

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

SURVEILLANCE VS. SECRECY: EVALUATING LEGISLATIVE ACCESS TO BANK RECORDS AND FINANCIAL PRIVACY IN INDIA

AUTHORED BY - JASMINE KERAJ

Affiliation: Department of Law, National University of Study and Research in Law, Ranchi,
Jharkhand, India

Abstract

The practice of banker-customer confidentiality lies at its core. Financial statements, naturally, reveal a lot about a client's finances, their transaction past, who their beneficiaries are, and how they spend their money. But this obligation of confidentiality is not without exceptions, and there are legal and conventional ones. The existing regulation requires banks to provide state authorities and regulators with private financial information for certain purposes, including banking supervision, tax examinations and money laundering prevention and control. It provides public agencies with access to be used for lawful enforcement purposes, but raises significant questions about the legitimate scope of governmental authority and misuse of private consumer information. This paper looks at how the Indian legal system struggles to balance government investigations with a citizen's right to bank privacy. In the end, it questions the effectiveness of the statutory restrictions in meeting the constitutional standards of legality and proportionality in a situation where the state requests that customers' data be shared.

Keywords: Right to Privacy, Article 21, State Surveillance, Legislative Access, Bank Records

Introduction

Banks cannot be conferred an unadministered right to disclose all the financial information they possess about a client. By virtue of their fiduciary and contractual obligations, financial institutions routinely handle comprehensive arrays of sensitive customer data including financial networks, business history and lifetime savings. Although confidentiality is an essential feature of this relationship, the statutory exceptions still dominate over rights. Such dominance can be seen wherein the law mandates disclosure in the State's interests of

regulation and enforcement.¹

The statutory architecture governing Indian banking is defined by a fragmented matrix of legislation, including the Reserve Bank of India Act, 1934, the Banking Regulation Act, 1949, the Income-tax Act, 1961, and the Prevention of Money-Laundering Act, 2002. Beyond these statutory boundaries, financial confidentiality is intrinsically bound to constitutional principles. The baseline protection of customer data held by financial institutions was explicitly addressed in *District Registrar & Collector, Hyderabad v. Canara Bank*, which scrutinized the privacy boundaries of bank-held records. This jurisprudential protection was subsequently elevated by the Supreme Court's seminal ruling in *K.S. Puttaswamy v. Union of India*, which firmly anchored the right to privacy within the fundamental guarantees of Article 21 of the Constitution of India. This includes informational privacy.²

A distinct legal inquiry is triggered when material in a defendant's possession is demanded under statutory investigative powers. To evaluate these requests, we have to look closely at the actual context and the specific words of the enabling law. For any government demand for bank records to survive a constitutional challenge, it must stand on three clear pillars: a precise statutory basis, a valid administrative goal, and clear safeguards to protect the data after retrieval.

The real question is whether there is a clear and precise statutory requirement with a strictly limited scope of application and strict working requirements. This is a difficult balance to achieve between States' surveillance and private autonomy in financial terms. The Indian law recognises that there is a fiduciary relationship between the bank and the customer. It does, however, provide direct avenues for data exchange when required for tax collection, tracking of hidden assets and anti-money laundering purposes. At present, financial privacy is loosely bound together by a confusing multitude of contract law, common-law heritage, constitutional concepts and banking laws. An access clause will never be a licence to enter into administrative fishing expeditions, which are fundamentally divorced from ordinary forms of access to the property. This study highlights the inherent structural conflicts and explores the scope of achieving this balance in the Indian law system by taking into account the interest of the state in keeping track of the money and the citizen's right to privacy with respect to keeping his records private. It poses an important question: Do the existing legislative lines provide adequate protection to ensure that state control is actually needed, justifiable, and properly scaled?

¹ *Tournier v. National Provincial & Union Bank of England*, [1924] 1 K.B. 461 (CA) 473.

² *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1, 264.

To address these questions, this paper relies on a doctrinal research methodology, engaging in a critical reading of core banking statutes, evolving judicial precedents, and authoritative academic commentary. The analysis concentrates squarely on the legal friction between a financial institution's common-law confidentiality obligations and the strict privacy benchmarks established under the landmark jurisprudence of K.S. Puttaswamy toward its customer and its statutory obligations to disclose data. While centered on Indian law, comparative principles are introduced where necessary to enrich the analysis. Specifically, the paper addresses three primary issues: the legal duties establishing banking confidentiality, the parameters under which public authorities can obtain this data, and whether the current framework provides adequate protection against executive overreach. Crucially, the objective is not to frame banking secrecy as a fundamental right, but rather to evaluate whether the existing exceptions to that secrecy are properly calibrated.

