Vanderbilt Journal of Entertainment & Technology Law

Volume 23 | Issue 4 Article 3

2021

Privacy Beyond Possession: Solving the Access Conundrum in Digital Dollars

Nerenda N. Atako

Privacy Beyond Possession: Solving the Access Conundrum in Digital Dollars

ABSTRACT

The advent of a retail central bank digital currency (CBDC) could reshape the US payments system. A retail CBDC would be a digital representation of the US dollar in the form of an account or token that is widely accessible to the general public. It would be a third form of US fiat money that is created and issued by the Federal Reserve and complementary to physical cash. CBDC proposals have suggested a myriad of retail CBDC design models with an overwhelming interest in a retail CBDC that either implements a centralized ledger system or some form of a distributed ledger system to process payments. The technology of a retail CBDC would enable instantaneous payments for consumers and greater transparency for government officials. Additionally, CBDC proponents are championing retail CBDC as a tool to promote financial inclusion. However, antiquated US privacy protections may be inadequate to safeguard against the potential risks to individual privacy within digital payments and consequently undermine financial inclusion. A retail CBDC system that is under the control of the Federal Reserve could bolster regulatory compliance and oversight but also exacerbate workarounds by government entities in the current US privacy framework that are concerning for individual privacy in the age of big data and dataveillance. A proper privacy framework governing retail CBDC records would alleviate risks to privacy and enhance public trust in a retail CBDC system. Refining the Privacy Act of 1974 or creating a new regulatory framework that is informed by both the Privacy Act and the impact of innovative data analytics would help balance the inherent tension between privacy and transparency of user identity and transactions within a retail CBDC system under the control of the Federal Reserve.

TABLE OF CONTENTS

Central banks around the world have undertaken various roles in promoting innovative digital payment solutions to advance several objectives, including financial inclusion and efficiency.[1] Relatedly, the rise of cryptocurrencies, such as Bitcoin, has demonstrated the need for a resilient digital currency in the global economy. Yet, the proliferation of cryptocurrency has sparked concerns about competition from private currencies and the privatization of monetary policy.[2] In 2019, Facebook was met with legislative and regulatory scrutiny when it announced a plan to develop Libra[3]—a price-stabilized cryptocurrency (also known as stablecoin) whose value is tied to a set of existing government-issued currencies.[4] COVID-19 has further highlighted the shortcomings of antiquated financial systems and accelerated central banks' exploration

1. *See* Michael S. Barr, Adrienne A. Harris, Lev Menand & Wenqi (Michael) Xu, *Building the Payment System of the Future: How Central Banks Can Improve Payments to Enhance Financial Inclusion* 23–27 (Univ. of Mich. Ctr. on Fin., L. & Pol'y, Working Paper No. 3, 2020).

2. *See* John Crawford, Lev Menand & Morgan Ricks, *FedAccounts: Digital Dollars*, 89 GEO. WASH. L. REV. 113, 115 (2021) [hereinafter *FedAccounts*].

3. Clare Duffy, *Facebook Gets More Official Pushback on Libra*, CNN, https://www.cnn.com/2019/07/03/tech/facebook-libra-us-lawmakers/index.html [https://perma.cc/M5UR-N72A] (last updated July 9, 2019, 4:28 PM).

4. *See* LIBRA ASS'N MEMBERS, WHITE PAPER V2.0, at 2 (2020), https://wp.diem.com/en-US/wp-content/uploads/sites/23/2020/04/Libra_WhitePaperV2_April2020.pdf [https://perma.cc/4PVQ-KFPS]. Libra Coins consist of a multicurrency coin and single-currency stablecoins. *Id.*

of innovative payment solutions, most notably central bank digital currency (CBDC).[5]

Specifically, central banks are exploring the concept of retail CBDC (or general purpose CBDC), which would be a digital form of fiat currency that is created and issued by a country's monetary authority, the liability of the monetary authority, and widely accessible to the general public.[6] A retail CBDC would function as an additional option to physical cash. This form of digital currency would modernize the US banking infrastructure by leveraging innovative technology to extend access to central bank money. The United States is confronting the need to reform its banking system not only to move towards a technologically advanced future and address lingering financial inclusion issues but also to join the global exploration of CBDC. The COVID-19 Pandemic (particularly the prolonged delay of stimulus payments) has demonstrated the clear need for critical government infrastructures to expand the functionality and utility of the dollar.[7] The US financial system currently excludes 6.5 percent of US households from the mainstream banking system (the unbanked population) and fails to serve the financial needs of 18.7 percent of US households (the underbanked population).[8] A retail CBDC could alleviate barriers to

5. *See* Paul Wong & Jesse Leigh Maniff, *Comparing Means of Payment: What Role for a Central Bank Digital Currency?*, FEDS NOTES (Aug. 13, 2020), https://doi.org/10.17016/2380-7172.2739 [https://perma.cc/V9BQ-E7G9] ("The COVID-19 pandemic has also led central banks to think further about potential enhancements to the general safety and efficiency of payment systems, including developing a digital currency"); *see also* Caitlin Reilly, *Delayed COVID-19 Aid Spurs Search for Faster Payments*, ROLL CALL (June 23, 2020, 6:59 AM), https://www.rollcall.com/2020/06/23/delayed-covid-19-aid-spurs-search-for-faster-payments/ [https://perma.cc/JL4S-QAKJ].

6. CODRUTA BOAR & ANDREAS WEHRLI, BANK FOR INT'L SETTLEMENTS, BIS PAPERS NO. 114, READY, STEADY, GO? – RESULTS OF THE THIRD BIS SURVEY ON CENTRAL BANK DIGITAL CURRENCY 4 (2021) [hereinafter BIS SURVEY].

7. Chris Brummer, Agnes N. Williams Rsch. Professor & Fac. Dir., Georgetown Inst. of Int'l Econ. L., Remarks at Digital Dollar Live, at 12:07 (July 21, 2020), *in* ACCENTURE, https://www.accenture.com/_acnmedia/PDF-130/Accenture-Digital-Dollar-Live-Video-Transcript.pdf#zoom=50 [https://perma.cc/U8DD-GNNT]; *see also* OUSMÈNE JACQUES MANDENG & JOHN VELISSARIOS, ACCENTURE, THE (R)EVOLUTION OF MONEY II: BLOCKCHAIN EMPOWERED CENTRAL BANK DIGITAL CURRENCIES 4 (2019), https://www.accenture.com/_acnmedia/PDF-105/Accenture-Revolution-of-Money-II-2019.pdf#zoom=50 [https://perma.cc/VUN6-ZME3].

8. FED. DEPOSIT INS. CORP., 2017 FDIC NATIONAL SURVEY OF UNBANKED AND UNDERBANKED HOUSEHOLDS 17 (2018), https://www.economicinclusion.gov/downloads/2017_FDIC_Unbanked_HH_Survey_Report.pdf [https://perma.cc/BZ5M-DRZ3] (finding that 6.5 percent of households were unbanked and 18.7 percent of households were underbanked in 2017).

participation in the US financial system by expanding access to the money supply or serving as a springboard to quality financial services.[9]

According to a survey conducted in 2020 by the Bank for International Settlements (BIS), nearly 86 percent of the sixty-five central banks that responded are exploring CBDC to some extent.[10] Central banks are examining retail CBDC for various motivations, including financial stability, monetary policy implementation, financial inclusion, efficiency in domestic and cross-border payments, and the safety and robustness of payments.[11] Countries all over the world have undertaken CBDC exploration projects at different stages of research or development.[12] Among these projects include the monetary authorities of the Bahamas, China, and Sweden. In October 2020, the Central Bank of the Bahamas launched the world's first "live" nationwide retail CBDC in the form of its Sand Dollar.[13] The People's Bank of China issued the first pilots of its digital yuan, formerly known as Digital Currency Electronic Payment (DCEP), in April 2020.[14] The first DCEP pilots processed over three million transactions, totaling more than RMB 1.1 billion ($162 million USD).[15] The Sveriges Riksbank initiated its e-krona project in response to the declining use of cash and is performing pilot tests of payment, deposit, and transfer capabilities for the e-krona.[16]

---

9. *See FedAccounts*, *supra* note 2, at 125–30; ACCENTURE & DIGIT. DOLLAR FOUND., THE DIGITAL DOLLAR PROJECT: EXPLORING A US CBDC 13 (2020) [hereinafter THE DIGITAL DOLLAR PROJECT], https://static1.squarespace.com/static/5e16627eb901b656f2c174ca/t/5f0c5d052d6235002637d0f6/1594645769165/Digital-Dollar-Project-Whitepaper_vF_7_13_20.pdf [https://perma.cc/4TEK-39S6].

10. BIS SURVEY, *supra* note 6, at 6.

11. *Id.* at 6–8.

12. *Id.* at 6.

13. *Id.* at 3; *see also* Sebastian Sinclair, *Central Bank of Bahamas Launches Landmark 'Sand Dollar' Digital Currency*, COINDESK, https://www.coindesk.com/central-bank-of-bahamas-launches-landmark-sand-dollar-digital-currency [https://perma.cc/94AG-DFGV] (last updated Oct. 21, 2020, 9:50 AM).

14. Ada Hui, *China Central Bank Official Reveals Results of First Digital Yuan Pilots*, COINDESK, https://www.coindesk.com/china-central-bank-official-reveals-results-of-first-digital-yuan-pilots [https://perma.cc/8N83-37U3] (last updated Oct. 9, 2020, 11:32 AM).

15. *Id.* ("The digital wallets processed . . . digital yuan transactions between April and August when the pilots launched and ended . . . making it the most widely used central bank digital currency (CBDC) in a commercial setting.").

16. Rafaela Lindeberg & Ott Ummelas, *Sweden Explores Moving to a Digital Currency*, BLOOMBERG, https://www.bloomberg.com/news/articles/2020-12-11/sweden-explores-the-feasibility-of-moving-to-a-digital-currency [https://perma.cc/ZDF3-AR45] (last updated Dec. 30, 2020, 9:04 AM).

