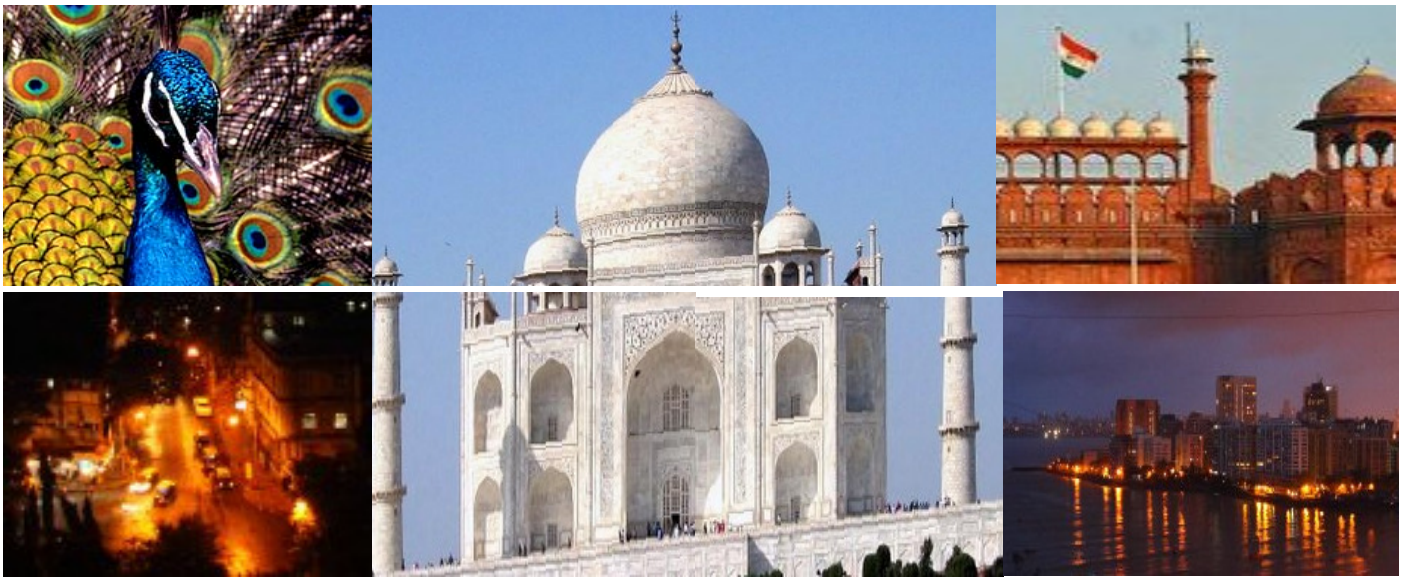
India Law News
A quarterly newsletter of the India Committee

ABA Section of International Law
Your Gateway to International Practice

VOLUME 9, ISSUE 2, DATA PRIVACY ISSUE 2017



DATA PRIVACY: HAVE BANKING LAWS IN INDIA KEPT PACE WITH TECHNOLOGY?

By Manisha Shroff, Nikita Nehriya, Ankit Chavan and Praneetha Vasan

With rapid advancement in science and technology, the role of technology in the banking sector has increased drastically. Technology has become an integral part of every aspect of the banking sector, from the banks' internal processes, to inter-bank money transfers and settlements, to banks' relationships and interactions with their customers. Internet and mobile banking are being used more and more, and their use is likely to significantly replace traditional brick and mortar banking. However, with such increased pervasiveness of technology comes the threat and risk of the misuse or failure of such technology, leading to the leakage of sensitive data and breach of customer confidentiality.

In light of this, it is important to examine the legislative framework governing data privacy in the banking sector in India today, and whether the extant laws provide adequate protection to customers' data privacy in the face of technological advancements.

Right to Privacy in India

Over the last few decades in India, the "right to privacy" has emerged as a well-established right, recognized as a part of the fundamental right to "protection of life and personal liberty" under Article 21 of the Constitution of India. A plethora of judicial decisions, such as *Kharak Singh v State of Uttar Pradesh* (AIR 1963 SC 1295), *People's Union for Civil Liberties v Union of India* ((1997) 1 SCC 301), and *Gobind v State of Madhya Pradesh* ((1975) 2 SCC 148), rendered by the Supreme Court in the country have contributed to the recognition accorded to the right to privacy.

However, the general right to privacy is not an absolute right; it is subject to the procedure established by law and the compelling interest of the State.

continued on page 10

EDITOR-IN-CHIEF'S COLUMN

Ashish Joshi

Dear India Committee,

On behalf of the Editorial Board, I am pleased to present the Summer Issue of India Law News. On a personal note, this is my first issue as the Editor-in-Chief. It's an honor to serve as the Editor of India Law News. I have some big shoes to fill: Bhali Rikhye, our esteemed Co-Chair and the outgoing Editor-in-Chief has set the bar high and done a marvelous job and steered the publication to great heights. I shall strive to meet the high standards set by Bhali and the editorial team. And with stellar team of editors consisting of Daniel Hantman, Poorvi Chothani, Aseem Chawla, Farrell Brody and Sylvana Sinha, editing and publishing India Law News is an act of collaboration and a labor of love. Thank you all for the wonderful job that you do.

This issue has a special focus on Data Privacy and features the following articles:

- Data Privacy: Have Banking Laws in India kept pace with Technology?
- Need for Robust Data Protection Controls for the Indian Insurance Sector
- Data Privacy: A Relic of the Past in the Times of Information Exchange?
- Debit and Credit Card Data Theft in India: Manifestation of Data Privacy and Data Protection
- Bring Your Own Device Policies: Legal Considerations

I would like to express my appreciation and gratitude to Arshad (Paku) Khan and Supratim Chakraborty, who served as our Guest Editors, for their analytical insight on the topic, invaluable guidance and leadership. Thank you also to all the authors who contributed to this issue; it's you who allow us to put out one informative issue after another on cutting-edge topics related to India. Last but not least, our continued thanks to Law Quest for providing desktop publishing support.

The Fall Issue of India Law News will have a special focus on Media and Intellectual Property Rights. Many thanks to Dr. Manoj Kumar who is serving as our guest editor for the Fall issue.

I hope you enjoy the issue. Our Editorial Board is always interested in hearing from you! Please feel free to contact me with your suggestions or ideas for future issues or articles at any time.

Sincerely,

Ashish Joshi
Editor-in-Chief
India Law News

CONTENTS

OVERVIEW

2 *Editors-in-Chief's Column*
3 *Guest Editor's Column*
6 *Co-Chair's Column*

★

COMMITTEE NEWS

28 *Submission Requests*
29 *Join the India Committee*

★

SPECIAL FOCUS

1 *Data Privacy: Have Banking Laws in India Kept Pace with Technology?*
14 *Need for Robust Data Protection Controls for the Indian Insurance Sector*
18 *Data Privacy: A Relic of the Past in the Times of Information Exchange?*
21 *Debit and Credit Card Data Theft in India: Manifestation of Data Privacy and Data Protection*
25 *Bring Your Own Device Policies: Legal Considerations*

★

GUEST EDITOR'S COLUMN

By Arshad (Paku) Khan and Supratim Chakraborty

It is a privilege for us to write the Guest Editorial for this issue of India Law News (ILN) on "*Data Privacy*". The international perspective around "right to privacy" is being widely discussed, debated and deliberated upon in recent times. The realization that personal information is a projection of individual personality has made the "right to privacy" a coveted human right— throughout the world and in India. We hope that the readers will benefit and gain perspective from the articles published in this issue.

Technological advancements have dramatically increased the volume of data that is collected, stored, processed, analyzed and transferred. Almost all businesses now obtain personal data to provide better and more customized services to their clients. Further, globalization, coupled with the proliferation of internet and mobile devices, has magnified the unrestricted transfer of data beyond national borders. With data, especially personal data, being shared in a large quantum, individuals are often being exposed to potential damage to their personal and financial interests by unauthorized use of such data.

The Indian judiciary has often read "privacy" as a fundamental right under Article 21 of the Constitution of India which guarantees "right to life and personal liberty". Further, the Information Technology Act, 2000 (Act) is one of the primary Indian laws dealing with data privacy and protection. However, the Act, as it was originally framed, did not specifically address data privacy and protection. Thus, it was amended in the year 2009 through the Information Technology (Amendment) Act, 2008, and concepts relating to "data privacy" and "data protection" were injected into the Act through provisions such as Section 43-A and Section 72-A. Whereas, Section 43-A of the Act mandates implementation and maintenance of reasonable security practices and procedures in relation to sensitive personal data or information (SPDI) and prescribes punishment for any breach of obligations stipulated thereunder, Section 72-A deals with the concept of "personal information" and sets out punishment for disclosure of such information in breach of a lawful contract or without the consent of the information provider.

To further bolster the efficacy of the existing legal regime, in the year 2011, the Government of India, formulated the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Rules). These Rules regulate the collection, disclosure, transfer and storage of SPDI. Further, to resolve interpretational ambiguities around these Rules, on August 24, 2011, the Ministry of Communication and Information Technology released a press note (Press Note) that elaborated upon various provisions of the Rules. Amongst other things, the Press Note clarified that the Rules relate to SPDI, and are applicable to a body corporate or any person located in India. The Press Note also put entities carrying out outsourcing related activities in India outside the purview of collection and disclosure requirements, as set out under the Rules.

