ANALYSIS OF THE JURISPRUDENCE OF BANKING SECRECY IN THE UNITED STATES OF AMERICA AND UNITED KINGDOM*

Abstract

Banking secrecy and e-banking are critical components of the financial services landscape, particularly in the United States and the United Kingdom, where technological advancements have reshaped traditional banking practices. This paper aims to analyze the jurisprudence surrounding banking secrecy and e-banking in these two jurisdictions, focusing on how legal frameworks have adapted to the challenges posed by digital banking, data privacy, and financial regulation. Utilizing a doctrinal research method, the study examines relevant statutes, case law, and regulatory guidelines to uncover the legal principles governing banking secrecy and e-banking practices. The findings revealed that both the US and the UK have developed robust legal mechanisms to address the complexities of e-banking while ensuring the protection of customer data. However, there are notable differences in their approaches to balancing privacy concerns with regulatory oversight, particularly in areas such as anti-money laundering (AML) compliance and data protection. The paper recommends enhancing cross-border legal collaboration and updating regulatory frameworks to better address the evolving risks in e-banking. By doing so, both jurisdictions can strengthen their financial systems while ensuring that banking secrecy and customer protection remains paramount in the digital age.

Keywords: Banking secrecy, E-banking, Financial crimes, Jurisprudence.

1. Introduction

Banking secrecy, also known as financial privacy, has long been a cornerstone of the relationship between financial institutions and their clients/customers. It embodies the principle that banks must protect the confidentiality of their customers' financial information from unauthorized disclosure. This concept has been fundamental to fostering trust in the banking sector, allowing customers to manage their finances with a sense of security. However, the advent of globalization, technological advancements, and the rise of financial crimes has increasingly tested the boundaries of banking secrecy, leading to significant legal and regulatory challenges. In the United States (US) and the United Kingdom (UK), two of the world's leading financial hubs, the jurisprudence surrounding banking secrecy has evolved in response to these pressures. Both jurisdictions have had to strike a delicate balance between maintaining the privacy of financial information and fulfilling their obligations to combat money laundering, tax evasion, and other forms of financial malfeasance. The regulatory frameworks in these countries have been shaped by a combination of domestic legislation, international agreements, and judicial interpretations, each contributing to a multipart and often contentious legal landscape.

2. The Jurisprudence of Banking Secrecy and E-Banking in the US and UK

United States of America:

By the late 1960s, US law enforcement authorities generally recognized that bank secrecy laws in foreign countries were proving to be a significant impediment to the effective investigation of organized crime and other criminal activities. At that time, the only effective means available to obtain information on financial transactions in foreign countries was the issuance of letters rogatory. While the use of letters rogatory is a time honored technique, it was and, to this day, remains cumbersome. Sometimes, it takes up to two years to obtain records by this method, and even when they are obtained, if they relate to the bank account of a customer and are protected by secrecy laws, they may not be disclosed.[1] In response to this problem, in 1970, the US Congress passed a law that has become popularly known as the Bank Secrecy Act (BSA).[2] It has been legislated to identify the financial flows of financial institutions and their sources to and from the United States on the one hand, and to achieve the interest of government authorities, especially the tax authority, in knowing the financial data of bank clients on the other hand.[3] In the United States, a variety of legal doctrines, grounded in contract, agency,[4] and tort[5] theory, recognize and protect the interest of individuals in financial privacy.[6] Some of these

***By Kingsley Chukwunonso EHUJUO, LLB, BL, LLM, ACArb, PhD (in-view),** Faculty of Law, Nnamdi Azikiwe University, Awka; Private Legal Practitioner, Chartered Arbitrator and Notary Public, E-mail: kcehujuo@yahoo.com, Phone: +234 806 775 2132; and

***Meshach Nnama UMENWEKE, PhD, FCIArb, FICMC, ACTI,** Professor of Tax Law, Faculty of Law, Nnamdi Azikiwe University, Awka, E-mail: meshaynau@yahoo.com, Phone: +234 803 709 0048.

[1] G L Hilsher, 'Banking Secrecy: Coping with Money Laundering in the International Arena' <https://www.elibrary.imf.org/display/book/9781557751423/ch12.xml> accessed 4 May 2024.

[2] Bank Secrecy Act, 1970

[3] M S Al-Ajami, Limits of the Bank's Commitment to Banking Secrecy and the Legal Implications of its Disclosure (Master Thesis in Law, Middle East University, Amman, 2001) 29.

[4] *Peterson v Idaho First Nat'l Bank*, 83 Idaho 578, 367 P.2d 284 (1961); *Grainy Dev. Corp. v Taksen*, 400 N.Y.S.2d 717 (Ct. App.), aff'd, 411 N.Y.S.2d 756 (1978),

[5] L Fischer, *The Law of Financial Privacy: A Compliance Guide* (Warren, Gorham & Lamont, 1983) 4.

