INTERTWINING TECHNOLOGY AND DATA PRIVACY: BRINGING STABILITY IN FINANCIAL INSTITUTIONS

By Shashwat Srivastava and Rachi Gupta
From Gujarat National Law University, Gandhinagar and Guru Govind Singh Indraprastha University, New Delhi respectively

ABSTRACT
"The world is one big data problem."
– Andrew McAfee, principal research scientist, MIT.

The most critical asset for financial institutions is Data and that is why Data playing such a pivotal role. Maintaining the integrity and availability of data is vital to financial markets globally. Data is an ideal target for malicious adversaries, with information theft being the most expensive and fastest-rising consequence of cybercrime.[1]

There is sharp increase in cyber-attacks and their consequences so banks & financial institutions are increasingly concerned about that. In an IIF survey of global banks, conducted in partnership with EY, both the Boards of Directors and Chief Risk Officers (CRO) deemed "Cybersecurity" to be a top strategic priority, second only to addressing new regulatory rules and supervisory expectations.[2]

Elder financial exploitation has been called "the crime of the 21st century."[3] *Deploying effective interventions has never been more important.*[4]

Data on cyber incidents is scarce and there have been very few quantitative analyses of cyber risk.[5]

India lags behind in comparison to many other countries regarding the protection of privacy & personal data because other Asian countries such as South Korea, which in 2016 strengthened its data privacy laws by imposing stricter penal provisions for violations, and Singapore, which protects privacy under the Personal Data Protection Act. As we all know India is amongst the fastest growing financial markets with a bewildering number of consumers, sustainable and appropriate measures must

[1] Accenture Security et al., The Cybercrime Evolution, Ninth Annual Cost of Cybercrime Study (July 17, 2019, 3:01 PM), https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf.

[2] Institute of International Finance et al., IIF/EY Release Seventh Annual Global Bank Risk Management Survey (July 17, 2019 3:29 PM), https://www.iif.com/Press/View/ID/1170/IIFEY-Release-Seventh-Annual-Global-Bank-Risk-Management-Survey.

[3] MetLife Mature Markets Institute et al., The MetLife Study of Elder Financial Abuse Crimes of Occasion, Desperation, and Predation Against America's Elders (July 17, 2019, 3:43 PM), https://ltcombudsman.org/uploads/files/issues/mmi-elder-financial-abuse.pdf.

[4] CFPB, What is elder financial exploitation? , Recommendations and report for financial institutions for preventing and responding to elder financial exploitation (July 20, 2019, 01:17 PM), https://files.consumerfinance.gov/f/201603_cfpb_recommendations-and-report-for-financial-institutions-on-preventing-and-responding-to-elder-financial-exploitation.pdf.

[5] Antoine Bouveret, Cyber risk and types of cyber-attacks, Cyber risk for the financial sector: A framework for quantitative assessment (July 21, 2019, 09:11 PM), https://www.imf.org/~/media/Files/Publications/WP/2018/wp18143.ashx.

be given effect to attain a balance between the rights and privacy of the customers and interests of financial institutions.

Overview

India has physical boundaries in the form of international borders with other countries, but there is no such 'boundary' in the cyber world. "Our cyber boundary is yet not defined and in today's world we do carry the obligation to protect our cyber boundaries also.[6]

Data privacy and rights attached to it are particularly paramount concerns for all the companies in the financial sector because banks and other financial institutions manage a large volume of sensitive information about their customers and the breach of the same can have dangerous consequences. Data privacy refers to who's allowed access to consumer information provided to institutions with whom they've entered into a business relationship.[7]

Financial services, hospitality and retail have been among the industry verticals that were most affected by data breach events in 2010. Collectively these three verticals accounted for around *87%* of data breach events recorded, with financial services accounting for almost *22%* of total breach cases reported across industries in 2010.[8]

In this age of digital exchange the issue of consent disappears because consumers might not realize their rights with financial institutions. A report released by Information Technology and Innovation Foundation in 2017 estimated the costs to national GDP by data localization and other barriers to data flows for certain countries as "reducing U.S. GDP by *0.1% to 0.36%*; increased prices of cloud services in Brazil and the European Union to *54% from 10%*, and reducing GDP by *0.7% to 1.7%* in Brazil, China, the European Union, India, Indonesia, Korea, and Vietnam."[9]

In 2018 in USA, *8.5%* of the data breach has occurred in the financial sector, including entities such as banks, credit unions, credit card companies, mortgage and loan brokers, investment firms and trust companies, payday lenders and pension funds and even financial authorities.[10] Data loss or data destruction are top-rated concerns for organizations.[11] For example, adversaries

[6] Arun Mohan Sukumar, India yet to sign treaty with other countries on Cybercrime says CBI special Judge, The Hindu, October 18, 2016 at https://www.thehindu.com/sci-tech/technology/internet/India-yet-to-sign-treaty-with-other-countries-on-Cyber-crime-says-CBI-special-Judge/article12546205.ece.

[7] Angila Stringfellow, The Importance of Data Privacy, The Ultimate Data Privacy Guide for Banks and Financial Institutions, (July 19, 2019, 4:00 PM), https://www.ngdata.com/data-privacy-guide-for-banks-and-financial-institutions/.

[8] Wade Baker el al., 2010 Threat Event Overview, 2011 Data Breach Investigations Report, (July 15, 2019, 1:07 PM), https://www.wired.com/images_blogs/threatlevel/2011/04/Verizon-2011-DBIR_04-13-11.pdf.

[9] Nigel Cory, Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? (July 15, 2019, 6:32 PM), http://www2.itif.org/2017-cross-border-data-flows.pdf.

[10] Nikki Florentino et al., Financial Impact of Cyber-security Incidents, The Impact of Cybersecurity Incidents on Financial Institutions (July 16, 2019, 11:02 PM), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_Generali_The-Impact-of-Cybersecurity-Incidents-on-Financial-Institutions-2018.pdf.

