Financial Data Protection in Indian Regulatory Policy: From 'Secrecy' and 'Confidentiality' to 'Privacy'

—Shohini Sengupta*

This article discusses the history and etymology of bank secrecy laws in England and United States, and its impact on financial legal jurisprudence in India. The article demonstrates that bank secrecy laws have been marred by several exceptions. This has consequently led to the development of both conceptual and linguistic ambiguity over financial data protection, evidenced both in judicial decisions and financial policies issued by the Reserve Bank of India. The article explores the harms of conflating secrecy and confidentiality with privacy, in the context of emerging literature on the dangers of excessive data collection in a digital financial ecosystem fostered by fintech companies. While exploring the new world order brought about by the onset of the novel corona virus pandemic in 2020, the article argues that there is an urgent need for RBI to welcome a distinct data protection law to protect financial consumers in India, instead of seeking exemptions from it.

***Keywords**: Financial data protection, fintech, bank secrecy, confidentiality, Reserve Bank of India.*

I. Introduction

"In reading the law, it is constantly necessary to remember the compositional, stylistic and semantic mechanisms which allow legal discourse to deny its historical and social genesis. It is necessary to examine the silences, absences and empirical potential of the legal text and to dwell upon the means by which it appropriates the meaning of other discourses and of social relations themselves, while specifically denying that it is doing so. It is, in short, politically necessary to take seriously the character of law as a social discourse."[1]

* BA LLB (Hons) (NLIU, Bhopal); MSc Law and Finance (University of Oxford), Assistant Professor of Research, Jindal School of Banking & Finance (JSBF).

1 Peter Goodrich, 'Law and Language: An Historical and Critical Introduction.' (1984) 11(2) Journal of Law and Society 173, 200 <www.jstor.org/stable/1410039>.

The 'sorites paradox' which originated in an ancient puzzle is an interesting linguistic experiment to determine the impact of terminology in philosophy. The paradox uses by example, certain vague terms like 'heap'- words with unclear or vague boundaries. The central question here is what makes something a heap- one grain of wheat, or two grains of wheat, and so on, till it leads to an absurd conclusion that no number of grains of wheat make a heap.[2] In most cases, law tries to solves this problem by placing the meaning of the word in a specific context, or in a certain legal system, using the wisdom of judges.[3] The sorites paradox can however present itself in varied forms. As this article goes on to demonstrate, with continued linguistic ambiguity, or conflation of different words, however seemingly similar, there is a profound impact on the development of legal principles, and consequently on people. Therefore, there is a need for creation of clear legal standards that reduce the obfuscations in legal regulatory language and prevent the paradox from being taken to its natural absurd conclusion.

The etymology of the word 'privacy' in England and the United States (US), and its consequent impact on financial and banking law jurisprudence in India is an interesting case in point. In India, as the article will demonstrate, the word 'privacy' has often been conflated with words such as 'secrecy' and 'confidentiality.' This is in spite of the fact that as early as 1890, 'privacy' was envisaged to be not simply a right arising out of contracts or a breach of confidence but as "rights as against the world."[4] It was found that the doctrines of contract and of trust were inadequate to support the required protection, and the law of torts must be resorted to. The right of property in its widest sense, including all possession, rights and privileges, and hence embracing the right to an inviolate personality, alone affords that broad basis upon which the protection which the individual demands can be rested.[5] As such, modern conceptions of privacy are a testament to the multifarious conceptions of privacy through the ages, of its myriad forms, extent, and consequently harms from its breach.

Financial privacy, consequently, should be a variant of a general right to privacy, available to consumers of all financial products and services, protecting them from unlawful access to their financial accounts by private and public bodies, and the unlawful disclosure, sharing, or commercial use of their financial information.[6] In India, the ambit of financial privacy relies, to a large extent, upon a plethora of technology and financial laws. The Information Technology

---

2 'Sorites Paradox', *The Stanford Encyclopedia of Philosophy* (1997) <https://plato.stanford.edu/entries/sorites-paradox/>.

3 'Law and Language', *The Stanford Encyclopedia of Philosophy* (2002) <https://plato.stanford.edu/entries/law-language/#VaguLangLaw>.

4 Samuel D. Warren and Louis D. Brandeis, *'The Right to Privacy'* (1890) 4(5) Harvard Law Review 193, 213.

5 Ibid., 211.

6 'Finance and Privacy' (Centre for Internet & Society) <https://cis-india.org/internet-governance/finance-and-privacy.pdf>.

(Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (IT Rules) are particularly important in this regard since they define "sensitive personal data or information", and include as personal information, data relating to passwords, financial information such as bank data, credit history, payment instrument details etc[7]. Therefore, the reach of financial privacy law(s) should include both public and private financial institutions, including regulators, Government bodies and ministries, financial institutions like banks, insurance companies, pension funds and credit information registries, in addition to several other like bodies.

However, for India, the entire gamut of financial information would far exceed just the stated bodies above and the strict boundaries of what constitutes 'personal information' under the IT Rules. A lot of financial information is collected either by non-financial bodies, or collected in conjunction, as a motley data set, along with other kinds of personal information. Financial information thus is typically collected *en masse* along with biometric data, gender, caste, health, telephonic and other non-financial data. Further, a number of government owned entities such as public sector banks and state co-operative banks are frequently used as delivery vehicles for carrying social welfare goals such as opening zero balance accounts, state-funded insurance, and pension plans. This *en masse* collection of data, financial and otherwise, is also possible because of near ubiquitous mandating or proliferation of the use of Aadhaar in India, which now forms the primary focus of a centralised digital identity and data collection system.[8] Any regulation of financial data in India would have to be connected with matters of both personal financial and interrelated non-financial information. Therefore, one can only imagine the import of a financial data protection law, even as a subsequent sub-set of a general data protection law in India.

In spite of that, the language of financial law and financial consumer protection policies, particularly within the realm of banking regulations, appears to often conflate 'privacy' with 'secrecy' and 'confidentiality.' This article will explore some of these financial legal policies in more detail, in an attempt to expressly state the harm from using these words synonymously, and thereby reducing the import of 'privacy' in financial transactions. While financial data protection would be concerned with financial consumers across multiple financial institutions and markets, this article, for the sake of deliberate simplicity and convenience, only delves into financial data protection for consumers of banking functions,

---

[7] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, r 3 <https://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf>.