Relative to other countries, the United States has been slow to embrace the concept of digital currency.[17] As of this writing, the Board of Governors of the Federal Reserve System[18] has not announced any plans to launch a CBDC in the near future, but it has shifted its position on CBDC from one of skepticism to one of insistence in remaining "on the frontier of research and policy development regarding CBDCs."[19] Federal Reserve Banks are now actively researching CBDC and relevant technologies.[20] The Federal Reserve Bank of Boston is collaborating with the Digital Currency Initiative at the Massachusetts Institute of Technology on a multiyear project exploring the use of technologies to test a hypothetical CBDC,[21] and the Federal Reserve Bank of New York established an innovation center via an initiative with the Bank for International Settlements to explore relevant trends and fintech developments.[22]

The decision to issue a retail CBDC is driven by both domestic circumstances[23] and seeming pressure for central banks to stay at the forefront of innovation.[24] The issuance of a US retail CBDC is almost inevitable given the rapid digitalization of the global economy and the ever importance of the US dollar as the world's reserve currency.[25] The issuance of other sovereign digital currencies presents the opportunity

---

17. Billy Bambrough, *The U.S. 'Falling Behind' on Digital Dollar*, FORBES (July 22, 2020, 4:52 AM), https://www.forbes.com/sites/billybambrough/2020/07/22/the-us-is-falling-behind-on-digital-dollar/?sh=61b7082420e9 [https://perma.cc/9U7U-PJGQ].

18. The Federal Reserve System is the US Central Bank and is composed of three key entities: the Federal Reserve Board of Governors, twelve Federal Reserve Banks, and the Federal Open Market Committee. *Structure of the Federal Reserve System*, FED. RSRV., https://www.federalreserve.gov/aboutthefed/structure-federal-reserve-system.htm [https://perma.cc/SVS2-9X23] (last updated Mar. 3, 2017). The use of "Federal Reserve" in this Note refers to the Federal Reserve System. *See id.*

19. *See* Lael Brainard, Governor, Bd. of Governors of the Fed. Rsrv. Sys., An Update on Digital Currencies, Speech at the Federal Reserve Board and Federal Reserve Bank of San Francisco's Innovation Office Hours (Aug. 13, 2020), *in* FED. RSRV., https://www.federalreserve.gov/newsevents/speech/brainard20200813a.htm [https://perma.cc/4A7B-SS4T].

20. *See id.*

21. *See id.*

22. *See id.*

23. BANK OF CANADA, EUR. CENT. BANK, BANK OF JAPAN, SVERIGES RIKSBANK, SWISS NAT'L BANK, BANK OF ENG., BD. OF GOVERNORS FED. RSRV. SYS. & BANK FOR INT'L SETTLEMENTS, CENTRAL BANK DIGITAL CURRENCIES: FOUNDATIONAL PRINCIPLES AND CORE FEATURES 2 (2020) [hereinafter BIS CBDC REPORT], https://www.bis.org/publ/othp33.pdf [https://perma.cc/YD7T-QT9V].

24. Jason Brett, *Why Chris Giancarlo Considers a Digital Dollar Mission Critical for the World*, FORBES (Apr. 26, 2020, 2:31 PM), https://www.forbes.com/sites/jasonbrett/2020/04/26/why-chris-giancarlo-considers-a-digital-dollar-mission-critical-for-the-world/?sh=2b6c131d3c41 [https://perma.cc/WJZ3-898Z].

25. *See id.*; THE DIGITAL DOLLAR PROJECT, *supra* note 9, at 31–32.

for sovereign states to bypass the global banking system or compete with the US dollar for global prominence.[26] The Federal Reserve is seemingly on the path to eventually issuing a retail CBDC in the future.[27] Furthermore, the Biden-Harris administration—particularly given the appointment of federal agency heads who are proponents of digital currency[28]—may accelerate the issuance of a retail CBDC in an effort to reassert US global governance.[29] The maintenance of the US dollar's prominence as a currency in the global economy also comes with additional responsibility in designing and implementing a US retail CBDC because a US digital currency would likely set the stage for the global community.[30] Therefore, the digital transformation of the world demands a resilient US digital payments infrastructure that provides immediacy and integration between payments and digital services—both domestically and internationally—and also ensures cybersecurity, privacy, and reliability.[31]

CBDC offers many benefits but also presents unique risks. CBDC would strengthen the traceability of money and offer financial regulators greater control, transparency, and oversight.[32] A CBDC

---

26. *See* THE DIGITAL DOLLAR PROJECT, *supra* note 9, at 32; *see also* Brett, *supra* note 24.

27. *See* Brainard, *supra* note 19.

28. *See* Michael J. Casey, *Money Reimagined: Letter to President Biden*, COINDESK, https://www.coindesk.com/money-reimagined-letter-to-president-biden [https://perma.cc/FH5L-FYR7] (last updated Jan. 22, 2021, 4:46 PM) (reporting on "Biden's crypto gang").

29. *See* George Ingram, *Renewing US Global Engagement in a Changed World*, BROOKINGS (Jan. 12, 2021), https://www.brookings.edu/blog/up-front/2021/01/12/renewing-us-global-engagement-in-a-changed-world/ [https://perma.cc/67XD-8ZTZ].

30. *See* Sharon Bowen, Former Comm'r, Commodity Futures Trading Comm'n, Remarks at Digital Dollar Live, at 24:31 (July 21, 2020), *in* ACCENTURE https://www.accenture.com/_acnmedia/PDF-130/Accenture-Digital-Dollar-Live-Video-Transcript.pdf#zoom=50 [https://perma.cc/U8DD-GNNT]; Sheila Warren, Head of Blockchain & Data Pol'y, Member of the Exec. Comm., World Econ. F., Remarks at Digital Dollar Live, at 29:02 (July 21, 2020), *in* ACCENTURE https://www.accenture.com/_acnmedia/PDF-130/Accenture-Digital-Dollar-Live-Video-Transcript.pdf#zoom=50 [https://perma.cc/U8DD-GNNT]; *see also* Tim Alper, *Fed Chief Bets That US's 'First-Mover Advantage' in CBDC Race Is Stronger than China's*, CRYPTONEWS (Jan. 15, 2021), https://cryptonews.com/news/fed-chief-bets-that-us-s-first-mover-advantage-in-cbdc-race-8913.htm [https://perma.cc/8RJ9-YU9C].

31. *See generally* Fabio Panetta, Member, Exec. Bd. of the Eur. Cent. Bank, Speech at the Deutsche Bundesbank Conference on the "Future of Payments in Europe" (Nov. 27, 2020), *in* EUROOPAN KESKUSPANKKI, https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp201127~a781c4e0fc.fi.html [https://perma.cc/9MM9-EQ5K] (explaining how digital transformation has impacted consumer demands).

32. *See* Sarah Allen, Srdjan Capkun, Ittay Eyal, Giulia Fanti, Bryan Ford, James Grimmelmann, Ari Juels, Kari Kostiainen, Sarah Meiklejohn, Andrew Miller, Eswar Prasad, Karl Wüst & Fan Zhang, *Design Choice for Central Bank Digital Currency: Policy and Technical Considerations* 11–13 (Glob. Econ. & Dev. at Brookings, Working Paper No. 140, 2020) [hereinafter Brookings Paper], https://www.brookings.edu/wp-content/uploads/2020/07/Design-Choices-for-CBDC_Final-for-web.pdf [https://perma.cc/B7SE-3QJB].

could provide the Federal Reserve a real-time, panoramic view of the financial system and bolster data sharing between government entities for regulatory interests, such as preventing money laundering.[33] Conversely, the enhanced visibility provided by a CBDC also poses a concern for individual privacy. What data will be collected by a CBDC? Who will have access to CBDC data? How will CBDC data be used? Moreover, a CBDC could be programmable—such that government officials can embed code in a retail CBDC that will enable them to see transactional history or other insights regardless of who directly operates the system.[34] Consequently, government officials could utilize a retail CBDC as a policy tool for economic benefit while also undertaking measures that may encroach on individual privacy if there is no clear boundary in place that limits use of retail CBDC data. The wide adoption of a retail CBDC necessitates serious consideration of privacy concerns to foster public trust in the system.[35] Although CBDC could leverage privacy-enhancing technologies to promote trust in the system, legal choices can further enhance trust in a CBDC amid regulatory obligations by providing parameters in the collection, access, and use of retail CBDC data.

This Note examines the inherent tension between privacy and transparency of user identity and transactions within a retail CBDC operated by the Federal Reserve. A retail CBDC would generally grant the Federal Reserve unprecedented access to personal information and financial data, and thereby implicate material privacy concerns. This Note suggests that the Privacy Act of 1974 be applied to CBDC records and refined in several ways to protect individual privacy or alternatively, a new regulatory framework informed by the Privacy Act be adopted to directly respond to the rising privacy demands of a retail CBDC. Part I discusses general technical aspects of a retail CBDC, provisions of the Privacy Act, key financial privacy laws, and current anti-money laundering and countering the financing of terrorism

33. *See id.* at 63–64. *See generally* Jennifer Shasky Calvery, Glob. Head of Fin. Crime Threat Mitigation & Grp. Gen. Manager, HSBC, Remarks at the Central Bank of the Future Conference: Panel No. 4—Anti-Money Laundering and Financial Inclusion (Oct. 2, 2019), *in* UNIV. OF MICH. CTR. ON FIN. L. & POL'Y, http://financelawpolicy.umich.edu/central-bank-of-the-future-conference [https://perma.cc/7X8H-WH7M] (providing ways AML practices can be improved, including "understanding from a high definition view of what is the probability that someone poses a high financial crime risk. Zoom in and understand where there is risk and pinpoint it and take appropriate actions.").

34. *See* Brookings Paper, *supra* note 32, at 64–66; *see also* BANK OF ENG., CENTRAL BANK DIGITAL CURRENCY: OPPORTUNITIES, CHALLENGES AND DESIGN 45–46 (2020), https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf [https://perma.cc/G6FX-B3FP].

