, it seems likely that in the next year, a comprehensive privacy legislation will be enacted in India.

Legal framework

Legislation

What legislation governs the collection, storage and use of personal data?

The collection, storage and use of personal data is largely regulated by the Information Technology (IT) Act 2000. Further, sectoral regulations impose additional data protection obligations in areas such as banking, telecoms and medical practice.

Section 43A of the IT Act provides for compensation in the event that a company fails to use reasonable security practices and procedures in order to protect sensitive personal data and such negligence results in a wrongful gain or loss. However, the statute provides for compensation only when a wrongful gain or loss results from the failure to observe reasonable security practices and procedures. It can be argued that this is nothing more than a codification of the law of negligence. This means that no negative consequence arises from the failure to observe reasonable security practices and procedures. Further, the IT Act defines 'reasonable security practices and procedures' as procedures stated by a law in force or as agreed by the parties and, in the absence

of both, the rules framed by the government. To date, no statute prescribes reasonable security practices and procedures. This means that if the parties (eg, a data subject and a data receiver) agree on the reasonable security practices and procedures to be adopted, the government-prescribed rules will not apply.

In an attempt to establish what constitutes reasonable security practices and procedures, the government issued rather basic and poorly written privacy rules. As stated above, these rules apply only if the parties have not agreed on their own reasonable security practices and procedures. The rules contain basic principles of privacy, such as:

- when sensitive personal data can be collected;
- requirements of notice and consent; and
- when sensitive personal data can be transferred.

Section 72 of the IT Act provides for a criminal penalty where a government official discloses records and information accessed in the course of his or her duties without the consent of the concerned person, unless permitted by other laws. The penalty prescribed is imprisonment of up to two years, a fine of up to Rs100,000 or both.

Section 72A of the IT Act provides for a criminal penalty where in the course of performing a contract, a service provider discloses personal information without the data subject's consent or in breach of a lawful contract and with the knowledge that he or she will cause or is likely to cause wrongful loss or gain. The punishment prescribed is imprisonment of up to three years, a fine of up to Rs500,000 or both.

Scope and jurisdiction

Who falls within the scope of the legislation?

Section 43A applies only to private organisations and does not include the government. Section 72A could theoretically apply to the government, but the possibility of it applying where government services are provided under a contract is limited. Section 72 exclusively addresses personal information accessed by a government official.

What kind of data falls within the scope of the legislation?

The IT Act sets out two types of data: personal information and sensitive personal data.

'Personal information' has been defined to mean any information that relates to a natural person that directly, indirectly or in combination with other information (that is likely to be available to a body corporate) is capable of identifying that person.

Section 43A of the IT Act regulates dealing with or handling sensitive personal data. The IT Act does not specifically define 'sensitive personal data', but provides that it means any personal information that the government prescribes as such. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data and Information) Rules 2011 define 'sensitive personal data' as personal information relating to:

- passwords;
- financial information such as bank account or credit card details;
- physical, physiological and mental health;
- sexual orientation;
- medical records and history; and
- biometric information.

Are data owners required to register with the relevant authority before processing data?

India has no specific data protection authority. Data owners need not register with any authority before processing data.

Is information regarding registered data owners publicly available?

This is not applicable, as data owners need not register with any authority.

Is there a requirement to appoint a data protection officer?

There is no requirement to appoint a data protection officer. However, the Privacy Rules require that a grievance officer be appointed to address discrepancies and the data subject's grievances. The service provider must provide the name and contact details of the grievance officer to the data subject.

Enforcement

Which body is responsible for enforcing data protection legislation and what are its powers?

India has no specific data protection authority, and thus matters are adjudicated by authorities empowered under the IT Act. The IT Act provides for the appointment of an adjudicating officer, who will oversee matters related to the contravention of the IT Act or its rules where the claim for injury or damages does not exceed Rs50 million. If the claim exceeds Rs50 million, the adjudicating authority will be the civil court. The secretary to the Ministry of Information Technology in each state government has been appointed as the adjudicating officer. The adjudicating officer has all the powers of a civil court, including the right to:

- summon persons and examine them under oath;
- demand the discovery or production of documents and other electronic records;
- request evidence on affidavits; and
- issue commissions for the examination of witnesses or documents.

The police can investigate offences under the IT Act, such as those outlined in Sections 72 and 72A.

Under specialised statutes relating to banking, telecoms and the medical field, the relevant sectoral regulator would be the responsible body.

Collection and storage of data

Collection and management

In what circumstances can personal data be collected, stored and processed?

