Indexed with IIJIF
Impact Factor : 1.021
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
A Peer-Reviewed Refereed Online Law Journal

INTERNET BANKING AND RIGHT TO PRIVACY: AN OVERVIEW

Dr. Rashmi K.S[1], Jyothi M.N[2]
[1]Associate Professor, [2]Research Scholar,
[1,2]Alliance School of Law, Alliance University, Bangalore.
[2]jyothimattada@gmail.com

INTRODUCTION

This article highlights the merits and demerits of Internet Banking and Privacy right in India based on technology. Banks facilitate investment through organize public savings. The Reserve Bank of India and Government liberalized the banking services which accelerated the growth of Banking sector to promote economic growth and Banking services to promote the growth of the banking sector and to promote economic growth and affluence. From 1990, the technology used more to convert the banking system from branch banking to customer-oriented.

Banking is a sector of the economy which is touching the lives of almost all classes of people. The banking system in India has a multi-layered structure with regional rural banks, rural and urban co-operative banks, commercial banks which includes nationalized banks, private sector banks, and foreign banks.

Technological advancement has made humans life easier, technological advancement like the invention of computers is widely using for numerous drives starting from the individual to large organizations across the globe. The Internet is a network of interconnected computer networks. It is the central component of today's world that enables people to connect and communicate. In today's world, the internet is not a commodity but an essential aspect of life. Every business transaction, as well as communication in general, is done using the internet and allied tools.

MEANING AND DEFINITIONS OF FEW TERMS WHICH REFERRED IN THIS ARTICLE

Bank: there is a difference of opinion in this regard according to some authorities, the word "Bank" itself is derived from the word "Bangus" or "Banque", meaning 'Bench'. One of the early bankers, the Jews in Lombardy transacted their business on benches in the market place. When a banker failed, his 'bench' was broken up by the people. The term "bankrupt" was derived from the breaking of 'Banco'. This is, however, ridiculed by Macleod, who claims that the term bunchier was never used to refer to Italian money changers. There are others, who believe that the word "Bank" is originally derived from the German word "Back" meaning a joint-stock fund, which was Italianised into "Banco" when the Germans were masters of a great part of Italy. This appears to be more possible.[3]

The term "**banking**" means the accepting, for lending or investment, of deposits of money from the public, repayable on demand or otherwise, and withdrawable by cheque, draft, and order or otherwise.

[1] Associate Professor, Alliance school of law, Alliance University, Bengaluru
[2] Research Scholar, Alliance School of Law, Alliance University, Bengaluru
[3] Tannan's Banking Law

Indexed with IIJIF
Impact Factor : 1.021
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
A Peer-Reviewed Refereed Online Law Journal

The term is wide enough to encompass all major transactions involving a bank. Therefore, it also widens the scope of offenses to be brought into the purview of banking frauds.

Electronic Form: According to Section 2(r) of the Information Technology Act, 2000, the words "electronic form", about information, means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer-generated micro fiche or similar device.[4]

Internet Banking: Meaning - the dawn of the Internet has marked the demise of traditional money. Banks have been the forerunner in harnessing the power of technology and are perhaps the biggest beneficiary of this great innovation. Ancient money apart from their notational value had their market worth; for instance, the gold coins or the silver coins were valuable according to their weight as well.

'Mobile payments' is defined as an information exchange between a bank and its customers for financial transactions through the use of mobile phones. It involves debit/credit to a customer's accounts based on funds transfer instruction received over the mobile phones.[5] The system involves the collaboration of banks, mobile payments service providers, and mobile network providers. The mobile payment systems, the banks provide the basic service framework, ensure compliance to KYC/AML norms, create a risk management and mitigation framework, and ensure settlement of funds. The mobile service providers are intermediaries for providing the telecom infrastructure and connectivity to the customers. Banks having a physical presence in India are authorized to offer mobile payment services and are restricted to bank accounts/credit card accounts in India which are KYC/AML compliant. The payment pertains to Indian rupee only. Such services are only available for the account holders of the bank. To facilitate the use of mobile phones for remittance of cash, banks are permitted to provide fund transfer services which facilitate the transfer of funds from the accounts of their customer for delivery in cash to the recipients.