In recent times, India has been experiencing a plethora of litigation, which are raising significant questions on data privacy and data protection that were not previously addressed. The Indian judiciary has been gradually accepting its importance and

imposing liability for breaches. For example, in the case of *Amit Patwardhan v Bank of Baroda*, the adjudicating officer observed that banks have a greater responsibility to safeguard customers' privacy, and reprimanded the bank for its actions in relation to the breach of customers' sensitive data. Further, the Supreme Court of India has recently issued notices to social media giants WhatsApp, Facebook and the Telecom Regulatory Authority of India to explain their legal position over privacy concerns raised in a petition on WhatsApp's data sharing policy (WhatsApp Case). Recently, the Karnataka High Court has also recognized an individual's 'right to be forgotten' on the internet.

For this edition, we have selected a few key sectors like banking and insurance to analyze the laws relating to data privacy existing in these sectors. Apart from sector specific analysis of data privacy and data protection laws, we have attempted to address topical issues such as "debit/credit card data thefts", the concerns surrounding "bring your own device" policy adopted by employers and have deliberated upon why in an increasingly "transparent" world, geared towards an automatic exchange of information on financial accounts owned by individuals, the relevance and importance of "data privacy" requires due consideration. The gamut of authors who have contributed to this special edition have been carefully selected based on their in-depth knowledge about the subject matter of their respective contributions.

Our first article is a well-researched piece by Manisha Shroff, Nikita Nehriya, Ankit Chavan and Praneetha Vasan. Their article explores whether the current banking laws in India have kept pace with technological advancements. The authors have analyzed the laws that endeavor to enhance data privacy and protection for banking customers in India.

Further, in an article co-authored by Anuj Sah and Rohan Singh, the contours of data protection in the Indian insurance sector has been mapped. The article seeks to address key aspects in relation to data protection laws in the insurance sector.

This is followed by Aditi Sharma's interesting piece, titled "*Data Privacy: A Relic of the Past in the Times of Information Exchange*?" that discusses the issues of data privacy of financial information and explores how the concern was addressed by enacting specific inter-governmental agreements for FATCA reporting. India's current information exchange regime is examined in detail in this article and provides context that is essential to ascertain whether privacy of financial data is validly considered in present times.

Nandini Khaitan and Aritri Roy Chowdhury have co-authored an article on "*Debit and Credit Card Data Theft: Manifestation of Data Privacy and Data Protection*". This article critically analyses Indian data privacy and data protection laws that seek to protect debit and credit card information and touches upon the various methods by which card users can safeguard themselves against data thefts.

"Bring your own device", popularly known as "BYOD", is the practice of allowing employees to bring their own personal electronic devices to workplace. However, use of personal devices in the workplace involves certain critical legal and data protection risks, where a conflict between the rights of the employer and that of the employee arises. In our final article, co-authored by Pallavi Thacholi and Deepthi Bavirisetty, these legal aspects involved in the practice of BYOD are discussed. Further, the authors have

attempted to suggest certain universal best practices that may be adopted to balance the conflicting interests of employers vis-a-vis their employees.

In the grandest sense, privacy is the foundation on which the edifice of human dignity is erected. Globally, the need to protect individual privacy is being acknowledged with immense vigor. The Indian jurisprudence on data privacy is evolving along with the changing paradigm and challenges relating to privacy. It may be relevant here to note that the Attorney General of India has recently assured the Supreme Court of India in the WhatsApp Case that, by October 2017, the Indian legislators would enact a new law to protect the crucial personal information of individuals that is shared while opening bank accounts, joining social media platforms and using various web applications. The law, if enacted as promised, will certainly strengthen the existing legal structure of data privacy of the country.

At this crucial juncture, we seek to share some interesting insights about the various facets of the existing data privacy and data protection regime through this edition. India itself is at the global crossroads in entrenching its role as one of the world's most important economies. At the same time, the entirety of the nearly 1.3 billion residents of India now have available electronic communication devices, like smartphones, that make the issue of data privacy/protection an immediate and enormous concern. India's role as a data processing center for the world makes both Indian and international privacy concerns all the more relevant. Given this context, we suspect that in the coming years, India will be one of the most important jurisdictions globally for data privacy issues.

We hope that you will find the articles useful and enjoy reading them!

Arshad (Paku) Khan and Supratim Chakraborty
Guest Editors

Arshad (Paku) Khan is Executive Director in Khaitan & Co's US Desk and Competition/Antitrust practice groups. He is based in the San Francisco Bay Area, US and New Delhi. Paku is one of the most experienced competition law experts in India. He has over 25 years of competition, merger control, corporate and related litigation experience. He has practiced competition law in both the US and the EU, having also served as a competition regulator in both these jurisdictions.

Supratim Chakraborty is an Associate Partner of Khaitan & Co, LLP, Kolkata. He focuses his expertise on corporate and commercial transactions such as mergers, acquisitions, joint ventures and general corporate law advisory. Supratim has advised eminent clients in relation to information technology laws including data protection and data privacy issues. He has advised several clients on various aspects of anti-bribery / anti-corruption law as well. Supratim is a regular contributor to eminent publications and has spoken at prestigious forums such as the Centre for Corporate Governance Research and Training (Institute of Company Secretaries of India). He has recently delivered a lecture on data privacy and data protection at the Government Law College International Law Summit (which was supported by the World Trade Organization, Geneva).

CO-CHAIR'S COLUMN

The India Committee is pleased to present India Law News' latest edition focused on Data Privacy, with Arshad (Paku) Khan and Supratim Chakraborty as Co-Guest Editors. This issue marks a change in editorial leadership of the India Law News. Bhali Rikhye, who had been editor-in-chief for several years has stepped down to focus on his duties as a Co-Chair of the India Committee. We are extremely pleased to announce that the leadership of the India Law News has now passed into the highly capable hands of Ashish Joshi. The Co-Chairs congratulate him on the publication of this issue and wish him every success during his tenure as Editor-in-Chief of India Law News.

As the Co-Guest Editors discuss in greater detail in their column in the following pages, this issue of India Law News has articles by various notable authors on various important areas in the field of data privacy. These include:

- Legal considerations involving workplace rules with regard to bringing personal smart phones and other devices into the workplace;
- Whether data privacy laws in India have kept pace with technology;
- The need for robust data protection controls in the Indian insurance sector;
- Data privacy and data protection laws regarding debit and credit card data theft in India;
- Whether data privacy is a relic of the past in the times of information exchange, with specific reference to the U.S.'s Foreign Account Tax Compliance Act of 2010 (FATCA).

The issue also includes a Case Notes column discussing recent noteworthy decisions in the Indian courts.

The year 2017 has been a busy one for the India Committee in other areas as well. As part of the American Bar Association (ABA) Section of International Law's Spring Meeting in Washington, DC (April 25 – 29, 2017), the Committee hosted a visiting delegation of lawyers led by President of the Bar Association of India and the Society of Indian Law Firms, Dr. Lalit Bhasin. In addition to attending events organized by the Section of International Law (such as the Spirit Cruise of Washington on the Potomac River), the Committee arranged several special activities for the delegation during the course of the Spring Meeting:

- Private meeting with senior ABA leadership, including ABA President Linda A. Klein and President-elect Hillarie Bass, ABA Section of International Law Chair Sara Sandford and Chair-elect Steven Richman, and Section Director Leanne Pfautz, (President Klein was unable at the last minute to attend, because she was called away to a meeting with members of Congress on Capitol Hill);

- Luncheon at McCormick & Schmick restaurant, hosted by the Committee and generously supported by law firm DLA Piper (whose partners include Committee past co-chair Erik Wulff);

India Law News

EDITORIAL BOARD (2017-2018)

Editor-in-Chief
Ashish Josh
Lorandos Joshi, Ann Arbor, MI

Co-Editors
Poorvi Chothani
LawQuest, Mumbai, India

Daniel Hantman
Much Shelist, Chicago, IL

Aseem Chawla
Amarchand Mangaldas, New Delhi

Farrell Brody
Chaffetz Lindsey, Brooklyn, NY

Sylvana Q. Sinha
Praava Health, New York, NY

Desktop Publishing
LawQuest, Mumbai, India

India Law News is published quarterly by the India Committee of the American Bar Association's Section of International Law, 740 15th Street, N.W., Washington, DC 20005.

India Law News endeavors to provide information concerning current, important developments pertaining to law in India, Committee news, and other information of professional interest to its readers. Articles reflect the views of the individuals who prepared them and do not necessarily represent the position of the American Bar Association, the Section of International Law, the India Committee, or the editors of *India Law News*. Unless stated otherwise, views and opinions are those of the authors and not of the organizations with which they are affiliated. This newsletter is intended to provide only general information and should not be relied upon in the absence of advice from competent local counsel.

SUBMISSION DEADLINES

Fall Issue	**August 1st**
Winter Issue	**November 1st**
Spring Issue	**February 1st**
Summer Issue	**May 1st**

Potential authors should review the Author Guidelines and send manuscripts via email to the Editorial Board.