The Privacy Rules specify that a body corporate may collect sensitive personal data:

- for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf; and
- if the collection of sensitive personal data or information is considered necessary for that purpose.

Are there any limitations or restrictions on the period for which an organisation may (or must) retain records?

Yes, the Privacy Rules specify that sensitive personal data cannot be retained for longer than is required for the purpose for which it was lawfully collected or as otherwise required under another law. Under the data retention provisions set out in various laws, companies are generally required to retain data for eight financial years.

Do individuals have a right to access personal information about them that is held by an organisation?

Under the Privacy Rules, data subjects have a right to review the information provided by them. The data controller, at the request of the data subjects, must correct any deficiencies or inaccuracies in the information provided. Further, data controllers must address data subjects' grievances in a timely manner and in any event within one month of receiving the grievance.

Do individuals have a right to request deletion of their data?

The Privacy Rules do not specifically provide data subjects with the right to request deletion of their data. However, data subjects have the right to withdraw their consent to process data. Once consent is withdrawn, data controllers and processors cannot process the data subject's sensitive personal data. If a data subject withdraws his or her consent, the data processor can stop the provision of services.

Consent obligations

Is consent required before processing personal data?

Under the Privacy Rules, the data subject's consent is required before processing any sensitive personal data. Consent must be obtained in writing by letter, fax, email or any mode of electronic communication. Consent must be express and thus implied consent is not recognised.

If consent is not provided, are there other circumstances in which data processing is permitted?

Prior express consent must be obtained from the data subject, with no exceptions. However, notably, the Privacy Rules apply only if the parties have not agreed to their own reasonable security practices and procedures.

What information must be provided to individuals when personal data is collected?

The Privacy Rules require data controllers to provide data subjects with the following information:

- the fact that the information is being collected;
- the purpose for which the information is being collected;
- the intended recipients of the information; and
- the name and address of the agency that is collecting the information and will retain it.

Data security and breach notification

Security obligations

Are there specific security obligations that must be complied with?

Section 43A refers to 'reasonable security practices and procedures', which have been defined as reasonable security practices and procedures as determined by a law in force (of which there is none) or as agreed to by the parties and, in the absence of both, the rules framed by the government (ie, the Privacy Rules). Accordingly, the parties are free to decide on the security standards to be adopted.

The Privacy Rules do not prescribe a particular security standard (although this is was what the rules were meant to do). Instead, they suggest that the International Standards Organisation/International Electrotechnical Commission 27001 or a code prescribed by an industry association and approved by the government can be used. Thus far, the government has approved no codes.

The banking regulations on the other hand require banks to follow ISO/IEC 27001 and ISO/IEC 27002. Similarly, the securities exchange regulations require stock exchanges, depositories and clearing corporations to follow standards such as ISO 27001, ISO 27002, COBIT 5.

Breach notification

Are data owners/processors required to notify individuals in the event of a breach?

The IT Act or the Privacy Rules do not require data owners or processors to notify individuals in the event of a breach.

Are data owners/processors required to notify the regulator in the event of a breach?

There are two scenarios under which data breach notifications are required to be made to the regulators. First, the banking regulations require banks to intimate the RBI in case of any cyber security incident within two to six hours of the breach.

Second, there are certain rules relating to notification of breaches to the Computer Emergency Response Team (CERT). The law is unclear as to whether such notifications are mandatory. Past enquiries with the CERT have resulted in a view that such notifications are voluntary. However, the CERT has recently taken the stand that such notifications are mandatory.

Separately, certain regulations that provide a safe harbour from third-party liability for intermediaries require the intermediaries, as part of their due diligence obligations, to notify the CERT in case of security breaches. The definition of 'intermediary' is wide and includes telecoms, ISPs, network service providers, web hosts, search engines, online payment and auction sites and online marketplaces. However, in practice, such a requirement would be relevant only to those organisations that might be held liable for third-party content.

The data breach regulations define ‘cybersecurity incident’ to mean any real or suspected adverse event in relation to cybersecurity that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, and information without authorisation. There is a further definition through a description of various incidents that constitute cybersecurity incident:

- targeted scanning or probing of critical networks and systems;
- compromise of critical systems and information;
- unauthorised access to IT systems and data;
- defacement of website or intrusion onto a website and unauthorised changes(eg, inserting malicious code or links to external websites);
- malicious code attacks (eg, spreading viruses, worms, Trojan horses, botnets and spyware);
- attacks on servers (eg, database, mail and DNS) and network devices (eg, routers);
- identity theft, spoofing and phishing attacks;
- denial of service and distributed denial of service attacks;
- attacks on critical infrastructure, SCADA systems and wireless networks; and
- attacks on applications such as e-governance and e-commerce.