ATM services: ATMs work on online transaction processing (OLTP). The OLTP applications consider the goal of availability, speed concurrency, and recoverability. ATMs are based on 24-hour access to cash, transfer fund between accounts, view account balances and mini statements, pin change options. ATMs in India are also gaining popularity because of the ease of payment and time-saving services. This has urged the RBI to issue directions and rules regarding its use and to avoid its misuse. Thus, the latest one is the New ATM Card Rules (Automated Teller Machine Rules, 2014)

Cybercafe: According to Section. 2(na) of the Information Technology Act, 2000, the words "cyber cafe" means any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public.

Cyber Security: According to section. 2(nb) of the Information Technology Act, 2000, the words "cybersecurity" means protecting information, equipment, devices, computers, computer resources, communication devices, and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

Data: According to Section. 2(o) of the Information Technology Act, 2000, the word "data" means a representation of Information, knowledge, facts, concepts or instructions that are being prepared or intended to be processed in a formalized manner, and maybe in any form(including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

[4] Nayan Joshi- Lawmann's Law of E-Crimes &Frauds-2017-Kamal Publishers
[5] Dr. Talat Fatima/2016/cyber Crimes/Eastern Book Company

Indexed with IIJIF
Impact Factor : 1.021
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
A Peer-Reviewed Refereed Online Law Journal

Intermediary: According to Section. 2(w) of the Information Technology Act, 2000, the word "intermediary", to any particular electronic records means any person who on behalf of another person receives, stores or transmits that record or provides any service for that record and includes telecom service providers, providers, search engines, online payment sites, online auction sites, online market places, and cyber cafes.

Privacy: According to Black's Law Dictionary, the Right to Privacy is a person's right to be free from any interference.

Right to Privacy:

Under Article 21 of the Constitution of India deals regarding right to life and personal life embrace Right to Privacy. The term privacy is an impulsive concept which was needed to be crystallized. Majority Laws like Law of Torts, Criminal Laws, and Property Laws recognize the scope of Article 21 is multi-dimensional Under the Constitution. Many cases are there on the fundamental right but none of the cases were considering privacy as a fundamental right. Privacy was recognised in a landmark case, K.S. Puttaswamy v. Union of India,[6] our Indian judiciary has, gave a distinctive dimension regarding Right to privacy and now, recognized as a fundamental right. After this right to privacy is not only recognised nationally but also recognised internationally under various conventions.

According to Black's Law Dictionary, Right to Privacy means a right to be let alone, the right of a person to be free from any unwarranted interference. Recently, a judgment was delivered by Justice D.Y. Chandrachud that overruled the principles evolved in the Habeas Corpus case in the case of Justice K.S. Puttaswamy and ors. V. Union of India, this evolved as a landmark judgment in the history of India with regards to the status of Right to Privacy.[7]

Informational Privacy is not an absolute right. Informational privacy is a fundamental right that individuals have a right to protect themselves from unauthorized access and use of their personal data. The right to control and to prevent unauthorized access and use of my data is a fundamental right.

EVOLUTION OF RIGHT TO PRIVACY

Ancient India:

Privacy in the ancient Hindus text is a practical concept. Certain matters such as worship, sex and family matters should be protected from disclosure is held under Hitopadesh. Even the ancient Indian text had references to a positive morality. This is because right to privacy was not restricted to a certain level.

This is the reason why Upendra Baxi is worried about the lack of compassion and humanity. Even ancient times had a positive morality.[8]

Modern India:

Right to Privacy was discussed for the very first time in debate of constituent assembly, where an amendment was made by K.S. Karimuddin, where B.R. Ambedkar gave it only conceited support and Right to Privacy was not incorporated in the Constitution of India. Till 1960 Privacy right was not considered as a fundamental right. The Privacy issue was considered as both fundamental right under

[6] (2018) 1 SCC 809

[7] Aarushi Sahu, Evolution of Right to Privacy in India, available at:https://www.legalbites.in/evolution-right-privacy-india/(last visited on Feb. 7, 2019).