- Private meeting with U.S. Congressman Raja Krishnamoorthi (representing Illinois' 8th District) at the U.S. House of Representatives, Capitol Building;

- Dinner at the Bombay Club Restaurant for members of the delegation and the Committee; and

- Committee meeting breakfast, where the delegation was recognized by ABA Section of International Law Chair Sara Sandford.

In addition, Committee past Co-Chair, Priti Suri, was honored at a luncheon at the ABA Section on International Law Spring Meeting where Ms. Suri was awarded the Mayre Rasmussen Award for the Advancement of Women in International Law for her role as a mentor and in opening doors for women and women lawyers in India. The delegation attended many events, including a luncheon.

After conclusion of the ABA Section of International Law's Spring Meeting, the delegation participated in an all-day program organized by the Committee and held at the offices of DLA Piper. The theme of the conference was: *Emerging Legal Challenges in the United States and India*.

Opening remarks were made by Dr. Bhasin. The keynote speakers were Mrs. Reenat Sandhu, Deputy Chief of Mission, Embassy of India, Washington, D.C., and Adam Clayton Powell, III, the American journalist, media executive, and scholar who currently serves as Director of Washington Policy Initiatives for the University of Southern California and is a University Fellow at the USC Center on Public Diplomacy. ABA Section of International Law Chair Sara Sandford, Chair elect Steven Richman, and Ronak D. Desai, counsel, United States Congress-Congressional Committee, also addressed the conference.

There were four panel discussions. Speakers on the panels included members of the visiting delegation and partners at U.S. law firms. The topics were:

- Sustainability and Shareholder Activism, focusing on hedge fund attacks on companies' sustainability initiatives by influencing their overseas supply chains including those in India;
- Cybersecurity Due Diligence in M&A transactions, focusing cyber risks and resulting uncertainties in asset valuation;
- Intellectual Property Rights under U.S. Government Contracts focusing on contracting strategies that Indian lawyers may want to discuss with their clients to ensure they do not unwittingly give up intellectual property rights to the U.S. Government or to a higher-tier subcontractor or a prime contractor; and
- A panel of members of the delegation who spoke on a variety of contemporary legal developments in India.

The delegation's visit to Washington was followed by a visit to the offices in New York of Nixon Peabody, LLC and Lazare Potter & Giacovas, LLP.

The India Committee is making plans to contribute to the content of the forthcoming ABA Section of International Law's Spring Meeting in 2018 in New York. We would like to remind those of our members who plan to attend to

contact any of the co-chairs to attend what we anticipate will be Committee sponsored panels and a Committee dinner during the course of the Spring Meeting.

In February 2017, the India Committee held a well-attended teleconference on Criminal Actions in Commercial Matters in India moderated our Vice Chair, Jaipat Jain. Many thanks to Jaipat for organizing this successful program. At present, the events subcommittee, chaired by Jaipat Jain, is preparing another teleconference on Mergers and Acquisitions in India. The program will be followed by an India Law News issue focused on Mergers and Acquisitions.

Each of these activities have been developed in support of the India Committee's main mission to serve as a forum for ABA Section of International Law members who have an interest in India legal, regulatory and policy matters, both in the private and public international law spheres. With conference panels and teleconferences/webinars, the Committee facilitates information sharing, analysis, and review on these matters, with a focus on the evolving India-U.S. relationship. Key objectives include facilitation of trade and investment in the private domain, while concurrently supporting democratic institutions in the public domain. The Committee believes in the development of relationships and understanding among the legal fraternity, bar associations, law students, business organizations in India and the U.S., as well as other countries, in an effort to support the global Rule of Law.

We encourage those of our readers who are not members to join the Committee, and those who are members but not actively involved, to contact one of the co-chairs to discuss ways in which you can get involved. We welcome your participation in the work of the Committee.

With best wishes to all our readers for a pleasant and enjoyable summer.

Shikhil Suri
Roland Trope
Bhali Rikhye

The Delegation Group with the Deputy Chief of the Embassy

Roland Trope, V. Lakshmikumaran, and Dr. Lalit Bhasin (Left to Right)

Roland Trope and V. Lakshmikumaran (Left to Right)

DATA PRIVACY: HAVE BANKING LAWS IN INDIA KEPT PACE WITH TECHNOLOGY?

By Manisha Shroff, Nikita Nehriya, Ankit Chavan and Praneetha Vasan

continued from page 1

Specific Laws Governing the Banking Sector

The maintenance of customer confidentiality and data privacy is a recognized obligation of all banks in India, present in both customary (non-statutory) banking law as well as the various statutes governing banks and the banking sector in India. Disclosure of customer information by banks in India is regulated in order to preserve and protect the customer's right to privacy.

Disclosure of credit information received by the Reserve Bank of India (RBI) is prohibited under Section 45E of the Reserve Bank of India Act, 1934. The obligation of fidelity and secrecy to customers is enshrined in Section 44 of the State Bank of India Act, 1955, Section 13 of the State Bank of India (Acquisition and Transfer of Undertakings) Act, 1980, Section 29 of the Credit Information Companies (Regulation) Act, 2005 (CIC Act), and Section 3 of the Public Financial Institutions Act, 1983. Similarly, the Payment and Settlement Systems Act, 2007 (PSS Act) imposes privacy obligations on payment system providers which manage online payment and settlement systems such as NEFT, RTGS, etc. Section 22 of the PSS Act prohibits system providers from disclosing the existence or contents of any document or part of any information given to them by a system participant (i.e., a customer).

Further, banks in India are regulated by the RBI and the various notifications, circulars, directions and guidelines issued by it from time to time, which obligate banks to maintain customer confidentiality and protect the privacy of customers' data. The RBI not only mandates customer data privacy for banks but also for financial institutions, such as NBFCs, CICs, and other entities regulated by it. The RBI's "Master Circular on Credit Card, Debit Card and Rupee Denominated Cobranded Prepaid Card Operations of Banks" issuing NBFCs' forbids banks and non-banking financial companies (NBFCs) from making unsolicited calls, delivering unsolicited credit cards and from disclosing customer information to any third party without the customer's specific consent. Similarly, the RBI's "Master Circular on Customer Service in Banks" contains a detailed section on the banks' "Customer Confidentiality Obligations", which envisages the banks' obligation of secrecy under customary banking law, and extends it by forbidding the disclosure of customer information for "cross-selling" or any other purpose.

Moreover, the RBI's recent "Master Circular on Mobile Banking Transactions in India" states that "*technology used for mobile banking must be secure and should ensure confidentiality*". It also requires banks to institute adequate risk control measures to manage the risk of breach of customer confidentiality and secrecy. Finally, the RBI's "Guidelines on Cyber Security Framework in Banks" requires banks to take appropriate steps in preserving the confidentiality of customer information, and to ensure that such confidentiality is not compromised in any situation.

Although the RBI master circulars and guidelines, along with the various statutes governing the banking sector, do provide some amount of security and provide for the maintenance of customer confidentiality and

privacy, there is a clear lack of enforcement. Enforcement of data privacy differs from case to case, and is dependent upon the particular banking sector institution and the contract in question. Unfortunately, such enforcement is not guaranteed through parliamentary sanctions.

The CIC Act governs companies engaged in collection of credit information. Section 19 of the CIC Act mandates every credit information company to take steps to ensure that the credit information maintained by it is accurate and complete, and duly protected against any loss or unauthorized access or use or unauthorized disclosure. Section 22 of the CIC Act prohibits unauthorized access to credit information, and prescribes a monetary fine for any unauthorized access in breach of the provisions of the CIC Act.

Although the CIC Act contains specific provisions for data protection, it is limited in its scope of application. It only imposes duties on credit information companies, credit institutions and specified users while processing credit information. Further, no specific authority has been established to ensure enforcement of the provisions under the CIC Act.

Protections under the Information Technology Act, 2000

To enhance the protection of sensitive information, the Prevention of Unsolicited Telephonic Calls and Protection of Privacy Bill, 2006 was introduced in the Rajya Sabha on 12 May 2006. However, more than 10 years later, there has been no evidence of such an enactment coming into force. In 2008, Section 43A and 72A of the Information Technology Act, 2000 (IT Act) were introduced by way of an amendment, to further the cause of data privacy and protection. Section 43A provided for compensation to be provided to any person by a body corporate that possesses, handles or deals with any sensitive personal data or information and causes a wrongful loss or gain to any person by negligently implementing or maintaining such data or information. Section 72A provides for punishment in case of any disclosure of sensitive personal information. Subsequently, in 2011, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules or the Rules) were introduced to create a more robust system for protection of sensitive personal data or information (SPDI). Among various kinds of information which constitute SPDI (and are hence protected under the SPDI Rules), is financial information such as bank account details, credit card or debit card or other payment instrument details. The judicial recognition of the need for data privacy in the banking sector can be seen in the case of *Punjab National Bank v Rupa Mahajan Pahwa* (IV (2015) CPJ 620 (NC)), in which Punjab National Bank had issued a duplicate passbook of a joint savings bank account, held between the petitioner and her husband, to an unauthorized person. The Delhi State Consumer Disputes Redressal Commission, while awarding compensation to the petitioner, held that there was a deficiency on the part of the bank in issuing the passbook and passing on some other information which was not to be disclosed to another person. Since banks are in possession of SPDI, they are intended to fall within the ambit of these rules. The various aspects that the SPDI Rules seek to regulate to maintain data privacy are discussed below.