35. Bowen, *supra* note 30, at 33:30.

(AML/CFT) jurisprudence and regulatory practices. Part II examines the efficacy of the Privacy Act's protections and identifies shortcomings of the Act in consideration of potential use cases of retail CBDC records, vulnerabilities for non-US citizens and non-US permanent residents, and government information-sharing practices under the Act's routine use exception. Part III suggests that retail CBDC records would likely constitute a "system of records" under the Privacy Act but necessitate stronger privacy protections that go beyond the mere possession of information in order to prevent use cases of big data that would undermine individual privacy in a retail CBDC and consequently thwart freedom of expression and freedom of association. It proposes either (1) amending the Privacy Act to balance the government's vantage point in a retail CBDC or (2) creating a new privacy framework informed by the Privacy Act that responds to the privacy demands of a retail CBDC under the control of the Federal Reserve. It recommends amending the Privacy Act to (a) expressly protect individuals who are noncitizens or nonpermanent residents of the United States, (b) prescribe permissible uses of retail CBDC records and implement a tiered access approach to the disclosure of CBDC records, (c) limit the routine use exception to protection under the Act in the context of a retail CBDC to prevent backdoor access to invasive government surveillance and unwarranted disclosure of individual records, (d) bolster procedural requirements for access to retail CBDC records, and (e) impose more stringent liability provisions for the misuse of retail CBDC records. This approach would strike a proper balance between privacy and transparency by preserving some expectation of individual privacy from needless government surveillance while permitting regulatory innovation and legitimate law enforcement actions.

I. INNOVATION AND PRIVACY IN DIGITAL PAYMENTS

A. What Is Central Bank Digital Currency?

Central bank digital currency is a digital form of fiat currency created and issued by a central bank.[36] Fiat money, such as the US dollar, is a currency that lacks intrinsic value and is declared a legal tender by government decree. Currently, the Federal Reserve issues two forms of fiat money—physical cash (banknotes)[37] and reserves (or

36. *See* BIS SURVEY, *supra* note 6, at 4.

37. *See* FED. RSRV. SYS., THE FEDERAL RESERVE SYSTEM: PURPOSES & FUNCTIONS 134–35 (10th ed. 2016), https://www.federalreserve.gov/aboutthefed/files/pf_complete.pdf [https://perma.cc/M4QX-9MHA]. Coins are not liabilities of the Federal Reserve Banks. *Id.* The

"wholesale" CBDC).[38] Physical cash is a liability of the Federal Reserve and distributed to the general public through depository institutions.[39] The general public can hold demand deposits at depository institutions (bank accounts) from which physical cash can be obtained.[40] Unlike physical cash, deposits are direct liabilities of the issuing intermediary.[41] Conversely, reserves held at the Federal Reserve are exclusive to qualified financial institutions and government entities.[42] A retail CBDC would be a third form of fiat money that is a liability of the central bank, complements physical cash, and can be made available to the general public through digital wallets or deposits held at the central bank or a financial intermediary depending on the policy choices of a CBDC.[43]

A retail CBDC is an opportunity to transform the dollar and US payments system. Innovative digital payment platforms, such as Venmo, have reshaped consumer expectations and normalized cashless transactions. Venmo is a peer-to-peer mobile payments application that offers users the ability to link their bank accounts, debit cards, or credit cards to a Venmo account (or digital wallet) from which users can transfer funds to other Venmo accounts.[44] Unlike Venmo, where a user must transfer funds from a financial intermediary to conduct transactions on the application, a CBDC could represent these funds. A CBDC would remove a step in the payment process by eliminating the transfer (information exchange) between financial intermediaries. The Federal Reserve could promote the realization of CBDC's slated opportunities by serving as a provider of a secure and resilient payments infrastructure that is widely accessible to the general public.[45]

Retail CBDC proposals have included various concepts with different design choices.[46] Retail CBDC can take the form of two

---

United States Mint issues coins and sells them to the Federal Reserve Banks, which in turn, sell them to depository institutions. *Id.*

38. *See* Laura Hopper, *Does the Federal Reserve Print Money?*, FED. RSRV. BANK ST. LOUIS (Nov. 1, 2017), https://www.stlouisfed.org/open-vault/2017/november/does-federal-reserve-print-money [https://perma.cc/X34A-NCW6]; BIS CBDC REPORT, *supra* note 23, at 4.

39. "Federal Reserve notes in circulation are liabilities of the Federal Reserve Banks and are collateralized by the assets of the Reserve Banks." FED. RSRV. SYS., *supra* note 37, at 134.

40. *See* THE DIGITAL DOLLAR PROJECT, *supra* note 9, at 26.

41. FED. RSRV. SYS., *supra* note 37, at 134.

42. *See FedAccounts*, *supra* note 2, at 115–16.

43. *See* BIS SURVEY, *supra* note 6, at 4.

44. *What Is Venmo?*, VENMO, https://help.venmo.com/hc/en-us/articles/221011388-What-is-Venmo- [https://perma.cc/7F9U-VKH2] (last visited Mar. 21, 2021).

45. *See* BIS CBDC REPORT, *supra* note 23, at 1.

46. Brookings Paper, *supra* note 32, at 10–11.

technical designs: "accounts" or "tokens."[47] An account is a representation of money in the form of electronic ledger entries.[48] An account-based CBDC would be a demand deposit account[49] denominated in CBDC and use a centralized ledger system.[50] The centralized ledger system would rely on a central authority (i.e., the Federal Reserve or a financial intermediary) to authorize CBDC transactions and control a ledger that records CBDC account balances.[51] For example, FedAccounts is an account-based CBDC proposal that offers the general public (US citizens, residents, and domestically domiciled businesses and institutions) the option to hold accounts at the Federal Reserve.[52] FedAccounts would differ from standard bank accounts in that they are fully sovereign base money and possess no fees or minimum balances, interest on balances, instant in-network payments, and no interchange fees.[53] For the purposes of this Note, an account-based CBDC possesses the aforementioned qualities of a FedAccount; and conversely, is available to all persons in the United States that satisfy Know Your Customer standards.

In contrast, a token is a bearer instrument.[54] A token-based CBDC could operate using distributed ledger technology (DLT).[55] Blockchain technology is mentioned in several CBDC proposals and is popularly known for facilitating Bitcoin transactions.[56] For example, the Digital Dollar Project is a token-based CBDC proposal that offers a tokenized dollar accessible to all persons in the United States. The proposed example would be fully fungible with Federal Reserve notes and reserves, potentially use a DLT-informed infrastructure, utilize the existing two-tiered banking system, and possess the potential for additional programmable capabilities.[57] For the purposes of this Note's

47. *See id.*; *see also* WORLD ECON. F., CENTRAL BANK DIGITAL CURRENCY POLICY-MAKER TOOLKIT 9 (2020) [hereinafter WEF TOOLKIT], http://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit.pdf [https://perma.cc/875R-5RBM].

48. *See FedAccounts*, *supra* note 2, at 124; KEVIN WERBACH, THE BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST 30 (2018).

49. Brookings Paper, *supra* note 32, at 10–11.

50. *See id.*

51. *See id.* at 19–22.

52. *FedAccounts*, *supra* note 2, at 116, 122.

53. *Id.* at 122–23.

54. *See* WERBACH, *supra* note 48, at 9 (explaining that cash is a bearer instrument, as it is valuable in itself).

55. Brookings Paper, *supra* note 32, at 11.

56. *See* WEF TOOLKIT, *supra* note 47, at 10–11. *See generally* THE DIGITAL DOLLAR PROJECT, *supra* note 9, at 11, 18 (explaining the tokenization of the dollar and distributed ledger technology).

57. *See* THE DIGITAL DOLLAR PROJECT, *supra* note 9, at 7–12, 18.

analysis, a token-based CBDC possesses the aforementioned qualities of the Digital Dollar Project proposal, but conversely, it uses a decentralized network under the control of the Federal Reserve notwithstanding how the CBDC is distributed to the general public. Like token-based CBDC, account-based CBDC could also use a permissioned blockchain. A retail CBDC could also use different types of DLT or non-DLT solutions.[58]

Due to current regulatory objectives, such as anti-money laundering compliance, it is unlikely a retail CBDC would be untraceable and enable complete anonymity like cash. The Congressional Research Service has conceded that a CBDC that allows absolute anonymity would be inconsistent with the current anti-money laundering regime.[59] Therefore, a retail CBDC—whether account-based or token-based—would not enable complete cash-like transactions because a CBDC would undoubtedly use a compliant ledger-based system.[60]

1. The Process of Payments

The key distinction between accounts and tokens is the payment verification process.[61] An account-based CBDC payments system would verify the identity of the account holder to circumvent identity theft.[62] In comparison, a token-based CBDC payments system would authenticate the validity of a token to avoid potential "electronic counterfeiting."[63] Additionally, the process of payments depends on the type of ledger technology (centralized versus distributed) of a CBDC.

Currently, retail payments between account holders at different banks use an automated clearing house (ACH) for the clearing and settlement of payments.[64] An ACH is a centralized system that clears and settles transfers between depository institutions.[65] "Clearing" is the

58. *See* Brookings Paper, *supra* note 32, at 12–24.

59. MARC LABONTE, REBECCA M. NELSON & DAVID W. PERKINS, CONG. RSCH. SERV., IF11471, FINANCIAL INNOVATION: CENTRAL BANK DIGITAL CURRENCIES 2 (2020).

60. *See* BANK OF ENG., *supra* note 34, at 47 ("[A]ny CBDC would need to be compatible with AML obligations, ruling out truly anonymous payments.").

61. *See* COMM. ON PAYMENTS & MKT. INFRASTRUCTURES & MKTS. COMM., BANK FOR INT'L SETTLEMENTS, CENTRAL BANK DIGITAL CURRENCIES 4 (2018) [hereinafter COMM. ON PAYMENTS], https://www.bis.org/cpmi/publ/d174.pdf [https://perma.cc/R453-XYXZ].

62. *See id.*

63. *See id.*

64. *FedNow Service: Frequently Asked Questions*, FED. RSRV., https://www.federalreserve.gov/paymentsystems/fednow_faq.htm [https://perma.cc/MN3F-7SM4] (last updated Aug. 6, 2020).