[6] *California Bankers Ass'n v. Shultz*, 416 U.S.21, 85 (1974)

rights are codified in the Right to Financial Privacy Act, which protects individual financial privacy rights from interference by the State.[7]

The Bank Secrecy Act,[8] enacted in 1970, imposes record keeping and reporting requirements on financial institutions in order to supply law enforcement with evidence of financial transactions.[9] The Right to Financial Privacy Act of 1978, enacted in response to the Supreme Court's decision to allow the requirements of the Bank Secrecy Act to override the protections of the fourth amendment in *United States v Miller*,[10] protects the rights of individuals to financial privacy. The Money Laundering Control Act of 1986 (the Act),[11] enacted to prevent parts of the Bank Secrecy Act from being circumvented by money launderers, supplements the Bank Secrecy Act and the Right to Financial Privacy Act, and creates new substantive criminal offenses for money laundering. The Banking Secrecy Act, for example, requires financial institutions to file reports with the Internal Revenue Service for all deposits, withdrawals, exchange payments, or transfers that exceed ten thousand dollars involving a United States financial institution.[12] Under Chapter 3, if an individual exports from, imports into, or receives within the United States currency or other monetary instruments in excess of ten thousand dollars, that individual must file a report with the customs office.[13] Furthermore, Chapter 4 requires any citizen, resident, or person doing business in the United States to report on his or her tax return a financial interest in, or authority over, a foreign financial account.[14]

The Right to Financial Privacy Act of 1978 (RFPA)[15] was enacted to restore the balance between an individual's right to privacy and the exigencies of law enforcement. In restrictive interpretations of the fourth amendment in *Schultz*[16] and *United States v Miller*,[17] the Supreme Court failed to recognize that individuals have a reasonable expectation of privacy in financial records even though the records are not owned or possessed by the individual. The RFPA provides, with a number of very important exceptions, that where the United States government requires a financial institution to provide information relating to its customers' financial records, the government must first obtain a subpoena, search warrant, or other appropriate authorization, comply with certain prior notice requirements, and certify to the financial institution that it has complied with the provisions of the RFPA. If the government fails to fulfill any of these requirements, the financial institution is prohibited from complying with its request for disclosure.[18] The exceptions to the application of the RFPA provide that the RFPA does not apply to records not identified with particular customers, to records required pursuant to the exercise of supervisory or regulatory authority, or to various other classes of records, including those requested by subpoena or court order issued in connection with proceedings before a grand jury. Records of corporations are not protected, as corporations are deemed not to have privacy rights.[19]

With the Money Laundering Control Act of 1986, Congress amended the Banking Secrecy Act to promote its enforcement.[20] One purpose of the amendments was to overrule a line of cases that allowed persons to escape liability when they structured their transactions to evade the reporting requirements.[21] The amendments also brought within the scope of the Banking Secrecy Act individuals who either prevent or attempt to prevent a domestic financial institution from filing a required report[22] or who cause such an institution to file a report that contains either a material omission or a misstatement of fact.[23] The amendments also provide for potential liability for persons who structure, attempt to structure, assist in structuring, or attempt to assist in structuring transactions with the intent to evade reporting requirements.[24] In addition, the amendments make it more difficult for certain institutions to obtain exemptions from the

[7] Title XI of the Financial Regulatory Interest Control Act of 1978, Pub. L. No. 95-630, 92 Stat. 3641.
[8] Bank Secrecy Act, 1970
[9] *California Bankers Ass'n v Schultz*, 416 U.S. 21 (1974),
[10] 425 U.S. 435 (1976)
[11] Money, Laundering Control Act of 1986
[12] Money, Laundering Control Act of 1986, § 1829b (referring to 31 U.S.C. § 5313 (1988) which mandates reports on domestic currency transactions); 31 C.F.R. § 103.22 (1990)
[13] Money, Laundering Control Act of 1986§ 1829b (referring to 31 U.S.C. § 5316 (1988) which mandates reports on exporting and importing monetary instruments); 31 C.F.R. § 103.23 (1990).
[14] 12 U.S.C. § 1829b (referring to 31 U.S.C. § 5314 (1988) which mandates recording and reporting foreign financial agency transactions); 31 C.F.R. § 103.24 (1990).
[15] Title XI of the Financial Institution Regulatory and Interest Rate Control Act of 1978, Pub. L. No. 95-630, 92 Stat. 3641, reprinted in 1978 U.S. CODE CONG. & ADMIN. NEWS 9305 (codified in scattered sections of 31 U.S.C.); see 31 C.F.R. § 14 (1986)
[16] *California Bankers Ass'n v Schultz* (n 9)
[17] *United States v Miller* (n 10)
[18] 1978 U.S. CODE CONG. & ADMIN. NEWS at 9278.
[19] 12 U.S.C.A. § 3401(4) (West Supp. 1985).
[20] Pub. L. No. 99-570, 100 Stat. 3207 (1986)
[21] C T Plombeck, 'Confidentiality and Disclosure: The Money Laundering Control Act of 1986 and Banking Secrecy' (1988) 22 *Int'l Law*, 84-85.
[22] 31 U.S.C. § 5324(1) (1988).
[23] *Ibid,* § 5324(2).
[24] *Ibid,* § 5324(3).