The Rules provide that a body corporate (in this scenario, a bank) must obtain the consent of the provider of sensitive information (Provider) before the collection of such information. Furthermore, such information can only be collected for lawful purposes connected with the function or activity of the bank and when the collection of the information is necessary for such purpose. Once the information is used for the purpose for which it was collected, it can no longer be retained.

Furthermore, there is a restriction on the transfer of such SPDI under the Rules. As in the case of collection, a bank can only transfer SPDI of the Provider with the consent of the Provider, and the transfer can be made only if it is necessary for the lawful performance of a contract.

Another angle the Rules seek to cover is the disclosure of information. Disclosures can only be made

by a bank when the prior permission of such disclosure is obtained by the Provider. However, the relevant rule provides for certain exceptions to the necessity for consent when:

- The disclosure is necessary to be in compliance with the law;
- The disclosure has been agreed to in a contract between the body corporate and the Provider; and
- A Government Agency mandates the SPDI for verification of identity, or for the prevention, detection and / or investigation of cyber incidents.

There are further restrictions on the third party who receives the SPDI to not disclose such information further and not to publish such information.

In addition to the conditions mentioned above, the SPDI Rules also lay down the security practices and procedures to be followed by banks who are in possession of SPDI. Further, all of the above details are to be published on the website of the body corporate in furtherance of their privacy policy.

The biggest challenge in relation to the SPDI Rules is that for the disclosure or transfer of information, the consent of the "Provider" is what is said to be required. However, it fails to envisage a situation where the Provider is in possession of SPDI connected to persons who are not the Provider. Therefore, there is a necessity to widen the scope of the Rules to provide that the consent of the actual person in relation to whom the SPDI pertains to (and not merely the Provider) will also be required for disclosure or transfer.

Further, Rule 6 allows for an exception to government agencies for the disclosure of information in specified scenarios. This may, however, result in the misuse of the information if the government agency is allowed to obtain SPDI without the requirement of a mandate.

Finally, the fast pace at which technology is changing will be a major challenge for the protection of sensitive information. Mobile phones, though not a method of collecting SPDI earlier, have become a major source of collection now. Therefore, keeping up with changing technology might prove to be a major challenge.

A Step in the Right Direction

The data protection laws of India, although recent, are focused on protecting the customer's right of privacy, and ensuring that adequate checks and balances are put in place by banks for instilling greater customer confidence and satisfaction. However, given that most of these developments are fairly recent and still in the process of being tested and upgraded, it would be best to label the current data privacy laws available in the Indian banking sector as a good start in the right direction. The law in India needs to keep up with the fast-changing pace of technology as well as changes in laws in other jurisdictions which have more evolved laws on data privacy as compared to India.

Manisha Shroff is a Partner in the Debt Capital Markets (DCM) and Banking Finance practice at Khaitan & Co, Mumbai. Manisha has over 10 years of work experience in banking and DCM. Prior to joining Khaitan & Co she has worked with Goldman Sachs. She has extensive experience in banking and finance and has advised on a myriad of cross border external commercial borrowings, offshore financings, bilateral and syndicated financings, acquisition finance, structured finance, mezzanine financing, banking regulation, loan and product documentation, debt recovery, consumer banking, bankruptcy, payment solutions, securitization, mergers and acquisitions in the financial services sector and regulatory advice. She has also advised on numerous derivative transactions, negotiations on ISDA documentation and CSAs.

Nikita Nehriya is a Senior Associate in the Banking & Finance practice at Khaitan & Co, Mumbai. She has worked on various lending transactions and is

acquainted with structuring of both offshore as well as domestic lending transactions.

Ankit Chavan is an Associate in the Corporate/Commercial practice group at Khaitan & Co, Mumbai. Ankit specialises in general corporate advisory work.

Praneetha Vasan is an Associate in the Corporate/Commercial practice group at Khaitan & Co, Mumbai. Praneetha specializes in general corporate advisory work.

NEED FOR ROBUST DATA PROTECTION CONTROLS FOR THE INDIAN INSURANCE SECTOR

By Anuj Sah and Rohan Singh

The past few years have witnessed a gradual movement towards digitization and electronic transactions across various sectors in India. Apart from the Indian Government's encouragement in this respect, digitization makes economic sense as well because of (i) cost-efficiency, and (ii) its potential to reach customers beyond their physical locations. In India's growing insurance sector, an added socio-economic rationale is the ability to achieve financial inclusion swiftly and efficiently by providing access to insurance products through the online medium. However, with increasing use of electronic means, there is a growing regulatory concern in ensuring data protection and privacy of policyholders' personal data.

India's insurance regulator, the Insurance Regulatory and Development Authority of India (IRDAI), has taken several progressive steps to increase digitization and to simultaneously require entities handling policyholders' information and customer data (insurance companies and their third-party outsourcing partners) to ensure that the data available with them is adequately protected. The need for data protection has been compounded from the recent introduction of the option available to policyholders to obtain and hold insurance policies in soft-copy, online format (rather than physical, original version). In this article, we examine the existing framework and the measures proposed by the IRDAI for creating a more robust data protection and cyber security regime in the insurance sector, which will be implemented in this financial year.

Existing Framework for Data Protection and Security

Information and data protection for insurance companies, like other companies, is primarily regulated under the umbrella legislation of the Information Technology Act, 2000 (IT Act). The IT Act and the rules framed thereunder regulate the dissemination, processing, retrieval and destruction of electronic data.

In 2011, the Government of India notified the Information Technology (Reasonable Security Practice and Procedure and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules). Rule 3 of the SPDI Rules defines "sensitive personal data or information" of a person to mean such personal information which consists of information relating to (i) password, (ii) financial information, such as bank account or credit card or debit card or other payment instrument details, (iii) physical, physiological and mental health conditions, (iv) sexual orientation, (v) medical records and history, (vi) biometric information, (vii) any detail relating to the above as provided to body corporate for providing service, and (viii) any information received under the above by body corporate for processing, stored or processed under lawful contract or otherwise. The proviso to Rule 3 excludes (i) any information freely available or accessible in public domain, or (ii) furnished under the Right to Information Act, 2005, or any other law being in force, from being considered sensitive personal data or information for the purposes of the SPDI Rules. Accordingly, insurance companies are required to create and implement a policy for privacy and disclosure of sensitive data, and to ensure that the consent of individuals providing their sensitive data is obtained prior to collection and transfer of such data.

Prior to the collection of data, an insurance company would need to ensure that the provider of such data is aware of the intended recipients of such data, the purposes of data collection, and the details of the agency collecting such data. The provider of data (in this case, a potential or an existing policyholder) has the choice to not provide data or may withdraw consent that was

previously given. However, in such a case, the insurance company may decide not to provide the insurance product. All disclosures of sensitive data (except in case of disclosures to government agencies or in order to comply with applicable law) require the prior consent of the provider of such data. In addition, the transfer of such data can only be carried out where the transferee ensures the same level of data protection, and such transfer is (i) consented to and (ii) undertaken for the performance of a lawful contract. Apart from these obligations, an insurance company is required to ensure that it has implemented reasonable security practices and procedures, in accordance with the SPDI Rules.

Section 43A of the IT Act states that the provider of data is entitled to compensation by way of damages (uncapped). Further, Section 72A of the IT Act imposes an obligation on data recipients to maintain privacy of personal information, and that any failure to maintain confidentiality makes the recipient liable to be penalized in accordance with the Section (i.e. imprisonment for a term which may extend to three years, or fine of up to INR 500,000 (approximately USD 7,743.52 (USD 1: INR 64.5701)).

Data Protection Measures in Existing Insurance Guidelines

The IRDAI made a significant recognition of the crucial status of data protection in its "Guidelines on Outsourcing of Activities by Insurance Companies", dated 1 February 2011 (Outsourcing Guidelines). The Outsourcing Guidelines provide for the applicable code of conduct and reporting requirements in relation to certain non-core activities which can be outsourced by an Indian insurance company to an external service provider. Paragraph 9.7 of the Outsourcing Guidelines specifically highlighted the risk of data protection and security being adversely affected by the geographical location of an outsourcing service provider. Accordingly, insurance companies were required to seek specific risk management expertise in assessing country risk, particularly legal and political conditions prior to executing outsourcing arrangements with an offshore service provider. Hence, data protection was, and continues to remain, a substantial concern of the industry regulator. One of the reasons for sensitivity in the movement of data outside India appears to be the questionable nature of the operation of existing Indian data protection laws and rules to such data once it has been moved to servers located outside India.