[11] Fred McClimans el al., The threat to data comes from within, The State of Cybersecurity and Digital Trust 2016 (July 18, 2019, 4:09 PM), https://www.accenture.com/t20160704T014005__w__/us-en/_acnmedia/PDF-23/Accenture-State-Cybersecurity-and-Digital-Trust-2016-Report-June.pdf.

stole documents related to a card processing system used by around *200* banks in the United States and Latin America, which could be potentially used for future attacks.[12] Manipulating credit scores, bank account numbers, and also market data containing the personal information on millions of consumers, healthcare patients and government workers could already be in use for various manipulation schemes.[13]

Emerging Global Data Privacy Trends

Data Breach Evolution

Nearly fifteen years ago serious data breaches began. This was the time when businesses began to digitize and store large databases online. But, the first major reported breach happened to internet giant AOL in 2004 when one of their employee sold details of 92 million users to the outside world.*[14] A data breach occurs when a hacker successfully infiltrates a data source and extracts sensitive information from financial institutions. The following are the steps usually involved in a typical breach operation:[15]*

A. *Research: The cybercriminal looks for all the weaknesses in the company's security.*
B. *Attack: The cybercriminal makes initial contact using either for a network or a social attack.*
C. *Exfiltration: Once having access to the computer the cybercriminal infringes upon the confidential company data by extracting the data.*

The following table shows the 10 biggest incidents reported regarding Data Privacy:[16]

Company/Organisation	Number of Records Stolen (In millions)	Date of Breach
Yahoo	3000	August 2013
Equifax	145.5	July 2017
eBay	145	May 2014
Heartland Payment Systems	134	March 2008
Target	110	December 2013
TJX Companies	94	December 2006
JP Morgan and Chase	83	July 2014
Uber	57	November 2017
U.S. Office of Personal Management	22	Between 2012 to 2014
Timehop	21	July 2018

[12] Anthony Cuthbertson, Bank Robber Hackers Steal Millions of Dollars in Silent Heists Across U.S. and Russia, Newsweek, December 12, 2017 at https://www.newsweek.com/bank-robber-hackers-steal-millions-dollars-silent-heists-745087.

[13] Maggie Overfelt, The next big threat in hacking - data sabotage, CNBC, March 09, 2016 at https://www.cnbc.com/2016/03/09/the-next-big-threat-in-hacking--data-sabotage.html.

[14] Chuck Lobert, Evolution of Data Breach (July 16, 2019 02:21 PM), https://www.vcsolutions.com/the-evolution-of-the-data-breach/.

[15] Trend Micro, What are the biggest breaches to date? , Data Breach 101: How they happen, what get stolen and where it goes (July 20, 2019 03:30 PM), https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101.

[16] Ibid.

Source – Trend Micro

Data breaches have gained widespread attention because financial institutions and businesses of all sizes have become increasingly reliant on digital data, cloud computing, and workforce mobility. In 2005 one of first data breaches of twenty-first century in financial sector occurred when 1.4 million credit card numbers and names on those accounts went public from DSW Shoe Warehouse.[17] *Another early landmark incident occurred in 1984, when database files of the credit reporting agency Experian (then TRW Information Systems) were breached.*[18]

Regulatory Focus

Legislature is increasingly focusing on enacting laws and implementing the same as soon as possible to maximize data privacy and minimize breach impact on businesses. This can be done in a threefold way as follows -

A. **Increasing government focus on law enforcement and breach notification** - Globally stricter law enforcement and tougher penalties on data breach violators is needed to restrict the infringement of personal data. In the European Union, data protection authorities have power to investigate and prosecute defaulters for non-compliance. On the other hand, U.S.A. has adopted breach notification requirements very early to mitigate the breaches, while several nations are still under the process of intensifying their law enforcement policies.

B. **Harmonization of data protection standards across regions** - There is no unified approach in data protection across the globe. Banks, insurers and capital markets firms which have multinational operations globally and dealing with offshore outsourcing partners and local governing bodies counters major problems because of non-uniformity in the law. The EU has resolved this issue by removing excessively bureaucratic and ineffective notification requirements. Infact many emerging nations are beginning to adopt EU's Data Protection Directive, in order to simplify their data security.

C. **Outsourcing destinations adapting privacy laws to help industry** - For enhancing data security standards and privacy concerns, most outsourcing destination countries (including India) have implemented new data privacy regulations. Initially, the privacy regulations in India requires institutions to obtain the consent of end customers before collecting their personal information. These kind of regulations would have carried a new set of challenges to the outsourcing business. But, with a major relief to the outsourcing businesses the Government of India have exempted outsourcing companies from such regulations in India.

India - The Reserve Bank of India time to time circulates guidelines, regulations and circulars to for maintaining confidentiality and privacy of banking customers' information, and with regards in 2006 RBI

[17] Symantec Corporation, A brief history of data breaches (July 20, 2019, 04:23 PM), https://www.lifelock.com/learn-data-breaches-history-of-data-breaches.html.

[18] Lily Hay Newman, The history of data breaches, Guide to Data Breaches (July 19, 2019, 05:18 PM), https://www.wired.com/story/wired-guide-to-data-breaches/.

and the Indian Banks Association established a body called the 'Banking Codes and Standards Board of India'. The main function of the said body is to maintain a set of voluntary norms which banks must enforce themselves through all internal grievances redressal mechanisms within each bank, and these mechanisms should include a designated "Code Compliance Officer" and an Ombudsman.[19]

India also have Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 which serves as the privacy regulations and require companies to provide privacy policies containing measures to restrict the circulation of sensitive personal data with additional security measures, in addition to restricting international data transfers.[20] Moreover, Section 5 of the IT Act, barring exceptional cases where disclosure of information is required by law or consent is given by the client, provides for maintaining privacy and confidentiality of customers' information by the banks and financial institutions where they have overtly agreed for keeping such information outside the reach of other organizations. Further, the Indian Banks Association's (IBA) code of conduct mentions a section on 'privacy of client's information' which all banks are legally bound to follow. To bolster and promote data protection, and developing security and privacy codes and standards the Data Security Council of India (DSCI), was setup as an independent self-regulatory body by NASSCOM (National Association of Software Companies). Its major formula is that consent should be free, informed, specific, clear, and capable of being withdrawn, and this consent forms the basis for processing personal data and information of clients.[21] Infact, DSCI has enforced best practice for data protection in lines with universal standards, and also addresses emerging disciplines of security and privacy.