[8] Evolution of Right to Privacy, India, available at:https://www.lawteacher.net/free-law-essays/constitutional-law/evolution-of-the-right-to-privacy-constitutional-law-essay.php(last visited on Feb7., 2019).

Indexed with IIJIF
Impact Factor : 1.021
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
A Peer-Reviewed Refereed Online Law Journal

the constitution and also common law right, in 1954 Supreme Court by an eight-judge bench in M.P.Sharma v. Satish Chandra[9] case, dismissed the existence of a right privacy on the basis of the makers of Constitution, while dealing with the power of search and seize documents from the Dalmia Group.[10]

The same right to Privacy issue was again made a comeback after long period of ten years approximately in the case of Kharak Singh v. State of Uttar Pradesh[11] before a six-judge bench of the Supreme Court but it was again rejected to be a fundamental right. It was held that Privacy is not a fundamental right, but it held that night visit violates the personal liberty. Justice Subba Rao, dissented that, Right to Privacy is still an essential component of personal liberty though such provision was not incorporated and declare as a fundamental right under Indian Constitution.[12]

CONSTITUTIONAL PROVISIONS AS TO RIGHT TO PRIVACY UNDER ARTICLE 21 –

No person shall ever be deprived of life or liberty except according to the procedure established under the law as envisaged under Article 21 of the Constitution of India infers the term life that is inclusive of Article 21 includes all those aspects of life which go to make a man's life meaningful, complete and worth living. The Supreme Court has adopted a strategy for expanding the ambit of Article 21 of the Constitution.[13]

Privacy Right came before the Supreme Court in the case of Gobind v. State of Madhya Pradesh[14] before the Three-Judge bench and for the first time Privacy was recognized under Personal Liberty under Indian Constitution. From then Privacy was recognized in fundamental rights. There is no such challenge faced of its existence till 2017. In 2017, in the case of K.S. Puttaswamy v. Union of India[15], before the nine-judge bench the same issue was raised and the court overruled the decision of M.P. Sharma and Kharak Singh decision. In this case it is clearly held that right to privacy is a fundamental right and it will remain the same while considering Article 14 – Right to Equality, Article 19 – Right to Freedom and Article 21 – Right to Life and Personal Liberty.[16]

RESERVE BANK OF INDIA GUIDELINES REGARDING CUSTOMERS' PRIVACY

RBI guidelines on Internet Banking, 2011[17]

Due to every increasing influence of information technology including the internet and core banking systems the RBI realized that almost every bank was at some stage of technology adoption, be it core banking, mobile banking, ATMs, Internet banking, etc. and therefore felt that there was a need to give

[9] AIR 1954 SCR 1077
[10] Supra
[11] AIR 1964(1) SCR 332.
[12] Supra
[13] Hinailiyas, "Right to Privacy under Article 21 and the Related Conflicts" • ,available at:http://www.legalservicesindia.com/article/1630/Right-To-Privacy-Under-Article-21-and-the-Related-Conflicts.html(last visited on Feb. 22, 2019).
[14] 1975 (2) SCC 14
[15] (2018) 1 SCC 809

[16] Decided on 24.09.2017available at: http://www.legalserviceindia.com/issues/topic1609-justice-ksputtaswamyretd-vs-union-of-india.html (last visited on Feb. 22, 2019).
[17] Guidelines on information security, electronic banking, technology risk management and cyber frauds; http://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.PDF

comprehensive guidance regarding these. It was to address this need that the RBI issued these guidelines to deal with issues relating to information security, electronic banking, technology risk and cyber frauds.