[8] Pam Dixon, 'A Failure to "Do No Harm" - India's Aadhaar Biometric ID Program and its Inability to Protect Privacy in Relation to Measures in Europe and the U.S.' (2017) 7 Health Technology 539-567, pp. 542, 544, 558, 561 <https://doi.org/10.1007/s12553-017-0202-6>.

both as a part of traditional banking companies in India, as well as contemporary fintech firms offering banking services.

In doing so, the article in the first part has attempted to introduce the present context in which financial data protection regime presents itself in India. In the succeeding (second) part, the article has charted the introductions to bank secrecy laws in common law jurisdictions, and the exceptions crafted by courts in an attempt to understand the origins of financial privacy in particular. In the third part, the article details the principles adopted by Indian courts in this regard, and the prevalent legal norms in the absence of a general or sector specific data protection law in the country. In the fourth part, the article analyses some of the recent banking and other legal-financial policies issued by the Reserve Bank of India (RBI), in order to demonstrate the continuance of the conflation of the right to 'privacy' with the obligation of banks and financial institutions to maintain 'secrecy' and customer 'confidentiality.' In the fifth part, the article cites some recent trends in fintech and international financial privacy literature, including evolving literature on the economic value of privacy protecting legislation. In the sixth part, the article will conclude by specifying the need to clarify the position of financial data protection clearly in enforceable law, taking into account the surrounding contours of financial policy in India, and specific challenges to it.

II. Common Law and Financial Privacy: Evolution of the Right of Bank Secrecy and Confidentiality

Common law, for the longest time, imposed a general contractual obligation of confidentiality on bankers to protect customer data. This common law rule of confidentiality was in itself quite significant because a bank account was always held to be a repository of important information about an individual or a business, including for example, the price of a depositor's house, their purchases, ascriptions to religious, political or charitable causes etc.[9] This was also in the larger context of the development of the 'right to privacy' to include the 'right to be let alone'[10], and the Supreme Court's decision in the United States to grant individuals a right to sue for the "invasion of privacy."[11] For all of these reasons, the obligation imposed on bankers was significant in even helping protect businesses, who could lose their strategic position if certain data was leaked to competitors.

However, over time, certain grounds of disclosure of 'secret' or 'confidential' information was deemed necessary. Finally, it was in the landmark case of

[9] *California Bankers Assn. v P. Shultz* 1974 SCC OnLine US SC 66 : 39 L Ed 2d 812 : 416 US 21, 79 (1974) (Douglas J., dissenting).

[10] Samuel D. Warren and Louis D. Brandeis, *'The Right to Privacy'* (1890) 4(5) Harvard Law Review 193.

[11] L.R. Fischer, *The Law of Financial Privacy* (1983) 5-7.

Tournier v National Provincial and Union Bank of England [12] that the Court of Appeal in England laid down the definitive law on banker's duty of confidentiality to a customer. However, the Court also laid down four exceptions to this rule: 1) disclosure under compulsion of law; (2) disclosure arising from a duty to the public; (3) disclosure to protect the bank's interest; and (4) disclosure by the express or implied consent of the customer. These exceptions were enunciated in light of the fundamental question raised before the Court over the degree to which a banker's duty of confidentiality to a customer extended. Here the Court held that even if the duty of confidentiality or non-disclosure was a legal duty, it was subject to a larger exception that "the banker may do what is necessary for the protection of his own interests."[13] In light of very broad considerations of what was considered necessary for a banker to protect her interests, these exceptions were carved.

As such, the contours of bank secrecy/confidentiality were circumscribed by these four exceptions. Now, a banker could not indiscriminately reveal information concerning a customer's account to third persons unless the said disclosure fell under one of the four qualifications.[14]

It is important to trace the development of bank secrecy and confidentiality norms, because it offers an insight into why it might be inappropriate to equate it to financial privacy today. This is especially given the wide berth provided to regulators to breach it. As it turns out, in almost all documented cases of the development of bank secrecy laws in several jurisdictions, the exceptions to it were instituted as an effective measure to protect people against financial crimes.[15]

---

[12] [1924] 1 KB 461.

[13] Ibid., 467.

[14] Mary Catherine Green, 'The Bank Secrecy Act and the Common Law: In Search of Financial Privacy' (1989) 7 Ariz. J. Int'l & Comp. L. 261 263.

[15] Historically, countries like the United States had low bank secrecy thresholds. On the other hand, countries like Austria, Liechtenstein, Greece, Luxembourg, Switzerland and Portugal, along with Denmark, France and Germany had stronger bank secrecy laws. Most commonwealth countries including India, the UK, Australia, Canada, Ireland, Singapore and Malaysia had medium protections accorded to banking information, See Philip R. Wood, 'Chapter 17 International Law of Bank Secrecy' in Robert C. Effros, Current Legal Issues Affecting Central Banks, Volume V. (USA: International Monetary Fund 1998) <https://www.elibrary.imf.org/view/IMF071/01508-9781557756954/01508-9781557756954/ch17.xml?language=en&redirect=true>; Globally, due to a growing impetus towards greater financial transparency, there has been a significant dilution of bank secrecy norms. This has created pressures on even countries like Switzerland and Philippines, which have traditionally been pioneers of bank secrecy laws. Since 2013, many British overseas territories agreed to automatic information sharing with Britain, France, Germany, Italy, and Spain,See Ray Flores, 'Lifting Bank Secrecy: A Comparative Look at the Philippines, Switzerland, and Global Transparency' (2015) 14 Wash. U. Global Stud. L. Rev. 779,796 <https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1555&context=law_globalstudies>; In some countries like the UK for instance, bank secrecy laws have been diluted through non-banking legislation like the Police and Criminal Evidence Act, 1984, The Drug Trafficking Offences Act, 1986 and the Prevention of Terrorism (Temporary Provisions) Act, 1989, See Michael Levi,