United States of America – The federal law in USA which deals with sharing and protecting client's private information is the Gramm-Leach-Bliley Act (GLB Act or GLBA) also known as the Financial Modernization Act of 1999. The GLBA is enforced by the Federal Trade Commission, the federal banking agencies, and other federal regulatory authorities, as well as state insurance oversight agencies.[22] In addition to all financial industry laws and regulation, the major credit card companies require businesses process, store or transmit payment card data to comply with the Payment Card Industry Data Security Standard (PCI-DSS).[23] The GLBA keeps stringent mandate over the banks and financial institutions to

[19] Hari Subramaniam et al., Is there any sector specific legislation that impacts data protection, India: Data Protection 2019 (July 20, 2019, 06:12 PM), https://iclg.com/practice-areas/data-protection-laws-and-regulations/india.

[20] Ashwini Sahu et al., Data Protection and Privacy Laws, India: Privacy of Client Data (July 16, 2019, 01:11 PM), https://www.centerforfinancialinclusion.org/india-privacy-of-client-data.

[21] Manas Ingle et al., Consent, Personal Data Protection Bill, 2018 (July 17, 2019, 07:12 PM), http://www.mondaq.com/india/x/730964/data+protection/Personal+Data+Protection+Bill+2018+An+Overview+With+Brief+Analysis.

[22] Juliana De Groot, A definition of GBLA Compliance, What is GBLA Compliance? Understanding the data protection requirements of the Gramm-Leach-Bliley Act in 2019 (July 20, 2019, 04:53 PM), https://digitalguardian.com/blog/what-glba-compliance-understanding-data-protection-requirements-gramm-leach-bliley-act.

[23] Steven Chabinsky, Is there any sector specific legislation that impacts data protection, USA: Data

restrict transfer and sharing of customers' Non-Public Personal Information (NPI). Further, the Safeguard Rules requires the banks and similar institutes to create written information security plan for its customers. In order to satisfy the GLBA, the Safeguard Rules also mandates the financial institutions to perform special employee management and training, among other requirements, for maintaining privacy of customers' information. The USA also have a separate legislation dedicated to frauds related to credit cards, called as Fair and Accurate Credit Transactions Act (FACTA), where it majorly imposes obligations on financial institutions and banks to institute programs to detect and ratify Identity theft cases.

European Union - On May 25, 2018, EU implemented European Commission's General Data Protection Regulations (GDPR) for data protection, with imposition of responsibilities on financial institutions of protecting sensitive personal data of their customers. According to GDPR, banks strictly needs consent to processing a customer's personal data with showing a "legitimate interest" in the data collected. The banks and financial institution under the regulations are obligated to take onus of data breaches that take place, accidental or otherwise, with complete transparency.[24] The GDPR has standardized various protections for consumer and personal data of EU citizens across EU member states.[25] Article 5 of the GDPR is the one which narrates the principle of personal data, providing lawful, fair and transparent manner of processing of personal data. The data collected can't be used for an ulterior purpose inconsistent with the reason behind its collection.[26]

Technological Evolution

New technology is increasingly being used by firms and institutions to enhance data protection and better control compliance-related costs. In order to restrict the access to sensitive information and keeping track of who has access to what information, the financial institutions and banks are investing more in identity management of the customers and clients. Moreover, nowadays financial institutions focus on simplifying data protection and controlling costs driven by the advent of new computing models, the deluge of backup applications, and the multitude of network choices because the complexity of data protection has increased for all organizations.[27]

With the pride of world's largest economy, USA also carries the stigma with largest data breaches in various organisations, with at least *12 incidents in past 15 years* involving the personal information of millions of customers being compromised.[28]

Protection 2019 (July 18, 2019, 07:11 PM), https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa.

[24]Ipswitch, Financial Services Data Transfers and GDPR (July 19, 2019, 11:13 PM), https://www.ipswitch.com/Ipswitch/media/Ipswitch/Documents/Resources/Whitepapers%20and%20eBooks/WP-FT-Financial-Services-Data-Transfers-and-the-GDPR.pdf?ext=.pdf.

[25] Mike Ulanski, What is it? , Full Analysis: The General Data Protection Regulation (July 20, 2019, 06:22 PM), https://marketing.wtwhmedia.com/full-analysis-the-general-data-protection-regulation/.

[26]Salami Emmanuel Akintunde, Principles, An analysis of the General Data Protection Regulation (EU) 2016/679 (July 20, 2019, 10:43 PM), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2966210.

[27] Santosh, supra, 14.

[28] Graham Buck, Biggest data protection breaches, Data privacy: 2018's technology and regulatory focus

Some technologies increasingly used by banks and financial institutions -

Distributed Ledger Technology - Distributed ledger technology (DLT) is a digital system in which the transactions and their details are recorded in multiple places majorly used for recording the transaction of assets unlike traditional databases, distributed ledgers have no central data store or administration functionality.[29] DLT has apparent potential to enhance efficiencies, resilience and reliability for a variety of financial sector players and infrastructures. [30]

Artificial Intelligence - Nils J. Nilsson has provided a useful definition: "Artificial intelligence is that activity devoted to making machines intelligent, and intelligence is that quality that enables an entity to function appropriately and with foresight in its environment."[31] The major Goals of AI is to implement Human Intelligence in Machines by creating systems that understand, think, learn, and behave like humans.[32] Using artificial intelligence techniques in the provision of financial services can increase efficiency, reduce costs, enhance quality, raise customer satisfaction levels and boost financial inclusion, mainly thanks to the possibilities they offer for automating operating processes and increasing analytical capacity.[33] AI has helped the field to grow, blossom, and advance at an ever-accelerating pace.