In a recent enabling step, the IRDAI has notified "Guidelines on Insurance e-commerce" (E-commerce Guidelines) on 9 March 2017. The primary objectives of the E-commerce Guidelines were to increase insurance penetration and enhance financial inclusion in a cost-effective manner by enabling (and regulating) electronic insurance transactions. Insurance companies and insurance intermediaries are permitted to create "Insurance Self-Network Platforms" (ISNPs) in the form of websites or mobile applications in order to market insurance products. The foundation of data protection is laid down in Clause 10 of the E-commerce Guidelines, which provide that ISNPs shall ensure (i) integrity of automatic data processing systems, (ii) data privacy, and (iii) existence of adequate internal mechanisms for reviewing, monitoring and evaluating its control, systems, procedures and safeguard. However, in order to ascertain that these internal data protection and integrity controls are performing their functions, the IRDAI has mandated that all ISNPs will need to facilitate an annual review of these controls, systems, procedures and safeguards by either an external certified information system auditor, chartered accounts with the necessary qualifications, or a CERT-IN expert. In addition to the aforementioned obligations, Clause 15 of the E-commerce Guidelines (which relates to privacy of personal information and data security) provides certain key data protection principles to be adhered to by ISNPs: (i) personal information collected during the course of an insurance transaction shall be kept confidential and ISNPs shall prevent its misuse, (ii) before commencing operations, an ISNP shall put in place measures to ensure data privacy and install adequate systems to prevent manipulation of records and transaction, and (iii) such safeguards should be continuously reviewed and reports should be made to sub-committees of the board of directors of owners of ISNPs for review and correction actions.

Further, the E-commerce Guidelines require ISNPs to have a pro-active fraud detection policy for insurance e-commerce activities, which are approved by the ISNP owner's board of directors. Given the above, it is quite clear that the IRDAI continues to emphasize the significance of data protection and integrity, while still providing an enabling framework for encouraging electronic insurance transactions and increased usage of electronic insurance policies.

A Step into the Future: Cyber Security for Insurers

A major shift towards data security was taken by the IRDAI when it notified the "Guidelines on Information and Cyber Security for Insurers" (Cyber Security Guidelines) on 7 April 2017. Section 3 of the Cyber Security Guidelines provides that they will apply to all data created, received or maintained by insurers, regardless of the form of the data, in the course of such insurers carrying out their business and functions. In addition, the IRDAI has specified a step-by-step timeline for achieving cyber security compliance by 31 March 2018. These include (i) preparation of a gap analysis report by 30 June 2017, (ii) formulation of cyber crisis management plan by 30 June 2017, (iii) finalization of an information and cyber security policy, approved by the insurance company's board of directors by 31 July 2017, (iv) formulation of an information and cyber security assurance program in line with the aforementioned board-approved policy by 30 September 2017, and (vi) completion of the insurance company's first comprehensive information and cyber security assurance audit by 31 March 2018.

The Cyber Security Guidelines have introduced an obligation on all insurance companies with at least three years of operation to appoint or designate a full-time employee as their Chief Information Security Officer (CISO) by 30 April 2017. The CISO shall report to the insurer's Head of Risk Management and is expected to be in constant touch with the insurer's Chief Information Officer in order to develop systems for security of information technology (although the information security and information technology functions are required to be segregated by the insurer). One of the key functions of the CISO is to build and lead an insurer's information security team to deliver the information security program. The CISO is responsible for articulating and enforcing policies to protect information assets and to form an "Information Security Committee" (ISC), a committee for which the CISO acts as the convenor. Some of the key functions of the ISC are (i) review of the high-level information security policy and recommendations to the insurer's board of directors on necessary changes to the policy, (ii) approve exceptions to the information security policy, (iii) discuss and direct information security risk mitigation, and (iv) ensure that the insurer's information security governance framework is supported by an information security implementation plan. The ISC is required to report to the risk management committee of the board of directors of the insurer twice each year. While the day-to-day information and data security policy-making and implementation is delegated to the CISO and ISC, the board of directors continue to remain responsible for the overall framework for cyber security policy and strategy and the information and cyber security assurance (implementation) program.

The Cyber Security Guidelines require insurers to identify management and access control arrangements in order to establish identity accountability and authentication such that business applications, systems, networks and computing devices only grant access to authorized users. This is a significant policy movement by the IRDAI since an insurer's security and access control procedures are required to control access, and thereby limit the chances of data theft, manipulation or unapproved transfers by the insurer's employees. In the event of any adverse effect on data volume or data integrity, these processes will allow an insurer to quickly and efficiently identify the source of such breach and to resolve the issue expeditiously.

The IRDAI has highlighted the importance of the five phases of data lifecycle: data at source, data in motion, data in use, data at rest and data destruction. Recognizing that the value of, and risks associated with data at each phase requires continuous data security, the Cyber Security Guidelines set out certain important

principles, namely (i) data should be segregated into critical and non-critical data, (ii) there should be an audit trail of access to critical data, (iii) access should be on a "need to know basis" and such access rights should be regularly reviewed, (iv) employees having access to data should be required to sign confidentiality undertakings, (v) security framework should be put in place to protect critical data on physical devices such as laptops and phones, (v) in the event that sensitive data is proposed to be shared with an outsourcing service provider, specific measures such as execution of non-disclosure agreements and/or protected emails should be used for such data disclosure, and finally (vi) effective mechanisms for data destruction should be available, including shredding, physical destruction of memory drives and deletions of system backups and offsite storage of data. While certain insurers may already have implemented best practices such as execution of confidentiality agreements with employees and non-disclosure agreements with outsourcing entities, the Cyber Security Guidelines provide a detailed framework for a more granular regulation of data protection in the insurance sector.

Moving Forward

Data protection and security will continue to remain a significant regulatory focus point in the insurance sector. There are multiple reasons for such regulatory intervention and oversight. These include (i) the general trends towards the growth of internet connectivity, usage of smartphones and overall expansion of e-commerce, (ii) the regulator's enabling framework for the increased usage of electronic methods of purchasing insurance policies and the holding of such policies in dematerialized formats; and (iii) the "invisible hand" of possibly reduced/ discounted pricing of electronic insurance policies (e.g., the E-commerce Guidelines explicitly permitting insurance companies to offer different pricing for insurance policies placed through ISNPs, as opposed to the traditional physical agency/marketing route). This financial year, in light of the implementation of each phase of data security measures prescribed under the Cyber Security Guidelines, is expected to be a watershed year in data privacy and cyber security in the insurance sector, as insurance companies attempt to streamline their existing data protection policies with the new regulatory prescriptions. Clearly, data protection will remain in the limelight in the insurance sector and will need to be organically regulated, based on the challenges faced in ensuring data security and privacy of policyholders' information. Considering the regulatory attention to data protection, the insurance industry appears to be on a path to ensuring protection for policyholders' information in a more robust manner.

Anuj Sah is a Partner at Khaitan & Co, Mumbai. Anuj is a member of the Firm's Mergers & Acquisitions, insurance and private client groups and regularly represents financial institutions, private equity investors, corporations and promoter families in a broad range of transactions and complex regulatory issues. Anuj has extensive experience in the insurance and financial services areas and has had a leading role in some of the most significant insurance M&A transactions in India in recent years. Anuj has also been recognized by Legal 500 in its 2017 rankings as a "Recommended Lawyer" in the insurance sector.

Rohan Singh is a Senior Associate in the General Corporate, Mergers & Acquisition and Private Equity group at Khaitan & Co, Mumbai. Rohan has represented foreign strategic investors, private equity funds and Indian companies in relation to minority investments and joint ventures in various sectors. He focuses on acquisitions and divestments in the insurance sector and on regulatory advice to Indian insurance companies, reinsurers and insurance joint venture partners. Rohan has also co-authored several articles in relation to various developments in the Indian insurance sector.

DATA PRIVACY: A RELIC OF THE PAST IN THE TIMES OF INFORMATION EXCHANGE?

By Aditi Sharma

Curbing tax avoidance and evasion has and continues to be one of the most critical goals for developed and developing countries alike. Recent times have witnessed sophisticated "tax planning" structures to mitigate tax costs, adoption of complex instruments, hybrid entities and more often by usage of intermediate jurisdictions that are extremely "tax friendly". Hand in hand with such strategies, the tax authorities at a global level have forged a formidable alliance to tackle their eroding tax base by simply joining hands to exchange information and co-operate with each other to prevent such evasion.

Several recent international developments unequivocally point towards the direction of achieving a robust network of automatic exchange of tax information. Namely, the Base Erosion and Profit Shifting (BEPS) project by the OECD aims (among other things) to "enhance transparency and certainty". Recent changes that have ramped up the information exchange regime include, (i) enacting inter-governmental agreements to implement the Foreign Account Tax Compliance Act (FATCA), (ii) implementation of the international tax information exchange agreements, (iii) revisiting and strengthening exchange of information provisions in double taxation avoidance agreements, and (iv) joining the Multilateral Competent Authority Agreement and adopting the Common Reporting Standard (CRS) on Automatic Exchange of Information (AEOI).

While tax transparency is the highlight of tax policy globally, it is essential to review whether financial data that is sensitive personal data is at risk of being misused. The right to privacy (a fundamental right guaranteed by the Indian Constitution as per several Supreme Court decisions) is and should not be an absolute right and is indeed subject to reasonable restrictions, such as necessary legal disclosures (as in the case of FATCA), and the taxpayer's consent to share such information. However, in cases where there is a lapse or breach on part of the financial institution in collecting and sharing financial information, one wonders if the current Indian regime is sufficient to address such a lapse or error. Further, it is also essential to ponder whether it is time for India to have a stand-alone privacy statute to keep up with the rapid strides of automatic exchange of information.

This article explores how data privacy concerns were validly raised and addressed while implementing FATCA (globally and in India) and some takeaways on balancing data privacy concerns with exchange of information.

