NOTE

MILLER IN A CASHLESS SOCIETY: FINANCIAL SURVEILLANCE AND THE FOURTH AMENDMENT

Matt Wostbrock*

In United States v. Miller*, the Supreme Court declared that the Fourth Amendment does not protect Americans' bank records because there is no reasonable expectation of privacy in the data. More recently, while limiting the third-party doctrine in* Carpenter v. United States*, the Court expressly left* Miller *standing by distinguishing the checks and deposit slips in* Miller *from the cell site location information in* Carpenter*. The* Carpenter *majority described the bank records in* Miller *as containing "limited types of personal information," but the continued use of that distinction relies on an outdated picture of financial technology and consumer habits. Financial records have evolved significantly since* Miller *was decided in 1976, and ever-increasing reporting and retention requirements have created massive financial databases. In an increasingly cashless society, financial records can reveal intimate and comprehensive information about nearly every American. Still, this Note recognizes that courts are unlikely to find them worthy of constitutional protection, and it does not argue that all searches of them should be subject to a warrant requirement. This Note instead aims to highlight our vast financial surveillance infrastructure, consider its costs and benefits, and advocate for Congressional narrowing of the procedures for access to and use of financial records by government agents.*

*J.D. Candidate 2024, Columbia Law School; B.S. 2018, University of South Carolina. My sincere thanks to Professor Kathryn Judge for her guidance and insights, and to the *Columbia Business Law Review* staff for their thoughtful feedback in preparing this Note for publication.

I. INTRODUCTION

> If these people had done bad things they ought to be ashamed of themselves and he couldn't pity them, and if they hadn't done them there was no need of making such a rumpus about other people knowing.[1]

[1] HENRY JAMES, THE REVERBERATOR 209 (1888).

In the time it will take you to read this Introduction,[2] about twenty-one Suspicious Activity Reports (SARs) will be filed.[3] SARs are reports from financial institutions to the federal government that are mandatory whenever those institutions witness illegal or unexplainable activity.[4] The forms contain detailed information about the reported individual or entity, including identifying information, any transaction details, and an explanation of the suspicion.[5] Law enforcement across the country can search these records without a warrant,[6] and may subpoena the financial institution for additional information on the reported party.[7]

The SAR process is only one piece of the larger financial surveillance infrastructure in the United States. Even without a SAR, if law enforcement believes that information would be relevant to an investigation, they may subpoena an institution for financial records.[8] Financial institutions are also required by statute to retain customer information for years.[9]

---

2 Brett Nelson, *Do You Read Fast Enough To Be Successful?*, FORBES (June 4, 2012), https://www.forbes.com/sites/brettnelson/2012/06/04/do-you-read-fast-enough-to-be-successful/?sh=4a6f280462e7s [https://perma.cc/F9DL-UAPP]. The average adult reads at 300 words per minute. If you are one of the few people who will read this student Note, you may be faster.

3 3,809,824 SARs were filed in 2023. *Suspicious Activity Report Statistics*, FINCEN, https://www.fincen.gov/reports/sar-stats [https://perma.cc/H4ZJ-H9LR] (choose "2023" from dropdown; then choose "All" for Industry Type; then generate search).

4 31 C.F.R. § 1020.320.

5 12 C.F.R. § 21.11. *See also* FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN SUSPICIOUS ACTIVITY REPORT (FINCEN SAR) ELECTRONIC FILING INSTRUCTIONS (Oct. 2012), https://www.fincen.gov/sites/default/files/shared/FinCEN%20SAR%20ElectronicFilingInstructions-%20Stand%20Alone%20doc.pdf [https://perma.cc/8MSA-2E4J].

6 FINCEN, FACT SHEET: THE FINCEN PORTAL, https://www.fincen.gov/sites/default/files/shared/Facts_FinCENPortal.pdf [https://perma.cc/RS4J-GC8P];
FinCEN, FACT SHEET: FINCEN QUERY, https://www.fincen.gov/sites/default/files/shared/Facts_FinCENQuery.pdf [https://perma.cc/D93C-BPR8].

7 12 U.S.C. § 3405.

8 *Id.*

9 31 C.F.R. §§ 1010.400–440.

These steps are all done below a probable cause standard, and without an independent arbiter to challenge whether the government has proven that the information is relevant to an ongoing investigation. Between 2019 and 2022, the Department of Homeland Security used this power to demand all border state transaction records over $500 from two large money transmitters.[10] This bulk surveillance program collected over six million transaction records and allowed unrestricted access to the data for hundreds of law enforcement agencies.[11]

Over the last 50 years, the government has built an extensive system of mandated recordkeeping and reporting by financial institutions, and increasingly many other businesses. With this information, they undoubtedly conduct legitimate investigations,[12] but critics contend that constitutional rights have been discarded in the process.[13] In *United States v. Miller*, the Supreme Court declared that the then-fledgling Bank Secrecy Act did not violate Americans' constitutional rights because people have no reasonable expectation of privacy in their bank records.[14] More recently, while limiting the third-party doctrine in *Carpenter v. United States*, the Court expressly left *Miller* standing by distinguishing the bank checks

[10] Matthew Guariglia, *Here's How ICE Illegally Obtained Bulk Financial Records from Western Union*, ELEC. FRONTIER FOUND.: DEEPLINKS BLOG (Mar. 10, 2022), https://www.eff.org/deeplinks/2022/03/heres-how-ice-illegally-obtained-bulk-financial-records-western-union [https://perma.cc/8Z4Z-PEWD].

[11] *Id.*; While some surveilled parties have sued the government and the money transmitters in response, they are unlikely to prevail as there is no constitutional protection of one's financial data, *see infra* Section II.B, and statutory rights are also limited. *See infra* Sections II.A, IV.A. As of this writing, defendants have filed motions to dismiss the complaint. Sequeira v. U.S. Dep't of Homeland Sec., 4:22-cv-07996 (N.D. Cal. Oct. 26, 2023).

[12] *FinCEN Recognizes Law Enforcement Cases Significantly Impacted by Bank Secrecy Act Filings*, FINCEN (May 19, 2020), https://www.fincen.gov/news/news-releases/fincen-recognizes-law-enforcement-cases-significantly-impacted-bank-secrecy-act [https://perma.cc/4EJG-BHVU].