reporting requirements.[25] The Banking Secrecy Act and its regulations[26] impose various reporting requirements on individuals and assorted 'financial institutions' for certain financial transactions.[27]Whoever willfully violates any regulation under this chapter shall be fined not more than $1,000 or imprisoned not more than one year, or both.[28] Whoever willfully violates, or willfully causes a violation of any regulation under this chapter, section 1829b of this title, or section 1730d of this title, where the violation is committed in furtherance of the commission of any violation of Federal law punishable by imprisonment for more than one year, shall be fined not more than $10,000 or imprisoned not more than five years, or both.[29] Existing section 5318 of the Bank Secrecy Act authorizes the Secretary of the Treasury to delegate compliance authority,[30] regulate compliance procedures, and prescribe exemptions from the requirements of the Bank Secrecy Act. The exemption authority granted by this section was designed to reduce unnecessary reports from retail enterprises, such as grocery stores, that deal directly with consumers and normally generate large volumes of cash.[31] New section 5318(f) provides that no person may qualify for an exemption unless the relevant financial institution prepares and maintains a statement that describes in detail the reasons why such person is qualified for such exemption and such statement is signed by the person seeking exemption.[32]

There is no doubt that the United States of America has always been vanguard of anti-money laundering and terrorist financing regime. The procedure for disclosing customers' secrecy is however well streamlined and regulated that it would be near impossible for a financial institution to abuse its customer's right to confidentiality under it. No financial institution is granted the omnibus power to arbitrarily stop a customer's transaction under the guise of compliance.[33] The procedure requires that a federal law enforcement agency investigating terrorist activity or money laundering may request that the Financial Crimes Enforcement Network (FinCEN) solicit on its behalf, certain information from a financial institution or a group of financial institutions on certain individuals or entities. The said law enforcement agency is, however, mandatorily required to provide a written Certification to FinCEN attesting that credible evidence of money laundering or terrorist activity exists. It is from the attestation that inferences can be eventually drawn as to whether or not the report or suspicion was made in good faith. Upon receipt of the Certification, FinCEN would request the financial institution first to confirm the identity of the particular customer, and second, whether or not such alleged suspicious transaction or account is maintained with the bank. The general guidelines specify that the record to be searched is limited to only the current account(s) maintained by the named subject during the preceding 12 months. Consequently, the level and frequency of such monitoring and reporting of suspicious activity will depend, among other things, on the risk assessment and the actual activity in the account.[34]

On the State level, the response to the Supreme Court's BSA/privacy analysis has been similar - a qualified recognition of financial privacy generally modeled after the congressional model. State level recognition of financial privacy flows from three sources: State constitutions, a common law duty of financial confidentiality, and state financial privacy legislation. The California Supreme Court in *Burrows v Superior Court* held that article 1, section 13 of the California Constitution provides a bank customer financial privacy in the bank's records of his other account.[35] The court determined that the depositor had a reasonable expectation that the bank would maintain the confidentiality of his account information.[36] A State agency violates this privacy interest when it acquires access to the information without first resorting to legal process.[37] One year later, the California Supreme Court extended this analysis in *Valley Bank of Nevada v Superior Court.*[38] Based on its earlier recognition of a constitutionally protected privacy interest, the court held that a customer has standing in a civil action to contest disclosure.[39] The court's reasoning was grounded in its continued refusal to allow a third party waiver of the customer's legitimate expectation of privacy. The assumption is that the institution decides disclosure requests on the basis of its own set of reasons instead of those of the client.[40] The effect of the case of

[25]Plombeck (n 21) 86
[26] 12 U.S.C. § 1730d (1988)
[27]*Ibid,* § 1953; 31 C.F.R. § 103.22 (1990).
[28]12 U.S.C. § 1956
[29]12 U.S.C § 1957
[30] 31 U.S.C.A. § 5318(a) (West Supp. 1986); *United States v Deak-Perera & Co*., 566 F. Supp. 1398 (D.C. Cir. 1983).
[31] 31 U.S.C.A. § 5318 (West Supp. 1986).
[32] Act § 1356(b); 51 Fed. Reg. 45108 (West Supp. 1986); 52 Fed. Reg. 11436 (West Supp. 1987).
[33] USA Patriot Act, s 806
[34]DSC Risk Management Manual of Examination Policies Federal Deposit Insurance Corporation <htpp://ffiec.gov/bsa_aml_infobase/documents/FDIC_Docs/BSA_Manual .pdf> accessed 5 May 2024; Report on USA Patriot Act Violations, North American Law Center, March 2017 <www.TNALC.org> accessed 5 May 2024.
[35]*Burrows,* 13 Cal. 3d at 238, 529 P.2d at 590, 118 Cal. Rptr. at 166.
[36]*Ibid,* 243, 529 P.2d at 593, 118 Cal. Rptr. at 169.
[37]*Ibid,* 245, 529 P.2d at 594-95, 118 Cal. Rptr. at 170-71.
[38] 15 Cal. 3d 652, 542 P.2d 977, 125 Cal. Rptr. 553 (1975).
[39]*Ibid,* 658, 542 P.2d at 980, 125 Cal. Rptr. at 556
[40]*Ibid,* 657, 542 P.2d at 979, 125 Cal. Rptr. at 555.