These included tax evasions, money laundering, regulatory proceedings and other civil and criminal prosecutions, all of which required regulators to probe into confidential financial information.[16] This ostensibly became the reason for the institution of the Bank Secrecy Act, 1970 in the United States (US), for instance. The Bank Secrecy Act, 1970 was originally enacted to require financial institutions to maintain records, and help identify the source, volume, and movement of currency and other monetary instruments transported or transmitted into or out of the United States.[17] Hence, the primary objective of instituting the legislation was focussed around anti-money laundering efforts, rather than protection of customer information and privacy. In fact, in *Stark v Connally*[18], the federal court in the US found that the requirements of the Bank Secrecy Act, 1970 may have an adverse impact on the rights of individuals, and was a violation of an individual's constitutional right to privacy.[19] Subsequent amendments to the Act have further sought to broaden the scope of the legislation to also include the Anti-Drug Abuse Act of 1986, which contained the Money Laundering Control Act of 1986, and the Money Laundering Suppression Act of 1994, the Annuzio-Wylie Anti-Money Laundering Act of 1992, and the Money Laundering and Financial Crimes Strategy Act of 1998. The sole focus of the Bank Secrecy Act, 1970 has been to strengthen anti-money laundering and counter-terrorist financing measures.[20] In this regard, a more privacy focussed legislation is the Gramm-Leach-Bliley Act, 1999 which requires financial institutions and companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.[21] Scholars in the US have noted that the reason behind instituting the Bank Secrecy Act was allegedly sinister, aimed at permitting the invasion of privacy by first requiring citizens to provide or make available to the Government certain information, and then supplying the information to an enforcement agency, with the individual having no remedy at either stage.[22]

'REGULATING MONEY LAUNDERING: The Death of Bank Secrecy in the UK.' (1991)31(2) The British Journal of Criminology 109 <www.jstor.org/stable/23638398>.

16 Philip R. Wood, 'Chapter 17 International Law of Bank Secrecy' in Robert C. Effros, Current Legal Issues Affecting Central Banks, Volume V. (USA: International Monetary Fund1998)407-409 <https://www.elibrary.imf.org/view/IMF071/01508-9781557756954/01508-9781557756954/ch17.xml?language=en&redirect=true>.

17 'History of Anti-Money Laundering Laws' (Financial Crimes Enforcement Network) <https://www.fincen.gov/history-anti-money-laundering-laws>.

18 347 F Supp 1242 (ND Cal 1972).

19 'The 1970 Bank Secrecy Act and the Right of Privacy' (1973) 14(4) Wm. & Mary L. Rev. 929. <https://scholarship.law.wm.edu/wmlr/vol14/iss4/7>.

20 'Bank Secrecy Act, Anti-Money Laundering, and Office of Foreign Assets Control' (Federal Deposit Insurance Corporation) 8.1-2 <https://www.fdic.gov/regulations/safety/manual/section8-1.pdf>.

21 'How to Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act' (Federal Trade Commission)< https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>.

22 Richard A. Posner, 'The Uncertain Protection of Privacy by the Supreme Court' (1979) 1979 The Supreme Court Review 173, 211 <http://www.jstor.org/stable/3109570>.

After the global financial crisis of 2008, bank secrecy laws have been diluted even further, since G20 countries compelled tax havens to sign bilateral treaties providing for exchange of bank information. While the policy effectiveness of this dilution of bank secrecy laws has been contested[23], the OECD famously declared that "the era of bank secrecy is over."[24]

Similarly, the Basel Core Principles and Guidelines on Customer Due Diligence for Banks prescribed 'know-your-customer' standards in 2001. These standards were focussed on identification and supervision of risks. To this effect, the Basel Committee on Banking Supervision had noted that supervisors or auditors should face no impediments in verifying the unit's compliance with KYC policies and procedures. Further, the standards mandated that supervisors "should have access to information on sampled individual customer accounts to the extent necessary to enable a proper evaluation of the application of KYC standards and an assessment of `risk management practices, and should not be impeded by local bank secrecy laws."[25] The standards also recommended that where bank secrecy laws and regulations of a certain jurisdiction prohibited the implementation of a more stringent KYC norm set by the bank's home country, host country supervisors ought to use their best endeavours to have such bank secrecy laws and regulations changed.[26]

Subsequently, the United Nations Global Program against Money Laundering, 1988 recommended deliberate exceptions to bank secrecy laws in most countries. The 1988 Program was a key instrument of the United Nations Office of Drug Control and Crime Prevention (through the 1988 U.N. Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention). It called upon countries to criminalize money laundering, to ensure that bank secrecy provisions did not impede the process of criminal investigations, and to facilitate legislative amendments for investigation, prosecution, and international cooperation.[27]

The principle of financial privacy not being without its limits or exceptions was discussed in detail in the *United States v Miller*[28], where the constitutionality of the US Bank Secrecy Act, 1970 was challenged. It was ultimately held

---

[23] Niels Johannesen and Gabriel Zucman, 'The End of Bank Secrecy? An Evaluation of the G20 Tax Haven Crackdown.' (2014) 6(1) American Economic Journal: Economic Policy 65 <www.jstor.org/stable/43189366>.

[24] 'The Era of Bank Secrecy is Over' (OECD, 26 October 2011) <http://www.oecd.org/tax/exchange-of-tax-information/48996146.pdf>.

[25] Basel Committee on Banking Supervision, *Customer Due Diligence for Banks* (October 2001), para 68 <https://www.bis.org/publ/bcbs85.pdf>.

[26] Ibid., paras 63, 66.

[27] Reserve Bank of India, *Report of the Technical Group on Market Integrity* (4 June 2002) para 3.10 <https://www.rbi.org.in/scripts/PublicationReportDetails.aspx?ID=280>.

[28] 1976 SCC OnLine US SC 70 : 48 L Ed 2d 71 : 425 US 435 (1976).

by the US Supreme Court that depositors had no fourth amendment privacy rights in records maintained by a financial institution pursuant to the Act. The court stated that even if the bank records were obtained by a defective subpoena served on the bank, "a person has no expectation of privacy in records which are in the possession of a bank", and that "there is no expectation of privacy."[29] The Court held that the depositor's expectation of privacy vested in the contents of the subpoenaed bank records. These bank records were voluntarily conveyed to the bank, and were revealed to bank employees in the ordinary course of business. Therefore, the Court concluded that the depositor/customer had no expectation of privacy in their personal banking records. In doing so, the Court referred to the general rule that had existed prior to *Miller*, that "issuance of a subpoena to a third party to obtain the records of that party does not violate the Fourth Amendment rights of a defendant."[30] In the US, the exceptions laid down in bank secrecy legislation have largely followed the Court's conception of financial privacy in *Miller*. These exceptions include the requirement to maintain detailed financial records and filing of reports with regulators, reporting of suspicious activities to regulators as a fulfilment of a public duty, and the protection afforded to financial institutions from being prosecuted for said disclosure of suspicious activity.