[13] Michael Gentithes, *The End of* Miller*'s Time: How Sensitivity Can Categorize Third-Party Data After* Carpenter, 53 GA. L. REV. 1039 (2019).

[14] United States v. Miller, 425 U.S. 435, 442 (1976).

and deposit slips in *Miller* from the cell phone location data in *Carpenter*.[15]

But financial technology has evolved greatly since *Miller* was decided in 1976, and in the past decade American society has increasingly relied on non-cash financial transactions.[16] The Covid-19 pandemic[17] and the proliferation of FinTech have only increased that trend.[18] Nearly every transaction we make is recorded by credit card companies, banks, merchants, and other actors.[19] These transactions reveal intimate details of our lives: where we travel, what we buy, who we associate with, what organizations we support, and more. The changes have altered financial records' connection to traditional Fourth Amendment values, and corresponding privacy

15 Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

16 *See generally* EMILY CUBIDES & SHAUN O'BRIEN, 2022 FINDINGS FROM THE DIARY OF CONSUMER PAYMENT CHOICE, FED. RSRV. BANK OF S.F. (May 5, 2022), https://www.frbsf.org/wp-content/uploads/sites/7/2022-Findings-from-the-Diary-of-Consumer-Payment-Choice-FINAL.pdf [https://perma.cc/VEG7-R87H].

17 WORLD BANK, *COVID-19 Drives Global Surge in Use of Digital Payments* (June 29, 2022), https://www.worldbank.org/en/news/press-release/2022/06/29/covid-19-drives-global-surge-in-use-of-digital-payments [https://perma.cc/32EJ-MXFN]; Kristi Egerth, *Cash Is No Longer King in Times of COVID-19*, DELOITTE, https://www2.deloitte.com/ch/en/pages/consumer-industrial-products/articles/cash-is-no-longer-king-in-times-of-covid19.html [https://perma.cc/7297-EMJA]; Anneke Kosse & Robert Szemere, *Covid-19 Accelerated the Digitalisation of Payments,* BANK FOR INT'L SETTLEMENTS (Dec. 9, 2021), https://www.bis.org/statistics/payment_stats/commentary2112.htm/ [https://perma.cc/EZ7Y-2XF4].

18 Ben Cohen, *Wait, When Did Everyone Start Using Apple Pay?*, WALL ST. J. (Aug. 18, 2022), https://www.wsj.com/articles/apple-pay-iphone-wallet-apps-11660780139?st=l1fbf12jpmgfj9m [https://perma.cc/Y8MC-L3X4]. Tech companies, like Apple, plan for people to "replace their physical wallet" and complete all transactions from their phones. Apple Pay is now accepted by 90% of retailers and used by around 75% of iPhone owners. Other companies have similar retail products that are pushing consumers away from cash. *Id.*

19 *See* DAVID W. PERIKINS, CONG. RSCH. SERV., R45716, LONG LIVE CASH: THE POTENTIAL DECLINE OF CASH USAGE AND RELATED IMPLICATIONS 11 (May 10, 2019).

protections are needed to keep the equilibrium.[20] Given this financial surveillance structure and our progression to a cashless society, we should reconsider the carte blanche law enforcement has in accessing Americans' financial information.[21]

However, a delicate balance must be struck, as "a probable cause standard for subpoenas would end many white-collar criminal investigations before they had begun."[22] The nature of those investigations usually necessitates reviewing documents before establishing probable cause, and courts have long applied legal doctrines with an eye towards the balance between crime and law enforcement.[23] In Fourth Amendment case law, courts have usually relied on categorical approaches to technology, and have largely been resistant to the mosaic theory, which would bring more case-by-case analysis of the volume and importance of the information collected.[24] A mosaic theory applied to financial records would more accurately protect the privacy interests of individuals, which are especially at risk when large volumes of data are collected. But this approach is criticized for lacking clear guidance; how would law enforcement know when they need to request a warrant, and how would judges weigh duration, content, platform, and other considerations to make consistent decisions?[25] Congressional rulemaking could take into account the

[20] *See* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011). Kerr's article mainly describes his equilibrium theory of the Fourth Amendment, but he explains the lack of protections for financial records by noting the increase in white-collar crime and the difficulty of enforcement.

[21] This student Note parallels some of 2023's public debate over Section 702 of the Foreign Intelligence Surveillance Act (FISA). If limiting collection is not in our national interest, we can partially assuage privacy concerns by regulating access to the collected data.

[22] William J. Stuntz, *O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment*, 114 HARV. L. REV. 842, 860 (2001).

[23] *Id.*; Kerr, *supra* note 20, at 509.

[24] Paul Rosenzweig, *In Defense of the Mosaic Theory*, LAWFARE (Nov. 29, 2017), https://www.lawfareblog.com/defense-mosaic-theory [https://perma.cc/3SLM-KNKF].

[25] *Id.*

legitimate law enforcement interests at play,[26] while slowing the current one-way ratcheting up of financial surveillance.

This Note argues that the financial surveillance of Americans has gone too far, justifications for it under constitutional principles have made a mess of legal doctrines, and Congress should turn the dial back to a happier medium. Part II explains the history of financial surveillance, starting with the Bank Secrecy Act, continuing with the War on Terror and the Patriot Act, and arriving at our current, near-total financial surveillance structure. It also explains the parallel developments in Fourth Amendment case law. Part III describes how *Carpenter*'s emphasis on "detailed, encyclopedic, and effortlessly compiled"[27] records that are made pursuant to technologies "indispensable to participation in modern society"[28] have made *Miller* "an unprincipled and unworkable doctrine,"[29] especially in light of changes in financial information since 1976. It describes justifications for the status quo, including its value to law enforcement, and concludes that no judicial solution adequately balances Americans' Fourth Amendment rights, basic financial privacy, and legitimate law enforcement interests in complex white-collar investigations. Finally, Part IV suggests some ways that Congress can better protect Americans' financial privacy, namely by limiting subpoenas' duration and adding suppression as a remedy for violations of The Right to Financial Privacy Act.