Valley Bank is a requirement that the bank take reasonable steps to notify the customer prior to disclosure. It is only through notice that the customer can exercise his right to challenge the process.[41]

A number of State courts have recognized a common law duty of financial confidentiality. According to the strongest theory, this duty arises from an implied contract between the financial institution and the depositor. Even in the United States of America, the decision in the *Tournier's* case was applied by an Appellate Court, in Florida, in the case of *Milohnich v First National Bank of Miami Springs*,[42] in determining whether or not financial privacy is based on contract or tort and the majority held that a bank had an implied contractual duty to maintain the confidential information of its customers.[43] Following the September 11 attacks, the USA PATRIOT Act was enacted in 2001 to enhance national security and address financial crimes, including terrorism financing. The Act expanded the scope of the BSA by imposing additional requirements on financial institutions, such as enhanced customer identification procedures and increased information sharing among banks and government agencies.[44]

The legal landscape surrounding e-banking in the US is constantly evolving to keep pace with technological advancements. The pioneers of online banking in the United States were first Net Bank in 1996, with WingSpan following in 1997. Traditional banks had developed earlier versions of telephone banking, but they started using internet banking in 1998.[45] Indisputably, the internet has revolutionized the way people manage their money and the growth of internet banking in the United States has been enormous. According to Nielsen Ratings, from fall of 2001 to fall of 2003, there was a 79 percent increase in the number of people conducting banking transactions over the internet. The United States established a legal framework for electronic records and signatures in interstate commerce.[46] Uniform Electronic Transactions Act (UETA)[47] adopted by many States, complements E-SIGN by addressing broader issues related to electronic transactions, including contract formation. The US also has the Electronic Fund Transfer Act (EFTA) which **p**rovides consumer protections for electronic fund transfers, including ATM withdrawals and online bill payments.[48] The jurisprudence of banking secrecy and e-banking in the US reflects a constant balancing act between protecting individual privacy and addressing security concerns. Legal frameworks and judicial decisions strive to ensure that financial institutions implement robust security measures while maintaining transparency and regulatory oversight.

United Kingdom:

In contrast to many countries, the UK has an uncodified Constitution, consisting instead of a number of different documents.[49] However, much of the UK's Constitution is materialised in written form and given the power of constitutional principles, such as parliamentary sovereignty,[50] the Royal prerogatives,[51] parliamentary privilege,[52] and constitutional conventions.[53] With regard to banking confidentiality, as the ECHR[53a] considered as part of the UK constitution, it is necessary to explore the protection of banking confidentiality within the ECHR, to examine how well banking confidentiality is protected therein. Under English, the bank's duty of secrecy or confidentiality, from a legal point of view, is well established on the basis of principles of contract as debtor and creditor.[54] *Tournier v National Provincial and Union Bank of England*[55] is the leading case in transforming the duty of confidentiality from a mere moral duty into a legal obligation. Tournier's bank account was overdrawn, and he reached an agreement with the Bank to repay on regular instalments of £1 per week. As he did not have a fixed address, he gave the Bank the address of his employer. After he failed to repay the agreed amount, the branch manager of the Bank called Tournier's employer for the purpose of getting Tournier's private address. While speaking, the branch manager informed Tournier's employer about his current overdraft, and that he was betting heavily. After becoming aware of Tournier's situation, his employer refused to employ him after his probationary period. For this, Tournier sued the bank for breach of confidentiality. Bankes LJ held:

[41] *Ibid,* 658, 542 P.2d at 980, 125 Cal. Rptr. at 556; *Charnes v DiGiocomo*, 200 Colo. 94, 612 P.2d 1117 (1980); *Commonwealth v DeJohn*, 486 Pa. 32,403 A.2d 1283, cert. denied, 444 U.S. 1032 (1979); *Suburban Trust Co. v Waller*, 44 Md. App. 335, 408 A.2d 758 (1979).

[42] *Milohnich v First National Bank of Miami Springs*, 224 So. 2d 759 (Fla. Dist. Ct. App. 1969)

[43] D Newcomb *et al*, 'United States' in G Godfrey (eds), *Neate and Godfrey: Bank Confidentiality* (Bloomsbury Professional 2010) 816.

[44] R A Baker, '*The USA Patriot Act and Financial Privacy: Balancing Security and Privacy*' (2005) 10 (1) *Journal of Financial Regulation*, 20-34.

[45] C K Laudon and G C Traver, *E-Commerce: Business, Technology, Society* (2nd edn, Pearson Education, 2003) 639.

[46] E-SIGN Act, 15 U.S.C. § 7001 et seq

[47] Uniform Electronic Transactions Act

[48] Electronic Fund Transfer Act, 15 U.S.C. § 1693 et seq

[49] D G Cracknell, *Constitutional and Administrative Law* (London: Routledge-Cavendish, 2007).

[50] I Loveland, *Constitutional Law: A Critical Introduction* (2nd edn, London, Butterworths, 2000) 19.

[51] *Ibid*, 75

[52] *Ibid*, 212

[53] *Ibid*, 246

[53a] European Convention on Human Rights

[54] *Foley v Hill* (1848) 9 ER 1002, 1005

[55] *Tournier v National Provincial and Union Bank of England* [1924] 1 KB, 481, 485

> On principle I think that the qualifications can be classified under four headings: (a) where disclosure is under compulsion by law; (b) where there is a duty to the public to disclose; (c) where the interests of the bank require disclosure; (d) where the disclosure is made by the express or implied consent of the customer'.