Big Data[34] - Big Data analytics is a method for analyzing large data patterns to reveal patterns, trends, and associations. Current technologies for e.g. - cloud services, the Internet of Things and Big Data – as well as future technological innovations and increased connectivity through 5G networks, are all examples of technologies which can deliver enormous benefits, but along with risks for data subjects.

Cloud Computing[35] - Cloud computing was defined by the UNCTAD Information Economy Report 2013 for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with on-demand self-service provisioning and administration. The cloud computing industry had already achieved a global market worth of *$127 billion* in 2017. Cloud services do not present unique and different

(July 16, 2019, 08:00 PM), https://capital.com/data-privacy-2018-s-technology-and-regulatory-focus.

[29] Margaret Rouse, Distributed Ledger Technology (July 15, 2019, 11:05 PM), https://searchcio.techtarget.com/definition/distributed-ledger.

[30] Harish Natrajan et al., Technological Challenges, Distributed Ledger Technology (DLT) and Blockchain (July 20, 2019. 12:49 PM), http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf.

[31] Peter Stone et al., Defining AI, Artificial Intelligence and life in 2030 (July 17, 2019, 05:23 PM), https://ai100.stanford.edu/sites/g/files/sbiybj9861/f/ai_100_report_0906fnlc_single.pdf.

[32] Rossoue B., Goals of AI, Artificial Intelligence (July 17, 2019, 05:45 PM), https://www.tutorialspoint.com/artificial_intelligence/artificial_intelligence_tutorial.pdf.

[33] Ana Fernandez, Introduction, Artificial Intelligence in Financial Services (July 17, 2019, 06:30 PM), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3366846.

[34] UNCTAD, Data Protection Regulations and international data flows: Implications for trade and development (July 17, 2019, 08:11 PM), https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.

[35] Ibid.

issues in data protection, rather they considerably enhances the complex nature of the current issues, especially with regards to cross-border data transfer.

Cyber Threats

The 21st century is the century of Big Data and advanced information .The government agencies are routinely using technologies which allow them to collect, store and share large quantities of data, which includes telephonic conversations, electronic payments among others. Further various business firms and financial institutions are storing personal data of their customers. This all is being done when the meaning of data privacy is under considerable controversy. The increasing technological power with a bad combination of declining clarity on agreement of privacy have no doubt created problems concerning law, policy and ethics.[36] *The Information Technology Act 2000* [37] *provides some sort of relief to Indian citizens yet there have been instances of leaking of Aadhaar information. For instance, when UIDAI while filing a criminal complaint suspended all Aadhaar based transactions by 3 entities namely, Axis Bank, Suvidhaa Infoserve and eMudhra for attempted unauthorized authentication and impersonation by illegally storing Aadhaar biometric data. Such breach was caught when a single individual performed 397 biometric transactions on these 3 platforms using a single fingerprint.*[38]

There have been some examples of such breaches globally as well. For instance in 2017 "Wanna Cry ransomware" netted 52 bitcoins or about 130000$. A group of hackers 'Shadow Breakers' breached the spy tools of the elite NASA-linked operation the 'Equation Group'. Further, they also released a sample of stolen data from NASA, whose decrypted key they offered to sell against bitcoins trade.[39] *Another group of hackers even hacked the Central Intelligence Bureau, USA publishing 8,761 documents stolen from the CIA.*[40] In June 2011, Citigroup U.S. reported that hackers were able to gain unauthorized access to personally identifiable information such as customer names, account numbers, and contact information of *360,083 customers*.[41] Citigroup Japan suffered a similar breach affecting *92,400 customers*.[42] Loss to bank by an insider traitor was again reflected when the Bank of America suffered a massive breach of atleast *US$10 million* even customers' data were sold criminals.[43] *Infact, these* banks and financial services

[36] Jeroen van den Hoven et al., Conceptions of Privacy and the value of privacy, Privacy and Information Technology (July 20, 2019, 11:53 PM), https://plato.stanford.edu/entries/it-privacy/.

[37] Information Technology Act, 2000.

[38] Komal Gupta et al., UIDAI temporarily halts Aadhaar Payment by Axis Bank, two others, LiveMint, February 28, 2017, at https://www.livemint.com/Industry/73F92SKvUKxyngjfx7O0aJ/UIDAI-temporarily-halts-Aadhaar-payments-by-Axis-Bank-two-o.html.

[39] Andy Greenberg, Hackers Claim to Auction Data They Stole From NSA-Linked Spies, (July 18, 2019, 05:26 PM), https://www.wired.com/2016/08/hackers-claim-auction-data-stolen-nsa-linked-spies/.

[40] Lily Hay Newman, The Biggest Cybersecurity Disasters of 2017 So Far (July 18, 2019, 06:00 PM), https://www.wired.com/story/2017-biggest-hacks-so-far/.

[41] Maria Aspan el al., Citi says 360000 accounts hacked in may cyber attack, Reuters, June 16, 2011, at https://www.reuters.com/article/us-citigroup-hacking/citi-says-360000-accounts-hacked-in-may-cyber-attack-idUSTRE75F17620110616.

[42] Citigroup data theft hits 90,000 in Japan, The Daily Star, August 07, 2011, at https://www.thedailystar.net/news-detail-197570.

[43] Robert McMillan, Insider data theft costs Bank of America $10 million (July 18, 2019, 11:15 AM), https://www.computerworld.com/article/2508552/insi

organizations were the targets of *25.7%* of all malware attacks in 2018 which is more than any other industry.[44] Direct losses due to cyber-attack are generally unrelated to the size of the financial institution targeted.
Majority of banks' and financial institutions' operations take place with the use of technology and without concrete cyber security measures such operations and transactions are under severe danger.