II.

A. Bank Secrecy Act and Financial Surveillance

The Bank Secrecy Act of 1970 (BSA) and the additional laws that followed were inspired in part by the idea that criminals conduct business in cash, and the banks should assist

[26] Aziz Z. Huq, *How the Fourth Amendment and the Separation of Powers Rise (and Fall) Together*, 83 U. CHI. L. REV. 139, 149 (2016).

[27] Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018).

[28] *Id.* at 2220.

[29] *Id.* at 2230 (Kennedy, J., dissenting).

the government in surveilling those activities.[30] As such, the BSA mandated recordkeeping and reporting by banks in order to maintain information that had a "high degree of usefulness in criminal, tax, or regulatory investigations or proceedings."[31] In passing that legislation, Congress was concerned about Americans' use of foreign financial institutions to evade legal or tax obligations.[32] Additionally, increases in sophisticated criminal activity flowing through domestic financial institutions necessitated increased government visibility of those schemes.[33] Law enforcement wanted a way to preserve the records of such crimes, which may have happened years ago and whose only witness was often the bank used to transfer funds. As a result, financial institutions were required to make and retain records of transaction details.[34] Access to those records by government authorities was to be controlled by the "existing legal process," which did not limit requests in time or scope.[35]

Other BSA provisions effectively invert the traditional warrant requirement—instead of the government requesting permission to search one's papers, businesses are compelled by statute to affirmatively report information to the government. The BSA first included a provision for banks and other financial institutions to tell the government, through a Currency Transaction Report (CTR), any time someone attempts a cash transaction over $10,000.[36] Breaking up the transaction into smaller amounts will not get around this reporting

[30] Bank Secrecy Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114; Robert J. Olejar, *Anti-Money Laundering v. the Right to Privacy*, 2008 N.J. LAW. 56, 59.

[31] Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 26 (1974). For an extended discussion on the background and purpose of the BSA, see *id.*

[32] *Id.* at 27–29.

[33] *Id.* at 27.

[34] 31 C.F.R. §§ 1010.300, 1010.400 (2022).

[35] *Cal. Bankers Ass'n*, 416 U.S. at 52. The existing legal process is controlled by statute since the Supreme Court later declared in *Miller* that there is no constitutional floor in searches of financial records. United States v. Miller, 425 U.S. 435 (1976). For federal authorities, The Right to Financial Privacy Act controls. 12 U.S.C. §§ 3401–3423.

[36] 31 C.F.R. § 1010.311 (2022).

requirement,[37] and is actually a federal crime itself.[38] A $10,000 transaction may seem like a high threshold for an individual, since most people would only exceed it for large purchases like a car, a down payment for a house, or Columbia Law tuition. But if the reporting requirement was adjusted for inflation, the 2022 threshold would be approximately $75,000.[39] As a result of the unchanged transaction threshold, a high volume of CTRs have been filed in recent years, including over 16 million in 2019.[40]

Policymakers saw financial surveillance as a great tool, and over time it was applied to solve problems besides tax evasion.[41] During the War on Drugs, these tactics were repurposed to combat cartels, which had been using the banking system to wash their enormous cash profits.[42] SARs, which became required after the Annunzio-Wylie Anti-Money Laundering Act of 1992, began to alert law enforcement to specific persons or entities relevant to their efforts.[43] As noted in the Introduction, these regulations mandate that banks, and now many other organizations, report suspicious or unexplainable financial activity to the government. Institutions are incentivized to over-file SARs defensively because scrutiny from

[37] 31 C.F.R. § 1010.330(b) (2022).

[38] 31 U.S.C. § 5324.

[39] INFLATION CALCULATOR, FED. RSRV. BANK OF MINNEAPOLIS, https://www.minneapolisfed.org/about-us/monetary-policy/inflation-calculator [https://perma.cc/DP5V-WVQ9] (enter "10000" and "1970"; then press "Calculate").

[40] 85 Fed. Reg. 29022, 29023 (May 14, 2020) (to be codified at 31 C.F.R. §§ 1010.310–314, 1021.311–313). For historic data, see also *Suspicious Activity Reports and Cash Transaction Reports, 2000-2015* (table), *in* Norbert Michel & David Burton, *Financial Privacy in a Free Society*, THE HERITAGE FOUNDATION (Sept. 23, 2016), https://www.heritage.org/markets-and-finance/report/financial-privacy-free-society [https://perma.cc/KV6V-RRUW].

[41] *BSA Timeline 1970-Present*, FINCEN, https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act/bsa-timeline [https://perma.cc/J4BE-GJNV] (last visited Sept. 10, 2023).

[42] *Id.*

[43] *Id.*; 31 U.S.C. § 5318(g).

regulators is most acute when instances of criminal activity are missed.[44]

When the War on Terror began, policymakers once again turned to financial surveillance as a powerful digital means to defeat real-world, violent crimes. The Patriot Act, in addition to its more infamous provisions on phone tapping and indefinite detention, included sections to expand financial reporting and surveillance tools.[45] More entities were required to file SARs and CTRs,[46] and the Department of the Treasury (Treasury) could now require that all financial institutions search their records for matches on particular names.[47] There is no judicial check on this Section 314 process, and it allows law enforcement to start with a target rather than beginning an investigation after receiving a SAR or CTR. Despite its post-9/11 origins, the majority of Treasury requests through this process have been unrelated to terrorism.[48]

---

[44] Richard Vanderford, *'Defensive' SARs Filings Remain an Issue, NY Regulator Says*, MLEX (Apr. 15, 2021), https://mlexmarketinsight.com/news/insight/defensive-sars-filings-remain-an-issue-ny-regulator-says [https://perma.cc/L5XK-L9ZP]; Carl Brown, *Not Enough Needles and Too Much Hay: The Problem with Suspicious Activity Reports*, GRC WORLD FS. (Feb. 2, 2021), https://www.grcworldforums.com/financial-crime/not-enough-needles-and-too-much-hay-the-problem-with-suspicious-activity-reports/719.article [https://perma.cc/4TXP-HNWF]; V. Gerard Comizio, Kevin L. Petrasic, Lawrence D. Kaplan & Helen Y. Lee., FINCEN SHARPENS TEETH WITH NEW ENFORCEMENT DIVISION – PRACTICAL CONSIDERATIONS FOR AVOIDING FINCEN'S BITE, PAUL HASTINGS, 3 (2013), https://webstorage.paulhastings.com/Documents/PDFs/stay_current_fincen_sharpens_teeth.pdf [https://perma.cc/EDS2-EB5L].