This pronouncement by Bankes LJ, established, for the first time, the existence of bank's implied contractual duty of secrecy and it is clear that it is not absolute. Until the decision of the *Tournier's* case, the bank's duty of secrecy to its customer has been held to be a moral duty only, and Bankes LJ stated that there was no authority on the point prior to this case.[56] Nevertheless, prior to the *Tournier's* case, there had been cases[57] where issues in relation to a breach of duty of secrecy had been litigated but no decision was made upon whether or not there existed a legal duty of secrecy or confidentiality. The courts were reluctant to impose a duty of secrecy on a bank and rather implied that the obligation was a matter of moral, not legal.[58] The reason for not imposing an obligation of secrecy on a bank despite a number of litigations, it is argued, is that banks would responsibly exercise the trust reposed in them and there was no need for the imposition of an obligation.[59] The third qualification to the bank's duty of confidentiality is where to do so is in the interest of the bank. In the *Tournier's* case, Bankes LJ, give as an example of this, circumstances 'where a bank issues a writ claiming payment of an overdraft stating on the face of the writ the amount of the overdraft'. Another example is where a bank had to dishonour a cheque. In the case of *Sunderland v Barclays Bank Ltd*,[60] a banker was asked by a customer why a cheque was dishonoured and he informed the customer that a series of cheques were made out by his wife to a bookmaker. The court accepted this by stating that the banker had to give reason why the cheque was dishonoured.

The Banking Services Review Committee (Jack Report)[61] in 1989 also identified the decision in *Tournier's* case as the general starting point of the history of bank's duty of secrecy. The Jack Committee recommended in its report[62] that the duty of confidentiality should be codified in order to protect customers from continued endless exceptions; however, the British Government rejected the recommendations, claiming that this might cause difficulties and confusion. Furthermore, the Jack Committee argues that the principle of confidentiality is a tradition which should be respected and if under threat, it should be strongly emphasized because 'its roots go deeper than the business of banking: it has to do with the kind of society in which we want to live'.[63] In its broader economic sense, a duty of secrecy can be justified on a number of grounds. Aplin *et al*[64] identified seven potential justifications for the imposition of a duty of secrecy, namely 'to incentivise the creation of certain information, to prevent socially undesirable expenditure of resources preserving secrecy, to prevent the unjust enrichment of one person at the expense of another, to preserve and promote ethical standards of conduct, to promote individual autonomy, to give effect to an implicit societal agreement and to promote the national interest.' Therefore, one can argue that there are strong justifications that favour the imposition of a duty of secrecy on banks that confidential financial information about customers need not be disclosed to third party except in certain circumstances.

Nevertheless, there are two legislations considered to be relevant to the duty to protect confidential information in the UK, to wit: the Data Protection Act 1998 (DPA 1998) and the Human Rights Act 1998 (HRA 1998). Under DPA 1998,[65] banks and other businesses are under obligation that they use personal information for the purpose(s) for which it was obtained and to protect it in the course of processing and transferring it. HRA 1998 incorporates the European Convention for the Protection of Human Rights and Fundamental Freedoms 1950 (ECHR 1950) into English law. Under the HRA 1998, courts are required to construe all legislations 'so far as it is possible to do so' in line with ECHR.[66] The HRA 1998 makes it unlawful for 'public authority' to act in a way that is incompatible with ECHR rights.[67] As courts are 'public authority,'[68] they have to act in a way that gives effect to ECHR's requirements. Courts are also authorised to declare legislation incompatible if found to be in contradiction with ECHR rights.[69] The HRA 1998 does not give private citizens the right to bring direct horizontal action against each other under ECHR, but it does have an indirect horizontal effect on proceedings brought by private citizens. The relevant Article of ECHR which duty of confidentiality has to fall under is Article 8. Under Article 8 (1), 'everyone has the right to respect for his private and family life, his home and his

[56] *Tournier* (n 55), 473
[57] *Hardy v Veasey* (1868) LR 3 Ex. 107
[58] *Ibid*.
[59] R Cranston, *Principles of Banking Law* (2nd edn, Oxford University Press, 2002) 168.
[60] (1938) 5 LDAB 163
[61] HM Treasury, 'Banking Services: Law and Practice' (Report by the Review Committee1989, Cm. 622) (Jack Report)) para. 5.1
[62] *Ibid,* 622
[63] *Ibid,* para 5.26
[64] T Aplin *et al*, *Gurry on Breach of Confidence: The Protection of Confidential Information* (2nd edn, Oxford University Press, 2012) 76 – 77.
[65] Data Protection Act 1998 s 4
[66] Human Rights Act 1998, s 3
[67] *Ibid*, s 6(1)
[68] *Ibid*, s 6(3)
[69] *Ibid,*s 4

correspondence'. Although, the rights under Article 8 are qualified, it is argued that there is evidence that Article 8 is influencing the development of the general law that protects confidence and there is no reason why this cannot be extend to bank's duty of confidentiality.[70]

Part 1, Schedule 1 of the Data Protection Act (DPA) defines personal data as, 'data which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual'. 'Processing' is given a wide meaning, and includes, 'obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including: (a) organisation, adaptation or alteration of the information or data, (b) retrieval, consultation or use of the information or data, (c) disclosure of the information or data by transmission, dissemination or otherwise making available, or (d) alignment, combination, blocking, erasure or destruction of the information or data'. Schedule 2, Paragraph 6 (1) of the DPA protects individuals against any unlawful use of their personal data, and controls processing and movement of such collective data. Moreover, according to the DPA, personal data should be used fairly and lawfully; personal data should be obtained for specific purposes, and all appropriate measures should be taken while storing this data in order to prevent any unauthorised misuse of individuals' data. The UK Banking Code has therefore been made wide-ranging enough to include all the personal information without any limitations:[71]