65. *Id.*

process of receiving and reconciling information about a payment and can include additional activities such as a fraud screening.[66] "Settlement" is the process of debiting and crediting account balances to transfer funds.[67] An ACH essentially connects the separate ledgers of different payment providers.[68] This results in delayed transfers and other significant inefficiencies.[69] Additionally, the Federal Reserve has a centralized payments infrastructure (real-time gross settlement (RTGS))[70] that processes interbank transfers (not retail payments) in real time.[71] Therefore, it is unnecessary for the Federal Reserve to rely on DLT for an account-based CBDC.[72] An account-based CBDC could use the Federal Reserve's RTGS system and offer instantaneous payments.[73]

Alternatively, a retail CBDC could use a distributed ledger system to facilitate transactions.[74] DLT enables a "shared state" between network participants without a central authority.[75] A series of smart contracts could be the mechanism to reconcile and complete the transfer of digital currency between users.[76] Smart contracts are computer code (or software programs) that execute instructions on a blockchain.[77] A smart contract verifies the legitimacy of the transaction.[78] If conditions of the transfer are met, the transaction will be recorded in the ledger and completed.[79] For example, user A initiates a promise that she will send a certain amount of bitcoin to user B. The transfer of bitcoin constitutes a contractual agreement (a specification

66. *Id.*

67. *Id.*

68. *See id.*

69. *See FedAccounts*, *supra* note 2, at 130–32.

70. *See id.*; Lael Brainard, Governor, Bd. of Governors of the Fed. Rsrv. Sys., Delivering Fast Payments for All, Speech at the Federal Reserve Bank of Kansas City Town Hall (Aug. 5, 2019), *in* FED. RSRV., https://www.federalreserve.gov/newsevents/speech/brainard20190805a.htm [https://perma.cc/EZS5-ZD9D].

71. *See FedAccounts*, *supra* note 2, at 130–32; *see also* COMM. ON PAYMENTS, *supra* note 61, at 7.

72. Helen Partz, *European Central Bank Execs Explain Why CBDCs Don't Need Blockchain*, COINTELEGRAPH (Sept. 21, 2020), https://cointelegraph.com/news/european-central-bank-execs-explain-why-cbdcs-don-t-need-blockchain [https://perma.cc/35CF-VGVP].

73. *See FedAccounts*, *supra* note 2, at 130–32.

74. *See* WEF TOOLKIT, *supra* note 47, at 10–11.

75. *See* WERBACH, *supra* note 48, at 64.

76. *See id.* at 63–64.

77. *Id.*

78. *See* Josh Stark, *Making Sense of Blockchain Smart Contracts*, COINDESK, https://www.coindesk.com/making-sense-smart-contracts [https://perma.cc/85HP-WGTP] (last updated June 7, 2016, 4:48 PM).

79. WERBACH, *supra* note 48, at 63–64.

of rights and obligations).[80] A smart contract ensures that user A does not renege on her promise to transfer bitcoin to user B by synchronizing the rights and obligations of the transfer (i.e., the amount of bitcoin) to execute the contractual agreement between user A and user B.[81]

2. Smart Money and Digital Privacy

A retail CBDC could leverage DLT (or numerous, trusted variations) to become "smart" money.[82] Smart money would be programmable and allow the Federal Reserve (or other government entities) precise control over a retail CBDC.[83] A retail CBDC could be non-fungible (unlike physical cash) to the extent that different capabilities are programmed into the CBDC.[84] Additionally, a retail CBDC would likely use a permissioned decentralized network. A permissioned decentralized network would enable the Federal Reserve to control who has access to the retail CBDC network, regulate the activity of CBDC users, and specify the terms under which the system grants shared access to transaction information for certain CBDC network participants.[85] For instance, the Federal Reserve could permit other governmental entities access to CBDC transaction data, or it could utilize smart contracts in a retail CBDC to receive certain insights that inform regulatory oversight.[86] On the other hand, the precise control over CBDC could also aid in the inappropriate surveillance discussed in Part III. The programmability of a retail CBDC offers endless possibilities but poses major risks for privacy in the absence of a proper privacy framework.

This Note focuses on a US retail CBDC that uses either a centralized ledger system or a permissioned decentralized system under the control of the Federal Reserve—particularly to the extent that the Federal Reserve is the central authority of CBDC records. This includes a CBDC system that requires the Federal Reserve to engage in recordkeeping, such as CBDC accounts directly held at the Federal Reserve; CBDC accounts held as "pass-through"[87] accounts at a

80. *Id.*

81. *Id.*

82. *See* Brookings Paper, *supra* note 32, at 47–48, 64–68; *see also* BANK OF ENG., *supra* note 34, at 41–42, 45–46.

83. *See* Brookings Paper, *supra* note 32, at 64–65; *see also* BANK OF ENG., *supra* note 34, at 45–46.

84. *See* Brookings Paper, *supra* note 32, at 64–65.

85. *See* WERBACH, *supra* note 48, at 60.

86. *See id.*

87. *See* Banking for All Act, S. 3571, 116th Cong. § 3 (2020) (as introduced by Sen. Sherrod Brown) (defining pass-through accounts).

financial intermediary; a CBDC token that is implemented on a ledger directly accessible by the Federal Reserve; and more broadly, a CBDC token that is programmable (i.e., embedded supervision via smart contracts)[88] by the Federal Reserve. It will exclusively address the inherent tension between individual privacy and financial integrity standards within a retail CBDC. Although a third party could manage regulatory due diligence for a retail CBDC system under the control of the Federal Reserve, such an arrangement would not preclude the Federal Reserve's direct access to financial records in its ledger or through generated insights. This Note will not discuss technical granularities of a retail CBDC, privacy-enhancing technologies, or cybersecurity.

B. The "Expectation" of Financial Privacy

Retail CBDC will inevitably generate a digital financial footprint given the incidence of transaction records. What this digital financial footprint reveals about individuals could implicate material privacy concerns. The scale of recordkeeping in a retail CBDC could amass a wide range of personal information and financial data into a system of records. Theoretically, this could result in government access to personal information that invades individual privacy. Thus, the successful implementation and wide adoption of retail CBDC requires a revised privacy framework to account for technological advancements.

1. Fair Information Practices: Privacy Act of 1974

Presently, the Federal Reserve is subject to the Privacy Act of 1974.[89] Congress enacted the Privacy Act to curb unwarranted invasions of individual privacy by federal agencies.[90] The Act was drafted in response to the increased use of information systems within government operations.[91] Innovations in computerized databases enabled federal agencies to easily cross-reference an individual's personal information and potentially compile various personal details

88. *See* Brookings Paper, *supra* note 32, at 47–48, 64–68; *see also* BANK OF ENG., *supra* note 34, at 41–42, 45–46.

89. 5 U.S.C. § 552a; 12 C.F.R. § 261a (2020).

90. *See* Privacy Act of 1974, Pub. L. No. 93-579, § 2(b), 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a) ("The purpose of this Act [enacting this section and provisions set out as notes under this section] is to provide certain safeguards for an individual against an invasion of personal privacy").

91. *See id.*

about an individual in a database.[92] The Privacy Act governs the collection, maintenance, use, and dissemination of personally identifiable information[93] contained in a system of records by federal agencies.[94] The Act allows US citizens and permanent residents to bring civil actions against the federal government for violations of the statute and provides for civil damages.[95] Note, the Act only protects US citizens and permanent residents, and therefore, undocumented immigrants and nonimmigrants (F-1 visa students, B1/B2 business visitors or tourists, K-1 visa fiancées, and individuals with temporary protected status) have no recourse under the Act for invasive government information practices.[96] The Act also imposes criminal penalties (a misdemeanor and a fine not more than $5,000) on (1) agency officers or employees who knowingly and willfully disclose information to an unauthorized person or agency, (2) agency officers or employees who willfully maintain a system of records in violation of notice requirements, and (3) any person who knowingly and willfully requests or obtains any record about an individual from an agency under false pretenses.[97]

A federal agency is permitted to maintain in its records only personal information that is relevant and necessary to accomplish the purposes of the agency, a statute, or an executive order.[98] Subsection (a)(3) of the Act defines "maintain" as synonymous with "maintain, collect, use, or disseminate."[99] "Record" refers to any type of information maintained on an individual, such as financial transactions.[100] Notably,

---

92. *See The Privacy Act of 1974*, EPIC, https://epic.org/privacy/1974act/ [https://perma.cc/5GEQ-9DGJ] (last visited Mar. 17, 2021) [hereinafter EPIC] (explaining the history of the Privacy Act of 1974).

93. *See* Memorandum from Clay Johnson III, Acting Dir., Off. of Mgmt. & Budget, to Heads of Exec. Dep'ts & Agencies, M-06-15, Safeguarding Personally Identifiable Information (May 22, 2006), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2006/m-06-15.pdf [https://perma.cc/952G-KGAS] ("[Personally identifiable information] can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or associated with a specific individual.").

94. *See* 5 U.S.C. § 552a; *see also Privacy Act of 1974*, U.S. DEP'T. OF JUST.: OFF. OF PRIV. & CIV. LIBERTIES, https://www.justice.gov/opcl/privacy-act-1974 [https://perma.cc/QDH9-ZQQY] (last updated Jan. 15, 2020).

95. 5 U.S.C. § 552a(g); *see* EPIC, *supra* note 92.

96. *See* EPIC, *supra* note 92.

97. 5 U.S.C. § 552a(i).

98. *Id.* § 552a(e).

99. *Id.* § 552a(a)(3).

100. *Id.* § 552a(a)(4) ("[T]he term 'record' means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions . . . or the identifying number, symbol, or other identifying particular assigned to the individual").

a "system of records" is a database "under the control of any agency" from which information is retrieved by a personal identifier, such as a name.[101] Hence, retail CBDC records under the control of the Federal Reserve would likely constitute a "system of records" maintained by the Federal Reserve pursuant to the Privacy Act and therefore be subject to protection.