[45] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[46] *Id.* §§ 356, 365; 31 C.F.R. § 1010.520 (2022).

[47] USA PATRIOT Act § 314; *see also* FINCEN, *FinCEN's 314(a) Fact Sheet* (Aug. 22, 2023), https://www.fincen.gov/sites/default/files/shared/314afactsheet.pdf [https://perma.cc/8EH8-W38Q] (facilitating the standard subpoena process so investigators are then aware of which banks to request further information from).

[48] FINCEN, *FinCEN's 314(a) Fact Sheet* (Aug. 22, 2023), https://www.fincen.gov/sites/default/files/shared/314afactsheet.pdf [https://perma.cc/8EH8-W38Q].

In the past year, Congress has also attempted to expand reporting requirements beyond financial services.[49] Already, the term "financial institution" had been expanded to include travel agencies, casinos, car and boat dealerships, the Postal Service, sellers of jewelry or precious metals, and any other business that Treasury thinks would have a "high degree of usefulness in criminal, tax, or regulatory matters."[50] Organizations may each have different thresholds for reporting requirements; for example, Money Service Businesses must report suspicious activity over $2,000 while the threshold for casinos is $5,000.[51] All financial institutions must verify and record the identity of transmitters, and banks must also create baselines for normal customer behavior and then monitor for anomalous transactions.[52]

[49] Peter D. Hardy & James Mangiaracina, *Closing the Gate: House Adopts ENABLERS Act Amendment to 2023 NDAA*, CONSUMER FIN. MONITOR (July 21, 2022), https://www.consumerfinancemonitor.com/2022/07/21/closing-the-gate-house-adopts-enablers-act-amendment-to-2023-ndaa/ [https://perma.cc/K48N-Q4CB]. The ENABLERS Act, if passed as part of the 2023 National Defense Authorization Act, would have added corporate formation and trust services, payment processors, and certain legal and accounting services to the entities covered by the Bank Secrecy Act's recordkeeping and reporting requirements. A previous version had also included art and antiquities dealers. The stated purpose of this legislation is to give authorities a broader net of potentially illicit transactions to watch over, and while it was ultimately removed from the 2023 NDAA, its supporters, including President Biden, hope to revive it in the future. Will Fitzgibbon, *US Senate Blocks Major Anti-Money Laundering Bill, the Enablers Act*, INT'L CONSORTIUM OF INVESTIGATIVE JOURNALISTS (Dec. 12, 2022), https://www.icij.org/investigations/pandora-papers/us-senate-blocks-major-anti-money-laundering-bill-the-enablers-act/ [https://perma.cc/95CW-J4S3].

[50] 31 U.S.C. § 5312(a)(2).

[51] FINCEN, SUSPICIOUS ACTIVITY REPORTING GUIDANCE FOR CASINOS 3 (2003), https://www.fincen.gov/sites/default/files/shared/sar_guidance_casino.pdf [https://perma.cc/8T96-DQL2]; *Money Services Business (MSB) Suspicious Activity Reporting*, FINCEN, https://www.fincen.gov/money-services-business-msb-suspicious-activity-reporting [https://perma.cc/4J6A-RYUR].

[52] 31 C.F.R. § 1010.312 (2021); 31 C.F.R. § 1010.410 (2016); 31 C.F.R. § 1010.220 (2022); *see, e.g.,* 31 C.F.R. § 1020.210 (2022) (describing the program requirements for banks); 31 C.F.R. § 1020.315(h).

Information from the financial surveillance system does not stay with Treasury. Law enforcement across the nation has access to an online database established by the Financial Crimes Enforcement Network (FinCEN),[53] where queries of individual names can return SARs or other financial data on the targets.[54] The Anti-Money Laundering Act of 2020 enabled further coordination and information sharing between FinCEN and law enforcement across the country.[55] There certainly will be a lot of information to share—in fiscal year 2019, more than 20 million total BSA reports were filed by over 97,000 American financial institutions.[56]

[53] *What We Do*, FINCEN, https://www.fincen.gov/what-we-do [https://perma.cc/ARU8-YDML] (last visited Sept. 10, 2023) ("FinCEN's mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.").

[54] FINCEN, FACT SHEET: THE FINCEN PORTAL, https://www.fincen.gov/sites/default/files/shared/Facts_FinCENPortal.pdf [https://perma.cc/C45T-WF5A] (last visited Sept. 10, 2023); FINCEN, FACT SHEET: FINCEN QUERY, https://www.fincen.gov/sites/default/files/shared/Facts_FinCENQuery.pdf [https://perma.cc/7E9Q-7WSY] (last visited Sept. 10, 2023).

[55] Norbert Michel & Jennifer Schulp, *Revising the Bank Secrecy Act to Protect Privacy and Deter Criminals*, CATO INST. (July 26, 2022), at 8, https://www.cato.org/sites/cato.org/files/2023-04/policy-analysis-932-update-4-12-23.pdf [https://perma.cc/4BCW-SL22].

[56] *What is the BSA Data?*, FINCEN, https://www.fincen.gov/what-bsa-data [https://perma.cc/VUZ8-BE5G] (last visited Sept. 10, 2023). The security of this enormous volume of data may also be questionable, as the federal government does not have a spotless record on information security, with notable hacking and leaking incidents. *See* David E. Sanger & Julie Hirschfeld Davis, *Hacking Linked to China Exposes Millions of U.S. Workers*, N.Y. TIMES (June 4, 2015), https://www.nytimes.com/2015/06/05/us/breach-in-a-federal-computer-system-exposes-personnel-data.html [https://perma.cc/BD4K-P2D2]; *FinCEN Files: All You Need to Know About the Documents Leak*, BBC NEWS (Sept. 21, 2020), https://www.bbc.com/news/uk-54226107 [https://perma.cc/RR8A-4P4X].