> A duty of confidence arises when confidential information comes to the knowledge of a person (the confidant) in circumstances where he has notice, or is held to have agreed, that the information is confidential, with the effect that it would be just in all the circumstances that he should be precluded from disclosing the information from others… to this broad general principle there are three limiting principles … the first ... is that the principle of confidentiality only applies to information to the extent that it is confidential ... the second limiting principle ... is that the duty of confidences applies neither to useless information, nor to trivia … the third limiting principle ... is that, although the basis of the law's protection of confidence is that there is a public interest that confidence should be preserved and protected by the law, nevertheless the public interest may be outweighed by some countervailing public interest which favours disclosure….[72]

There are two reported cases involving major international fraud where the English courts have relaxed the duty of banker confidentiality on public duty grounds. In *Price Waterhouse (a firm) v BCCI Holdings (Luxembourg) SA*,[73] a firm of accountants applied to the court for a declaration that its duty of confidentiality did not prevent it from supplying documents and information to a British Government inquiry into the collapse of Bank of Credit and Commerce International ('BCCI'). The accountants wished to voluntarily supply confidential bank documents to an inquiry into, reportedly, the biggest bank fraud in history. The High Court granted the declaration, holding that the public interest in confidentiality was outweighed by the public interest in disclosure of confidential documents. Millett J stated that: 'The duty of confidentiality, whether contractual or equitable, is subject to a limiting principle. It is subject to the right, not merely the duty, to disclose information where there is a higher public interest in disclosure than in maintaining confidentiality'.[74]

The court considered that there was a strong public interest in disclosing documents to an inquiry that was mandated to investigate the supervisory functions and performance of the Bank of England in the context of an international fraud that had damaged the reputation of the British financial system. In *Pharaon v Bank of Credit and Commerce International SA (in liq) (Price Waterhouse (a firm) intervening)*,[75] another case concerning the collapse of BCCI, the issue was whether the duty of confidentiality under English law was outweighed by the public interest in disclosure to a private party litigant in American civil proceedings. UK case law has significantly shaped the jurisprudence of banking secrecy and e-banking. For instance, the case of *R v Oakes*[76] highlighted the tension between banking secrecy and the need for law enforcement access to financial records. The court emphasized that while banking confidentiality is important, it must be balanced against legitimate law enforcement interests in investigating financial crimes. Another case is the case of *Lloyds TSB v Mark*,[77] the High Court considered issues related to the disclosure of customer information under the DPA. The court reinforced the principle that while financial institutions must protect customer information, they are also obligated to comply with lawful requests for disclosure, particularly when required for regulatory or legal purposes. The Proceeds of Crime Act 2002 (POCA) also plays a critical role in addressing financial crimes, including money laundering. It requires financial institutions to report suspicious activities and implement anti-money laundering

[70] EP Ellinger and others, *Ellinger's Modern Banking Law* (5th edn Oxford University Press, 2011) 175-176.
[71] Banking Code 2005, Para. 11.1
[72] *Attorney-General v Guardian Newspapers Ltd* (No. 2) 1990, 1 AC 109, at 281-2
[73] [1992] BCLC 583.
[74] *Price Waterhouse (a firm) v BCCI Holdings (Luxembourg) SA* (n 72) 601
[75] [1998] 4 All ER 455
[76] *R v. Oakes* [1997] EWCA Crim 1287
[77] *Lloyds TSB v. Mark* [2007] EWHC 2924 (QB)

measures. While POCA enhances transparency, it also creates tension with banking secrecy by mandating disclosure of certain financial information.[78] The Financial Services and Markets Act, 2000 (FSMA) provides the regulatory framework for financial services in the UK, including e-banking. It grants the Financial Conduct Authority (FCA) broad powers to supervise and enforce compliance with financial regulations, including those related to data protection and privacy.[79] The Electronic Communications, Act 2000 provides a framework for electronic transactions, including e-banking. It addresses issues related to electronic signatures, records, and communications, facilitating the legal recognition of digital transactions and contributing to the regulatory environment for e-banking.[80] This Act aims to support the growth of e-commerce while ensuring the integrity and confidentiality of electronic communications. The Cybercrime Act, 2019 addresses emerging threats in the digital space, including cyber-attacks and data breaches. The Act enhances the UK's ability to combat cybercrime and imposes obligations on organizations, including banks, to protect against and report cyber incidents. It aligns with international efforts to strengthen cyber security and maintain the confidentiality of financial information.[81] As a member of the international community, the UK adheres to global standards and agreements related to financial privacy and e-banking. This includes compliance with international conventions and collaboration with other countries to address cross-border financial crimes and data protection issues.[82]