Federal agencies possessing personally identifiable information must provide safeguards for confidentiality and follow procedural requirements to permit access to the information.[102] In the absence of an enumerated exception under the Act, federal agencies are prohibited from disclosing any record contained in a system of records to third parties or other agencies without the written request or prior written consent of the individual to whom the record concerns.[103] One of these exceptions is for a "routine use."[104] Federal agencies must publish a notice in the Federal Register when establishing a new system of records and describe, among other things, the nature of the records maintained in the system and each routine use of the records (including "categories of users and purpose of such use").[105] Law enforcement agencies (e.g., the CIA, FBI) can also exempt themselves from many of the Act's requirements.[106]

Despite notice and consent requirements, the "routine use" exception has been criticized for allowing a great amount of disclosures.[107] Routine use is the disclosure of a record for a purpose that is "compatible" with the purpose for which the information was collected.[108] The meaning of "compatible" is vague but can encompass "functionally equivalent uses and other uses that are necessary and proper."[109] Hence, agencies can establish a broad routine use that includes every potential use of data as long as the routine use is compatible with, rather than identical to, the purpose for which the information is collected.[110] This has been criticized as enabling "mission creeps" for a system of records by allowing agencies' expansions of

101. *See id.* § 552a.

102. *See id.*

103. *Id.* § 552a(b).

104. *See id.* § 552a(b)(3).

105. *Id.* § 552a(e)(4).

106. *See id.* § 552a(j)–(k).

107. *See* EPIC, *supra* note 92.

108. 5 U.S.C. § 552a(a)(7).

109. Guidance on the Privacy Act Implications of Call Detail Programs, 52 Fed. Reg. 12,990, 12,993 (Apr. 20, 1987).

110. *See* EPIC, *supra* note 92.

routine uses that go beyond intended purposes over time.[111] Additionally, agencies may disclose records indicating a potential violation of law under the routine use exception to law enforcement agencies for the purposes of investigation or prosecution (despite the purpose for which the records were collected).[112]

2. Strictly Confidential Tax Records

The Internal Revenue Service's (IRS) information-sharing policy with the Social Security Administration (SSA) is a notable example of a policy choice that advances the IRS's objectives by limiting government information-sharing practices. The IRS provides individual taxpayer identification numbers (ITINs) to individuals who do not have or are ineligible for a social security number.[113] Thus, undocumented immigrants can file taxes with the IRS with an ITIN despite unconventional circumstances of their employment.[114] The IRS is permitted to share certain information about individual earnings to the SSA for the purpose of determining each worker's entitlement to social security benefits.[115] However, the SSA is prohibited from sharing that information with others, including the Department of Homeland Security (DHS), despite its law enforcement purpose.[116] IRS officials have previously expressed that sharing tax information with DHS would decrease tax collection and compliance; and moreover, such a practice would generally discourage individuals from complying with tax laws.[117] Although sharing information with DHS would aid its enforcement efforts, this interest does not warrant denying privacy protections for many individuals.[118]

---

111. *See id.*

112. 5 U.S.C. § 552a(b)(3); *see also* OFF. OF PRIV. & CIV. LIBERTIES, U.S. DEP'T. OF JUST., OVERVIEW OF THE PRIVACY ACT OF 1974 (2020).

113. Beverly Bird, *Filing Taxes as an Undocumented Worker*, BALANCE, https://www.the-balance.com/undocumented-immigrant-taxes-rules-and-requirements-4778580 [https://perma.cc/GF74-2UDD] (last updated Jan. 16, 2021).

114. *See id.*

115. Jennifer Chang Newell, *Will Immigration Authorities Use Our Taxes to Go After Immigrants?*, ACLU (Apr. 23, 2018, 5:15 PM), https://www.aclu.org/blog/immigrants-rights/deportation-and-due-process/will-immigration-authorities-use-our-taxes-go [https://perma.cc/DA33-SFX7].

116. *Id.*

117. *Id.*

118. *Id.*

3. Financial Integrity

Unraveling the inherent tension between privacy and transparency in a CBDC requires determining the permissible level of anonymity within financial transactions. Generally, physical cash provides the highest degree of privacy because it allows peer-to-peer transactions between parties without the facilitation of an intermediary or any recordkeeping of transactions in a ledger. The untraceable nature of cash enables a significant level of anonymity, which can also aid illicit and illegal activities, such as money laundering, tax evasion, and the financing of terrorism.[119] Conversely, cash held in a bank account creates a digital footprint (i.e., account holdings and financial transaction data) that is visible to the bank and potentially accessible by the government. A retail CBDC would similarly enable recordkeeping of financial transactions while also allowing the federal government unprecedented access to individual financial information through the elimination of a third-party intermediary.

The Federal Reserve will undoubtedly adhere to existing financial laws and regulations to ensure the integrity of a CBDC. All financial institutions operating within the United States are subject to the Bank Secrecy Act of 1970 (BSA).[120] The BSA requires financial institutions to assist in preventing and detecting money laundering, countering the financing of terrorism, and detecting suspicious activities.[121] Banks are required to file currency transaction reports for cash transactions over $10,000 in one business day[122] and file suspicious activity reports for questionable activities.[123] In 2001, following the 9/11 attacks, the BSA was amended by the PATRIOT Act.[124] Title III of the PATRIOT Act requires US banks to develop a Customer Identification Program to curb the financing of terrorist organizations.[125] Banks must verify a customer's identity, suitability, and risks before opening new

119. *See* Tommaso Mancini-Griffoli, Maria Soledad Martinez Peria, Itai Agur, Anil Ari, John Kiff, Adina Popescu & Celine Rochon, *Casting Light on Central Bank Digital Currency*, IMF Staff Discussion Note, at 20, SDN/18/08 (Nov. 12, 2018); *see also Money Laundering*, FATF, https://www.fatf-gafi.org/faq/moneylaundering/ [https://perma.cc/D6QC-GJKP?type=image] (last visited Mar. 21, 2021).

120. *Bank Secrecy Act*, OFF. OF THE COMPTROLLER OF THE CURRENCY, https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html [https://perma.cc/NMP4-53VD] (last visited Mar. 21, 2021).

121. *See* Bank Secrecy Act, 31 U.S.C. § 5311, *amended by* USA PATRIOT Act, Pub. L. No. 107-56, tit. III, 115 Stat. 272, 296 (2001).

122. *See* 31 C.F.R. § 1010.311 (2021).

123. *Id.* § 1010.320

124. USA PATRIOT Act, Pub. L. No. 107-56, tit. III, 115 Stat. 272, 296 (2001).

125. *See id.*

bank accounts and maintain Customer Identification Program records for five years after an account is closed.[126] These customer due diligence rules are also known as Know Your Customer laws; they are intended to protect banks from being used for criminal activity by allowing banks to collect and analyze personally identifiable information to screen and create customer profiles.[127] Therefore, bank records are "private" in the sense that they are not readily available to others. However, the degree of privacy in bank records is limited under the current rule of law.

The Financial Crimes Enforcement Network (FinCEN)—a bureau of the US Department of the Treasury—is charged with implementing, administering, and enforcing compliance with the BSA.[128] FinCEN's duties and powers include serving as the Financial Intelligence Unit of the United States, maintaining an accessible database of financial transaction information, determining trends and methods in financial crimes, and analyzing and sharing information to support law enforcement investigations at the federal, state, local, and international levels.[129] The agency has numerous data-access Memoranda of Understanding with federal, state, and local law enforcement and regulatory agencies. The Memoranda of Understanding grant direct access to FinCEN's BSA data through the FinCEN portal. The FinCEN portal houses the FinCEN Query search engine—a tool similar to Google, which enables users to access and easily analyze up to eleven years of FinCEN data.[130] Users can apply filters and narrow search results, access enhanced data, and import lists of data (i.e., names, ID numbers, and addresses) to be used as criteria.[131] FinCEN's Query search application is part of an ongoing effort to modernize the implementation of the BSA.[132]

---

126. *See* 31 C.F.R. § 1020.220.

127. *Bank Secrecy Act*, *supra* note 120.

128. 31 U.S.C. § 310.

129. *See id.*

130. *Support of Law Enforcement*, FINCEN, https://www.fincen.gov/resources/law-enforcement/support-law-enforcement [https://perma.cc/9VA7-YKJK] (last visited Mar. 21, 2021); Press Release, Fin. Crimes Enf't Network, FinCEN Query Now Available for Authorized Users: IT Modernization Program Is on Schedule and Within Cost (Sept. 10, 2012), https://www.fincen.gov/sites/default/files/news_release/20120910.pdf [https://perma.cc/9LTF-LSSZ]; FIN. CRIMES ENF'T NETWORK, FACT SHEET: THE FINCEN PORTAL (2021), https://www.fincen.gov/sites/default/files/shared/Facts_FinCENPortal.pdf [https://perma.cc/6KQ3-SWJ9].

131. *See* THE FINCEN PORTAL, *supra* note 130.

132. *See FinCEN's IT Modernization Efforts*, FINCEN, https://www.fincen.gov/fincens-it-modernization-efforts [https://perma.cc/7S5K-7ZJQ] (last visited Mar. 17, 2021).

4. Is There a Right to Financial Privacy?

In *United States v. Miller*, the Court held that there is no legitimate expectation of privacy in bank records under the Fourth Amendment.[133] The Court concluded that bank records are not confidential information but rather "negotiable instruments" that contain information voluntarily provided to banks.[134] Additionally, the Court acknowledged that Congress, in enacting the BSA, assumed the lack of a legitimate privacy expectation in bank records and intended banks to engage in recordkeeping because bank records are useful to criminal and regulatory investigations and proceedings.[135] *Miller* solidified the third-party doctrine, which provides that an individual has no "reasonable expectation of privacy" in information that she voluntarily shares with a third party and, therefore, lacks Fourth Amendment protection against warrantless search and seizure of this information.[136] This Note will not further discuss the application of the Fourth Amendment to a retail CBDC; however, it is worth highlighting that Congress and the Supreme Court have already struck a balance between privacy and BSA compliance that permits some intrusion of privacy for federal objectives.

In response to the *Miller* case, Congress enacted the Right to Financial Privacy Act of 1978 (RFPA) to protect customer financial records from federal government scrutiny.[137] The RFPA creates a statutory Fourth Amendment protection for bank records by requiring federal government authorities seeking customer financial records from a financial institution to obtain one of the following: customer authorization, administrative subpoena or summons, search warrant, judicial subpoena, or a formal written request.[138] Additionally, federal government officials must provide an individual with written notice of the government's intent to obtain the records, an explanation for why the records are being sought, and an opportunity to object to a financial institution supplying the records.[139] However, there are many exceptions to the notice requirement and instances where no notice is

133. *See* U.S. v. Miller, 425 U.S. 435, 442 (1976).