Here are the five biggest threats to a banks' cyber security -[45]

1. ***Unencrypted Data*** *– When the data is not converted into secured code, the data would be prone to unauthorized data access. Hence all data stored at financial institutions should always be encrypted, by this, even if the data is stolen, the hackers can't immediately use them.*

2. ***Malware*** *– The bank's data security comes under great risk, every-time they are connected with end user devices (such as computers and cells) which possess malware in them.*

3. ***Third Party Services that Aren't Secure*** *– The most genuine mistake a bank would commit, is when in order to provide better services to their customers, they employ third party services. Sensitive data may be at risk in such situations if the third party services don't possess authentic cyber security measures.*

4. ***Data That Has Been Manipulated*** *– Without stringent cyber security systems, the financial institutions are prone to serious data manipulations by the hackers. Under this attack, the hacker don't steal the data, but rather change it, and such an attack is difficult for the financial institutions to detect and ultimately causing million dollars of damages.*

5. ***Spoofing*** *- A newer type of cyber security threat is spoofing in which hackers impersonate a banking website's URL with a website that looks and functions exactly the same.*

The World Economic Forum in collaboration with McKinsey, conducted a study which suggests that "if the pace and intensity of attacks increase and are not met with improved defenses, a backlash against digitization could occur, with large negative economic implications". They estimate that "over the next five to seven years $9 trillion to $21 trillion of economic value creation, worldwide, depends on the robustness of the cyber-security environment".[46]

Balancing Innovation with Data Privacy and Information Governance

The dignity of the human person, and a healthy community, can be protected only if the expansion of economic opportunity is

der-data-theft-costs-bank-of-america--10-million.html.

[44] Zeljka Zorz, Which cyber threat should the financial institutions be on the lookout for? (July 19, 2019, 08:00 AM), https://www.helpnetsecurity.com/2019/04/30/2019-cyber-threats-finance/.

[45] Stan Jaslar, The 5 biggest threat to a bank's cyber security (July 18, 2019, 07:19 PM), http://www.sqnbankingsystems.com/sqn-blog/the-5-biggest-threats-to-a-banks-cyber-security.

[46] Natasha Nelson, Cyber risk management, How companies achieve balance between technology enables innovation and cyber-security (July 18, 2019, 03:11 PM), http://web.mit.edu/smadnick/www/wp/2016-01.pdf.

balanced with human rights and respected mutual responsibilities.

- Bishop Paul Tighe, Secretary of the Pontifical Council for Culture, The Vatican.

The global flow of digital data has risen dramatically over the last three decades from close to zero to more than a zettabyte (one trillion gigabytes) globally. A 2017 paper by the International Data Corporation estimates that by 2025, the world "will create and replicate *163ZB of data*," which would be a tenfold increase over 2016.[47] *Recent incidents like Cambridge Analytica appropriating Facebook's data and other similar security breaches where personal data of customers is transferred from private entities, clearly shows the loophole in data portability which is undermining people's privacy.*[48]

The core of banking is to protect personal data from fraud which means safeguarding customers' financial assets. The digitization of financial details has triggered for true data-driven activity, where rather being a liability, data is source of value for customers.

However, the aim must be to achieve both, i.e., economic growth with innovative solutions for clients and fundamental right to privacy, and there must be balance between data privacy and financial institutions, instead on keeping them at odd ends.[49]

Hence, for banks and financial institutions the major challenge is to allow disclosure of data to support technological advancements, and also providing security to sensitive personal information, to counter privacy concerns of the customers.[50] *For this, first data privacy principles ever adopted were called "Fair Information Practices" (FIP), which provides for openness and disclosure of information alongwith a set personal data security framework.*[51]

Financial institutions need to affirm the regulators and shareholders that they carry active programs to prevent financial crime and also having a robust mechanism to manage the monetary and financial risks associated with financial crime.[52]

These days banks and financial institutions use a giant tech ecosystem with partners, sharing data to build better digital experiences for the customers, which puts serious questions on privacy but without much legal guidance and rules on assuring and maintaining data privacy, they are

[47] David Reinsel et al., From Business Background to Life-Critical, Data Age 2025: The Evolution of Data to Life-Critical, (July 15, 2019, 10:34 PM), https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/workforce/Seagate-WP-DataAge2025-March-2017.pdf.

[48] Jeni Tennison, Balancing Act: Innovation vs. Privacy in the age of Data Portability (July 19, 2019, 12:42 PM), http://thegovlab.org/balancing-act-innovation-vs-privacy-in-the-age-of-data-portability/.

[49] Matthew Blake et al., Customer Data Challenges, The Appropriate Use of Customer Data in Financial Services (July 18, 2019, 11:12 PM), http://www3.weforum.org/docs/WP_Roadmap_Appropriate_Use_Customer_Data.pdf.

[50] PDPC Singapore, Balancing Innovation and Personal Data Protection (July 19, 2019 02:00PM), https://www.pdpc.gov.sg/-/media/Files/PDPC/New_DPO_Connect/oct_15/pdf/BalancingInnovation.pdf.

[51] SAS India, Big Data Privacy (July 20, 2019, 09:08 PM), https://www.sas.com/en_in/insights/articles/data-management/big-data-privacy-four-ways.html.

[52] Steve Culp, For banks, better data management means more effective fraud and crime prevention (July 20, 2019 09:38 PM), https://www.forbes.com/sites/steveculp/2014/06/06/for-banks-better-data-management-means-more-effective-fraud-and-crime-prevention/#7b05334420a7.

forced to take the self-regulation route just like the crypto-currency businesses.[53]

All the discussions about privacy are knitted with the use of technology. Initially Samuel D. Warren and Louis Brandeis wrote an article on privacy[54] protesting against the intrusive activities of the journalists and arguing for "right to be left alone" and the principle of "inviolate personality". Hence, after the publication of this article, for the first time the debate about privacy had erupted, considering the conflict between one's right to decide the extent of his details being shared and the right of others in the society to know about individuals.