B. The Fourth Amendment's Evolution and Exclusion of Financial Records

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[57]

The Fourth Amendment was largely a response to British use of "writs of assistance, a form of general warrant" that did not specify the person or place to be searched and did not require evidence to be presented to a judge.[58] In the early republic, state constitutional analogues were used to protect against arbitrary searches of one's home without specific, judicially-approved warrants.[59]

Scholars largely agree that Fourth Amendment doctrine is now somewhat unclear, although they disagree on why that is.[60] Scholars, and courts too, have struggled with what values the Fourth Amendment prioritizes and how those should be balanced against the needs of law enforcement and public safety.[61] Most of Fourth Amendment law now focuses on determining whether something is a search or not, rather than the reasonableness question, because searches have been deemed presumptively unreasonable without a warrant,[62]

---

57 U.S. CONST. amend. IV.

58 Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1194 (2016).

59 *Id.* at 1276–80. Since federal criminal investigations were rare at the time, and the Fourth Amendment did not apply to the states yet, there was not much case law directly applying the Amendment.

60 *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 505 (2007) (compiling various opinions on the cause of confusion in Fourth Amendment doctrine).

61 Anna Lvovsky, *Fourth Amendment Moralism*, 166 U. PA. L. REV. 1189, 1204–05 (2018).

62 *See infra* note 69 and accompanying text. This approach is not without criticism. *See* Carpenter v. United States, 138 S. Ct. 2206, 2238, 2243–45 (2018) (Thomas, J., dissenting).

and even subpoenas are not sufficient for records that meet the search test.[63]

Traditionally, categorizing an action as a "search" hinged on whether an interest in a "tangible property" right had been invaded.[64] This property-based understanding of the Fourth Amendment was mostly static until the mid-20th century. It allowed consistency and predictability for law enforcement, courts, lawyers, and the public, but came to be under-exclusive.[65] With technological changes, new investigative tactics became possible which were intrusive, but not quite trespasses. In 1967, the Supreme Court was presented squarely with the question of whether there could be a search when there was not a physical intrusion.[66]

The Supreme Court shifted the doctrine significantly in *Katz v. United States*, taking into account expectations of privacy.[67] There, police had used a recording device to capture a suspect's phone call from a public telephone.[68] The Court made clear that a physical trespass was no longer a requirement of search, and that searches without warrants were presumptively unreasonable.[69] Although the officers may have objectively had probable cause for their actions, the majority held that the lack of review by a judicial officer was decisive.[70] But *Katz* is most famous for the rule that came from a concurrence. Justice Harlan pronounced that in determining if a search had occurred, a court should consider whether the defendant had manifested a subjective expectation of privacy

63 Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018). Indeed, one of the main arguments of Justice Kennedy's dissent was that the subpoena process provided sufficient procedural checks. *Id.* at 2228 (Kennedy, J., dissenting). The majority, of course, disagreed, stating "this Court has never held that the Government may subpoena third parties for records in which the suspect has a reasonable expectation of privacy." *Id.* at 2221.

64 Katz v. United States, 389 U.S. 347, 352–53 (1967).

65 *Id.* at 353.

66 *Id.* at 350.

67 *Id.* at 351 ("[W]hat he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").

68 *Id.* at 348.

69 *Id.* at 352–53, 357.

70 *Id.* at 356.

and whether society was prepared to accept that expectation as reasonable.[71]

After *Katz*, lower courts applied the expectation of privacy test to financial records. The Fifth Circuit reasoned in *United States v. Miller* that since the government could not compel someone to produce their "private papers to establish a criminal charge against him," forcing a third party to do so would also violate a target's rights.[72] After finding distillery equipment in a truck and warehouse rented by Miller, the United States Attorney's Office subpoenaed his banks for his financial records.[73] Miller was not notified at the time and later argued that the prosecution should not have been able to use those records to prove his alcohol production and tax evasion charges.[74] The issue was whether the subpoena, which was not issued by a court or grand jury, qualified as adequate legal process under the BSA and the Fourth Amendment.[75] While the BSA allowed government access to financial records through the existing legal process, the Fifth Circuit ruled subpoenas were insufficient as a constitutional matter.[76]

However, the Supreme Court reversed that decision, and in the process announced the beginnings of an explicit third-party doctrine.[77] The Court stated that there was no reasonable expectation of privacy in financial records or other information voluntarily turned over to third parties, and the BSA's retention provisions did not change that.[78] Since there was no

[71] *Id.* at 361 (Harlan, J., concurring).

[72] United States v. Miller, 500 F.2d 751, 757 (5th Cir. 1974) (quoting Boyd v. United States, 116 U.S. 616, 622 (1886)), *rev'd*, 425 U.S. 435 (1976).

[73] United States v. Miller, 425 U.S. 435, 437 (1976).

[74] *Id.* at 438.

[75] *Miller*, 500 F.2d at 757–58.

[76] *Id.*

[77] *Miller*, 425 U.S. at 444. The third-party doctrine holds, generally, that people have no reasonable expectation of privacy in information handed over to third parties. Therefore, it is not a search when the government accesses this data. Some scholars argue that this was always an implicit part of Fourth Amendment law, with the labeling just changing in the 1970s. *See* Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 115 (2015).

[78] *Miller*, 425 U.S. at 441–43.

protectable Fourth Amendment interest in financial records, even a defective subpoena did not raise constitutional concerns.[79] The majority distinguished *Katz* by explaining that "the nature of the particular documents" was key in determining whether they were knowingly exposed to the public or meant to be kept as private, and decided that checks and deposit slips were better categorized as negotiable instruments "exposed to [bank] employees in the ordinary course of business," rather than as the defendant's personal papers.[80] It was therefore not a search when the prosecutor used a subpoena instead of a warrant to access this information, "even if a criminal prosecution is contemplated at the time of the subpoena is issued."[81] Since no "search" occurred, there were no Fourth Amendment issues.