134. *Id.* at 442.

135. *See id.* at 442–43 (quoting 12 U.S.C. § 1829b(a)(1)).

136. *See id.*

137. 12 U.S.C. §§ 3401–3422.

138. *See id.*

139. *See id.*; *see also* FED. RSRV., RIGHT TO FINANCIAL PRIVACY ACT: CONSUMER COMPLIANCE HANDBOOK 1 [hereinafter RFPA HANDBOOK], https://www.federalreserve.gov/boarddocs/supmanual/cch/priv.pdf [https://perma.cc/GG94-FBJ9].

required.[140] Notably, the RFPA provides a significant allowance for banks acting under the BSA.[141] A bank is not required to inform a customer when it discloses financial information under certain circumstances, such as when it files a suspicious activity report with the FinCEN.[142] Generally, law enforcement investigations seek financial transaction records to uncover hidden assets or suspicious behavior that may reveal criminal activity or actors.[143] Therefore, there is an inevitable clash between privacy and transparency.

II. ANTIQUATED PRIVACY PROTECTION

Privacy concerns are generally rooted in the issue of trust, and therefore, could be overcome through design choices and appropriate legal frameworks that enhance trust in a retail CBDC.[144] The Federal Reserve's unique access to individual information and financial data from CBDC records could strengthen the anti-money laundering and countering the financing of terrorism regimes and also enable extraordinary government surveillance if left unchecked. Hypothetically, government actors could abuse the Federal Reserve's newfound access to individual financial records for inappropriate purposes.[145] Therefore, privacy choices in a retail CBDC must protect users' information from abuse or needless government surveillance and must allow permissible access to financial information for law enforcement and regulatory compliance and supervision. Notably, privacy protection must keep pace with existing and emerging technological advances.

A. System of Records

The unique characteristics of databases further exacerbate the concern that a retail CBDC system could be misused for unwarranted access to personal information. The Privacy Act protects personally

140. *See* RFPA HANDBOOK, *supra* note 139. The exceptions include disclosures not identified with particular customers; disclosures pursuant to the functions of supervisory agencies; disclosures in accordance with procedures under the Internal Revenue Code; disclosures pursuant to any federal statute or rule, administrative subpoena, law enforcement inquiry, and judicial proceedings; and disclosures relevant to a violation of the law. *Id.*

141. *See id.*

142. *See id.*

143. *See Money Laundering*, *supra* note 119.

144. *See generally* WERBACH, *supra* note 48, at 19–23 (explaining the general relationship between privacy and trust).

145. *See generally* Brookings Paper, *supra* note 32, at 38 (providing potential scenarios that pose privacy risks).

identifiable information contained in a system of records from which data is retrieved by a personal identifier, such as a name and social security number.[146] It is probable that a retail CBDC database may index individual information by a personal identifier given existing BSA regulations and practices. The Federal Reserve (or a third-party operator) would likely conduct regulatory due diligence for retail CBDC accounts (or wallets) in a fashion similar to current procedures at financial intermediaries with some potential allowances for any financial inclusion goals. Moreover, a retail CBDC system could also use pseudonymous identifiers to manage the identity of a CBDC holder (or account).[147] An individual's identity would be anonymous to the extent that a pseudonym (not an actual identity) is shared during transactions.[148] Additionally, a retail CBDC could serve as a springboard for digital identity use cases.[149] Therefore, the determination of account identity versus individual identity in a retail CBDC would be necessary to appropriately address privacy concerns.[150]

Under existing BSA regulations, the Federal Reserve (or a third-party operator) would be required to engage in recordkeeping of retail CBDC transactions and store individual information for an extensive period of time in a database.[151] Protection under the Privacy Act applies only to a database from which data is retrieved by a personal identifier[152]—leaving wide latitude for an agency to choose nonpersonal identifiers to circumvent many Privacy Act provisions. For instance, retail CBDC users could be indexed in a system by IP address, which does not identify a person on its own and must be linked to other information to associate it with a specific individual. Therefore, the Federal Reserve could bypass requirements under the Privacy Act by indexing CBDC users by pseudonymous identifiers and still maintain unprecedented amounts of individual data *not* subject to protective measures against invasive government information practices. This

146. *See* EPIC, *supra* note 92.

147. *See id.* at 38–41.

148. *See id.* at 38–41, 87 (explaining that pseudonymous CBDC accounts would still reveal more information about transactions to central banks than existing systems do).

149. *See id.* at 27–31.

150. *See* Warren, *supra* note 30, at 36:10 ("The one thing I think that gets lost in the conversation is the distinction between identity of the person and indeed the account."); David Treat, Senior Managing Dir., Accenture, Remarks at Digital Dollar Live, at 01:06:11 (July 21, 2020), *in* ACCENTURE, https://www.accenture.com/_acnmedia/PDF-130/Accenture-Digital-Dollar-Live-Video-Transcript.pdf#zoom=50 [https://perma.cc/U8DD-GNNT].

151. *Bank Secrecy Act*, *supra* note 120.

152. *See* 5 U.S.C. § 552a.

shortcoming demonstrates the inefficacy of Privacy Act protections in an increasingly digital economy.[153]

B. Routine Uses and Information Sharing

The accessibility of retail CBDC records under the control of the Federal Reserve would further exacerbate the shortcomings of the personal identifier requirement under the Privacy Act when considering existing government information-sharing practices.[154] A retail CBDC would create a database of financial transaction records and other personal information under the control of the government. Government agencies have the ability to access multiple public and private databases and manipulate data to generate detailed insights about individuals.[155] Retail CBDC data in combination with data analytic tools could augment other government databases through existing information-sharing practices among government agencies. This would create endless possibilities for the relationship between CBDC data and government oversight. The FinCEN has acknowledged that its collection of financial data from financial institutions under the BSA has aided in anti-money laundering, countering the financing of terrorism, and other financial crime investigations because law enforcement and intelligence investigators can combine FinCEN data with other collected data to draw more accurate identifications of respective subjects from information such as banking patterns, businesses and personal associations, communication methods, previously unknown addresses, and travel patterns.[156] With the advent of technological innovations, a retail CBDC database under the control of the Federal Reserve could bolster existing information-sharing practices but needlessly track detailed personal information about individuals. Therefore, the concern over privacy in a retail CBDC is not only the government's mere possession and disclosure of individual data but also the potential for what the government can do with this data.[157]

The Federal Reserve could have unprecedented access to individual financial data that the government would traditionally access through a third party, such as a commercial bank. Ordinarily,

153. *See* EPIC, *supra* note 92.

154. Angelique Carson, *So the Privacy Act Falls Short, but What to Do?*, IAPP (Nov. 4, 2014), https://iapp.org/news/a/so-the-privacy-act-falls-short-but-what-to-do/ [https://perma.cc/5HKW-H6MP].

155. *See id.*

156. *The Value of FinCEN Data*, FINCEN, https://www.fincen.gov/resources/law-enforcement/case-examples [https://perma.cc/EZ7W-S5P2] (last visited Mar. 17, 2021).

157. *See id.*

the federal government has access to financial records through lawful procedures or voluntary information-sharing protocols with banks under the BSA.[158] Information-sharing practices could be especially ripe for misuse under the routine use exception to certain Privacy Act protections if government entities utilize the exception as a backdoor opportunity to compile individual financial data from retail CBDC records. The routine use exception would allow government agencies to extract retail CBDC information from the Federal Reserve's database for uses that could be construed as "compatible" with the purpose for which CBDC records are collected. A compatible use under the Act's routine use exception could encompass whatever the Federal Reserve deems is "functionally equivalent" or "necessary and proper" for a purpose for which retail CBDC data is collected.[159] Thus, a retail CBDC could be programmed to communicate endless information to government entities as long as the purpose for an entity's access to the information could be construed as compatible with the Federal Reserve's purpose for collecting CBDC records. For instance, the "collection" of CBDC records could constitute the information that is generated by the base programming underpinning the retail CBDC infrastructure itself. Additional smart contracts embedded in a CBDC for different uses, such as regulatory supervision, could support "compatible uses" of information. Therefore, the programmability of a retail CBDC could constitute a new, innovative method for information sharing. The purpose for collecting CBDC records would essentially circumscribe what uses are compatible under the routine use exception. Therefore, enumerated purposes for collecting CBDC records would not only define use cases but would also be a way to prospectively craft information-sharing practices.

1. Wavering Privacy Protection

Information-sharing practices in the context of a retail CBDC could pose a concern for individuals not currently protected under the Privacy Act. The Act does not expressly protect personally identifiable information of individuals who are not US citizens or permanent residents.[160] Traditionally, federal agencies have adopted internal policies to extend Privacy Act protections to noncitizens and

158. *See* 12 U.S.C. §§ 3401–3422.

159. *See* U.S. DEP'T. OF JUST.: OFF. OF PRIV. & CIV. LIBERTIES, *supra* note 94.

160. *See* 5 U.S.C. § 552a(a)(2) ("[T]he term "individual" means a citizen of the United States or an alien lawfully admitted for permanent residence").

nonpermanent residents under certain circumstances.[161] However, on January 25, 2017, then-President Trump issued an executive order that discouraged these internal privacy policies and ordered federal agencies to exclude individuals who are not US citizens nor lawful permanent residents from Privacy Act protections.[162] The executive order contained immigration enforcement priorities and encouraged more information sharing about noncitizens and nonpermanent residents to facilitate immigration enforcement.[163] The absence of express protection for noncitizens and nonpermanent residents leaves a segment of the population in a precarious position because noncitizens and nonpermanent residents can be subject to invasive government information-sharing practices without any legal recourse. The lack of protection under the Privacy Act would deter noncitizens and nonpermanent residents from participating in a retail CBDC payments system and would further marginalize them from the mainstream financial system. This could have a domino effect and deter others who have relations (social, business, etc.) with noncitizens and nonpermanent residents from using a retail CBDC payments system to avoid compromising the privacy of noncitizens and nonpermanent residents. Therefore, the Privacy Act should be amended to expressly protect noncitizens and nonpermanent residents.