FATCA – What the Fuss is About

FATCA provisions were introduced in the U.S. Internal Revenue Code (§ 1471 - 1474) to address concerns about revenue loss arising from offshore tax abuse, concealment of U.S. sourced income and undeclared accounts held by U.S. taxpayers. The obligation to report "U.S. persons" and details of their financial information rests on reporting "financial institutions", failing which a 30% withholding tax/penalty was levied on certain U.S. sourced "withholdable" payments made to such financial institutions.

Since the imposition of FATCA, compliance was perceived to be extra-territorial; in a sense, financial institutions were stuck between a rock and a hard place. They could either comply with FATCA on the one hand or adhere to local laws that provided for protection of financial and other sensitive data of taxpayers. Recognizing the inherent difficulties that posed as stumbling blocks, the U.S. Internal Revenue Service

(IRS), in order to facilitate reporting of financial accounts held by U.S. persons, with proper legal sanctions, allowed foreign financial institutions to enter into specific agreements for FATCA compliance. The FATCA provisions contained in the Internal Revenue Code (IRC) allowed financial institutions to either directly enter into agreements with the IRS for reporting information or the IRS was empowered to enter into inter-Governmental agreements with countries to maneuverer the local data privacy laws that restricted the sharing of information.

Modalities and Workings of Inter-Governmental Agreements (IGA)

In order to encourage foreign financial institutions to comply with FATCA reporting, the IRS provided for compelling reasons to enable governments to enter into IGAs. The IGA addressed the main concerns at one go, providing both the U.S. as well as its counter-parts who would execute the IGA, a solution to achieve FATCA compliance in a legally compliant manner. The rationale for executing the IGA was to (i) address data privacy concerns; (ii) implement them in municipal/local law; (iii) avoid withholding penalty; and (iv) avoid closure of "recalcitrant" (non-cooperative) account holders.

IGAs can be classified into two broad categories – Model 1 and Model 2 IGAs. Model 1 IGAs provided for a reporting mechanism whereby the relevant data of U.S. persons would be shared with the domestic tax authority which would in turn share the same with the U.S. IRS. The latter provide for the data to be shared directly with the U.S. IRS. Needless to say, these formats of the IGA were largely provided to harmonize FATCA reporting with the prevailing data privacy regimes of each jurisdiction. For instance, the provisions of Data Protection Act, 1998, in U.K. and the E.U. Data Protection Directive were examined in detail in the FATCA context to facilitate reporting. Countries amended extant laws to provide financial institutions a legal basis to report accounts in furtherance of their FATCA obligations. Similarly, provisions for express consent and undertakings from account holders prior to the financial institution sharing the information and for rights of taxpayers to receive copies of information being sent etc. were reviewed closely.

India signed a Model 1 reciprocal IGA with the U.S. on 9 July, 2015. The IGA with U.S. was executed in furtherance of the information exchange clause of the existing tax treaty with U.S. (Article 28). The recitals of the India – U.S. IGA recognized that "*FATCA has raised a number of issues, including that Indian financial institutions may not be able to comply with certain aspects of FATCA due to domestic legal impediments*". Until the enactment of express provisions in the (Indian) Income Tax Act, 1961 (ITA) (discussed below) the (Indian) Information Technology Act, 2000 read in conjunction with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 required the express consent of the information provider for collecting sensitive personal data or information (which includes financial information).

Facilitating FATCA

Identifying the need to amend local laws, in tandem, the Indian Government, enacted Section 285BA vide the Finance Act, 2014 to the ITA. The provision states that certain taxpayers (categories defined therein) were required to report specified financial transactions along with necessary documents in prescribed formats. Further, the Income Tax Rules, 1962 were amended to include the specific rules and instructions on the due diligence procedures and review of financial accounts. Further, the prescribed form (Form 61) has also been introduced to enable Indian financial institutions to report the accounts annually to the Indian Government.

Interestingly, the rules enable information exchange between the countries for both FATCA and CRS purposes by expressly stating the thresholds for reporting and processes for doing so for both '"US reportable accounts" and "US account holders"' and "other accounts" and "other account holders".

Implications on Data Collection

In light of the foregoing, financial institutions that have a reporting obligation under FATCA and CRS, have updated their KYC and account opening forms to ensure that the information provided by the account holders enables them to ascertain whether the account holder is a "U.S. person" (in case of individuals – residency, permanent address, citizenship, identification are indicators; in case of companies –– trusts, entities, place of incorporation, residency of partners and parties such as settlor etc. are indicators). Accordingly, the financial institution must undertake annual reporting in Form 61B of such "U.S. persons", their account details (e.g., name, address, tax identification number, account balance).

Importantly, depending on the level of review mandated as per the Income Tax Rules, express self-declarations are being sought from account holders to certify their FATCA status in addition to information pertaining to their citizenship and tax residency status.

Thus, from a data privacy perspective, the account holder acquiesces to submit correct and true information recognizing the fact that such information may be shared with tax authorities (both Indian and foreign).

While there is a steady progressing towards a transparent world, what is essential is that data freely, and automatically exchanged is subject to the overarching right to privacy. There is no taking away from the fact that the right to privacy is subject to disclosures as mandated by the law, however, such disclosures must include checks and balances to ensure that data shared and exchanged is not misused.

Currently, there is no judicially tested case or discussion between competent authorities (India and U.S.) on the implications of FATCA non-compliance. In fact, recently, the Central Board of Direct Taxes (CBDT) has issued a Press Release (dated 11 April, 2017) requiring Indian financial institutions to obtain the self-certification from account holders by 30 April 2017, failing which "the accounts would be blocked" disabling the account holder from transacting through such account. The necessity and importance of the self-declaration highlights both the need for verifying the information provided as well as the express consent of information provider required to share sensitive information with tax authorities.

Account holders today are provided little flexibility to amend the terms of the self-declaration and KYC documentation. As a result, do information exchange concerns override those of data privacy? Express legislative changes (in addition to India being an early adopter of CRS) mandating FATCA and CRS reporting signal that currently the emphasis is on automatic exchange of information.

Specific redressal of lapses in the processes for collecting and sharing information should be examined. For instance, cases where a financial institution is not required to collect or review data as per FATCA or CRS and proceeds to do so anyway should be reviewed. Another instance that has been debated is the use of stolen data. The breach of confidentiality in such cases and resulting loss of reputation even in genuine cases should be evaluated and addressed. Policy considerations would need to balance admissibility of such evidence on the one hand and the dominant objective of curbing efforts of earning money through illegitimate means on the other.

Perhaps, it is time to revisit current data privacy laws in India in light of the rapidly evolving information exchange laws.

Aditi Sharma is a Principal Associate in the Direct Tax and Private Client Practice at Khaitan & Co, Mumbai. She assists clients on wide ranging domestic and international tax planning matters including advice on FATCA and CRS reporting, tax structuring and transactional tax matters. She has also worked closely with high-net worth individuals to plan their succession and Indian estate.

Debit and Credit Card Data Theft in India: Manifestation of Data Privacy and Data Protection

By Nandini Khaitan and Aritri Roy Chowdhury

In September 2016, the discovery of a possible theft of 3.2 million debit cards' data from ATMs operated by a well-known payment service provider caused a flutter in the Indian financial sector. It rang an alarm that made Indian fiscal policy makers sit up and take note of the threats that such card payment systems were exposed to. Further, since the announcement of the "demonetization" measure on 8 November 2016, there has been a statistical growth of 267% in the transactional value of digital payments, according to government data updated until December 2016. This has warranted adequate safety cushions to be provided to millions of Indians who are now rapidly transitioning from a cash-based economy to a cashless one.

The issues concerning data breach are extremely dynamic in nature. Along with a sturdy legal framework, an evolving mechanism is needed to combat the new methods through which debit/credit card data theft occurs. Through this article, we analyze the existing laws governing protection of data relating to payment instruments and discuss their shortcomings. Further, we aim to address the concern of debit card/credit card data thefts by touching upon the best practices that may be adopted to combat data privacy breach.

The Law: Its Structural Framework

A host of skeletal Indian laws provide the basic legal framework for protection of customers' data. Among the existing laws, the Information Technology Act, 2000 (IT Act) is important legislation in India that seeks to protect data of an individual, and imposes penalties for any breach. However, the IT Act, as it was originally framed, did not adequately address the concerns relating to data protection and data privacy, and it was amended in the year 2009 to incorporate Sections 43A and 72A to address these concerns.

Section 72A of the IT Act deals with the concept of personal information, and imposes criminal liability on any person who discloses personal information with intent to cause wrongful loss or wrongful gain, in breach of lawful contract or without the consent of the information provider. Thus, it casts an obligation upon any person, including an intermediary, who under the terms of a lawful contract intentionally discloses any personal information to any other person without authorization. Any breach of obligations imposed upon by this section mandates a punishment with imprisonment for a period which may extend to three years or with a fine of up to INR 500,000 (approximately USD 7743 (USD 1: INR 64.5701)) or with both. However, an exception has been carved out where an intermediary (as defined under the IT Act) will not be liable for any breach if it follows the guidelines prescribed under the IT Act and the Information Technology (Intermediaries Guidelines) Rules, 2011.