I. Banking Confidentiality: The Banker-Customer Relationship

The mandate of banking secrecy is a direct corollary of the foundational relationship established between a bank and its customer. A bank obtains access to the personal data of the customer, regarding the customer's account, when providing services to the customer. Sir John Paget observed that “a bank must not disclose anything about the state of account with reference to whether it is overdrawn or not save upon reasonable and proper occasions”. The legal position of this obligation has been unclear throughout history. A bank cannot claim to have honestly intended to act in the customer's best interest and therefore justify disclosure.³

The contractual basis of this obligation and the exceptions have been outlined in *Tournier v. National Provincial & Union Bank of England*. The Court of Appeal acknowledged that there could be situations where disclosure would be justified. These exemptions encompass mandatory legal disclosures, pressing public interest duties, measures vital for safeguarding the institution's proprietary interests, and instances supported by the explicit or implicit authorization of the account holder.⁴ Therefore, banking secrecy imposes a conditional obligation.

India adopts this general rule of non-disclosure, codifying specific data protections within legislative provisions like Section 45E of the Reserve Bank of India Act 1934. Credit information covered by sections 45C and 45D is protected. There are exceptions to this

³ John Paget, *The Law of Banking* 77–78 (3d ed. 1922).

⁴ *Tournier*, [1924] 1 K.B. at 473.

restriction under section 45E(2), and the production and inspection of specified statements and disclosure of the credit information by courts, tribunals and other authorities which are covered under section 45E(3).⁵

Section 45E only provides specific protection for the credit information. This is different from the general obligation between the bank and the customer. Legal obligations will need to be considered when determining whether any disclosure would be lawful.⁶

II. Banking Secrecy: Legislative Exceptions And Disclosure

The Indian legal framework does not provide for absolute bank secrecy, but contains various statutes allowing access to financial information for tax, regulation and law enforcement purposes. Whether a request for financial information is lawful will depend on the statute invoked, the reason for requesting the information, the nature of the information required and whether the correct procedures have been followed.⁷

Section 246 of the Income-tax Act 2025 allows certain income tax authorities to exercise powers relating to discovery and inspection, attendance, examination under oath of persons (this includes banking company officers) and production of books of account and documents. The Income-tax Act 1961 has been repealed with effect from April 1, 2026. The 2025 Act contains saving provisions in relation to the 1961 Act.⁸

Prevention of Money Laundering Act, 2002 imposes on banking companies (among others) the obligation to keep records and report certain information. Sections 12, 12A and 12AA provide reporting and record-keeping obligations, the provision of information to the Director and additional due diligence requirements for certain transactions. This makes it easier to prevent and detect money laundering.

We must recognise the very fine line between an agency obtaining information and a bank disclosing it.⁹ For instance, Section 45E of the Reserve Bank of India Act, 1934, shields credit data by explicitly barring courts, tribunals, or other authorities from demanding its disclosure or inspection. However, a bank's internal duty to report data to its regulator is entirely separate from its permission to share that data with external third parties.

Different authorities whether tax agencies, anti-money laundering bodies, or banking

⁵ The Reserve Bank of India Act, No. 2 of 1934, India Code (1934), § 45E.

⁶ M.L. Tannan, Tannan's Banking Law and Practice in India § 11.76, at 228–29, § 11.79, at 229–30, § 11.80.5, at 231 (Vinod Kothari ed., 28th ed. 2021).

⁷ RT6JFcbxM6q8fPWFTBU78vJdm2ugTp42N7

⁸ The Income-tax Act, No. 43 of 1961, India Code (1961).

⁹ The Prevention of Money-Laundering Act, No. 15 of 2003, India Code (2003).

regulators do operate under distinct mandates. As their roles differ, we have to look closely at the exact scope of their statutory powers. Even when a law forces a bank to disclose information, that data cannot simply be passed around or used for entirely unrelated matters. Ultimately, the three factors are critical: what information is being sought, who is being asked to provide it, and which statutory requirements apply. Having the legal right to access financial records never translates into a license to share them indiscriminately. To truly understand the boundaries, one must parse the relevant legislation to see exactly what can be gathered, who it can be shared with, when it can be made public, and what legal remedies exist if that data is misused.

In the final analysis, these sweeping statutory powers must always be balanced against the fundamental right to privacy, which is protected under Article 21 of the Constitution of India¹⁰ and firmly established in the landmark Justice K.S. Puttaswamy ruling.¹¹

Banking confidentiality relies on legal controls governing how the financial information is obtained and used. The essential point to consider here is whether the legal framework adequately distinguishes between information that needs to be accessed for regulatory purposes and information disclosed beyond the scope of legal authority. This is key in ensuring that there is a balance between legitimate public interests such as tax, regulation and law enforcement and protecting the customer's financial information.