The above list includes not just breaches, but also cyberattacks which do not result in actual breaches.

Electronic marketing and internet use

Electronic marketing

Are there rules specifically governing unsolicited electronic marketing (spam)?

India has no laws governing marketing through email or fax. In 2015 a badly worded provision to address spam was struck down by the Supreme Court as unconstitutional.

The IT Act does not cover electronic marketing. This is covered by the Telecom Commercial Communication Customer Preference Regulations set out by the Telecom Regulatory Authority of India (TRAI). Under the regulations, individuals can register their numbers on a do-not-call registry. Individuals can also register to receive certain categories of information, including information regarding:

- banking, insurance, financial products and credit cards;
- real estate;
- education;
- health;
- consumer goods and automobiles;
- communication, broadcasting, entertainment and internet technology; and
- tourism and leisure.

Further, text messages can be sent if the message is transactional in nature. Transactional messages cover only prescribed areas, which include information relating to:

- a banking, securities or insurance account;
- air and rail travel schedules and reservations;
- an educational institution; and
- e-commerce companies in relation to transactions.

The regulations also allow messaging by identified social media organisations such as Facebook and Yahoo. There are also limits on how many text messages a non-telemarketer can send a day.

Telemarketers that make marketing calls or send marketing messages must:

- be registered with the TRAI;
- obtain separate telecoms resources specifically for engaging in telemarketing;
- obtain separate telecoms resources for sending transactional messages; and
- synchronise their databases with the do-not-call registry regularly.

The law also requires telecoms service providers to have backend integration with the do-not-call registry. Thus, if a message is meant to be sent to a person on the do-not-call registry and is not transactional in nature or does not fall within a selected exception, the telecoms service provider's IT systems will automatically block the message.

Various penalties have been prescribed where telemarketers violate the regulations. Fines range from Rs25,000 for a first violation to Rs250,000 for a sixth violation. On the sixth violation, the telemarketer will be blacklisted and prohibited from using any kind of telecoms resources in India.

Cookies

Are there rules governing the use of cookies?

Indian law does not directly deal with the use of cookies or equivalent technology.

Section 43 of the IT Act imposes a restriction on accessing, downloading, copying or extracting any data, computer database or information from any computer, computer system or computer network without the permission of the owner or the person in charge. The IT Act imposes both compensation and criminal penalties in case of a breach. The IT Act's language in this regard is broad enough to cover cookies and accordingly consent is technically required for the use of cookies.

Data transfer and third parties

Cross-border data transfer

What rules govern the transfer of data outside your jurisdiction?

The Privacy Rules permit the transfer of sensitive personal data or any information to a person outside India, provided that the person ensures the same level of data protection as that under the Privacy Rules. Further, transfers are permitted only if they are necessary for the performance of a lawful contract with the provider or where the provider has consented to the transfer.

The Reserve Bank of India (RBI) regulations on outsourcing permits banks to transfer data outside India, provide that:

- the offshore regulator will not obstruct the arrangement or prevent inspections by the RBI or auditors;
- the availability of records to the management and RBI would withstand the liquidation of the offshore provider or the bank in India;
- the offshore regulator does not have access to the data simply because the data is being processed overseas; and
- the jurisdiction of the courts in the offshore location would not extend to the operations of the bank in India.

The outsourcing regulations also require customer data to be isolated and clearly identified and that there be no comingling of data.

The telecoms regulations impose restrictions on transfer of customer accounting and user information outside of India, except with regard to roaming information and remote access to such data from outside India. This restriction applies to remote access to such data from outside India.

The government's recently announced cloud policy also require vendors who provide cloud-based services to the government to ensure that all relevant data is stored on servers in India.

Are there restrictions on the geographic transfer of data?

The Privacy Rules permit the transfer of sensitive personal data or any information to a person outside India, provided that the person maintains the same level of data protection as provided for under the Privacy Rules. Further, transfers are permitted only if they are necessary for the performance of a lawful contract with the provider or where the provider has consented to the transfer.

In accordance with a recent, little-known company law provision relating to maintenance of accounts, if a company's books, papers and books of accounts are maintained in electronic form outside India, a backup must be stored on servers physically located in India. This rule has not been strictly enforced by the regulators, as it runs contrary to the increasingly common practice of multinationals, which use global accounting systems to maintain the accounts of entities worldwide, including Indian entities.