Security:

- Security baselines: It is the banks' responsibility to ensure that the minimum security baselines are being followed by their service providers to ensure the confidentiality and security of their customer data.
- Backup records: a cloud computing system must ensure backup of all its clients' information.
- Security steps: An institution may take various steps to ensure that its policies and procedures are in place to minimize risks associated with the handling of sensitive data. This includes identifying and implementing minimum security baselines for all third party providers:
  - Address, agree, and document specific responsibility of the respective parties in outsourcing to ensure adequacy and effectiveness of security practices, including identifying obligations and liability in the event of breach or default
  - Discuss and agree on the instances where customer data shall be accessed and user groups who will have access to the same. Access to a banks' data should be strictly on a need to know basis
  - Ensure that employees are informed about the policies and procedures related to the handling of sensitive data.
- Confidentiality: agreements should ensure that the confidentiality of customer's information is maintained even after the contract has expired or is terminated. Agreement should also contain controls that ensure the protection of customer data in case of unauthorized access or disclosure.

Choice and Consent

- Default termination: Contracts between banks and service providers should include conditions for default termination / early exit option for contracts, may also include situations when a service provider goes bankrupt, goes under liquidation, (whether within India or any other location), or receives judicial indictment for a breach of confidentiality or security.

Security

- Encryption: Use of transaction-enabled mobile banking channels requires encryption controls to ensure security of data in transmission. Normally, a minimum of 128-bit SSL encryption is expected. Banks should only select encryption algorithms which are well established international standards and which have been subjected to rigorous scrutiny by an international cryptographer community or approved by authoritative professional bodies, reputable security vendors or government agencies.
- Fraud Risk Management: It is also necessary that customer confidential information and other data/information available with banks is secured adequately to ensure that fraudsters do not access it to perpetrate fraudulent transactions. Appropriate steps need to be taken to ensure data/information/system security at the Bank. Information security and appropriate access control procedures ensure that only employees who are required to know particular information have access to the same and can put through transactions. Further, a bank's systems need to be adequately secured to ensure that no un-authorised person carries out any system modifications/changes. Appropriate verification procedures should also be incorporated at all channels such as phone banking, ATMs, branches and internet to ensure that only genuine transactions are put through. All

the above security measures should be under continuous review for further strengthening. Details in this regard were covered in chapter on information security.

Gopalkrishna Working Group Report, 2011[18]

In April 2011 the RBI's Internet Banking guidelines were reiterated in the G Gopalakrishna Working group on security in E-Banking. The working group created a report advising banks to implement and follow the privacy policies and procedures established by the guidelines. However, the report is meant to enhance the current guidelines to ensure that electronic banking privacy in India is on a par with international standards. Accordingly, the report recommends changes to the current Indian framework to make it more robust. These are meant to set a common minimum standard for all banks to adopt, as well as lay down the best practices for banks to implement in a phased manner for a safer and sounder banking environment.

A few of the recommendations include:

- Establish a Chief Information Security Officer;
- Create and implement risk assessments;
- Restrict internal and external access to information to a 'need to know' basis while not impeding regulatory access to data/records and other relevant information;
- Put in place strong data security measures;
- Data transfers should be completed electronically rather than manually to avoid data manipulation. Banks should also have a strong migration policy.
- RBI should still be allowed the right to order inspection of the processing centre, the books, and the accounts.
- Banks should put in place a transaction monitoring and surveillance process to identify irregular transactions.
- ATM cards should be chip based to make it more difficult to steal and reproduce data.
- Boards and senior management of banks should ultimately be responsible for managing outsourced operations.
- Banks must be transparent to the regulator about how much information is outsourced, and the terms and conditions of contracts between banks and service providers should be carefully defined.