Breach and Regulation

Indian Perspective

International recognition has been given to Right to privacy under Article 8 of European Convention and Article 12 of Universal Declaration of Human Rights. The foundation of right to privacy is on line of dignity and not secrecy.[55]Over the last few decades in India, under Article 21 of the constitution, the "right to privacy" has emerged as a well-established right. A plethora of judicial decisions, such as *Kharak Singh v State of Uttar Pradesh*[56] *People's Union for Civil Liberties v Union of India*[57], and *Gobind v State of Madhya Pradesh*[58], rendered by the Supreme Court in the country have contributed to the recognition accorded to the right to privacy.[59]

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*[60], in this case Punjab National Bank had issued a duplicate passbook of a joint savings bank account, which held between the petitioner and her husband, to an unauthorized person. In this case while awarding compensation to the petitioner the Delhi State Consumer Disputes Redressal Commission, 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. Another case where the Court held that the Bank had been negligent in operating sensitive data and hence awarded compensation to the customer is *Umashankar Shivasubramanian v. ICICI Bank*.[61]

Even after so many developments and technological growth India still lags behind to cybersecurity and data protection in comparison to the more technologically advanced countries of the world. Recently,

[53] Arpit Ratan et al., An approach to data privacy for Indian banks and financial institutions (July 20, 2019 02:23 PM), https://blog.signzy.com/an-approach-to-data-privacy-for-indian-banks-and-financial-institutions-a8b9681dade1.

[54] Jeroen, supra, 32.

[55] Shraddha, Justice K.S. Puttaswamy v. Union of India and Ors: A Critical Analysis, What impact the recent right to privacy judgment will have on recent law? (July 15, 2019, 04:22 PM), https://blog.ipleaders.in/right-to-privacy-judgment-impact/.

[56] Kharak Singh vs. State of U.P. and Others, AIR 1963 SC 1295.

[57] People's Union for Civil Liberties vs. Union of India and Another, 1997 (1) SCC 301.

[58] Gobind vs. State of Madhya Pradesh and Another, (1975) 2 SCC 148.

[59] Manisha Shroff et al., Data Privacy: Have banking laws in India have kept pace with technology? (July 14, 2019, 11:01 PM), https://www.khaitanco.com/PublicationsDocs/IndiaLawNews-KCOcoverageManishaShroff-Copy%20(2).pdf.

[60] Punjab National Bank v Rupa Mahajan Pahwa, 2015 SCC OnLine NCDRC 3008.

[61] Nikita Nehriya et al., Enforcement, Data privacy in the banking sector: Striking a balance (July 14, 2019, 11:11 PM), https://bankingfrontiers.com/data-privacy-banking-sectorstriking-balance/.

the Supreme Court of India, in *Justice Puttaswamy (Retd.) and Anr. v. Union of India and Ors.*,[62]upheld the overall validity of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (the "**Aadhaar Act**").

A total 50 incidents of cyber-attacks affecting 19 financial organizations have been reported from November 2016 to June 2017.[63] These attacks have been reported majorly on payment gateways or digital payment interfaces which include e-wallets like Paytm, Jio-Money, etc. and these incidents have only been reported in relation to the financial sector with many unreported incidents also took place in other sectors. Further, the country has witnessed a total of 1.71 lakh cyber-crimes in the last three and half years, which is at least one cyber-attack being reported every 10 minutes.[64] In the year 2012 about 112 government websites, including those of Bharat Sanchar Nigam Ltd, Planning Commission and Ministry of Finance, were hacked in the period of just three months.[65]

Globally companies have developed comprehensive regulatory frameworks to protect an individual's rights and sensitive information of clients. Considering the lack of proper legislation dedicated to protection of data privacy in the nation a Committee under the Chairmanship of Justice B. N. Srikrishna was setup in July 2017 to examine various issues related to data protection in India, and to recommend methods to address them and ultimately suggesting a draft data protection Bill.[66]After one year committee came up with the Personal Data Protection Bill, 2018 dedicated towards a security regime for sensitive, private and confidential data, being applicable on both individuals and businesses. The bill has been broadly based on the lines of GDPR recently notified in European Union and landmark judgment of the Supreme Court of India declaring right to privacy as a fundamental right. The bill has given a very wide definition to sensitive personal data which also includes financial data among others.[67] The Bill regulates the processing, transferring, collection and sharing of personal data within India. It will also apply to foreign data being stored or processed in India.

International Perspective

The Aadhaar verdict in India has led a tremendous change in the mindsets of citizens regarding privacy and data

[62] K.S. Puttaswamy (Retired) and Another vs. Union of India and Another, (2019) 1 SSC 1.

[63] Keshav Batra, Total of 50 cyber-attack incidents reported in financial sector: Govt, The Indian Express, August 1, 2017, at https://indianexpress.com/article/technology/tech-news-technology/50-cyber-attack-incidents-reported-in-financial-sector-govt-4777350/.

[64]Chethan Kumar, One cybercrime in India every 10 minutes, The Times of India, July 22, 2017, at https://timesofindia.indiatimes.com/india/one-cybercrime-in-india-e very-10-minutes/articleshow/59707605.cms.

[65] Megha Mandavia, 112 government websites hacked in 3 months: Sachin Pilot, The Economic Times, March 15, 2012, at https://economictimes.indiatimes.com/tech/internet/112-government-websites-hacked-in-3-months-sachin-pilot/articleshow/12270733.cms.

[66] Justice B.N. Srikrishna et al., Note on The Personal Data Protection Bill 2018, A free and fair digital economy protecting privacy, empowering Indians (July 20, 2019, 08:39 PM), https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf.

[67] Suneeth Katarki et al., Categories of Data, The Personal Data Protection Bill, 2018 - Key Features and Implications (July 18, 2019, 09:47 PM), http://www.mondaq.com/india/x/727550/data+protection/The+Personal+Data+Protection+Bill+2018+Key+Features+And+Implications.

infringement. After Aadhaar incident people started questioning the authorities about the security of their personal information. Some more incidents regarding confidential information happened in developed countries like U.S. & U.K. e.g. "Wanna Cry ransomware" , which has already led to a lot of hues and cries because the confidential information of the citizens were at stake.