However, pursuant to several technological developments that allowed more access to financial institutions and Governments to collect intimate data about people's lives and credit information in general, the Right to Financial Privacy Act, 1978 was passed. In most parts, this legislation was enacted to supplement the Bank Secrecy Act, and provide some level of protection to the customers. It prohibited disclosure of a customer's bank records to the federal government unless the customer was notified and a statutory "waiting period" had expired.[31]

However, in general, the common law development in both the UK and the US, in spite of implying a duty on bankers and financial institutions of non-disclosure of certain kinds of customer data to third parties without consent, incorporated several exceptions. These exceptions have largely been along the lines of the exceptions carved out by the US Supreme Court in *Miller*. As much as

---

[29] 1976 SCC OnLine US SC 70 : 48 L Ed 2d 71 : 425 US 435, 441-443(1976).

[30] Nancy J. Nicol, 'No Expectation of Privacy in Bank Records - United States v. Miller' (1976) 26 DePaul L. Rev. 146, 152; *United States v National State Bank* 454 F 2d 1249 (7th Cir 1972) (the customer has neither a proprietary nor custodial interest in bank records); *United States v Gross*, 416 F 2d 1205 (8th Cir 1969), cert. denied, , 25 L Ed 2d 427: 397 US 1013 (1970) (customer has no standing because records are not his property); *Harris v United States*, 413 F 2d 316 (9th Cir 1969) (customers have no rights in the records of their bank); *Galbraith v United States*, 387 F 2d 617 (10th Cir 1968) (customer has no standing to challenge the seizure of his bank records since records are the property of the bank); *Cole, In re* 342 F 2d 5 (2nd Cir 1965), cert. denied, 14 L Ed 2d 723 : 381 US 950 (1965) (customer has no standing because records are the property of the bank).

[31] Mary Catherine Green, 'The Bank Secrecy Act and the Common Law: In Search of Financial Privacy' (1989) 7 Ariz. J. Int'l & Comp. L. 261, 272.

this serves to prevent financial crimes and money laundering, in the vast exception of financial privacy laws, or even in the presence of financial privacy laws, it becomes both easier, and more convenient to exclude more and more of the confidentiality principle severing large portions of it into categories of exceptions. Moreover, in countries like India where the issue is compounded by an express lack of a general data protection law, bank secrecy and confidentiality laws continue to offer the entire gamut of protection to a financial customer. In such a case, conflating the right to secrecy and confidentiality with privacy becomes even more dangerous. This is made even more dangerous when this easy synonymity between secrecy, confidentiality and privacy is accompanied by the liberal use of exceptions mentioned above. It has sometimes been argued that perhaps a better approach than prescribing blanket exceptions would be to weigh the rights of the customer with the Government's interest in obtaining the particular information.[32] However, as other academics such as Daniel Solove[33] have pointed out, this may achieve little because balancing privacy interests against a larger Government/security interest severely short changes the privacy interest while inflating the security interests.

Therefore, Solove argues that privacy has a societal value. Privacy, he argues, is pluralistic in its conception. As such, the harms emanating from its breach are also pluralistic and therefore should not be simply viewed as a debate between an individual right against the greater social good. As such, even when arguing for exceptions to be put on bank secrecy or confidentiality laws, it might be limiting to construct privacy only as a singular, individualistic right, weighed in its totality against a wider and more ambiguous security interest. Thus, Solove suggests considering the extent of marginal limitation on the effectiveness of a Government information gathering or data mining program, the only way to construct the debate between blanket security interest and privacy would be by focussing on judicial oversight and data minimization procedures. Viewed in this light, the conversation pivots from a narrow myopic vision of privacy versus security, to a more nuanced understanding of oversight mechanisms, and a very clear need for a data protection law. This is followed by sector specific guidance, envisioning these oversight mechanisms and clearly articulated financial data protection principles.

III. Over Reliance on Miller: Case of Bank Secrecy in India

Like England, there are a number of legislations in India that oblige banks to maintain secrecy/confidentiality, while also laying down the exceptions. These include the State Bank of India Act, 1955 (section 44), the Banking Companies (Acquisition and Transfer of Undertakings) Act, 1970/1980 (section 13), the

[32] Ibid.

[33] Daniel J. Solove, 'I've Got Nothing to Hide and Other Misunderstandings of Privacy' (2007) 44 San Diego Law Review 745, 772.

Regional Rural Banks Act, 1976 (section 25) and the Reserve Bank of India Act, 1934 (Chapter IIIA). This is supplemented by Section 43A of the Information Technology Act, 2000 and the IT Rules, 2011 framed under that Act, which, *inter alia*, give protection to sensitive personal data or information of customers of body corporates.

The banker's obligation to maintain secrecy of the financial customer has also been espoused in multiple cases, including *Shankarlal Agarwalla v SBI*[34], *K.J. Doraisamy v SBI*[35]. In all of these cases, citing the *Tournier* case in England, courts have held the law relating to bank secrecy and confidentiality to be the same as the laws in England. It has been expressly stated that there exists

> *"an implied term of the contract between a banker and his customer that the banker will not divulge, to a third person without the express or implied consent of the customer, either the state of the customer's account or any of his transactions with the bank or any information relating to the customer, acquired through the keeping of his account unless the banker is compelled to do so by order of a Court or the circumstances give rise to a public duty of disclosure , or protection of the banker's own interest requires it.*"[36]

However, in both *K.J. Doriasamy* and *Mohan Products*, it is interesting to see courts frame the question of the right of the borrower to not have their photographs published (right to privacy) as a 'tension' or contestation to the bank's right to adopt any lawful method for the recovery of its dues, including the publication of the photograph of the defaulter. It was ultimately held in these cases that the right to privacy was not an absolute or inviolable right. Therefore, the duty of the bank to maintain secrecy is superseded by a larger public interest as well as by the bank's own interest under certain circumstances.[37] Further, in all these cases, the courts cited the English law to state that the duty of the Bank to disclose information to the public or the interest of the Bank requiring disclosure superseded the duty of secrecy it owed to its customer.