Legal suggestions made by the committee include:

- Specify punishments for phishing;
- Put in place and strengthen a legal system to ensure that banks are monitoring transactions in compliance with Anti-Money Laundering legislation;
- Redefine 'electronic cheque' under the Negotiable instruments Act;
- Clarify the term 'intermediary' under the IT Act;
- Clarify whether an individual can be bound by transactions entered into via electronic means;
- Appoint agencies to help courts value electronic records. (even if they have not been digitally signed);
- Determine the legal encryption level under the IT Act and establish a committee under section 84A to set rules regulating the use of encryption;

[18] See http://bit.ly/hgjdgt

Indexed with IIJIF
Impact Factor : 1.021
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
A Peer-Reviewed Refereed Online Law Journal

- Ensure that banks are not held criminally and civilly liable for fraud that a customer commits;
- Strengthen the data protection standards found under Information Technology Act section 43A, 72, and 72A. These recommendations have been met with mixed reviews from the public, For example, critics pointed out that the IT Act already provides punishment for phishing attacks, and many worried about the proposal to exempt banks from liability. The report does not provide a comprehensive overview of the various regulations related to banking in India and provides a way forward.[19]

IMPLEMENTATION OF PRIVACY REGULATORY POLICIES WITH RESPECT TO ELECTRONIC BANKING

India, unlike other countries like the United States, does not have specific legislation or a framework regulating and protecting the privacy of financial data. According toCyber Law expert, Mr. Vijayashankar, the concept of confidentiality and the secrecy of financial data has evolved as part of banks' usual practice. The concept of keeping financial data private and secure has evolved over the years. Due to the anti-fraud provisions of the law, banks have started keeping their financial data under lock and key. Thus, privacy (specifically data breaches) is not seen as a protected right (while fraud is) and privacy protection for financial information is established predominantly through individual contracts. These practices, though effective in some circumstances, result in inconsistent and incomplete protection for financial data. Additionally, the lack of enforcement leaves a large gap between policy and implementation.

Under the law, banks are responsible for all transactions involving fraudulent activities. However, in most cases, the onus is usually on the customer. As another example, the KYC norms were developed to detect and prevent money laundering, broadly understood in Indian law as any criminal act that uses the banks as a facilitator. As part of the KYC procedures, banks are required to verify and identify customers, and are responsible for monitoring of their transactions and following up on anything suspicious. In practice, the KYC norms have become a document verification checklist that banks comply with because it's required. Due diligence is rarely given to thoroughly investigating of banking clients, and often the job of following through with the KYC norms is outsourced by banks to another company.

Another weakness of the Indian banking regulatory framework is that the laws have not been amended across the board to take into consideration e-transactions and Internet banking. Therefore, in some cases the same banking regulations that safeguard manual transactions are being extended to electronic ones. This is proving to be inadequate, as privacy risks are higher in the case of electronic transactions. The gaps in the Indian financial regulatory framework have also allowed wide powers of search and seizure to be given to law enforcement and the authorities. Broadly speaking, four bodies have the ability to access financial data. These include the police (but only with case-by-case authorisation), the courts, the Reserve Bank of India, and the intelligence agencies (where authorisation for specific cases is not required).

The inconsistencies in the implementation and structuring of the financial regulatory framework have left individuals vulnerable to privacy violations of their financial data. In India the most frequently reported privacy violation is banking fraud. The increasing number of criminals who use financial information to commit crime raises the question whether the current regulations are adequate to prevent

[19] See http://bit.ly/Ty28NN

Indexed with IIJIF
Impact Factor : 1.021
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
A Peer-Reviewed Refereed Online Law Journal

and punish such crimes. In 2011, the Economic Times reported that as many as 11,195 suspicious transaction reports (STRs) were detected by the Finance Ministry's Financial Intelligence Unit (FIU) between 2006 and 2010.[20] A May 2011 news report revealed that individuals, by working closely with mobile service providers, intercept SMSs that contain the details of financial transactions. These individuals stop any 'alert' SMSs sent from a bank and use a replacement SIM card to send the transaction details to their phone.[21]

Similarly, in June 2011 a scam was discovered in which fraudsters had set up a fake company selling car accessories that offered a discount to buyers who's used a card. When people entered their PINs on their mobile devices, the devices copied the details stored in their card details. This issue highlights the need for regulations and legislation to prevent crime. Subsequently, the card details were used to clone the card, and the PIN enabled the withdrawal of money.[22] At present, as discussed above, Indian banks are not taking responsibility for wrongful withdrawals.[23] In another example, in June 2011 six people were able to hack into an account in the ICICI Bank, Chandigarh, and fraudulently sell INR 94 lakhs worth of shares in the shareholder's name. Similarly, in May 2012 the RBI issued a public statement warning against fraudulent emails being sent to banking customer's under the auspices of a new security platform being adopted by the bank.[24]

