Data protection and privacy in India

India | August 27 2019

Law and the regulatory authority

Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

India does not have a dedicated law on data protection and privacy. India has also not adopted any international instruments on privacy or data protection. Specific provisions on privacy are found in the Information Technology Act 2000 (IT Act). The IT Act is based on the United Nations Model Law on Electronic Commerce adopted by the United Nations Commissions on Internal Trade law on 30 January 1997 vide resolution A/RES/51/162. A plethora of laws in areas such as banking, telecoms and the medical field prescribe obligations of confidentiality. Banking regulations deal with when financial institutions can transfer data overseas and the types of data that cannot be transferred overseas. Telecom regulations, by and large, prevent the transfer of customer information overseas. The code of conduct of medical practitioners prevents disclosure of patient information. The insurance regulations restrict transfer of claims-related data overseas.

The IT Act contains three provisions on data protection and privacy. Section 43A provides for compensation in the event one is negligent in using reasonable security practices and procedures (RSPP) in protecting sensitive personal data and information (SPDI) and this results in a wrongful gain or wrongful loss. It should be noted that this law provides only compensation, and only when a wrongful gain or loss results from the failure to observe RSPP. It can be argued that this is nothing but a codification of the law of negligence. This means that there is no negative consequence arising merely from the failure to observe RSPP. Further, RSPP is defined to mean such procedures stated by a law in force or as agreed to by the parties, and in the absence of both, the rules framed by the government. There is no statute that prescribes RSPP. This means that if parties - for example, an employer and an employee - agree on the RSPP to be adopted, the rules of the government would not apply.

In the guise of prescribing what constitutes RSPP, the government has issued somewhat basic and not very well-written privacy rules. As stated above, these rules apply only if the concerned parties have not agreed on the RSPP that would apply. These rules contain basic principles of privacy such as when SPDI can be collected, requirements of notice and consent, when SPDI can be transferred, among others.

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 he or she does so with the intention to cause, or knowing he or she is likely to cause, wrongful loss or wrongful gain.

Section 72 prescribes criminal punishment if a government official discloses records and information accessed by him or her in the course of his or her duties without the consent of the concerned person or unless permitted by other laws.

Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

There is no specific data protection authority in India. The IT Act provides for an adjudicating officer to be appointed to adjudicate whether a person has contravened the IT Act or its rules where the claim of injury or damages does not exceed 50 million rupees. If the claim exceeds 50 million rupees, the adjudicating authority would 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 powers of a civil court. These include summoning the attendance of persons and examining them on oath, requiring the discovery or production of documents and other electronic records, receiving evidence on affidavits and issuing commissions for the examination of witnesses or documents.

The police have the power to investigate offences under the IT Act such as under section 72 and section 72A.

Under specialised statutes relating to banking, telecom and in the medical field, the relevant sectoral regulator has powers.

Legal obligations of data protection authority

Are there legal obligations on the data protection authority to cooperate with data protection authorities, or is there a mechanism to resolve different approaches?

There is no data protection authority in India.

Breaches of data protection

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Under section 43A, if a breach results in a wrongful gain or wrongful loss, the adjudicating officer can order compensation to be paid. The law does not prescribe what the maximum compensation is. Under section 72, the punishment is imprisonment of up to two years or a fine of up to 100,000 rupees, or both. Under section 72A, the punishment is imprisonment of up to three years or a fine of up to 500,000 rupees, or both. Other laws provide for penalties under those statutes for breach of confidentiality provisions.

Scope

Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The provisions under the IT Act apply to all sectors, though laws specific to particular sectors would apply concurrently. Section 43A relates to a body corporate and the rules issued thereunder exclude government from the meaning of body corporate. Section 72A covers all types of organisations. Section 72 relates only to a government officer.

It should be noted, as described in question 1, that under section 43A, the parties concerned can agree among themselves on the RSPP to be adopted. If they do so, then the privacy rules passed by the Indian government would be excluded.

Since section 72 dealing with breach of confidentiality by a government officer is subject to other laws, if another law permits the disclosure of the information by a government officer, such disclosure would not be a violation of section 72.