In the landmark case of *Distt. Registrar v Canara Bank*[38] it was heartening to note that the Supreme Court derogated from the *Miller* case (even citing detailed criticisms) to state that any law interfering with the personal liberty of a person had to satisfy a triple test of - the prescription of a procedure, the procedure withstanding the test of one or more fundamental rights, and the law and procedure authorizing the interference with personal liberty and right of privacy

---

[34] 1984 SCC OnLine Cal 188 : AIR 1987 Cal 29.
[35] 2006 SCC OnLine Mad 1043 : (2006) 4 Mad LJ 1877.
[36] *Tournier v National Provincial and Union Bank of England*, [1924] 1 KB 461.
[37] *K.J. Doraisamy* (n 35), paras 24, 29.
[38] (2005) 1 SCC 496, paras 47, 48 and 53.

being right, just, and fair, and not arbitrary, fanciful or oppressive. Significantly, both in this case, and in *K.S. Puttaswamy v Union of India*[39], the court made reference to Professor Tribe's treatise, where he observes that the majority in *Miller* confused 'privacy' with 'secrecy' and that "even their notion of secrecy is a strange one, for a secret remains a secret even when shared with those whom one selects for one's confidence."[40] Further, in both of these cases the court repudiated the notion that a person who places documents with a bank would, as a result, forsake an expectation of confidentiality. In the view of the Court, even if the documents cease to be at a place other than in the custody and control of the customer, privacy attaches to persons and not places and hence the protection of privacy is not diluted.[41]An interesting facet that emerged from these cases,was the reaffirmation that the right to privacy emanated from the liberties guaranteed by Article 19 and from the protection of life and personal liberty under Article 21 of the Constitution of India.[42]

However, it must be noted that a number of judicial decisions in India have dealt with financial privacy and data protection, without using these specific words, and relying on words such as 'confidentiality.' For instance, in *ICICI Bank Ltd. v Umashankar Sivasubramanian*[43], the Telecom Disputes Settlement and Appellate Tribunal found the bank to be negligent in disclosing confidential information such as password of the customer, specifically stating that section 43A of the IT Act, 2000 creates a special responsibility to protect sensitive personal data or information in a computer resource and a liability to pay compensation for certain kinds of negligence. The Tribunal went so far as to state that a bank's electronic records in a computer were required to have a safe and secure procedure of access, without ever mentioning or situating this in the context of privacy.[44] This is also evidenced in the decision of the National Consumer Disputes Redressal Commission in *PNB v Rupa Mahajan Pahwa*.[45]

Of course, in the context of India, subsequent jurisprudence on the subject like the Justice B.N. Srikrishna Committee Report[46] stated explicitly that not every security incident would qualify as a personal data breach, and that the very definition of personal data breach would be structured around three key principles of information security - confidentiality, integrity and availability. Confidentiality breach, the report stated, implied an unauthorised or accidental disclosure of, or access to, personal data. This is unlike an integrity breach, which constituted an

---

39 (2017) 10 SCC 1.
40 Ibid., para 480.
41 Ibid., para 75.
42 Ibid., para 77.
43 2019 SCC OnLine TDSAT 1561.
44 Ibid.
45 2015 SCC OnLine NCDRC 3008.
46 Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians* (27 July 2018) 63.

unauthorized or accidental alteration of personal data. Integrity breach, also an availability breach which occurred when there was an accidental or unauthorised loss of access to, or destruction of, personal data.

From the cases discussed above, it is clearly that there has been an over-reliance on *Miller*, with courts circumscribing a financial customer's right to privacy over her financial information. However, subsequent judicial pronouncements such as *Canara Bank* and *Puttaswamy* have refocussed the conversation back to privacy, explicitly distinguishing it from privacy. This trend has been noticed in other cases as well, where reliance has been placed on the effective protection of customer's sensitive personal data or information. Although there is still an absence of a holistic data protection legislation, there is overwhelming evidence to suggest that the synonymous use of 'confidentiality', which is at best, only one part of informational security, with privacy or data breach is both harmful, and in clear derogation from contemporary judicial and policy prescriptions.

However, as is explored in the following part of the article, for financial privacy, legal linguistic ambiguity continues to be observed, particularly across recent banking policies issued by the banking regulator in India.

IV. Continued Linguistic And Conceptual Ambiguity In Bank Regulatory Policy

In 2002, in a report on "Information Systems Security Guidelines for the Banking and Financial Sector"[47], RBI raised concerns over rising privacy expectations, especially for electronic money, given the then recent advancements in the smart card technology and cryptography, which enabled organisations to issue tokens capable of storing and exchanging value.[48] Amongst other things, the regulator articulated the need to put restrictions on the collection of information for marketing purposes on the purchase by the customers, and laid down requirements for organisations to follow, along with a requirement to follow privacy audits.[49] These requirements included financial organisations to review all privacy laws and regulations which involve credit information, including updating itself on all national privacy legislations. Organisations were also recommended to review their business operations from time to time to assess whether the information on their customers and employees were adequately protected. They were also directed to put in place specific policies and procedures concerning how the

[47] Reserve Bank of India, Annexure: Information Systems Security Guidelines for the Banking and Financial Sector (part 1 of 2) (11 March 2002) <https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?ID=277>.

[48] Ibid., para 4.14.

[49] Ibid., para 4.16.5.

information was gathered, used and protected, with these methodologies adopted to meet the legal requirements.[50]

However, the word 'privacy' continued to be used synonymously with the word 'confidentiality' in the report. This synonymous use of privacy and confidentiality was also seen in the 'Citizen's Charter' issued in 2012 by public sector banks. In this Citizen's Charter, banks committed to maintaining the privacy *and* confidentiality of customer's personal information, except when the disclosure was mandated by law, public duty, bank interest, and customer consent.[51]

In 2014, RBI issued a "Charter of Customer Rights", enshrining five broad principles for protection of bank customers, including the customer's 'right to privacy'[52]. The right to privacy envisaged under the Charter related to a customer's personal information, which had to be kept confidential unless specific consent was sought by a financial service provider to reveal it, or a particular mandate requested for revealing of such information. In addition, the Charter provided customers with a right to be informed *ex-ante* about mandated business purposes, and the right to be protected against all kinds of communications, electronic or otherwise, which infringed upon their privacy.[53] However, the Charter did not define what privacy meant, and seemed to be a reiteration of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011[54], framed under section 43A of the Information Technology Act, 2000.