The third-party doctrine effectively ended any hope that financial records would be protected by the Fourth Amendment, but Congress responded to the decision by enacting The Right to Financial Privacy Act.[82] The law restricts federal authorities to accessing an individual's financial records by customer authorization, administrative subpoena, search warrant, judicial subpoena, or written request.[83] Importantly, it contains a notification requirement when the federal government requests a customer's information, but there are exceptions, including whenever secrecy is believed to be necessary for an ongoing investigation.[84] The RFPA also gave individuals standing to challenge a subpoena under the Act,[85] but they need to prove that the "records requested are not relevant to

79 *Id.* at 441 n.2.

80 *Id.* at 442.

81 *Id.* at 444.

82 Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401–3423. Congress stated the RFPA was a response to *Miller*, but *Miller* simply upheld the BSA statutory scheme which Congress itself created and has since expanded. The RFPA does not apply to state and local authorities, but some states have similar statutes. *Right to Financial Privacy Act*, ELECTRONIC PRIVACY INFORMATION CENTER, https://epic.org/the-right-to-financial-privacy-act/ [https://perma.cc/8YPY-B3S4] (last visited Sept. 8, 2023).

83 12 U.S.C. §§ 3404–08.

84 12 U.S.C. §§ 3404–09.

85 12 U.S.C. § 3410.

the agency's" legitimate law enforcement inquiry, which can be defeated if the government shows it "touches a matter under investigation."[86]

The Court's other cases since 1976 have recognized that Fourth Amendment law must evolve with changes in technology. In *Kyllo v. United States*, the majority was concerned with preserving the "degree of privacy against government that existed when the Fourth Amendment was adopted."[87] There, a thermal imaging tool was used from a public street to determine that certain areas of a house were abnormally warm, leading to further investigation for marijuana production.[88] The Court was confronted with whether new technology could change the extent of privacy enjoyed by Americans, as naked-eye surveillance of the home would not have been a search.[89] In declaring that this was indeed a search, it noted "the rule we adopt must take account of more sophisticated systems that are already in use or in development."[90]

While focus had shifted away from a property-based conception of the Fourth Amendment, the Supreme Court reminded lower courts in *U.S. v. Jones* that the *Katz* expectations test was not the only part of the search analysis.[91] *Katz* was an addition to the common law trespass test, and an

86 Sandsend Fin. Consultants, Ltd. v. Fed. Home Loan Bank Bd., 878 F.2d 875, 882 (5th Cir. 1989). There are also procedural grounds on which a plaintiff could succeed, if "the agency has not substantially complied with the RFPA." *Id.*

87 Kyllo v. United States, 533 U.S. 27, 34 (2001).

88 *Id.* at 29–30.

89 *Id.* at 31–32. For example, if there was snow on the roof that was melting abnormally fast, a police officer would not need a search warrant to observe this. Here, the technology only captured heat emitted from the home, not heat inside the home. While these are often very similar, the distinction is critical, although fuzzy. The technology enhanced the view of the outside of the home but did not technically peer inside of it. An advanced listening device could operate the same way, capturing conversations that occur inside the home but only by picking up external sounds which are too faint for an unassisted ear to hear. *See id.* at 35.

90 *Id.* at 36.

91 United States v. Jones, 565 U.S. 400, 406–07 (2012).

action could be ruled a search under either framework.[92] In *Jones*, placing a tracker on someone's car was ruled a search because the act itself was a trespass, even though the defendant did not have an expectation of privacy on public roads.[93]

In 2018, *Carpenter* upset the third-party doctrine when the Court declared that cell site location information (CSLI) was protectable even though it was voluntarily given to private companies.[94] There, the majority distinguished information given to third parties through activities "indispensable to participation in modern society."[95] Since there was no way to stop sharing the data while using a phone, "in no meaningful sense does the user voluntarily" consent to sharing.[96] The Court also took issue with the amount of data being shared, and "the nature of the particular documents sought" there was pivotal too, as location data is extensive, can accurately track where a phone travels for years, and may reveal particularly private information.[97] However, the *Carpenter* majority explicitly said *Miller* was not being overturned, as they considered checks and deposit slips less intrusive than cell site location data.[98]

C. *Miller* after *Carpenter*

Unsurprisingly, financial records search cases since *Carpenter* have pointed to its clear validation of *Miller*.[99] Courts have also extended *Miller* to new forms of financial technology.

In *Zietzke v. United States*, the district court realized it was in the "unenviable position" of attempting to understand how *Carpenter* distinguished bank records from CSLI, since "little

92 *Id.* at 409.

93 *Id.* at 404–05.

94 Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

95 *Id.*

96 *Id.*

97 *Id.* at 2219–20. However, the location data at issue here was only created when the defendant "made or received calls." *Id.* at 2214.

98 *Id.* at 2220.

99 Presley v. United States, 895 F.3d 1284, 1291 (11th Cir. 2018); Standing Akimbo, LLC v. United States through Internal Revenue Serv., 955 F.3d 1146, 1165 (10th Cir. 2020).

guidance" had been given for the task.[100] There, when faced with a summons for a user's records from a cryptocurrency exchange, the court focused on *Carpenter*'s discussion of physical location.[101] It noted that there was no location surveillance in these cryptocurrency transactions, so the movant could not point to the same concerns at issue in *Carpenter*.[102] Accordingly, the petitioner's challenge to the records request was denied.[103]

Only one circuit court appears to have waded into this issue so far. In *United States v. Gratkowski*, the Fifth Circuit confronted whether an individual had a right to privacy in his information on the Bitcoin blockchain. The court concluded that the defendant's records were more similar to the bank records in *Miller* than the location data in *Carpenter*.[104] The court reasoned that using Bitcoin is not an inescapable part of daily life and that "it is well known that each Bitcoin transaction is recorded in a publicly available blockchain."[105] In regard to the transaction data that was subpoenaed directly from Coinbase, the court thought "a person's virtual currency transactions" are infrequent and do not provide an "intimate window" into their life, and like in *Miller*, the information was voluntarily provided to a third party.[106] They also relied on the fact that limited information—the amount, the sending party, and the receiving party—was gathered from his transactions.[107]

While the D.C. Circuit sidestepped this question in *Witaschek v. District of Columbia*, it left open that *Carpenter*

100 Zietzke v. United States, 426 F. Supp. 3d 758, 768 (W.D. Wash. 2019).

101 *Id.*

102 *Id.* at 769.