These news items raise questions of liability and effectiveness.[25] In response to these inconsistencies, the Financial Sector Legislative Reforms Commission (FSLRC) is considering a single, harmonized and uniform law applicable to all banks and giving the central bank the power to sanction the takeover of a co-operative bank by commercial banks.[26]

TERMS AND CONDITIONS FROM PRIVATE AND PUBLIC SECTOR:

Private and public sector banks in India implement terms and conditions with implications for their customers' privacy. For example: the private bank ICICI has established a policy that allows the bank to share all information relating to a client's application with other ICICI Group companies, banks, financial institutions, credit bureaus, agencies, statutory bodies, tax authorities, central information bureaus, and other persons as ICICI Bank and its Group Companies deem necessary or appropriate as may be required for use or processing of the information. Furthermore, under the terms the ICICI Bank and its group companies will not be liable for how that information is used. This contract is non-negotiable and can be changeable at any time at the will of the Bank.[27] These terms encompass the various banking laws and also refer to any future bodies that the legislature may create. Public sector banks are regulated by statute and owe their customers a duty of secrecy. For instance, under The State Bank of India Act, 1959 prohibits banks from sharing any information about their clients except in accordance with their duties and practices. The bank cannot share any information about its clients

[20] See http://bit.ly/QwqFwk
[21] See http://bit.ly/iZoziA
[22] See http://bit.ly/kDSqWF
[23] See http://bit.ly/RM1z10
[24] "RBI warns against fraud email", *Economic Times*, May21, 2012, http://bit.ly/P1A6FR20(last accessed on June 16, 2019).
[25] http://bit.ly/kvzrdS
[26] http://bit.ly/PTOUWh
[27] See http://bit.ly/P7xRzj

Indexed with IIJIF
Impact Factor : 1.021
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
A Peer-Reviewed Refereed Online Law Journal

except in accordance to the law and when necessary and appropriate.[28] These privacy policies have to comply with all of the laws as discussed above.

SUGGESTIONS AND CONCLUSION

Considering ourselves a part of a society, we often countermands that we are individuals first and in this world each and every person or individual need his/her private space. So as to give each individual the right to enjoy their private moments without the prying eyes of the world. Right to privacy is a basic right that is applicable to everyone under the Indian Constitution. It is not an absolute right but it can be subjected to certain restrictions. Right to privacy does not always mean absolute right. It can be subject to certain restrictions that are necessary to prevent crime and public disorder but, it can also be derived from a contractual relationship or a political one.

This right is very important for banks and their clients. Due to the nature of the world we live in, the protection of our privacy is very important. It should not be compromised to the extent that it should be given to everyone. Privacy should not be restricted in every aspect. However, it is subjected to various restrictions under the provisions of the Constitution of India and other applicable laws. One needs to understand that Privacy should be kept in mind while dealing with the world. It should not be used to explain to the rest of the world..

From the discussions that have been it may be suggested that:

Suggestions for the protection of Privacy Right of the Electronic Banking customers given by the researcher by analysing the Right to Privacy and Regulatory Policies of the RBI Committees are as follows:

- Curb the lack of standards for information sharing between financial institutions by adopting proper mechanism.
- Mechanism should be set-up for distinguishing between types of financial data collected and shared during transactions.
- Proper system should be adopted to curb the standards for prohibiting obtaining customer information by false pretences.
- Banks should require issuing comprehensive notices to customers.
- Mechanism should set-up for clear legal redress for individuals.
- Legislation pertaining to Finance should contain adequate security safeguards as according to the security procedures for financial institutions provided by RBI Guidelines.
- Harmonized protection for online and offline data should to provided by banks.

[28] State Bank of India (Subsidiary Banks) Act 1959 s. 52.