In the regulatory sandbox framework[55] released earlier last year, the sandbox applicants were prohibited from being allowed any regulatory relaxations with respect to the security of data storage and access to payment data of stakeholders, customer privacy and data protection requirements.[56] Further, the criteria of selection for testing as per the framework also required a robust IT infrastructure to ensure customer privacy and data protection in compliance with existing laws and regulations[57], specifying the mandate for seeking explicit consent from customers. However, apart from shifting the burden of understanding complicated fintech innovation to unnuanced financial consumers by relying on the consent architecture, the framework also did not prescribe any penalties or compensation

---

50 Ibid., para 4.16.

51 Public Sector Banks, *Citizen's Charter: A Charter for Customer Services* (12 March 2012)7 <https://financialservices.gov.in/sites/default/files/Draft_Citizen_Charter-1%20final.pdf>.

52 Reserve Bank of India, *Charter of Customer Rights* (3 December 2014) <https://www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=32667>.

53 Ibid.

54 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 <https://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf>.

55 Reserve Bank of India, 'Enabling Framework for Regulatory Sandbox' (13 August 2019) <https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=47869>.

56 Ibid., cl 6.2.

57 Ibid., cls 6.5.1 (g), (h) and (i).

for financial consumers, for derogation from the mandatory requirement of safeguarding customer privacy and data protection. The framework also did not create reasonable and proportional distinctions in responsibilities based on the firm's size, complexity, and internal organization, all of which may have a bearing on the ability of the entity to collect and process sensitive financial data of the consumer. This becomes significant because unlike other countries like the US, India does not have an overarching and dedicated financial consumer law or a financial privacy legislation.[58]

Similarly, in the National Strategy for Financial Inclusion (NSFI): 2019-2024[59], one of the objectives highlighted in the policy was "customer protection and grievance redressal." Within this objective, the policy stated that apart from empowering customers with the knowledge of resources available for resolution of their grievance, adequate safeguards would need to be ensured to protect the customer's right to privacy, with special regards to her biometric and demographic data. However, the policy failed to discuss financial privacy as a distinct objective or mention what safeguards in particular needed to be ensured to achieve this. Further, the policy stated that the emerging risks from digital financial services mandated a strong consumer protection architecture. As such, the policy recommended that data protection and information/cyber security ought to be addressed under the consumer protection framework. The Policy also placed significant currency on creating a safe environment based on principles of consent and privacy, one which could be achieved through increased consumer awareness and financial literacy.

As has been demonstrated in this article and particularly in this part, there has been a consistent linguistic conflation between 'privacy'; and 'confidentiality' and bank 'secrecy' in India, evidenced both in court decisions and legal policy. However, in recent banking regulatory policy, there is an added conceptual conflation between 'data protection' and 'consumer protection.' There is an established legal paradigm where consumer law has typically been concerned with fair contracting by consumers, encapsulating certain mandatory rights to create a fair playing field, versus data protection law that aims to enhance fair processing of data. Other differences have been articulated to argue that while consumer protection law can be seen to merely set a floor in its pursuit of a sufficiently high level of consumer protection, data protection law, due to its clearly articulated purposes of protecting people from processing and (free) movement of personal

[58] Shohini Sengupta, 'Holes in RBI's Sandbox for Fintech' *Hindu Business Line* (2 May 2019) <https://www.thehindubusinessline.com/opinion/holes-in-rbis-sandbox-for-fintechs/article27015153.ece>.

[59] Reserve Bank of India, *National Strategy for Financial Inclusion (NSFI): 2019-2024* (10 January 2020) 22 <https://www.rbi.org.in/scripts/PublicationReportDetails.aspx?ID=1154>.

data, sets both a floor and a ceiling.[60] In this regard, while modern legal policies such as the EU draft Digital Content Directive tries to harmonise and move towards a digital future where consumer law and data protection laws can complement each other[61], a complete capture of data protection solely within consumer protection law has typically not been advised, especially without any changes being made to existing consumer protection laws. It is advised that consumer protection law be used to correct structural and institutional power exerted over data subjects, and that the said law needs to have robust enforcement. In fact, without effective enforcement, expecting beneficial effects from applying consumer protection law will not yield satisfactory results.[62]

Therefore, for India in particular, where there is an absence of an all-encompassing financial consumer protection law, a data protection law might empower individuals with significant autonomy and choice that is currently not available under any existing statute. At a bare minimum, this should include the right to accuracy, purpose limitation, accountability, storage limitation, data security, purpose limitation, lawfulness, fairness and transparency.[63] It must be noted that certain rights like privacy by design, the right to data portability, the right to be forgotten, the right to object etc. are novel rights in the Indian legal landscape, and existing consumer protection law may not be able to holistically provide for these adequately. In the absence of a holistic law akin to GDPR in India, customers will have to rely either on the protections entailed in the Information Technology Act, 2000, or in scattered financial legislation as mentioned in Part III of the article. It must be noted that none of the extant laws in India replicate in scope or objective, the fundamental objectives of GDPR, that is, the protection of natural persons when their data is processed, protection of their fundamental rights and freedoms with respect to data protection and freedom of movement of personal data for processing purpose.

Of course GDPR is not the only framework of data protection that should be considered for effective protection of financial consumers. For instance, scholars have argued that the 'informed consent' model for consumer data protection championed by GDPR and other like legislation harbour real weaknesses in

---

[60] Dan Jerker B. Svantesson, 'Enter the Quagmire – the Complicated Relationship Between Data Protection Law and Consumer Protection Law' (2018) 34(1) Computer Law & Security Review 25.

[61] Natali Helberger, Frederik Zuiderveen Borgesius and Agustin Reyna, 'The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law' (2017) 54(5) Common Market Law Review 1427.

[62] Michiel Rhoen, 'Beyond Consent: Improving Data Protection Through Consumer Protection Law' (2016) 5(1) Internet Policy Review <https://doi.org/10.14763/2016.1.404>.

[63] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1, art 5.

effectively protecting the privacy of consumers in developing countries[64]. While this consent model may accelerate financial inclusion, there is also a danger of added risks including fraudulent use of biometric data, unanticipated aggregation of multiple data points, and disclosure of sensitive personal information to Governments without a transparent process or rule of law.[65] Other scholars have argued that there needs to be a shift from 'privacy self-management' which takes refuge in consent, to focusing on whether people have meaningful control over their data.[66] In developing countries where certain irresponsible lending practices are not well regulated, financial inclusion policies that are solely focused on increasing access may not translate into empowerment. Thus, the debate over the protection of sensitive financial information of customers in these countries may need to shift from the dominant informational privacy context to more local conceptions privacy, including dignity, identity and freedom from oppression.[67]

There is therefore significant merit in explicitly recognising these additional dimensions to consumer rights and autonomy, and using existing legal constructs of consumer protection law, which may be both outdated and inadequate would only seek to diminish the expansive scope of data protection and privacy.