103 *Id.*

104 United States v. Gratkowski, 964 F.3d 307, 312 (5th Cir. 2020).

105 *Id.* Thus, the implication is that there is no expectation of privacy.

106 *Id. See also* United States v. Miller, 425 U.S. 435, 441–43 (1976).

107 *Gratkowski*, 964 F.3d at 311–12. In this case, the limited information of sender and receiver was sufficient as evidence, since the defendant had paid for access to a child exploitation website.

might impact the privacy analysis for financial records.[108] There, tax enforcement investigators had used summonses to confirm that the defendant was lying about his part-year residency in the District.[109] Defendant argued that the information was protectable after *Carpenter* because it revealed his location history, and that it should be suppressed since the request had not been presented to a neutral magistrate.[110] But since the conduct at issue took place before *Carpenter*, the court avoided the issue and stated that the good-faith exception would apply even if the documents implicated a legitimate privacy interest.[111] Meanwhile, state courts have historically produced mixed results on the reasonable expectation of privacy in financial records, and the one that has taken it up post-*Carpenter* pointed to the upholding of *Miller*.[112]

In this way, the third-party doctrine can be straightforward for lower courts to apply; they can use the categorical tests and wait until the Supreme Court adds any new forms of technology to the exceptions list. However, in isolated instances, courts have been accepting of a mosaic theory of the Fourth Amendment to grapple with the potential for data aggregation, though not applied directly to financial records.[113] The majority in *Carpenter* also sidestepped the question of whether accessing fewer days of CSLI would have produced the same result, lending support to the idea that the volume

108 Witaschek v. District of Columbia, 254 A.3d 1151, 1157 (D.C. Cir. 2021).

109 *Id.* at 1154.

110 *Id.* at 1157.

111 *Id.* at 1157–58.

112 State v. Adame, 476 P.3d 872, 876–77 (N.M. 2020).

113 *See infra* Section III.C.2; Commonwealth v. Henley, 171 N.E.3d 1085, 1102–07 (Mass. 2021) (rejecting the application of the third-party doctrine to public transportation and agreeing that an extensive search of one's metro card records could constitute a search under the mosaic theory, while holding that two days' worth of data was not a search); Kelly v. United States, 281 A.3d 610, 614 (D.C. Cir. 2022) (determining that the two-day real-time tracking of a suspect's metro card usage was not a search by analogizing to *Henley* and *Carpenter*, and weighing the amount of data received rather than applying a simple categorical approach to metro cards).

of data, and not just categorical approaches to technology, may impact whether something is a search.[114]

III.

A. Changes in Financial Technology and Consumer Practices

> With a cashless trail, you were fated always to be what you had always been; you couldn't flee far from your name, your purchases, even your network of friends. You were always, by your cards or cell phone, outed as yourself.[115]

1. Technology and Consumer Practices

As law enforcement's tools have expanded, changes in technology and Americans' habits have contributed to making financial records a one-stop investigative shop.

Over time, the information within financial records has greatly expanded.[116] No longer do people use credit cards occasionally, checks often, and cash as the primary means for transactions. Now, using cash has become increasingly rare as finance has been digitalized on the consumers' side as well; cards and mobile pay dominate retail transactions.[117] Financial "[t]echnology is no longer a quirky addition to our daily routines," it is essential to operating in the modern world.[118]

---

114 "[W]e need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search." Carpenter v. United States, 138 S. Ct. 2206, 2217 n.3 (2018).

115 Nathan Heller, *Imagining a Cashless World*, NEW YORKER (Oct. 3, 2016), https://www.newyorker.com/magazine/2016/10/10/imagining-a-cashless-world [https://perma.cc/WS5S-T9YB].

116 Gentithes, *supra* note 13, at 1075–76.

117 *See generally* CUBIDES & O'BRIEN, *supra* note 16.

118 Nicholas Anthony, *Why Don't Americans Have Stronger Financial Privacy Rights?*, CATO INST. (Oct. 28, 2021), https://www.cato.org/blog/why-

The pandemic accelerated existing trends in the digitalization of finance.[119] From 2016 to 2021, cash usage share, by percentage of all payments, decreased by 11%.[120] By 2022, over 40% of Americans said "*none* of their purchases in a typical week are paid for using cash, up from 29% in 2018 and 24% in 2015."[121] Americans used less cash because of changing preferences towards credit cards and increases in peer-to-peer mobile app payments, among other reasons.[122] Card use is often quicker and users receive rewards from payment processors for each swipe.

Additionally, cash usage decreased because consumers are making fewer purchases in person, instead substituting online retail purchases and remote payments for food and drinks.[123] Online purchases made from the home, with possibly more expectations of privacy, show up on one's bank statement just the same as a trip to the mall. Most Americans buy things online using smartphones or computers, and nearly a third make weekly purchases online.[124] These statistics are more pronounced in younger Americans, with over 90% of those between the ages 18 to 49 using smartphones to make online purchases.[125] Additionally, by 2022, over 75% of

dont-americans-have-stronger-financial-privacy-rights [https://perma.cc/P2EP-T2GU].

119 Kate Marino, *The Pandemic-Fueled Decline of Cash*, AXIOS (July 16, 2021), https://www.axios.com/2021/07/16/legal-cash-economy-decline-pandemic [https://perma.cc/8ZWC-PPSU].

120 CUBIDES & O'BRIEN, *supra* note 16, at 6.

121 Michelle Faverio, *More Americans Are Joining the 'Cashless' Economy*, PEW RSCH. CTR. (Oct. 5, 2022), https://www.pewresearch.org/fact-tank/2022/10/05/more-americans-are-joining-the-cashless-economy/ [https://perma.cc/74EH-3CZH].

122 CUBIDES & O'BRIEN, *supra* note 16, at 9–11.

123 *Id.* at 6–8. Between 2016 and 2021, the share of in-person purchases and peer-to-peer payments dropped from 92% to 82%.