III. PRIVACY IN THE AGE OF RETAIL CBDC

The privacy policy of a retail CBDC under the control of the Federal Reserve should be responsive to technological innovations and the sociopolitical reality of privacy. The novelty of a retail CBDC creates regulatory uncertainty around the Federal Reserve's appropriate role in safeguarding individual privacy and bolstering regulatory innovation. A retail CBDC—whether account-based or token-based—would provide the government direct and real-time access to personal information and financial data. The scale and success of a retail CBDC system relies on trust.[164] The public must trust that

161. Stephen Nattrass, *Executive Order Removes US Privacy Act Protection for Canadians*, NORTON ROSE FULBRIGHT (Mar. 2017), https://www.nortonrosefulbright.com/en/knowledge/publications/01bc866e/executive-order-removes-us-iprivacy-acti-protection-for-canadians [https://perma.cc/QK37-Q9VD].

162. *See id.* (noting that citizens of EU countries are entitled to protection under the Privacy Act pursuant to the Judicial Redress Act of 2015); *see also* Exec. Order No. 13,768, 82 Fed. Reg. 8,799, 8,802 (Jan. 30, 2017).

163. Exec. Order No. 13,768, 82 Fed. Reg. at 8,000–01.

164. *See* Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 39 (2021) ("Trust is also essential in our personal and commercial relationships."). *See generally* WERBACH, *supra* note 48, at 20–25 (explaining the importance of trust in human conduct).

the government will not misuse CBDC data and the government must trust that the CBDC system will not empower bad actors.[165] Thus, a proper privacy framework for a retail CBDC would help facilitate integrity within the system to build trust among the participants and operators of the CBDC system.[166] Broader protections for privacy may be required as the general public's privacy expectations shift with society's increasing awareness of the impact of data. Amending the Privacy Act in the context of a retail CBDC that is under the control of the Federal Reserve could harmonize individual privacy and regulatory innovation. Alternatively, a new regulatory framework informed by the Privacy Act that implements the forgoing refinements to the Privacy Act and responds to the arising privacy demands of a retail CBDC could better serve privacy concerns, enhance transparency, and promote equal access. Furthermore, defining rules that govern the use of CBDC data could promote transparency in the payments system.[167]

A. Smart Money, Big Data, and Civil Liberties

Conceptualizing privacy as the mere possession of information may no longer be appropriate in the context of a retail CBDC that is under the control of the Federal Reserve.[168] Technological innovations, such as big data, can transform the mere possession of CBDC data into a mechanism from which the government extrapolates data-informed conclusions for decision-making. Big data maximizes computation power and algorithmic accuracy to identify patterns and generate insights from large data sets.[169] Big data flourishes in large data sets because the abundance of data offers more accurate and precise intelligence and knowledge.[170] Regulating only the possession of CBDC records could create absurd results for personal privacy in the age of big data. For instance, government officials could use retail CBDC transaction records that include references to social movements (e.g., donations) and combine this information with data from other agency databases, public records, private databases, government intelligence systems, social media accounts, or any other available information system to potentially uncover political dissidence, identify social activists, undermine constitutionally protected activity, or support the

165. *See* WERBACH, *supra* note 48, at 20–21.

166. *See id.*

167. *See id.* at 27.

168. *See* Carson, *supra* note 154.

169. Danah Boyd & Kate Crawford, *Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon*, 15 INFO. COMM. & SOC'Y 662, 663 (2012).

170. *See id.*

undertaking of coercive measures to squash public expression (e.g., freeze CBDC accounts or wallets to block financial support for protests).[171]

The combination of retail CBDC records and big data could bolster dataveillance on a mass scale.[172] Dataveillance tracks metadata—which is essentially data about data.[173] Financial records can reveal numerous details and insights about an individual's life, such as medical conditions, political affiliations, and location.[174] Currently, private firms use this data to predict consumer behavior and future company performance.[175] Lenders use financial data to predict likelihoods of divorce, travel patterns, and creditworthiness.[176] Direct access to financial records could aid the government in curbing tax evasion and monitoring monetary expenditures because the federal government could similarly employ predictive analytics with retail CBDC records to identify an individual's behavior and movement. This could also detect suspicious activities and be advantageous to BSA compliance and enforcement. However, detailed analytics could also have far-reaching consequences for individual privacy. CBDC records could be repurposed to support government surveillance under current privacy laws and could even be unhinged to the extent that such surveillance targets vulnerable segments of the population.

The unchecked repurposing of retail CBDC records to augment other government data sets could increase the likelihood of racial profiling and other arbitrary means of targeting segments of the population. The incidence of US government surveillance targeted at

---

171. *See* Allie Funk, *How Domestic Spying Tools Undermine Racial Justice Protests*, FREEDOM HOUSE (June 22, 2020), https://freedomhouse.org/article/how-domestic-spying-tools-undermine-racial-justice-protests [https://perma.cc/CB7K-P3AF]; *Nigeria: Punitive Financial Moves Against Protesters*, HUM. RTS. WATCH (Nov. 13, 2020, 12:00 AM), https://www.hrw.org/news/2020/11/13/nigeria-punitive-financial-moves-against-protesters [https://perma.cc/N9CA-WCMR] (discussing an example of a punitive financial measure undertaken by the Central Bank of Nigeria to suppress EndSARS protests in 2020).

172. *See* April White, *A Brief History of Surveillance in America*, SMITHSONIAN MAG. (Apr. 2018), https://www.smithsonianmag.com/history/brief-history-surveillance-america-180968399/ [https://perma.cc/UB2F-G8FW].

173. *See id.*

174. Benjamin Powers & Marc Hochstein, *Could a Digital Dollar Compete on Privacy? Fed Chairman Powell Hints It Might*, COINDESK, https://www.coindesk.com/could-a-digital-dollar-compete-on-privacy-fed-chairman-powell-hints-it-might [https://perma.cc/CLY6-J67R] (last updated Feb. 13, 2020, 12:05 PM).

175. *See id.*

176. *See Is the Credit Scoring Written in Your DNA?*, FINAI (Sept. 15, 2017), https://www.finai.com/en/newsroom/is-the-credit-scoring-written-in-your-dna/index.htm [https://perma.cc/23V7-9N58].

social movements, activists, or ethnic minority communities—such as the civil rights movement,[177] Black Lives Matter organizers or supporters,[178] and AMEMSA (Arab, Middle Eastern, Muslim, and South Asian) communities following 9/11[179]—demonstrates the need to not only safeguard the possession of retail CBDC records but also the use of records. The failure to regulate *how* individual CBDC records can be used would ignore potentially harmful effects of big data, such as the generation of various insights about individuals or the unethical use of data aggregation to segment and target individuals for unspecified purposes.[180] Prescribing permissible uses of retail CBDC records would ensure a retail CBDC system is not repurposed to undermine fundamental rights or arbitrarily monitor individuals absent suspicion of criminal activity. Moreover, a privacy framework must keep pace with technological advancements in data analytics.

The relationship between individuals and the government also warrants consideration.[181] The spirit of the Fourth Amendment demonstrates that the government stands in a different position than private entities, such as financial institutions.[182] A financial institution monitoring financial transactions within its system is required by law

177. *See* Noa Yachot, *History Shows Activists Should Fear the Surveillance State*, ACLU (Oct. 27, 2017, 3:45 PM), https://www.aclu.org/blog/national-security/privacy-and-surveillance/history-shows-activists-should-fear-surveillance [https://perma.cc/D3C8-X5VH].

178. *See, e.g.*, Funk, *supra* note 171; George Joseph, *Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson*, INTERCEPT (July 24, 2015, 2:50 PM), https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson/ [https://perma.cc/6Z35-ZS9N]; George Joseph, *Undercover Police Have Regularly Spied on Black Lives Matter Activists in New York*, INTERCEPT (Aug. 18, 2015, 5:27 PM), https://theintercept.com/2015/08/18/undercover-police-spied-on-ny-black-lives-matter/ [https://perma.cc/U3TL-9NKY] (reporting on undercover police officers attending Black Lives Matters protests in New York and tracking protestors' movements). *Compare* Wendi C. Thomas, *Police Have Been Spying on Black Reporters and Activists for Years. I Know Because I'm One of Them*, NEIMAN LAB (June 10, 2020, 8:00 AM), https://www.niemanlab.org/2020/06/police-have-been-spying-on-black-reporters-and-activists-for-years-i-know-because-im-one-of-them/ [https://perma.cc/XB6B-65FT], *with Facebook Letter to Memphis Police Department on Fake Accounts*, EFF (Sept. 19, 2018), https://www.eff.org/document/facebook-letter-memphis-police-department-fake-accounts [https://perma.cc/7Y9U-AQHM] (discussing an example of the Memphis Police Department using Facebook for surveillance of individuals for political reasons).

179. *See* CITY & CNTY. OF SF HUM. RTS. COMM'N, COMMUNITY CONCERNS OF SURVEILLANCE, RACIAL AND RELIGIOUS PROFILING OF ARAB, MIDDLE EASTERN, MUSLIM, AND SOUTH ASIAN COMMUNITIES AND POTENTIAL REACTIVATION OF SFPD INTELLIGENCE GATHERING (2010), https://sf-hrc.org//sites/default/files/Documents/HRC_Publications/Articles/AMEMSA_Report_Adopted_by_HRC_022411.pdf [https://perma.cc/C9X3-5Q27].

180. *See* Solove, *supra* note 164, at 42–44, 49–50.

181. Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1156–57 (2002).