See above for restrictions on transfer of banking and telecoms data.

Third parties

Do any specific requirements apply to data owners where personal data is transferred to a third party for processing?

The Privacy Rules regulate the disclosure or transfer of sensitive personal data to a third party. The disclosure of sensitive personal data or information is permitted if:

- it has been agreed in a contract with the provider;
- it is necessary to comply with a legal obligation; or
- the provider has given its prior consent.

Disclosures can be made only to a third party that observes the same level of data protection as provided by the Privacy Rules. Further, transfers are permitted only if they are necessary for the performance of a lawful contract with the provider or where the provider has consented to the transfer.

A clarification issued by the Ministry of Communications and Information Technology appears to suggest that some of the Privacy Rules apply only between a data subject and a data processor, and not between two entities. However, in accordance with the Privacy Rules, any third party that receives information must ensure the same level of protection as stated under the Privacy Rules. The two provisions are thus not entirely harmonious.

The Privacy Rules require data processors to disclose the name and address of every agency which will have access to personal information when collecting information from a data subject. This includes onward transfers. Since the transfer of sensitive personal data from a data subject to a data processor is subject to restrictions, these restrictions will also apply to a further transfer from one data processor to another.

Penalties and compensation

Penalties

What are the potential penalties for non-compliance with data protection provisions?

Under Section 43A, if a breach results in a wrongful gain or loss, the adjudicating officer or the courts (as the case may be) can order compensation to be paid. There is no maximum compensation prescribed.

The following penalties apply:

- Under Section 66 (use of cookies without consent), the penalty is imprisonment of up to three years, a fine of up to Rs500,000 or both.
- Under Section 72, the penalty is imprisonment of up to two years, a fine of up to Rs100,000 or both.
- Under Section 72A, the penalty is imprisonment of up to three years, a fine of up to Rs500,000 or both.

Compensation

Are individuals entitled to compensation for loss suffered as a result of a data breach or non-compliance with data protection provisions by the data owner?

The IT Act provides for compensation to be paid if the data processor is negligent in using reasonable security practices and procedures to protect sensitive personal data and this results in a wrongful loss or gain. The terms 'wrongful gain' and 'wrongful loss' are not defined in the IT Act, but are defined in the Penal Code.

'Wrongful gain' is defined as a gain by unlawful means of property to which the person gaining is not legally entitled. 'Wrongful loss' means loss by unlawful means of property to which the person losing it is legally entitled.

While the definitions in the Penal Code cannot be entirely relied on for the purposes of Section 43A since the purpose of the provisions are different, they do have some persuasive value. Given the manner in which Section 43A is drafted and the meaning of 'wrongful gain' and 'wrongful loss' under Indian laws, it is likely that actual damage would be required in order to claim compensation.

Cybersecurity

Cybersecurity legislation, regulation and enforcement

Has legislation been introduced in your jurisdiction that specifically covers cybercrime and/or cybersecurity?

India has no specific cybercrime legislation. The IT Act and Penal Code cover cybercrimes punishable in India.

What are the other significant regulatory considerations regarding cybersecurity in your jurisdiction (including any international standards that have been adopted)?

The IT Act imposes no regulatory consideration regarding cybersecurity; instead, it provides an option for the data subject and data processor to determine the security standard. The Privacy Rules do not prescribe a particular security standard (despite the fact that this is what they were meant to do) but merely suggest that International Standards Organisation/International Electrotechnical Commission (ISO/IEC) 27001 or a code prescribed by an industry association and approved by the government could be used. Thus far, no code has been approved by the government.

The Reserve Bank of India has prescribed detailed guidelines on information security, electronic banking, technology risk management and cyber frauds which apply to banks. The guidelines require the use of encryption technology of at least 128 bit secure sockets layer and implementation of ISO/IEC 27001 and ISO/IEC 27002.

Which cyber activities are criminalised in your jurisdiction?

Punishable cyber activities include:

- hacking;
- identity theft;
- cyber terrorism;
- privacy violations;
- cheating by impersonation; and
- publication of obscene materials.

Which authorities are responsible for enforcing cybersecurity rules?

The IT Act provides for an adjudicating officer to be appointed where a person has contravened the IT Act or its rules and the claim of injury or damages does not exceed Rs50 million. If the claim exceeds Rs50 million, the adjudicating authority will be the civil court. The secretary to the Ministry of Information Technology in each state government has been appointed as the adjudicating officer. The adjudicating officer has the same powers as a civil court, including the right to:

- summon persons and examine them under oath;

- require the discovery or production of documents and other electronic records;
- request evidence on affidavits; and
- issue commissions for the examination of witnesses or documents.