Along with a conflation and attempted disharmonious integration of data protection and consumer protection laws, there is also a tendency in the aforementioned regulatory policies to reduce the right to privacy of financial consumers to a singular construct of 'consent.' This is seen in both the RBI's fintech policies and regulatory sandbox frameworks discussed above. As has been explicitly laid down in *K.S. Puttaswamy v Union of India*[68], taking significant inspiration from GDPR, there is consensus over the fact that consent is one of the many ways to test the legality of data processing. The Supreme Court in *Puttaswamy* lays down clear tests of the judicial review standard being legality, legitimate aim, proportionality and procedural guarantees. Article 6 of the GDPR also lays down six ways to test legality, of which consent is one such criteria (the others being performance of contract, compliance with legal obligations, protection of vital interests, tasks carried out in public interest, and legitimate interests). In the absence of a clear articulation of these standards, the regulator limits its own ability in parts to process or allow for processing of data which may be important for a wide variety of reasons.

---

[64] Katharine Kemp and Ross P. Buckley, Protecting Financial Consumer Data in Developing Countries: An Alternative to the Flawed Consent Model (2017) 18 Georgetown Journal of International Affairs 35 <www.jstor.org/stable/26395922.>.

[65] Ibid., 36.

[66] Daniel J. Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2012) 126 Harv. L. Rev. 188.

[67] Kemp and Buckley (n 64) 42.

[68] (2017) 10 SCC 1, paras 310-314, 638.

The need for a separate data protection law, distinct from a consumer protection law has been reiterated in a number of jurisdictions. For instance, even where there exists a right to privacy as in the EU Charter of Fundamental Rights[69], there is an independent and separate right to data protection under Article 8 of the Charter. The Charter's inclusion of an independent right to data protection has been stated to differentiate it from other key human rights documents which generally treat data protection as a subset of the right to privacy. This specific and independent right to data protection has been argued to provide individuals with more rights over more types of data than the right to privacy, including enhanced control over personal data, fostering the development of individual personality, and reducing the power and information asymmetries between individuals and data processors.[70]

However, the most important contribution to a data protection law, as has been evidenced in the US, has been to provide individuals with remedies beyond compensatory damages. This includes remedies such as statutory or treble damages, specifically where victims of data breaches or privacy violations have not been seen to always experience clear and immediate pecuniary or reputational harm[71]. With many recent policies such as the regulatory sandbox guidelines, there isn't even a clear prescription of penalties or remedies for financial data or privacy breaches. As Solove once said, "privacy lacks dead bodies."[72] The banking regulator seems to accept Solove's statement on face value and in simply framing privacy as a consumer rights problem, the banking regulator betrays a certain myopia about foreseeable harms of privacy breaches, the imagination of the law, and the remedial action that can be made available to financial consumers.

V. Recent Trends in Fintech and the Financial Data Protection

The importance of financial privacy is perhaps most felt in the burgeoning push towards financial inclusion across the world, especially through digital finance. Like many other countries, India's push for digital financial inclusion has also been evidenced through the use of banking services of various kinds. Over the years, this has been done through specialized banks such as payment banks, and small and micro finance banks, which have proliferated because of newer

[69] EU Charter of Fundamental Rights [2012], OJ C326/391 <https://eur-lex.europa.eu/eli/treaty/char_2012/oj>.

[70] Orla Lynskey, 'Deconstructing Data Protection: The Added-Value of a Right to Data Protection in the EU Legal Order' (2014) 63 International & Comparative Law Quarterly 569.

[71] Congressional Research Service, 'Data Protection Law: An Overview' (25 March 2019) 59 <https://fas.org/sgp/crs/misc/R45631.pdf>.

[72] Daniel J. Solove, 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy' (2007) 44 San Diego L Rev 745, 768.

kinds of banking licenses issued by RBI.[73] However, even with the recent, rapid burgeoning of fintech firms, the disintermediation from traditional banking institutions has never been too severe, and there is a growing body of evidence for this, including Apple Pay and Google Pay which continue to interact with traditional banks for payment access.[74] This means that concerns with effectively safeguarding financial privacy of customers, especially the rural unbanked population, is only going to grow with the rapid advancement of novel forms of digital financial services, banking and otherwise. Despite this, there is little acknowledgement of growing financial data protection risks in India. For instance, the Report of the Committee on Deeping Digital Payments[75], constituted by RBI and chaired by Nandan Nilekani frames privacy largely as a consumer awareness and financial literacy problem. Further, the recommendations on deepening financial inclusion and managing the ecosystem on data does not state India's lack of a robust data protection policy, and instead asks the regulator to increase data collection on digital payments.

The thrust towards achieving financial inclusion through fintech was the central focus of RBI's national strategy for financial inclusion 2019-2024 as well.[76] The Report mentioned that given India's "Jan Dhan-Aadhaar-Mobile trinity" and the expanding role of fintech and digital money, there was a need for massive data collection efforts, and in particular, a need to go beyond data collected from financial service providers alone. It is important to mention here that 'financial inclusion' (increasing access to formal financial services) is distinct from 'financial data inclusion' (which involves merging people's biometric information with their bank account and other financial information to enable tracking). The latter, specifically in the context of forced financial inclusion, has not been necessarily shown to result in greater welfare of unbanked populations. Further, even in case of voluntary financial inclusion, the wide use of digital technologies is known to have increased data security breaches and lowered customer trust in digital finance.[77] Hearteningly, researchers have found a link between financial and banking sector reforms and the stimulation of financial innovation, the promotion of digital banking culture, and the infusion of financial inclusion.[78] It has also been found that effective consumer protection frameworks which apply to digital

[73] See RBI's 'on-tap' licensing <https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=48807>.

[74] Howell E. Jackson, 'The Nature of the Fintech Firm' (2020) 61 Wash U J L & Pol'y 9, 13.

[75] Reserve Bank of India, *Report of the Committee on Deepening of Digital Payments* (17 May 2019) <https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=47068>.