182. *See id.*

to do so[183] and will not automatically implicate due process concerns.[184] However, the government's direct access to such information could more readily be used against individuals absent procedural safeguards.[185] On one hand, a retail CBDC is a voluntary option like a private-sector financial service; therefore, individuals will have a choice to use private financial services in lieu of a retail CBDC payments system. On the other hand, a retail CBDC is a public option slated to transform the US payments system in hopes of wide adoption for success. Therefore, the breadth of power at the government's disposal—despite an individual's freedom to choose to use a retail CBDC—can be employed to control individual behavior and effectively reduce a retail CBDC to an authoritative tool that infringes upon civil liberties. A privacy framework must (1) prescribe what information the government should know and when the government should know this information and (2) provide stringent liability provisions for the misuse of retail CBDC data to limit the imposition of arbitrary state power. The programmable capabilities of a retail CBDC should also be limited to purposes that would bolster economic benefits. Technological innovations should be used appropriately to ensure the integrity of a retail CBDC system. The current BSA regime demands some intrusion into privacy to ensure the integrity of the US financial system. Thus, retail CBDC users would engage in a "trust tradeoff."[186] CBDC users would enjoy the benefits of the payments system (e.g., reliability and efficiency) in exchange for the cessation of some privacy to ensure the integrity of a CBDC system.[187] CBDC would be a voluntary, public option that supplements physical cash and private-sector payments options. Thus, CBDC users would also have to trust that their information would not be misused by government actors to willingly engage in the aforementioned tradeoff in a retail CBDC system.[188]

183. *See* Bank Secrecy Act, 31 U.S.C. § 5311, *amended by* USA PATRIOT Act, Pub. L. No. 107-56, tit. III, 115 Stat. 272, 296 (2001).

184. *See The Right to Financial Privacy Act*, EPIC, https://epic.org/privacy/rfpa/#:~:text=The%20reaction%20to%20the%20Supreme,records%20maintained%20by%20financial%20institutions [https://perma.cc/S653-3QBQ] (last visited Mar. 17, 2021) (explaining the purpose of the Right to the Financial Privacy Act and procedural requirements for bank records).

185. *See* Solove, *supra* note 181, at 1156.

186. *See* WERBACH, *supra* note 48, at 28 (conceptualizing "trust trade-off").

187. *See id.*

188. *See id.*

B. Permissible Vantage Point

Retail CBDC records under the control of the Federal Reserve would likely classify as a "system of records" under the Privacy Act and be subject to safeguards that protect personally identifiable information that is accessible from a retail CBDC ledger. A retail CBDC payments system raises the concern of mass or targeted government surveillance because systems can potentially give rise to a more detailed and systematic compilation of personal data about individuals.[189] The system of records classification would protect individual information from inappropriate information-gathering and information-sharing practices between government agencies by requiring government entities to undergo certain procedures before accessing personal information.

Additionally, information generated from a retail CBDC system is collected by default (i.e., location, vendor, transaction amount, item, etc.) and not necessarily by consent.[190] A retail CBDC reliant on ledger technology could use privacy-enhancing technology to limit the type of information that is exposed to the Federal Reserve, but this does not eliminate the fact that some information must be collected to record transactions. Moreover, more information may be required to comply with existing BSA recordkeeping standards.

A proper privacy framework could manage access to the direct vantage point that a retail CBDC would provide to government officials. Limiting the availability of the routine use exception under the Privacy Act for retail CBDC records could help establish a permissible vantage point for government actors. Since agencies establish their own routine uses and thereby determine the compatibility of such uses,[191] it is crucial that a privacy framework define permissible uses of retail CBDC records to provide parameters around the routine use. The RFPA provides relevant guidance on procedural protections that can augment current disclosure safeguards under the Privacy Act.[192] For instance, under the RFPA, government authorities seeking customer financial records from a financial institution must obtain one of the following: customer authorization; administrative subpoena or summons; search warrant; judicial subpoena; or a formal, administrative written request. Therefore, the Privacy Act should be

189. *See* Solove, *supra* note 181, at 1156.

190. *See id.*

191. *See* U.S. DEP'T. OF JUST.: OFF. OF PRIV. & CIV. LIBERTIES, *supra* note 94.

192. *See* Right to Financial Privacy Act (RFPA) of 1978, 12 U.S.C. § 3401; *see also The Right to Financial Privacy Act*, *supra* note 184.

amended to ensure that government access to individual financial information from retail CBDC records is subject to the same procedural requirements. Additionally, more stringent liability provisions than those under the Privacy Act should be implemented for the unauthorized use, disclosure, and access of retail CBDC records. Regulatory compliance, such as currency transaction reports[193] and suspicious activity reports,[194] necessitates some flexibility in the access to retail CBDC records. Therefore, the routine use exception could capture regulatory compliance under the BSA. Additionally, the Federal Reserve should provide actual notice to retail CBDC users about its information practices—such as the nature and extent of information sharing for regulatory purposes. The Privacy Act (or a new regulatory framework) must create a permissible vantage point for government actors and limit needlessly invasive information-sharing practices across government agencies. Failure to balance individual privacy expectations and government interests could discourage wide adoption of a retail CBDC, marginalize segments of the population, and erode public trust in the government.

C. Equal Protection

Motivations for a retail CBDC include reducing reliance on financial intermediaries and expanding access to capital. The plain text of the Privacy Act precludes protection for individuals who are not citizens or permanent residents of the United States. This would only serve to discourage and effectively exclude their participation in a retail CBDC system. The failure to extend protection to individuals who are not citizens or permanent residents—particularly undocumented immigrants—would undermine the trust and transparency in the system by maintaining a lawful workaround for inappropriate information practices. Additionally, it is antithetical to the CBDC goal of financial inclusion to further marginalize a segment of the US population for whom the private sector currently provides alternative means of access to the financial system. Therefore, it is imperative that the Privacy Act (or a new regulatory framework) expressly protects individuals who are not citizens or permanent residents of the United States. Additionally, the privacy framework governing CBDC records should incorporate a rule similar to the IRS's policy and prohibit the disclosure of an

193. 31 C.F.R. § 1010.311 (2021) (outlining the filing obligations for currency transaction reports).

194. *Id.* § 1010.320.

individual's immigration status, which may be revealed or speculated from Know Your Customer procedures or retail CBDC transaction data.

D. Innovative Regulatory Compliance and Oversight

Retail CBDC has the potential to transform financial regulatory compliance and enforcement. A retail CBDC's panoramic view of financial transactions could enable the creation of non-fungible money.[195] Monetary policy can be implemented in a CBDC to impose conditions, such as spending limits on "helicopter money."[196] Helicopter money is a form of quantitative easing that involves a monetary authority distributing central bank money directly to the population in lieu of money distribution by financial intermediaries.[197] For instance, the Federal Reserve could utilize a retail CBDC for helicopter money to more effectively ensure that households have access to government stimulus funds during the ongoing pandemic or any other economic crisis.[198] The ability to control money in a retail CBDC system would not only aid monetary policy but also enable regulators to implement more risk-based approaches to BSA enforcement. Therefore, the privacy framework of a retail CBDC must strike a proper balance between innovative financial regulation and individual privacy. This should involve implementing tiered access to CBDC records such that individual information is not indiscriminately disclosed to government actors.[199] A tiered access approach to disclosure could be captured under procedural requirements for government access to individual records and the routine use exception under the Privacy Act. The nature of the disclosure should implicate which requirement or exception is warranted. For example, if a government entity is seeking individual information in pursuit of a legitimate law enforcement purpose, then permissible means enumerated under the RFPA—such as a subpoena—should govern the disclosure. On the other hand, the Federal Reserve may aid the FinCEN under the BSA by providing

195. *See* Brookings Paper, *supra* note 32, at 47–48, 64–68.

196. *See id.* at 62–64.

197. Press Release, Simon Youel, Positive Money, Issue Digital Cash or Lose Trust in Money, Report Warns (Apr. 23, 2020), https://positivemoney.org/2020/04/press-release-issue-digital-cash-or-lose-trust-in-money-report-warns/ [https://perma.cc/QPZ4-XXCR].

198. *See id.*

199. Sriram Darbha & Rakesh Arora, *Privacy in CBDC Technology*, BANK OF CAN. (June 2020), https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9/ [https://perma.cc/LG84-PWVJ].

insights from retail CBDC records not tied to an individual identity via the routine use exception.

IV. REIMAGINING THE US PRIVACY FRAMEWORK FOR A RETAIL CBDC

The increased digital transformation of payments creates unique privacy demands. Though a retail CBDC has the promise to transform the way in which individuals transact, it must respect privacy limits. The Privacy Act of 1974 is a legal solution that could balance privacy in a retail CBDC. Alternatively, a new regulatory framework informed by the Privacy Act and aforementioned refinements to the Act in Parts I and II could be instituted to more effectively protect personal data in a retail CBDC system. Whether the Privacy Act is applied (and amended) or a new regulatory framework is adopted to protect retail CBDC records will largely depend on future insights from ongoing exploration of the technology, benefits and risks, and governance of a US retail CBDC. Moreover, the privacy framework governing a retail CBDC should (1) classify CBDC records as a database (or "system of records"), (2) prescribe permissible uses of retail CBDC records, particularly as it concerns government information-sharing practices of retail CBDC data, (3) impose similar procedural requirements to those under the RFPA for government access to individual CBDC records, (4) impose more stringent liability provisions than those under the Privacy Act for the misuse of retail CBDC data, (5) expressly protect individuals who are neither US citizens nor permanent residents, and (6) provide flexibility for innovative regulatory compliance and enforcement. Notably, the distinctive features of a retail CBDC system may necessitate an entirely new framework to protect individual privacy in a retail CBDC.[200] A new regulatory framework that incorporates remedies for shortcomings of the Privacy Act and addresses the emergence of new financial technologies would be more applicable and adaptable to innovations in payments.[201]

A privacy framework that defines permissible parameters in the collection, access, and use of retail CBDC data would enhance public transparency and protect individuals while providing flexibility for legitimate law enforcement, financial regulation, and innovation. Balancing the inherent tension between privacy and transparency of user identity and transactions within a retail CBDC system under the

200. Yesha Yadav & Chris Brummer, *Fintech and the Innovation Trilemma*, 107 GEO. L.J. 235, 264 (2019).

201. *See id.*

control of the Federal Reserve would facilitate the successful implementation of a widely accessible retail CBDC that embraces technological innovation and fosters financial inclusion.

Nerenda N. Atako[*]

[*] J.D. Candidate, Vanderbilt University Law School, 2022; B.A., University of California, Santa Barbara, 2015. The Author would like to thank her family and friends for their unwavering support and encouragement. The Author would also like to thank Professor Kristen Johns, Professor Morgan Ricks, and Professor Yesha Yadav for their guidance. Finally, a special thank you to the board and staff of the *Vanderbilt Journal of Entertainment and Technology Law* for their insightful feedback and meticulous work throughout the writing and publication of this Note.