In accordance with the IT Act, the Ministry of Communication and Information Technology set up the Computer Emergency Response Team (CERT), which acts as the nodal agency for resolving cybersecurity incidents in India. It is responsible for scanning cyberspace for cybersecurity vulnerabilities, breaches and malicious activity and can block webpages and websites. CERT's functions include:

- collecting, analysing and disseminating information on cyber incidents;
- forecasting and providing alerts of cybersecurity incidents;
- taking emergency measures to address cybersecurity incidents; and
- coordinating cyber incidents response activities.

Although CERT is the nodal body for handling cybersecurity incidents, neither the IT Act nor any rules thereunder require individuals or body corporates to report cybersecurity incidents to CERT.

Under specialised statutes, the relevant sectoral authorities in the banking, telecoms and medical field have power to enforce cybersecurity rules.

Cybersecurity best practice and reporting

Can companies obtain insurance for cybersecurity breaches and is it common to do so?

Many leading insurers in India have launched insurance schemes offering coverage against cyber risks. With the increased rate of cybercrime, organisations have begun to consider insurance as an option and many have already insured themselves against these risks.

Are companies required to keep records of cybercrime threats, attacks and breaches?

There is no obligation under the IT Act or the rules made thereunder to keep records of any security incident. However, from a limitation perspective, companies should retain all such records for a minimum period of three years.

Are companies required to report cybercrime threats, attacks and breaches to the relevant authorities?

There are two scenarios under which data breach notifications are required to be made to the regulators. First, the banking regulations require banks to intimate the RBI in case of any cyber security incident within two to six hours of the breach.

Second, there are certain rules relating to notification of breaches to the Computer Emergency Response Team (CERT). The law is unclear as to whether such notifications are mandatory. Past enquiries with the CERT have resulted in a view that such notifications are voluntary. However, the CERT has recently taken the stand that such notifications are mandatory.

Separately, certain regulations that provide a safe harbour from third-party liability for intermediaries require the intermediaries, as part of their due diligence obligations, to notify the CERT in case of security breaches. The definition of 'intermediary' is wide and includes telecoms, ISPs, network service providers, web hosts, search engines, online payment and auction sites and online marketplaces. However, in practice, such a requirement would be relevant only to those organisations that might be held liable for third-party content.

The data breach regulations define 'cybersecurity incident' to mean any real or suspected adverse event in relation to cybersecurity that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, and information without authorisation. There is a further definition through a description of various incidents that constitute cybersecurity incident:

- targeted scanning or probing of critical networks and systems;
- compromise of critical systems and information;

- unauthorised access to IT systems and data;
- defacement of website or intrusion onto a website and unauthorised changes(eg, inserting malicious code or links to external websites);
- malicious code attacks (eg, spreading viruses, worms, Trojan horses, botnets and spyware);
- attacks on servers (eg, database, mail and DNS) and network devices (eg, routers);
- identity theft, spoofing and phishing attacks;
- denial of service and distributed denial of service attacks;
- attacks on critical infrastructure, SCADA systems and wireless networks; and
- attacks on applications such as e-governance and e-commerce.

The above list includes not just breaches, but also cyberattacks which do not result in actual breaches.

Are companies required to report cybercrime threats, attacks and breaches publicly?

Companies need not report any cybersecurity incident publicly.

Criminal sanctions and penalties

What are the potential criminal sanctions for cybercrime?

The penalties for cybersecurity incidents vary depending on the type of cybercrime. Typical penalties include imprisonment for one to five years, a fine of between Rs100,000 and Rs500,000 or both. In case of a tort claim, there is no upper limit on compensation and the courts may determine the amount on a case-by-case basis.

What penalties may be imposed for failure to comply with cybersecurity regulations?

Section 43A provides for compensation in the event of negligence with regard to reasonable security practices and procedures when protecting sensitive personal data and this results in a wrongful gain or loss.

Section 72A provides for criminal punishment if, in the course of performing a contract, a service provider discloses personal information without the consent of the person concerned or in breach of a lawful contract and with the knowledge that he or she will cause or is likely to cause wrongful loss or gain. The punishment prescribed is imprisonment for up to three years, a maximum fine of Rs500,000 or both.

Kochhar & Co - Stephen Mathias and Naqeeb Ahmed Kazia