III. Banking Records And The Right To Privacy

Banking records can provide insight into an individual's financial dealings and relationships. Sharing this data does not mean the information is suddenly stripped of its private status; the exact legal basis allowing the state to access it must always be put to the test. The Supreme Court laid the groundwork for this protection in *District Registrar & Collector, Hyderabad v. Canara Bank* by directly confronting government overreach into private documentation. By confirming that the link between an account holder and a bank is inherently confidential, the Court drew a firm line in the sand. The core lesson of the judgment is clear i.e, private papers do not lose their constitutional protection or their private character the moment they are placed in the custody of a third-party financial institution.¹²

The constitutional architecture governing data protection in India underwent a paradigm shift with the Supreme Court's landmark ruling in *Justice K.S. Puttaswamy v. Union of India*. By

¹⁰ *Puttaswamy*, (2017) 10 SCC at 264.

¹¹ India Const. art. 21.

¹² *District Registrar & Collector v. Canara Bank*, (2005) 1 SCC 496.

placing the right to privacy under Article 21, the nine-judge bench changed the game for the financial sector through what it called "informational privacy." This concept means that individuals have real control over their personal and financial history, meaning the government cannot just treat private bank records like an open book. The court did realize that privacy has to be balanced against real state interests, but it made it clear that arbitrary overreach is completely off-limits. Because of this, if the state wants to look into financial data, it has to clear three specific hurdles: there must be an actual law allowing it, a legitimate public purpose behind it, and the intrusion must be strictly proportional to the problem it is trying to solve.¹³ At the same time, these rulings do not give anyone a free pass to hide their banking data completely. Instead, they show why we need to separate lawful access from unfair, sweeping interference. To figure out if a state request for financial information is valid, you have to look at the legal mechanics behind it why the request was made in the first place, what specific law gives them the power to ask for it, and what actual protections are in place to stop that data from being misused.

IV. Financial Data Protection: Moving from Secrecy to Privacy

Presently the academic research for financial data protection has focused heavily on where traditional banking secrecy runs into modern rules about personal data. On this front, Shohini Sengupta provides a great breakdown that separates the overlapping ideas of 'secrecy,' 'confidentiality,' and 'privacy' inside India's financial regulatory system¹⁴. Along the same lines, Gautam Bhatia looks at the broader picture, mapping out the constitutional rights connected to state surveillance laws¹⁵. These articles indicate that whilst data must be obtained lawfully, there is consideration of why it is being obtained, whether it is proportionate, safe, how long it is kept for and whether it will be passed on.

Atul Singh's discussion on data protection in India shows how the Credit Information Companies (Regulation) Act, 2005 in conjunction with section 45E of the Reserve Bank of India Act, 1934 can create a situation where there are requirements to disclose information and confidentiality protections in place.¹⁶

¹³ Puttaswamy, (2017) 10 SCC at 264.

¹⁴ Shohini Sengupta, *Financial Data Protection in Indian Regulatory Policy: From "Secrecy" and "Confidentiality" to "Privacy,"* 12 J. Indian L. & Soc'y 85, 85–88, 97–105 (2021).

¹⁵ Gautam Bhatia, *State Surveillance and the Right to Privacy in India: A Constitutional Biography*, 26 Nat'l L. Sch. India Rev. 127, 127–34, 145–58 (2014).

¹⁶ Atul Singh, *Data Protection: India in the Information Age*, 59 J. Indian L. Inst. 78, 78–80, 90–94 (2017); The Credit Information Companies (Regulation) Act, No. 30 of 2005, India Code (2005); The Reserve Bank of India Act, No. 2 of 1934, India Code (1934), § 45E.

Examining recent legislative developments, a 2025 study by Pratishtha Nandi and Chanjana Elsa Philip evaluates the structural implications of the Digital Personal Data Protection Act 2023 within the Indian financial landscape. Their analysis specifically details how this statutory framework transforms data governance protocols and updates compliance metrics regarding consumer privacy in the banking sector. This Act has been implemented in phases. As of 27th October 2026, the provisions identified for implementation by this date have been implemented. However, the main provisions relating to data processing will not be implemented until 13th May 2027.¹⁷

Jurisprudence underscores the necessity of distinguishing between broad regulatory oversight and targeted state interventions into individual accounts. For instance, while *Joseph Kuruvilla Vellukunnel v. Reserve Bank of India* affirms the extensive supervisory authority vested in the central bank, its ratios focus on systemic institutional management rather than the direct expropriation of personal consumer data. Conversely, *Shankarlal Agarwalla v. State Bank of India* directly addresses the boundaries of traditional banking confidentiality, delineating the operational threshold of recognized exceptions to non-disclosure. Recognizing the potential for regulatory overreach within this paradigm, the Reserve Bank of India issued a seminal administrative directive on February 11, 1998, explicitly titled "Furnishing of Data Violation of Secrecy Obligations," which sought to curb unauthorized data dissemination by financial institutions.¹⁸