Recently in United Kingdom (UK), Minister of state for Digital, Culture, Media and Sports (DCMS) spoke about the new Data Protection Law (DPL) which would include the concept of 'Right to be Forgotten' by companies.[68] *The said law would expand the ambit of "Personal Data" to include IP address, internet cookies, and DNA. On the other hand, USA is following a sectorial approach. Sensitive data of its citizen which is grouped in classes on the basis of their utility, and therefore, USA has mixed legislation for Data Protection.*

EU has its own Data Protection Act which is quite advance and has all kinds of laws and regulations to cope up with the requirements of this contemporary world and mitigate infringement of data privacy. Comprehensive data protection and open banking legislation has been enacted in Europe that views protection of data as a human right and violation of the same follows stringent actions. The GDPR reinforces data protection requirements and establishes new individual rights which includes data portability and the right to be forgotten. The new rules give EU citizens far more control over the use and storage of their data and specifies punitive fines, for companies that fail to keep that data safe, up to 20 million euros or 4% of global revenue, whichever is greater.[69]

The United States, regulates all breaches of personal data within industries on a federal level so the Gramm-Leach-Bliley Act applies to financial institutions and to businesses that provide financial products and services. In terms of enforcement, the Federal Trade Commission (FTC) promotes consumers' protection of personal data and can investigate and address a company's failure to comply with their own privacy practices.[70]

Data Privacy Recommendations and Solutions

Today, data privacy laws are having their existence in almost all major countries, and are developing for the upliftment of the customers. The rules and regulations all revolve around data security, accountability, access, data integrity, consent, disclosure, and notice, the stringency levels of these laws and their enforcement differ in different jurisdictions and nations.

The Wall Street Journal reported that, a record of *$355 million* in outstanding credit card debt is now owned by persons who didn't even exist physically as recently as 2017.This type of synthetic identity fraud caused by fictitious people is generating harm by casting doubts on the entire consumer credit ecosystem.[71]

In 2017, financial services were the second most targeted industry of ransomware after healthcare.[72] *EUDPA says that "Personal*

[68]GOV.UK, Government to strengthen UK data protection law (July 16, 2019, 08:44 PM), https://www.gov.uk/government/news/government-to-strengthen-uk-data-protection-law.

[69] Trend Micro, supra, 10.

[70] Matthew Blake et al., supra, 45.

[71] Dean Nicolls, 5 Emerging cybersecurity threats facing financial services (July 16, 2019, 09:11 PM), https://www.jumio.com/5-cybersecurity-threats-financial-services/.

[72] Kaspersky, KSN Report: Ransomware and malicious cryptominers 2016-2018 (July 16, 2019,

data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."[73]

The problem with the Indian IT Act, 2000 is that although it deals with the issue of the data protection and privacy, but not in a holistic manner rather in a partial manner. This clearly reflects a lack of actual framework in the IT Act, 2000 regarding the data protection, quality of cyber security systems and transparency of the data. The challenge faced by banks is that, at on hand they are trying to have to innovative and compelling financial services experiences for the interest of the customer, but on the other hand such innovations invites threat to data privacy for which they need to regulation stringent data privacy policies.

Moreover, in order to help prevent and detect financial crime alongwith major loopholes, banks need both an integrated (and timely) data set and the ability to bring all sophisticated analytics and maintenance to bear on the data to generate useful insights. Three such major elements that comprise this capability are:[74]

A. ***Enhanced data quality*** *– Global banks operating in different regions using multiple data sources for their business, face this data quality issue. Hence to address this major challenge, banks need to prepare themselves to establish central data screening and reconciliation processes, and also improving their data governance.*

B. ***Analytics to transform data into information, and information into insight*** *– Most of the organizations face the problem regarding the lack of the right data and by using data-driven decision-making banks allows themselves to gain a better and smooth understanding of the various physical, societal, financial and commercial aspects of their operating environment.*

C. ***Application of data visualization techniques*** *– With increase in volume and complexity of data, key software providers are adopting data visualization techniques for allowing complex data to be viewed by business experts through a visual interface. This visual view allows investigators to view transactions flow across multiple accounts, to identify new pattern in major financial crime cases.*

The primary goal for all financial institutions is to preserve customer trust and many financial institutions does not currently have a separate privacy office for combating cybercrimes. Institutions must hold an internal "privacy summit" that convenes key stakeholders from the lines of business, technology, compliance, and law to identify and understand what the data is, where it resides, how it is classified, and how it flows through various systems. For example, financial, medical, and PII are subject to different restrictions in different area. Financial Institutions need to develop

---

02:59 PM), https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2018/06/27125925/KSN-report_Ransomware-and-malicious-cryptominers_2016-2018_ENG.pdf.

[73] ICO UK, Sending personal data outside the European Economic Area (Principle 8) (July 17, 2019, 04:55 PM), https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/.

[74] Steve Culp, supra, 48.

appropriate global data-transfer agreements for PII and other data that falls under privacy requirements. Further, they need to recognize and adhere to privacy requirements when developing core business processes and cross-border data flows.[75]

McKinsey and Company recommend another great tactic of "golden record" for approaching data privacy that companies can adopt to become data stewards for every personal-data processing activity in a company to ensure compliance and traceability that goes "beyond documenting the system inventory and involves maintaining a full record of where all personal data comes from, what is done with them, what the lawful grounds for processing are, and whom the data are shared with." With the right records, resources, banks, and financial institutions must also see how they can ensure data privacy into their services and offerings by design and by default.[76]

Financial institutions around the world have adopted the FireEye technology which actually enables firms of all sizes to detect and defend against exploits and advanced attacks that bypass their traditional security measures.[77] The Consumer Financial Protection Bureau's (CFPB or Bureau) Office for Older Americans provides recommendations for banks and credit unions to accompany the Advisory for Financial Institutions on Preventing and Responding to Elder Financial Exploitation, issued simultaneously.[78]

Suggestions

From the above discussion the following suggestions can be made - [79]

1. In India there is a dire need for a constitutional amendment and specific or special law too regarding data privacy and cybercrimes, whereby right to privacy can be guaranteed expressly. Such an amendment and laws are necessary to give recognition to the right to privacy, and to provide a wider and meaningful definition to personal liberty enshrined under Article 21 of the Constitution.
2. We must evolve National Policy to guarantee to individuals their rights to control the collection, disclosure, transfer, process and distribution of their sensitive personal or financial information. The vital component of the policy is to legislate the basic tenets of fair information, ultimately providing them rights such as right to limit data

[75] Andrew Toner, Closer to fine: Separating data privacy from information security (July 16, 2019, 07:43 PM), https://www.pwc.com/us/en/financial-services/publications/viewpoints/assets/fs-viewpoint-data-privacy-and-information-security.pdf?source=post_page.