Other sector-specific laws provide for exceptions relating to those sectors. For example, a doctor could disclose information in circumstances where there is a serious and identified risk to a specific person or community. Banking laws refer to the duty of confidentiality in the context of other laws, practices and usages customary among bankers.

Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

Yes, the Indian Telegraph Act 1885 and the Information Technology Act 2000 permit the government to engage in surveillance based on certain criteria that is in the interests of the sovereignty and integrity of India, security of the state, friendly relations with foreign states, public order or for prevention of incitement of the commission of an offence. These grounds are based on reasonable restrictions to free speech contained in the Constitution of India.

All surveillance has to be approved in writing by the Home Secretary of the central government or the relevant state government as the case may be. The Home Secretary is the most senior of bureaucrats tasked with maintaining law and order. Indian law does not require the permission of a court to engage in surveillance.

Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

Many laws provide a duty on service providers to maintain confidentiality of customer information. For example, medical laws deal with maintaining confidentiality of patient information. Such laws, for example, relate to medical termination of pregnancy and mental health. The code of ethics for medical professionals also prescribes that doctors must maintain confidentiality of patient information.

Banking laws also deal with protection of confidentiality of customer information. This is provided both in statutes relating to banks and payment systems as well as regulations passed by India's central bank, the Reserve Bank of India (RBI), on customer servicing, credit card operations of banks, among others.

A statute dealing with credit information companies requires credit information companies and credit institutions (banks, etc) to adopt principles relating to collection of information, processing of such information, protection of data and the manner of access and sharing of data. The principles are not prescribed by the law or by the regulator but have to be framed by the concerned credit information companies and institutions.

The RBI has prescribed detailed guidelines on information security, electronic banking, technology risk management and cyber frauds. In particular, the guidelines mention that banks must report breaches to the RBI and require use of encryption technology of at least 128-bit SSL and implementation of ISO/IEC 27001 and ISO/IEC 27002. Further, the banking regulations require banks to appoint a chief information security officer who will be responsible for articulating and enforcing the policies that banks use to protect their information assets apart from coordinating security-related issues.

RBI regulations on outsourcing also deal with the ability of banks to transfer data outside India. This is permitted, provided 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 there can be no comingling of data. Telecom laws, by and large, prohibit the 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. A recent notification issued by the RBI imposes restrictions on overseas transfers of payment system data by payment system operators.

PII formats

What forms of PII are covered by the law?

While section 72A covers personal information, section 43A covers SPDI. Personal information means information that relates to a natural person, which either directly or indirectly in combination with other information available or likely to be available with a body corporate is capable of identifying such person. SPDI covers the following:

- passwords;
- financial information such as bank account or credit card or debit card or other payment instrument details;
- physical, physiological and mental health conditions;
- sexual orientation; medical records and history; and

- biometric information.

The law does not distinguish personal information on the basis of the format of the information, such as electronic as opposed to physical records. However, the laws on SPDI are applicable only to SPDI in electronic form.

Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The law does not specify whether it applies only to PII owners or processors of PII established or operating in the jurisdiction. After the privacy rules were notified, there was some concern that they would apply to the SPDI of foreign nationals that was being processed in India by the many business process outsourcing businesses in India. The government then issued a press note to clarify that it relates only to a body corporate or person located within India. Further, data processing as a result of a contract between two entities is not covered by the privacy rules. While the clarification is not entirely clear, the accepted view is that this does not apply to foreign personal information being processed in India.

The law does allow transfer of SPDI out of India only if the recipient ensures the same level of data protection.

Covered uses of PII

Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners? Do owners', controllers' and processors' duties differ?

The law is not entirely clear on this point, though there is a clarification that appears to suggest that the privacy rules relate to a party that collects the data directly from the providers of the information and does not relate directly to a situation where the processor of the information receives the information from another body corporate. At the same time, the law allows transfer of SPDI only if the recipient ensures the same level of data protection. The two provisions are somewhat contradictory as one exempts onward transfers and the other appears to apply the rules to onward transfers.