V.Regulatory Transparency & Limits To Access

A general reliance by the Reserve Bank on its fiduciary relationship with regulated banks to retain information pursuant to the statutory mechanisms established under the Right to Information Act, 2005 was rejected by the Supreme Court in *Reserve Bank of India v. Jayantilal N. Mistry*. The decision highlighted that the RBI has a duty to the public and depositors under statute. This decision is important as it clarifies that regulatory bodies cannot claim absolute privilege to refuse to disclose information because it was obtained due to their supervisory role. The scope of this decision is strictly limited to public disclosures via the RTI framework,

¹⁷ Pratishtha Nandi & Chanjana Elsa Philip, *An Analysis of Data Protection and Privacy Laws in the Banking Sector in India*, 7 Int'l J. Legal Sci. & Innovation 686, 686–98 (2025), <https://ijlsi.com/article/view/ananalysis-of-data-protection-and-privacy-laws-in-the-banking-sector-in-india>; The Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023), § 1(2); G.S.R. 843(E), Gazette of India, Extraordinary, pt. II sec. 3(i) (Nov. 13, 2025).

¹⁸ *Joseph Kuruvilla Vellukunnel v. Reserve Bank of India*, AIR 1962 SC 1371, 1962 Supp. (3) SCR 632; *Shankarlal Agarwalla v. State Bank of India*, AIR 1987 Cal 29, ¶ 10–12, 27–28; Reserve Bank of India, *Furnishing of Data—Violation of Secrecy Obligations*, DBOD.No.BP.BC.12/21.01.023/98 (Feb. 11, 1998).

meaning it provides no standalone right for individuals to extract private financial data.¹⁹

A critical boundary line separates these public records from situations where regulatory or penal agencies demand banking documents under independent statutes. While the RTI Act serves to open government files to public scrutiny, criminal investigations operate inside their own closed procedural corridors.

No investigative body can legally outrun the narrow terms of its authorizing legislation. Consequently, citing Jayantilal N. Mistry to justify routine, unchecked state intrusion into client accounts represents a serious misinterpretation of the precedent. Every single demand for compelled data production must be measured against its explicit legislative backing, its true evidentiary value, and the precise restrictions placed on the state entity. When an enforcement agency deploys a statutory weapon to force evidence out of a defendant, the procedural and constitutional framework governing the case undergoes a total transformation. It is due to this, we have to look closely at both the context of the request and the specific law backing it up. Data management protocols cannot stop at the moment of collection; statutory rules must rigidly govern how financial information is handled, retained, and purged. At its core, the legal friction does not stem from a total prohibition on state access to bank ledgers. Rather, the analysis must isolate whether public officials can point to an explicit, narrowly tailored legislative mandate that authorizes intrusion for that particular dispute. If the operational boundaries are left vague or fluid, administrative overreach becomes an absolute certainty. Securing sensitive consumer data requires strict statutory limits that prevent state entities from piercing confidentiality outside of explicitly justified exceptions.

VI. Conclusion

Maintaining balance between state imposed transparency and client confidentiality is a challenging task for the existing legal system in India. In practice, the basic fiduciary relationship between a bank and a customer is repeatedly tested throughout the process of tax compliance reviews, asset tracking audits and anti-money laundering investigations. The actual issue is a structural issue where India does not have a single, consolidated financial secrecy law. We have a patchwork quilt of common-law, contracts, courtroom precedents and bits and bytes of sector rules.

It is so broken that any exception they allow a state to have bank records must be construed with caution. The officials are not free to go out on a limb or blanket this law and alter it to

¹⁹ *Reserve Bank of India v. Jayantilal N. Mistry*, (2016) 3 SCC 525.

become a blank check for fishing through a citizen's entire savings history. With the judiciary establishing clear privacy walls under the Article 21, the government has to prove them to be exact cause, clear intent, and irrefutable privacy protection each and every time that it seeks the ledger of its customer.

The intricacies of these knots are in the complex interplay of three Supreme Court precedents: Canara Bank, Puttaswamy and Jayantilal N Mistry. Public interest alone is enough to warrant government access to the account records, but given the limited applications and clearly defined principles of intrusion and the transparency of the procedures. Together, these cases prove that while the state has a legitimate right to regulate financial systems, that power must always be constrained by clear, proportional, and legally sound operational boundaries. Each case adjudicates a different structural facet of financial privacy and state disclosure. A transparent system of rules as to what information can be gathered used stored and communicated, who will be responsible if it is abused, and from whom, and what may be done with it and to what degree, would be beneficial. Such a setup would not prevent the necessary regulation but would lend it greater legitimacy, in that the information would be disclosed legally, appropriately, proportionately, securely, and transparently. Bank secrecy should only be compromised in explicit legal circumstances.