[76] Daniel Mikkelsen, Tackling GDPR compliance before time runs out (July 15, 2019, 11:13 AM), https://www.mckinsey.com/business-functions/risk/our-insights/tackling-gdpr-compliance-before-time-runs-out?source=post_page.

[77] Fire-eye, Financial Services (July 18, 2019, 03:19 PM), https://www.fireeye.com/solutions/financial-services.html.

[78] Consumer Financial Protection Bureau, Recommendations and reports for financial institutions on preventing and responding to elder financial exploitation (July 20, 2019, 01:09 PM), https://files.consumerfinance.gov/f/201603_cfpb_recommendations-and-report-for-financial-institutions-on-preventing-and-responding-to-elder-financial-exploitation.pdf.

[79] Conclusion and Suggestions (July 20, 2019, 11:14 PM), https://shodhganga.inflibnet.ac.in/bitstream/10603/98806/17/17_conclusion%20and%20suggestion.pdf.

collection, data transfers, and secondary uses of the data among others.

3. Banks and financial institutions should use encryption and multi-factor authentication process.[80] By this, they would have control over the personal information in their database, since encrypted information is safe in transit, on the network, and even in cloud. Further, with multi-factor authentication, having more than one method process of identification to have access to data, would provide an added layer of protection to personal information saved in their database even if the system is being hacked.
4. Banks and financial institutions should engage working with a data risk security advisor, who would help them to evaluate their security system and electronic information, and at the same time would help in identifying and rectifying the weak link of their security system which is prone to cyber threats and data leakage.
5. With regards to the employees of the banks and financial institutions, instead of allowing access to every confidential and private database, the employees should only be allowed the necessary database which falls under the part of his or her work. This has become a major preventive measure, considered numerous cases of breach of privacy where employees shares confidential information with the outside world. Further, the employees should be restricted to use only devices issued by the banks or financial institutions.[81]

If the above suggestions are implemented through appropriate measures and at right place in right manner then, it is sincerely hoped that the right to privacy can be protected more effectively.

Conclusion

Data is the pollution problem of the information age, and protection privacy is the environmental challenge.

- *Schneier Bruce.*
-

India is a very fast growing economy where lots of data and sensitive information is being transferred from one place to other, specifically from India to foreign jurisdictions so there is an urgency of law and legal framework to monitor all such transfer, store and regulation of data. In this cyber world where whole world is a kind of family (Vasudhev Kutumbakam) India do not have an adequate Data Protection Act which becomes a slab and this prevents India to become one of the developed cyber economies.

Till now the only act which deals with some sort of Data protection in India is Information Technology Act but it is a general act and not a special act which covers all the issues regarding protection of data and consumer concerns. Moreover, it is sometimes not able to punish the cybercriminal because of loopholes in it. So, India should introduce a new legislation for Data Protection so that in future no criminal can abscond from the law and justice can be delivered. The cost implications of a data breach from monetary and reputational

[80] Cloud Carib, A layer approach to data security, What can banks and financial institutions can do to increase security (July 20, 2019, 10:04 PM), https://info.cloudcarib.com/blog/what-can-banks-financial-institutions-do-to-increase-security.

[81] Infosec, The Checklist, A security checklist for the financial institutions (July 20, 2019, 11:37 PM), https://resources.infosecinstitute.com/a-security-checklist-for-financial-institutions/#gref.

perspective are increasing exponentially for all financial institutions. Most importantly the risk management team of every financial service institute needs to play a pivotal and active role in shaping policies regarding data security for better results.

The Herjavec Group has predicted that the global annual cost of cybercrime is estimated to increase to around *USD 6 trillion by 2021, from USD 400 billion in early 2015*.[82] Similar estimates can be found by organizations such as Juniper Research and the World Economic Forum, and in a July 2017 report, Lloyd's of London estimates that a single global cyber-attack could result in damages of as much as USD 121 billion.[83] All such data give us serious threats regarding privacy of information and customer rights. Financial services organizations are a critical part of the infrastructure of the world's economy. Like all companies, they need to win new customers and differentiate with innovative products and services.[84] In India the draft of Data Protection Bill, 2018 uses global privacy regimes and lays down key provisions to promote transparency and hold data fiduciaries/organizations accountable for their actions. The Bill allows exemptions for important purposes such as legal proceedings .journalism, research but on the other hand bill could be questioned if there is necessity and proportionality required for infringements to an individual's right to privacy. But some amendments regarding the privacy in finance sector and implementation of the bill is required as the cases infringement of personal information are increasing day by day. So we have to work in this arena for the betterment of society. Moreover, we must acknowledge that innovation and privacy of customers must go hand in hand, it must be like two side of the same coin otherwise India as a nation would never be able to stand globally in developed economies as well as eminent nation which actually give priority to personal rights.

*****

[82] Steve Morgan et al., Digital Growth, Hackerpocalypse: A Cybercrime Revelation (July 20, 2019, 07:11 AM), https://www.herjavecgroup.com/hackerpocalypse-cybercrime-report/.

[83] Trevor Maynard et al., Counting the cost: Cyber exposure decoded (July 17, 2019, 02:19 PM), https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2017/cyence/emerging-risk-report-2017---counting-the-cost.pdf.

[84] Spiros Antonatos et al., Privacy by design for financial services organizations in GDPR era (July 19, 2019, 06:08 PM), https://www.ibm.com/blogs/research/2019/02/privacy-financial-services-gdpr/.