International Standards on Banking Secrecy and E-Banking

Nearly all countries with developed legal systems respect banking secrecy. The differences between the countries are of degree rather than substance. There is little divergence on the rule that a bank may not disclose information on its customers to other private persons. However, there is significant divergence on the degree to which banks must disclose such information to government authorities. The main debate, therefore, centers on the extent to which the country should have direct access to information kept by banks about its citizens or the citizens of another country. However, this is not by any means the only debate.[83]There are no international standards that specifically address both banking secrecy and e-banking. However, there are a number of international standards and recommendations that apply to each area individually. For instance, the Financial Action Task Force (FATF) is an inter-governmental organization that sets international standards for combating money laundering and terrorist financing. FATF Recommendation 40 on Customer Due Diligence (CDD) is a key standard that requires banks to identify and verify their customers, and to understand the nature and purpose of their banking relationships.[84] Another recommendation of the FATF addresses the need for timely and effective international cooperation in criminal matters. It emphasizes the importance of having legal mechanisms in place to facilitate the exchange of information and evidence between countries, which can affect how banking secrecy is managed across borders.[85] The Basel Committee, established by Central Banks in 1974, provides international banking standards to enhance the safety and soundness of the global banking system. The Basel guidelines focus on various aspects of banking, including risk management and supervision. The Basel III framework, in response to the 2008 financial crisis, introduced requirements for capital adequacy, liquidity, and risk management. While it primarily focuses on financial stability, Basel III also indirectly affects banking secrecy by establishing standards for transparency and disclosure, which can influence how financial institutions manage and disclose information.[86]

The European Union (EU) is notable for measures taken to pierce banking secrecy at the international level. There are at least two reasons for this. First, the concept of a single international market requires a harmonized secrecy and disclosure duty for financial transactions. Second, because only one authorization is required to trade in any of the member States, the 'single passport', bank secrecy needs to be synchronized, and regulatory authorities need to be able to exchange information. This practice is stretched to include exchanges of tax information. Not all member States wholly share the view that information should be freely exchanged for bank supervision purposes. Austria, Greece, Luxembourg, and Portugal have tight secrecy laws compared to other member states. Bank secrecy is only one of the areas where the idea of the unitary country conflicts with autonomy.[87] The General Data Protection Regulation (GDPR) which came into effect

[78] Home Office, '*Proceeds of Crime Act 2002*', <https://www.gov.uk/government/collections/proceeds-of-crime-act> accessed 22 August 2024.
[79] Financial Conduct Authority (FCA), '*Financial Services and Markets Act 2000*', <https://www.fca.org.uk/firms/financial-services-markets-act-2000> accessed 22 August 2024.
[80] J Smith, *The Electronic Communications Act 2000: A New Legal Framework for E-Commerce* (Cambridge University Press 2001).
[81] UK Government, '*Cybercrime Act 2019'*<https://www.gov.uk/government/collections/cybercrime-act-2019> accessed 22 August 2024.
[82] UK Government, '*Cybercrime Act 2019'*<https://www.gov.uk/government/collections/cybercrime-act-2019> accessed 22 August 2024.
[83]P R Wood, 'International Law on Bank Secrecy' <https://www.elibrary.imf.org/display/book/9781557756954/ch039.xml> accessed 5 May 2024.
[84]Bank Secrecy Act/Anti-Money Laundering (BSA/AML) <https://www.fdic.gov/resources/bankers/bank-secrecy-act/> accessed 5 May 2024.
[85] FATF, '*FATF Recommendations',* <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html> accessed 22 August 2024.
[86] Basel Committee on Banking Supervision (BCBS), '*Basel III: A Global Regulatory Framework for More Resilient Banks and Banking Systems'*<https://www.bis.org/publ/bcbs189.htm> accessed 22 August 2024.
[87]Wood (n 83)

on May 25, 2018, is a comprehensive data protection regulation adopted by the European Union. Although it is an EU regulation, its extra-territorial reach means that it applies to any entity processing the personal data of EU residents, including financial institutions operating outside the EU. Article 5 sets out principles for data processing, including the requirement to process data lawfully, fairly, and transparently. It mandates that financial institutions ensure the security and confidentiality of personal data, including data related to e-banking (European Union, 2016). Article 32 requires organizations to implement appropriate technical and organizational measures to ensure the security of personal data. This includes safeguarding against unauthorized access and ensuring the confidentiality of electronic communications, which is crucial for e-banking.[88]

The UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 (The Vienna Convention, as it is commonly referred to, has been ratified by over 100 countries.[89] It sets out minimum standards; requires countries to criminalize drug trafficking and the international laundering of the proceeds; and provides for mutual legal assistance. This convention specifically overrides bank secrecy. It is the most far-reaching multilateral treaty on criminal assistance).[90] A number of countries trace bank secrecy back to provisions in their Constitutions, which, for example, protect the privacy of citizens[91] or guarantee the individual's right to an uninhibited development of his personality.[92] It appears unusual that bank secrecy is actually constitutionally entrenched, and the discussion of the constitutional basis appears to be often no more than an indication of a parallel desire to protect individual freedom by entrenching privacy against the country. Where bank secrecy has indeed been elevated to an issue of constitutional significance, the effect may be that a higher parliamentary majority is required to change the law and that violations are justiciable before a constitutional court set up to protect the Constitution. An example is section 38 of the Austrian Banking Act of 1993. However, there have been decisions in a number of jurisdictions where, for example, search and seizure powers by the tax authorities have been held not to be unconstitutional.[93]