[76] Reserve Bank of India, *Enabling Framework for Regulatory Sandbox* (13 August 2019), cl 6.2 <https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=47869>.

[77] Peterson K. Ozili, 'Impact of Digital Finance on Financial Inclusion and Stability' (2018) 18(4) Borsa Istanbul Review 329, 335 and 339.

[78] A.A. Shaikh, R. Glavee-Geo and H. Karjaluoto, 'Exploring the Nexus Between Financial Sector Reforms and the Emergence of Digital Banking Culture: Evidences from a Developing Country' (2017) 42 Research in International Business and Finance 1030.

financial services are critical for building the necessary trust critical for financial inclusion.[79]

Recent empirical literature on the economics of privacy regulation, particularly for the growing fintech market has also shown that privacy breaches for even a few consumers can depress the market price for data, and lead to a false conclusion that financial consumers do not value privacy, leading in turn to excessive data generation/collection.[80] Further, there is evidence to suggest that financial consumers like users of online lending platforms show willingness to pay for more privacy-protective offers, thereby reducing the demand for fintech companies that engage in excessive data collection. Therefore, privacy breaches and excessive data collection can impose costs on fintech firms, demonstrating the social and economic benefit that can arise from greater privacy-protection regulation such as the GDPR.[81] Therefore, this adds to the growing body of literature, and both social and economic rationale for having effective data protection policies for consumers.

VI. Conclusion

With the onset of the novel corona virus pandemic (Covid-19), there has been an increased push worldwide for the adoption of digital finance and banking methods to promote social distancing. In this regard, the International Monetary Fund (IMF) has warned that the risks to stability and integrity, including from operational constraints, cyberattacks, fraud, money-laundering, data, and privacy issues that are always present, may worsen if the use of digital financial services is scaled up in times of crisis.[82] Further, the IMF has highlighted the need for many countries to adapt their regulatory and policy frameworks with regard to the provision of payments and financial services and questions related to taxation or data privacy. Most importantly, it has warned against any large-scale move to digital financial services where existing concerns over Government or private use of data, especially payments data, could be exaggerated during a crisis. They have warned that this could create legitimate concerns about a surveillance state because there was a risk of usual checks and balances provided by democratic oversight or business regulation to be short-circuited during crisis episodes.[83]

---

[79] L. Malady, 'Consumer Protection Issues for Digital Financial Services in Emerging Markets' (2016) 31(2) Banking & Finance Law Review 389.

[80] Daron Acemoglu, Ali Makhdoumi, Azarakhsh Malekian and Asu Ozdaglar 'Too Much Data: Prices and Inefficiencies in Data Markets' (2019) CEPR Discussion Papers 14225, C.E.P.R. Discussion Papers 36.

[81] Huan Tang, 'The Value of Privacy: Evidence from Online Borrowers' (2019) 8, 36 <https://wpcarey.asu.edu/sites/default/files/huan_tang_seminar_paper.pdf>. This also includes other recent privacy focused legislation such as the California Consumer Privacy Act.

[82] Itai Agur, Soledad Martinez Peria, and Celine Rochon, 'Digital Financial Services and the Pandemic: Opportunities and Risks for Emerging and Developing Economies' (2020) IMF Special Series on Covid-19 1.

[83] Ibid., 8.

In sharp contrast to the IMF's warnings mentioned above, recent reports have suggested that RBI has sought an exemption from the country's draft data protection bill, requesting that "the monetary, regulatory and supervisory functions of the RBI as well as its role as the operator of payment systems may be exempt from the purview of the Bill."[84]

However, as this paper has demonstrated, even without such an exemption being sought, banking policies have demonstrated both conceptual and linguistic ambiguity and conflation in matters relating to financial data protection and confidentiality. This paper has demonstrated that historically, the adoption of bank secrecy laws has always been accompanied by severe limitations posed by law enforcement authorities on the pretext of security concerns and prevention of financial crimes, even though privacy and security are not *prima facie* contesting ideas. This problem is further complicated in India by the linguistic ambiguity between privacy and confidentiality/secrecy evidenced in both court decisions and contemporary banking policies issued by the RBI, without any protection offered by a general data protection law or a financial consumer protection law. The push towards increased financial inclusion through the adoption of fintech also exaggerates these concerns over financial data protection, particularly for the unbanked population, who may be more vulnerable than their urban and financially more literate counterparts. Lastly, RBI's demand for seeking an exemption from the country's draft data protection bill amidst the global pandemic juxtaposed with IMF's express warnings to the contrary create serious concerns over the trust and accountability expected of the apex banking regulator of the country.

Given the growing body of literature on the clear social and economic benefits emanating from the institution of privacy enhancing legislation across the world, it is hoped that financial regulators, but more specifically RBI will welcome a distinct data protection law. The lack of a separate data protection law in India, combined with an absence of a cross-sectoral financial consumer protection law creates both an urgent need, and an opportunity for the Government and RBI to craft clear legal standards that reduce the obfuscations in legal regulatory language. As this article has demonstrated amply, the synonymous use of words such as 'confidentiality', 'secrecy' and 'privacy' creates euphemisms and poorly grounds assumptions about the agency of financial customers. In the sorites paradox for instance, the classic example of fuzzy and blurred words like 'heap' and 'bald' throw up paradoxical arguments over what exactly constitutes a heap. While a certain amount of philosophical vagueness may be unavoidable, deliberate obfuscation in legal language over crucial issues such as privacy, identity and

[84] 'RBI Seeks Exemption from Data Protection Laws', *Hindustan Times* (10 September 2020) <https://www.hindustantimes.com/india-news/rbi-seeks-exemption-from-data-protection-law/story-kwQzNs614s0C56VK6HTCJP.html#:~:text=The%20Reserve%20Bank%20of%20India,the%20matter%20who%20spoke%20on>.

dignity particularly in a developing country like India, creates pragmatic problems over assertion and judicial enforceability of rights[85]. Therefore, reframing the discourse to seek linguistic clarity to assert a right to privacy for financial consumers, without using euphemistic language to couch privacy in 'confidentiality' and 'secrecy' will help and prevent sorites paradox from being taken to its natural absurd conclusion - in this case, a derogation from global best practices and increased harm from privacy violations during an unprecedented global pandemic.

[85] Roy Sorensen, 'Vagueness Has No Function in Law' (2001) 7 LEG 387, 408.