To further bolster the efficacy of the existing legal regime, in the year 2011, the Government of India formulated the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) under Section 43A of the IT Act. These SPDI Rules mandate that any "body corporate" that collects sensitive personal data or information (SPDI) (i.e. personal information containing information relating to, inter alia, password, bank account or credit card or debit card or other payment instrument details) must implement and maintain reasonable security practices and procedures in relation to such SPDI. Section 43A of the IT Act further imposes civil liability on any "body corporate" that is negligent while handling SPDI. The IT Act broadly defines "body corporate" to include any

company, firm, sole proprietorship or association of individuals engaged in commercial or professional activities. The scope of these SPDI Rules are wide, and it comprehensively imposes an obligation upon any person or their agent who collects SPDI. Thus, all shopkeepers, merchants, restaurants, online shopping portals etc., with whom a customer shares debit/credit card details, are covered by the SPDI Rules.

Whilst Section 72A of the IT Act imposes a general obligation on "any person" for any intentional disclosure of personal information (obtained through a lawful contract), Section 43A imposes liability only on "body corporates" for negligent disclosure of SPDI.

Apart from the IT Act, there are various other sectoral laws that envisage the protection of financial information of customers. The Public Financial Institutions (Obligations as to Fidelity and Secrecy) Act, 1983 contains provisions that prohibit public financial institutions, such as banks, from divulging any information that is entrusted to them by their customers. In addition to this, the Banking Codes and Standard Board of India (BCSBI) issued a voluntary "Code of Bank's Commitment to Customers" (Code) in August 2009 that sets the minimum standards of banking practices to be adopted while dealing with individual customers. The Code specifically states that banks shall maintain the confidentiality of a customer's information even after the customer has severed the relationship with the bank, except when such information is required by law. Further, the RBI's Master Circular on "Credit Card, Debit Card and Rupee Denominated Cobranded Prepaid Card Operations of Banks", dated 1 July 2015 (Master Circular), applicable to banks and non-banking financial companies (NBFC), stipulates certain guidelines which are to be strictly adhered to.

In relation to credit card operations, the Master Circular seeks to hold the card issuing bank/NBFC responsible as the principal for all acts of omission or commission of their agents. Banks/NBFCs often outsource the various credit card operations to third party service providers for services, such as marketing the bank's products/services. At times, it has been observed that these third parties disclose the information shared with them without obtaining due permission. One of the outcomes of such unauthorized data disclosure is unsolicited product calls that are made to consumers after tracking their financial information and spending habits. In light of the above, the Master Circular requires banks/NBFCs to be guided, *inter alia*, by the need to ensure confidentiality of the customer's records while making the choice of agent. RBI has reserved the right to impose penalty on any bank/NBFC under the provisions of the Banking Regulation Act, 1949 and the Reserve Bank of India Act, 1934, respectively, for violation of any of these guidelines in relation to credit cards stipulated in the Master Circular.

For debit cards, the Master Circular specifies that the bank shall ensure full security of such cards, and the losses incurred by any party on account of breach of security or failure of the security mechanism shall be borne by the bank. Further, banks issuing co-branded debit cards (i.e., cards that are jointly sponsored by a bank and a retail merchant), should not reveal any information relating to customers obtained at the time of opening the account or issuing the card. The co-branding non-banking entity should not be permitted to access any details of customers' accounts that may violate the bank's secrecy obligations.

The usage of debit/credit cards in the digital age, at various points of sale, is dynamic in nature. This makes it difficult for the existing legislations governing data theft to gauge the different kinds of breaches that may occur. Hence, it may be beneficial to have an umbrella legislation which could govern various aspects of data theft, some of which are discussed hereinafter.

Card Data Theft: Modus Operandi

There are many ways through which debit and credit card data theft occurs. The theft is not confined to instances where the bank discloses SPDI to a third party without the consent of the information provider, but may also occur in some of the following ways:

- **Hacking**: Unauthorized access / control over computer network / computer security systems for an illicit purpose is called hacking. The most common method employed to steal card data is by hacking into websites and e-payment gateways to access sensitive financial information.

- **Skim and Clone:** The equipment is set up at business premises that can illegally collect PIN and card information. For example, when the card is handed over for the transaction, the card is first run through a device that sends the magnetic strip information to the financial institution and then swiped again to record the information into a hidden device that allows them to duplicate the card data while simultaneously recording the PIN.

- **RFID Readers**: Radio Frequency Identification (RFID) is a generic term for technologies that use radio waves to provide RFID labels on any object. Once an object has been RFID identified, it is easy to read information off it. Credit and debit cards often use this technology because of the ability of RFID enabled cards to operate wirelessly and remotely with the help of RFID readers without swiping such a card in any machine. However, a fallout of this technological advancement is that thieves are now installing RFID readers that help them extract the card details from the wallet of the card holder without any physical contact, even when the wallet is inside a pocket or a bag.

- **Internet Banking**: Internet banking services and IT-related services are generally outsourced by banks due to financial reasons and lack of adequate in-house technical infrastructure. This outsourcing of data involves a considerable threat of SPDI being saved or retained by third parties without authorization and then misused.

There are various other methods through which the data stored in the card can be stolen. These cards are used both nationally and internationally making it an extremely difficult task to promulgate an umbrella legislation that would protect consumers from data thefts across the border. It is imperative that customers also adopt certain safety measures to ensure that the legislative efforts to protect their card data is fortified by their own actions.

Consumer Efforts: Do your Bit

The "Guidelines in Information Security, Electronic Banking, Technological Risk Management and Cyber Frauds" issued by the RBI envisages a customer to be well-equipped through "self-help" to prevent any unfortunate data breaches. Further, in the Press Release dated 24 October 2016 on "ATM / Debit Card Data Breach", the RBI has advised customers to change their PINs periodically and has warned them against disclosing their card details to any person over phone or email.

We recommend that debit/credit card users be diligent about their own security. The following practices may be adopted to prevent any unauthorized data usage of payment cards:

- **Activate card usage alerts:** Activating card usage alerts immediately notifies a customer about any activity that take places through their payment cards, through SMS and e-mail. This helps customers to quickly detect any misuse and report the same to stall any further misappropriation.

- **Usage of bank maintained ATMs to withdraw money**: ATMs are either maintained by banks or maintained by stores and malls in collaboration with banks. Bank-maintained ATMs are usually equipped with better security mechanisms (e.g., video cameras, guards etc.) and also provide greater privacy (through ATM isolated rooms) than ATMs placed and maintained by stores such as Big Bazaar, malls and other places. Thus, it is always advisable to use ATMs maintained by banks to withdraw money.

- **Destroying old cards**: Old cards should be destroyed and shredded into pieces. Further, out of abundant caution, these pieces should be disposed of in different places so as to make reconstruction of the shredded cards difficult.

- **Use a secure network**: It is very important to use a secure network while engaging in an e-transaction on online commercial portals in order to keep the card details secure.

With cashless transactions being promoted on a massive scale, and the Attorney General of India's announcement that the government is actively "mulling data protection regime through a legislation", it seems that the existing protections will be fortified further. However, this effort has to be supplemented by the user's own vigilance to prevent/mitigate any potential loss.

Nandini Khaitan is a Partner of the Khaitan & Co, LLP, Kolkata, and heads a Litigation and Dispute Resolution team in Kolkata. She has vast experience in commercial and intellectual property litigation and has appeared before various tribunals and courts, including the Supreme Court of India.

Aritri Roy Chowdhury is an Associate in the Corporate Practice group at Khaitan & Co, LLP, Kolkata. Aritri specializes in general corporate and data privacy advisory work.

Bring Your Own Device Policies: Legal Considerations

By Pallavi Thacholi and Deepthi Bavirisetty

Employers are increasingly encouraging employees to bring their own personal electronic devices—such as phones, tablets, and computers—to the workplace. This is a departure from the earlier position where companies provided company-owned devices to employees. This shift to a "Bring Your Own Device" or "BYOD" policy by corporates is being done for reasons such as flexibility and familiarity for their employees. It also helps companies limit costs on IT infrastructure and maintenance.

A BYOD policy in the workspace and the resultant blurring of the personal and professional lives of the employees raises several issues regarding data protection, security, and ownership for employers, and privacy of employees, as the devices contain personal information like passwords, messages, emails, etc. It is now standard practice for employers to monitor employee activities on company-owned devices or company networks. However, the same level of surveillance may not be appropriate in the case of personal devices. This article discusses some of these issues and attempts to provide certain universal best practices that employers can adopt to balance their business interests and the privacy of their employees.

Employer's Rationale for Monitoring

Under Section 17 of the Indian Copyright Act, 1957 (ICA), the employer is the first owner of copyright in the case of any work made in the course of the employee's employment, subject to exceptions carved out by parties through a contract.

Unlike in the case of employees, where ownership of intellectual property created during the course of employment automatically vests with the employers, intellectual property created by independent consultants does not automatically vest with employers. Intellectual property created by independent consultants requires specific assignment in favor of the employer. Section 19 of the ICA requires such assignment to be in writing and signed by the assignor. Further, an assignment can be done for prospective purposes as well, and need not be restricted to existing work. Thus, companies must ensure that they execute written contracts with independent consultants, which contain specific intellectual property right assignment clauses, for both pre-existing and prospective work done for them. This is relevant for a company adopting a BYOD policy as well.