In view of the divergent international attitudes toward bank secrecy, there are bound to be international conflicts between courts. Typically, the head office or parent of a bank in one jurisdiction is legally obliged to disclose information held by its foreign branch or subsidiary, which is legally obliged not to disclose by the foreign law applying where the branch or subsidiary is located. Many of the cases have involved the extra-territorial jurisdiction of US law and courts. The US courts have sometimes permitted a 'good faith' defense if the US bank acted in good faith by endeavoring to comply with the US order for disclosure by its foreign branch or subsidiary but is frustrated because disclosure would involve a violation of foreign law.[94]

3. Lessons for Nigeria

Nigeria has a lot to learn from both the US and UK regarding banking secrecy. Below is a breakdown of the two countries' approaches and potential lessons for Nigeria:

***Balancing Privacy and Transparency*:** Nigeria can learn from the challenges faced in finding the right balance between privacy rights and transparency obligations in the banking sector. The US follows a compliance-based system. Banks are required to report suspicious activity and comply with Know Your Customer (KYC) regulations. This helps identify and prevent money laundering and terrorist financing. It is essential to constantly evaluate and potentially revise legal frameworks to ensure that customer confidentiality is maintained while also preventing illicit activities like money laundering.

***Regulatory Framework*:** Nigeria should consider implementing a comprehensive legal framework specifically addressing banking secrecy such as the US Banking Secrecy Act in order to enhance the stability of the financial system and increase customer and investor confidence in the banking sector. While regulatory bodies play a significant role in ensuring banking secrecy, having specific laws can further strengthen the protection of customer information.

Security Challenges in E-banking: Nigeria needs to address security challenges in e-banking, such as fraudulent activities and cyber threats. These challenges stem from issues like international barriers to law enforcement, lack of

[88] European Union, '*General Data Protection Regulation (GDPR)',*<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679> accessed 22 August 2024.

[89] UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances

[90]Wood (n 83)

[91] J Fernandez-Armesto and L Hiniker, 'Spain' in F Neate and R McCormick (eds.), *Bank Confidentiality* (International Bar Association,1990) 187 (quoting Article 18.1 of the Spanish Constitution)

[92] W Hauser, 'Germany' in F Neate and R McCormick (eds.), *Bank Confidentiality* (International Bar Association, 1990) 129 (discussing protections under Article 2 of Germany's Constitution).

[93]*United States v Miller*, 425 U.S. 435 (1976); Fernandez-Armesto and Hiniker (n 96) 643-644

[94]Restatement (Third) of the Law of Foreign Relations § 442 (1987); SocieteInternationale pour Participations Industrielles et Commerciales, *S.A. v. Rogers*, 357 U.S. 197 (1958) (good faith defense recognized by Supreme Court); *Ings v Ferguson*, 282 F.2d 149 (2d Cir. 1960)

standard implementation, and communication infrastructure for law enforcement agents. Tackling these issues, along with improving national databases and cyber security measures, can lead to a more secure e-banking environment.

Jurisprudence Analysis: Nigeria can benefit from analysing the jurisprudence of banking secrecy and e-banking in other jurisdictions like the US and UK. For instance, under DPA 1998,[95] banks and other businesses are under obligation that they use personal information for the purpose(s) for which it was obtained and to protect it in the course of processing and transferring it. There is no doubt that the United States of America has always been vanguard of anti-money laundering and terrorist financing regime. The procedure for disclosing customers' secrecy are however well streamlined and regulated that it would be near impossible for a financial institution to abuse it customer's right to confidentiality under it. No financial institution is granted the omnibus power to arbitrarily stop a customer's transaction under the guise of compliance.[96]

4. Conclusion and Recommendations

The law of bank secrecy is primarily concerned with compulsory disclosure. The bank's duty of secrecy has been well established for such a long time and it is an essential feature of the bank-customer relationship. In some jurisdictions, the duty of bank secrecy is based on constitution or criminal code. The duty is not absolute but subject to qualifications. It allows the disclosure of financial information of customers to a third party where there is compulsion by law, where it is in public interest, where it is in the bank's interest and where the customer consents to it. By virtue of its nature, a professional relationship imposes on the professional person, who is confided or whose professional service is engaged, a duty to respect the confidentiality of disclosure made to him in his professional capacity. This duty applies to bankers, doctors, solicitors and other professionals. While the extent of the duty of each of these professionals differs from each other by virtue of their peculiarity, they all share the same underlying principle on which the duty of confidentiality is founded. Launching public awareness campaigns to educate customers about the benefits and risks of e-banking can help build trust and confidence in online banking services. Providing guidance on safe banking practices, recognizes potential scams, and reporting suspicious activities can empower customers to protect their financial information. The UK and US have both established themselves as major players in the global financial system. While their approaches differ slightly, Nigeria can learn valuable lessons from both in regards to banking secrecy and e-banking. Thus, Nigeria should learn from their well-defined regulations and reporting structures to strengthen its own AML framework, while calibrating the level of banking secrecy allowed. There is however need for a synergy between the CBN and the National Orientation Agency to educate e-banking consumers on their rights and remedies in law. The work also recommended that an independent body be established for the resolution of e-banking consumer disputes and complaints. Establishing partnership between financial institutions, regulatory bodies, law enforcement agencies and cyber security experts can facilitate information sharing and collaboration in combating financial crimes and enhancing data security in the banking sector. This collaborative approach can strengthen the overall resilience of the financial system.

[95] Data Protection Act 1998 s 4

[96] USA Patriot Act, s 806