Legitimate processing of PII

Legitimate processing – grounds

Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Yes, SPDI cannot be collected unless the information is collected for a lawful purpose connected with a function or activity of the party collecting or using the information and the collection of the SPDI is considered necessary for that purpose. Apart from this, there are also notice and consent requirements.

Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

Section 43A and the privacy rules relate to SPDI, which has a narrower meaning than personal information. Personal information is referred to in section 72A. See question 1 for definitions of both SPDI and personal information.

Data handling responsibilities of owners of PII

Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

While collecting SPDI, the provider must be made aware through reasonable steps of the following:

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

Consent must be obtained from the provider of the SPDI regarding purpose of usage before collection of the information. Further, of the three grounds on the basis of which disclosure of SPDI is permitted to a third party, one relates to the provider of the information agreeing to the same and another relates to it being permitted under a contract with the provider.

Exemption from notification

When is notice not required?

There is no exemption to providing notice. It may be noted, however, that the privacy rules may not apply where the parties have agreed on their own terms of RSPP. The privacy rules also do not appear to apply to transfer of SPDI from one entity to another as opposed to from an individual provider of his or her own information to a data processor. It should also be noted that the privacy rules do not apply to the government.

Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

No, the privacy rules do not offer individuals any degree of choice or control over the use of their information, although consent is required as to the purpose of the use so the individual may simply refuse to permit the use of his or her SPDI or withdraw his or her consent later. The collecting party then has the option not to provide the goods or services for which the information was sought.

Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

The privacy rules deal with this only indirectly. In regard to currency, the SPDI cannot be retained for longer than is required for the purpose for which the information can lawfully be used or is otherwise required under any other law for the time it is in force. As regards accuracy, the provider of the information has the right to review the information it provided and correct any inaccuracy. However, this appears to relate only to information provided by the individual and not information collected separately.

Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

Yes, the privacy rules specify that the SPDI cannot be retained for longer than is required for the purpose for which the information can lawfully be used or is otherwise required under any other law currently in force.

Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

Yes. SPDI cannot be collected unless:

- the information is collected for a lawful purpose connected with a function or activity of the party collecting or using the information;
- the collection of the SPDI is considered necessary for that purpose; and
- the information collected is used for the purpose for which it has been collected.

There is no requirement however that the purpose of use must be specific in its description.

Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

The privacy rules do not provide for any exceptions or exclusions. The purpose of collection or usage must be mentioned in the privacy policy. Further, consent is required as to the purpose of usage. Strictly speaking, if the new purpose is not covered by the purpose for which consent was given, the SPDI cannot be used for the new purpose. Since consent is required as to the purpose of use, change in the purpose, whether through the privacy policy or otherwise, would require the consent of the provider of the information. It must be noted that the privacy rules do not require that the purpose must be described in specific terms. It would appear, therefore, that if consent is obtained for a broad purpose, this would be sufficient.

Security

Security obligations

What security obligations are imposed on PII owners and service providers that process PII on their behalf?

Section 43A refers to RSPP, which is 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, that is, the privacy rules. Accordingly, the parties can agree on the security standards to be adopted. The privacy rules do not stipulate a particular security standard (though that was what the rules were meant to do). The privacy rules merely suggest that IS/ISO/IEC 27001 or a code prescribed by an industry association and approved by the government could be used. So far, no code has been approved by the government.

The banking regulations 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, etc.

Notification of data breach

Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

There are two situations in which data breach notifications apply. First, banks are required to notify the central bank, that is, the Reserve Bank of India, in case of any cybersecurity incident within two to six hours.

Second, the intermediaries, as part of their due diligence requirement in order to make use of safe harbour from content liability, are required to report cybersecurity incidents to the Computer Emergency Response Team (CERT) as soon as possible. This is not a mandatory requirement and is required only if the intermediaries intend to use the safe harbour protection from content liability.

The definition of 'intermediary' is wide and includes telecommunications companies, ISPs, network service providers, web hosts, search engines, online payment/auction sites, online marketplaces, etc.