As employers have a stake and ownership over all the work created by its employees and/or independent consultants, they are eager to monitor the work of these individuals. Employers also use surveillance to pre-empt security breaches and to ensure that their employees maintain confidentiality of company information. In addition, the Information Technology Act, 2000 (IT Act) requires companies dealing with sensitive personal data or information to implement reasonable security practices and procedures (i.e., policies that contain managerial, technical, operational, and physical security control measures commensurate with the protected information). Especially in a BYOD scenario, implementing such measures could prove tricky for employers. For instance, if the company policy requires encryption of all sensitive data on company-owned computer devices, employers must also ensure that an employee's device is compliant with this requirement. Ultimately, it is the employer that faces potential liability for not ensuring the implementation of mandated reasonable security practices and procedures if an employee's personal device is hacked and unencrypted personal data is stolen. This potential liability risk of employers favors the argument of employee monitoring and surveillance.

Right to Privacy: A Judicial and Legislative Perspective

Indian law currently does not explicitly protect an employee's right to privacy. Several notable judicial pronouncements such as *Kharak Singh vs. State of Uttar Pradesh* (1963 AIR 1295) and *Gobind vs. State of Madhya Pradesh* (1975 AIR 1378) have read the "right to privacy" into the fundamental "right to life and personal liberty" under Article 21 of the Constitution of India (Constitution). However, fundamental rights are enforceable only against the state and not against private entities.

In a notable exception of what seems to be judicial oversight, the Supreme Court of India (Supreme Court) invoked Article 21 of the Constitution when deciding upon a claim of an individual's right to privacy against a private entity in the case of *Mr X vs. Hospital Z* (1998 8 SCR 296). During the course of a blood test conducted at Hospital Z, Mr X was diagnosed as HIV +, the disclosure of which, resulted in the cancellation of Mr X's marriage to Ms Y and Mr X facing discrimination in the community. Mr X approached the Supreme Court, arguing that there was a violation of his right to privacy as a result of the hospital disclosing his confidential medical information. Using the test of proportionality, the Supreme Court held that the danger of harm to Ms Y outweighed Mr X's right to privacy. It concluded by stating that there was no violation of Mr X's right to privacy.

The key takeaway here is the adjudication of a claim by the Supreme Court with the horizontal application of right to privacy of an individual against a private entity. Further, in the context of employee privacy, the rationale of the Supreme Court in coming to its decision can be extended to argue that the test of proportionality can be used to justify the supersession of an employee's right to privacy in the case of potential violation of the employer's trade secrets that warrants certain levels of surveillance.

As data protection and privacy laws are still relatively nascent in India, there has not been any jurisprudence with respect to usage of BYOD devices. Therefore, we have to look at foreign case laws, which may have persuasive value. The case of *Rajaee vs. Design Tech Homes*, No. H-13-2517, 2014 WL 5878477 (S.D. Tex. Nov. 11, 2014), before a district court in Texas, analyzed the issue. The plaintiff, Rajaee was an erstwhile employee of Design Tech Homes, the defendant. The plaintiff's personal phone was configured by the defendant and was connected to the company's server, enabling the defendant to access company-related emails, contacts and calendar. Shortly after the plaintiff resigned, the defendant remotely reset the plaintiff's phone. This resulted in not only the deletion of the plaintiff's work-related data, but the entirety of his personal data as well. Aggrieved by this, the plaintiff approached the court, seeking damages against the company, which dismissed his claim. This was on the grounds that the employee could not produce any evidence of loss / any cost incurred on the ground of the actions of the company. This included any costs involved in responding to, investigating, or remedying the deletion of data, restoring the data, etc.

In the absence of any clear judicial right to privacy, employees can take recourse under the provisions of IT Act. The IT (Amendment) Act, 2008 specifically addressed the lacunae in relation to data protection and privacy, and enabled individuals to seek compensation from body corporates for failure to protect their personal information.

As discussed above, companies collecting or processing sensitive personal data or information must have reasonable security practices and procedures in place. The concepts of "reasonable security practices" and what constitutes "sensitive personal data and information" was further fleshed out through the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. Rule 2(i) of the aforementioned rules defines "personal information" as any information that relates to a natural person, which directly or indirectly, in combination with other information available, or likely to be available to a body corporate, is capable of identifying an individual. Sensitive personal data and information relates to information such as passwords, financial information (such as bank account or credit card or debit card or other payment instrument details), etc. The reasonable security practices must be commensurate with the sensitivity of the data involved.

Additionally, there have been attempts to pass the Personal Data Protection Bill (Bill) in order to bolster privacy law in India. This Bill seeks to widen the scope and meaning of "sensitive personal data and information" to include information such as political affiliation, religion, race and caste. This Bill was first introduced in 2011. If passed, this would increase the ambit of employee privacy in India, and would provide corresponding remedies as well to employees.

BYOD Best Practices

Certain employers use keystroke monitoring mechanisms in order to track every keystroke entered by employees on their devices. While the legality of such keystroke mechanisms has not been considered by Indian courts so far, if such monitoring mechanisms are deployed on BYOD mobile devices, an employer must obtain the prior written consent of its employees and disclose the full extent of its monitoring. This is because employees would have a reasonable expectation of privacy with respect to the contents of their BYOD devices. Further, if in the course of usage of a device wherein keystroke monitoring has been installed, an employer collects sensitive personal data and information, such as passwords and financial information, it must take reasonable security measures to safeguard such information.

Few other BYOD best practices that may be adopted:

1. Employers should have a comprehensive written BYOD policy that contains a list of "blocked sites" at the workplace and sets out acceptable usage of network and device protocols.
2. The BYOD policy must be accompanied with corresponding consent / waiver forms at the time of joining the organization, consenting to employers accessing their personal devices and waiving any claims for loss of personal data or damage that may arise due to such access.
3. At the time of resignation / termination of the employee, such forms can provide for deletion of all company related data and information from their personal devices and certify that no back-ups of company related data and information are there on hard drive, personal cloud network, etc.

Measures such as the above ensure that the employees are adequately informed of the extent of privacy that they can reasonably expect from their employers at work even with respect to their personal devices used for work purposes. This will also largely insulate employers from legal claims in this regard.

Pallavi Thacholi is a Senior Associate and Deepthi Bavirisetty is an Associate at Khaitan & Co, Bengaluru. They are a part of the Firm's corporate practice with a focus on Mergers & Acquisition, private equity, venture capital and other strategic/financial investments. Apart from the aforesaid, they both also advise domestic and international clients on regulatory and legal aspects of employment and labour laws, including on issues of data privacy, data protection, intellectual property, and compliance and risk management.

SUBMISSION REQUESTS

Annual Year-in-Review

Each year, ABA International requests each of its committees to submit an overview of significant legal developments of that year within each committee's jurisdiction. These submissions are then compiled as respective committee's *Year-in-Review* articles and typically published in the Spring Issue of the Section's award-winning quarterly scholarly journal, *The International Lawyer*. Submissions are typically due in the first week of November with final manuscripts due at the end of November. Potential authors may submit articles and case notes for the India Committee's Year-in-Review by emailing the Co-Chairs and requesting submission guidelines.

India Law News

India Law News is looking for articles and recent Indian case notes on significant legal or business developments in India that would be of interest to international practitioners. The Fall 2017 issue of India Law News will carry a special focus on **Media and Intellectual Property Rights**. Please read the Author Guidelines available on the India Committee website. Note that, India Law News does not publish any footnotes, bibliographies or lengthy citations. Submissions will be accepted and published at the sole discretion of the Editorial Board

INDIA COMMITTEE

The India Committee is a forum for ABA International members who have an interest in Indian legal, regulatory and policy matters, both in the private and public international law spheres. The Committee facilitates information sharing, analysis, and review on these matters, with a focus on the evolving Indo-U.S. relationship. Key objectives include facilitation of trade and investment in the private domain, while concurrently supporting democratic institutions in the public domain. The Committee believes in creating links and understanding between the legal fraternity and law students in India and the U.S., as well as other countries, in an effort to support the global Rule of Law.

BECOME A MEMBER!

Membership in the India Committee is free to all members of ABA International. If you are not an ABA International member, you may become one by signing up on the ABA website. We encourage active participation in the Committee's activities and welcome your interest in joining the Steering Committee. If you are interested, please send an email to the Co-Chairs. You may also participate by volunteering for any of the Committee's projects, including editing a future issue of the *India Law News*.

Membership in the India Committee will enable you to participate in an online "members only" listserv to exchange news, views or comments regarding any legal or business developments in or concerning India that may be of interest to Committee members.

We hope you will consider joining the India Committee!

LEADERSHIP (2017-2018)

Co-Chairs

Bhali Rikhye

Roland Leslie Trope

Shikhil Suri

Immediate Past Chairs

Sajai Singh

Sanjay T. Tailor

Senior Advisors

Aaron Schildhaus

Eric B. Wulff

Priti Suri

Sanjay Tailor

Sajai Singh

Vice Chairs

Hanishi Thanawalla Ali

Raj Barot

Joe Bryant

Aseem Chawla

Poorvi Chothani

Jaipat Jain

Ashish Jejurkar

Ashish Joshi

Viren Mascarenhas

Kavita Mohan

J.L.N. Murthy