The data breach notifications are somewhat unclear as to whether breach notifications are mandatory or not, since the actual language states that parties 'may' notify the CERT. More recently, the CERT has been taking the view that breach notifications are mandatory for all parties and not just for intermediaries.

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 without authorisation. There is a further definition through a description of various incidents that constitute cybersecurity incidents. These are:

- targeted scanning or probing of critical networks and systems;
- compromise of critical systems or information;
- unauthorised access of IT systems or data;
- defacement of a website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites, etc;
- malicious code attacks such as spreading of viruses, worms, Trojans, botnets or spyware;
- attacks on servers such as database, mail and DNS, and network devices such as 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, e-commerce, etc.

The Ministry of Communication and Information Technology has set up CERT under the IT Act. CERT is 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 web pages and websites.

Internal controls

Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

The privacy rules provide for the need to appoint a grievance officer to address discrepancies and grievances of providers of information. There is no requirement for the appointment of a data protection officer.

Record keeping

Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

No requirements have been prescribed for maintaining internal records or establishing internal processes or documentation except the suggestion in the privacy rules that IS/ISO/IEC 27001 is one such security standard that could be adopted.

New processing regulations

Are there any obligations in relation to new processing operations?

There are no obligations in relation to new processing operations under the present law. A new privacy statue is under way and it may include obligations relating to new processing operations.

Registration and notification

Registration

Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

No, owners and processors of PII are not required to register with the supervisory authority.

Formalities

What are the formalities for registration?

Not applicable.

Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Not applicable.

Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

Not applicable.

Public access

Is the register publicly available? How can it be accessed?

Not applicable.

Effect of registration

Does an entry on the register have any specific legal effect?

Not applicable.

Other transparency duties

Are there any other public transparency duties?

There are no such duties imposed under the present law.

Transfer and disclosure of PII

Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

The law regulates the disclosure or transfer of the SPDI to a third party. This is possible if it has been agreed in a contract with the provider, it is necessary for compliance of a legal obligation or prior permission is given by the provider.

Further, the privacy rules prescribe that SPDI can be transferred only to a third party that observes the same level of data protection as provided by the privacy rules. Further, the privacy rules prescribe that transfer is permitted only if necessary for the performance of the contract with the provider or where the provider has consented to the transfer. At the same time, a clarification appears to suggest that some of the privacy rules apply only between the individual provider of the information and the owner of PII and not between two entities. The two provisions do not entirely read harmoniously together.

Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

There are no restrictions other than those stated above.

Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

SPDI or any information can be transferred to a person outside India if he or she ensures the same level of data protection as provided by the rules. Further, such transfer is permitted only if necessary for the performance of the contract with the provider or where the provider has consented to the transfer.

Further, Indian company law requires companies that maintain their books of accounts and books and papers in electronic form outside India to keep a backup of such books of accounts and books and papers in servers physically located in India.

Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

No, transfer of PII does not require notification to or authorisation from a supervisory authority.

Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The law is not entirely clear on this matter. Transfer of SPDI to a third party can be done only if it agrees to ensure the same level of protection under the privacy rules. We believe that it follows, therefore, that if transfer of PII from the owner to a service provider is subject to restrictions, the restrictions should apply to a further transfer from the service provider to another service provider. It may also be noted that notice has to be given to the provider of the information of the name and address of every agency that will have access to such information. This would, therefore, cover onward transfers.

Rights of individuals

Access

Do individuals have the right to access their personal information held by PII owners? Describe how this right can be exercised as well as any limitations to this right.

Yes, they have a right to access their personal information and also correct the same, but this appears to relate only to personal information provided by them and not personal information obtained separately.

Other rights

Do individuals have other substantive rights?

By and large the rights of individuals are covered in the answers to the questions in this chapter.

Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Yes, the law provides for compensation to be paid if the owner is negligent in using RSPP to protect the SPDI and it results in a wrongful loss or wrongful gain. The terms ‘wrongful gain’ and ‘wrongful loss’ are not defined in the IT Act but are defined under the Indian Penal Code. ‘Wrongful gain’ is defined to mean gain by an 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 entirely be accepted under section 43A, since the purpose of the provisions are different, we believe they do have some persuasive value. In our view, given the manner in which section 43A is constructed and the meaning of ‘wrongful gain’ and ‘wrongful loss’ under Indian laws, it is more likely that actual damage would be required.

Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Compensation can be awarded by the adjudicating officer if the claim for damages does not exceed 50 million rupees. If the claim exceeds 50 million rupees, the rights would be exercisable through the judicial system.

Exemptions, derogations and restrictions

Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

As stated in question 20, the privacy rules come out of the power of the government to prescribe what RSPP is. RSPP is as per a law in force or as agreed between the parties and only in the absence of both would the rules of the government (that is, the privacy rules) apply. Accordingly, if the parties (eg, employer and employee or service provider and customer) agree on the RSPP, then the privacy rules would not apply. Further, through the definition of body corporate, the privacy rules do not apply to the government.

Supervision

Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

Yes, decisions of the adjudicating officer can be appealed to the Cyber Appellate Tribunal. Decisions of the Cyber Appellate Tribunal can be appealed to the High Court.

Specific data processing

Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

Indian law does not deal directly with the use of cookies or equivalent technology. Indian law does provide for both compensation and criminal punishment where, without the permission of the owner or the person in charge of the computer, computer system or computer network, a person downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network. Read literally, it would appear that consent is required for the use of cookies. However, it is possible to get around this by including such usage in the terms of use. Under Indian contract law, as long as there is reasonable sufficiency of notice that certain terms apply to the use of a website and the terms are not unfair or unconscionable, these terms are likely to be enforceable against the customer or user.

Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

Indian law does not deal with marketing through email or fax. In 2015, a badly worded provision that appeared to deal with spam was struck down by the Supreme Court of India as being unconstitutional.

The IT Act does not cover electronic marketing. This is covered by 'do not call' rules framed by the Telecom Regulatory Authority of India (TRAI).

A person can list his or her number on the 'do not call' registry, after which marketing calls and SMS cannot be sent to him or her. One can, however, select certain exception categories, in which case unsolicited communications in those categories can be sent to the customer. Messages can continue to be sent if they are transactional in nature. A list of types of transactional messages has been published. A significant feature of the new regulations is the back-end technical implementation of the same.

A telemarketer has to take special telecoms resources for making telemarketing calls and SMS. The telecoms companies will ensure that their systems are connected to the registry so a call or message will not go through to someone who is listed on the registry. Separate resources have to be taken for transactional messages so they can be sent to persons listed on the 'do not call' registry.

Penalties have been prescribed for violation of the regulations. A person is entitled to three counts - on the third count, the person will be blacklisted and cannot receive any telecom resources for a period of two years.

Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

India does not have any rules or regulations governing the use of cloud computing services. The TRAI has recently released a consultation paper on cloud computing. The consultation paper points out several issues relating to cloud services, such as interoperability, data security, data localisation, data ownership, cross-border movement of data and taxation of cloud services. The consultation paper is open for public comments, and based on the public comments and discussion with the stakeholders TRAI may soon come out with regulations governing the use of cloud computing services.

Update and trends

Key developments of the past year

Are there any emerging trends or hot topics in international data protection in your jurisdiction?

Key developments of the past year46 Are there any emerging trends or hot topics in international data protection in your jurisdiction?

There are major changes planned in the data protection space. The Supreme Court of India in August 2017 delivered a landmark judgment declaring the right to privacy as a fundamental right. The Ministry of Electronics and Information Technology, set up on 27 July 2018, released the much-awaited draft Personal Data Protection Bill 2018 (the Bill). The Bill has 112 sections and runs to 64 pages. It is India's first attempt towards a specific data protection and privacy statue in India. A large portion of the Bill seems to have been adopted from the recent global data protection regulations of the EU and it includes concepts such as the right to be forgotten, privacy-by-design, consent-based approach, data localisation requirements, data protection officers and data protection authority among others. The Bill is still a draft and has not been finalised. Once finalised, it will be presented to Parliament.

Kochhar & Co - Naqeeb Ahmed Kazia and Stephen Mathias