124 Michelle Faverio & Monica Anderson, *For Shopping, Phones Are Common and Influencers Have Become a Factor—Especially for Young Adults*, PEW RSCH. CTR. (Nov. 21, 2022), https://www.pewresearch.org/fact-tank/2022/11/21/for-shopping-phones-are-common-and-influencers-have-become-a-factor-especially-for-young-adults/ [https://perma.cc/3ZTU-TT6D].

125 *Id.*

Americans had already used one of PayPal, Zelle, Venmo, or Cash App for peer-to-peer payments, citing their ease of use.[126] Government authorities have easy access to all of those transactions, even if some are initiated in private spaces.

A cashless society increases not only the volume of financial data available but also alters its character. When the entries that appear in financial statements are comprehensive, they reveal intimate information that raises further privacy concerns.[127] Each credit card purchase pinpoints the exact location and time that you were at a store or subway stop. Financial information can be particularly sensitive in the First Amendment context.[128] Our bank records can show which political party someone donated to, which church they attend, and any legal but disfavored organizations or activities they participate in.[129] There are also network effects at play.[130] The details gleaned from financial records increase exponentially as a comprehensive picture of a person's life is drawn, and artificial intelligence may be used to "find patterns and relations that humans would never consider."[131]

---

126 Monica Anderson, *Payment Apps Like Venmo and Cash App Bring Convenience—and Security Concerns—to Some Users*, PEW RSCH. CTR. (Sept. 8, 2022), https://www.pewresearch.org/fact-tank/2022/09/08/payment-apps-like-venmo-and-cash-app-bring-convenience—and-security-concerns—to-some-users/ [https://perma.cc/4BH6-KZJ3].

127 Peter P. Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance*, 77 WASH. U. L.Q. 461, 469 (1999).

128 Gentithes, *supra* note 13, at 1074 (citing Buckley v. Valeo, 424 U.S. 1 (1976)).

129 The privacy worry is not mainly that these legal activities will be prosecuted, but that "[f]reedom of thought, expression, and action are key to unlocking each person's unique potential to contribute to society. Untargeted government surveillance programs, even well-intentioned ones, threaten that freedom." Commissioner Hester Peirce, *Statement of Hester M. Peirce in Response to Release No. 34-88890*, SEC (May 15, 2020), https://www.sec.gov/news/public-statement/peirce-statement-response-release-34-88890-051520 [https://perma.cc/XP5N-Q2FA] (related to surveillance in securities markets).

130 Swire, *supra* note 127, at 469.

131 William Magnuson, *Artificial Financial Intelligence*, 10 HARV. BUS. L. REV. 337, 358 (2020).

What exactly are privacy advocates worried about when discussing the financial surveillance infrastructure? To many, granting the government more power to surveil transactions, and making it easier to block people from their finances,[132] would be extremely dangerous.[133] They often point to the potential for authoritarian actions and note how "[m]any businesses, dissidents, and human rights groups maintain accounts outside the countries where they are active" in order to

[132] Bradford Newman, *The Digital U.S. Dollar Is a Threat to Civil Liberties*, BITCOIN MAG. (July 20, 2022), https://bitcoinmagazine.com/culture/digital-dollar-threat-civil-liberties [https://perma.cc/DQM3-Q96M] ("Last year the Canadian government ordered financial firms to cease facilitating any transactions from 34 crypto wallets tied to funding trucker-led protests over COVID-19 vaccine mandates."). *See also* Walter Olson, *Canada Says It's Un-Freezing Protestors' Accounts. The Controversy Isn't Going Away.*, CATO INST. (Feb. 25, 2022), https://www.cato.org/blog/canada-says-its-un-freezing-demonstrators-bank-accounts-controversy-isnt-going-away [https://perma.cc/8T4Q-3CSE]. While the Canadian government did not need a central bank digital currency to take these actions, privacy advocates see more government control in this space as dangerous because it imposes fewer steps that could be used to curtail the lawless use of such powers.

[133] Justin Amash (@justinamash), X (formerly TWITTER) (Aug. 31, 2023, 11:58 AM), https://twitter.com/justinamash/status/1697277614975590851 [https://perma.cc/SWP2-FMN7] ("Decentralize money. No digital dollar. A digital U.S. currency would be one of the most dangerous developments in history. When government can simply flip a switch to block all your transactions, it controls your entire life. We need a wall of separation between money and state."); *see also Governor Ron DeSantis Announces Legislation to Protect Floridians from a Federally Controlled Central Bank Digital Currency and Surveillance State*, OFF. OF GOVERNOR RON DESANTIS (Mar. 20, 2023), https://www.flgov.com/2023/03/20/governor-ron-desantis-announces-legislation-to-protect-floridians-from-a-federally-controlled-central-bank-digital-currency-and-surveillance-state/ [https://perma.cc/5TQX-M2KY]. While the proposed legislation is of dubious constitutionality, its existence highlights the concern some influential political constituencies have with the creation of a Central Bank Digital Currency (CBDC). *See* Jesse Hamilton, *Florida's DeSantis Waging Toothless Campaign Against Digital Dollars, Lawyers Say*, COINDESK (May 17, 2023), https://www.coindesk.com/policy/2023/05/17/floridas-desantis-waging-toothless-campaign-against-digital-dollars-lawyers-say/ [https://perma.cc/8APB-J8EL].

avoid suppression.[134] During the Hong Kong protests, pro-democracy protestors waited in long lines at subway stations to purchase their trips with cash, so that financial surveillance couldn't place them at the protest.[135] The existence of surveillance, in this field and others, produces chilling effects and cloaking costs for legitimate activities either forgone or participated in at higher costs.[136] The "banking transactions of an individual give a fairly accurate account of his religion, ideology, opinions, and interests,"[137] and many innocent people could have good reasons to keep that information from government authorities. The Canadian government's response to the 2022 "Freedom Convoy" protest makes some worry that "even relatively free governments are sometimes willing to use private financial information to quell nonviolent protests."[138] There, without court orders, authorities froze bank accounts tied to persons associated with a disruptive, anti-government protest.[139]

New abortion laws mean that the related financial data is now relevant to many state authorities, and is therefore accessible without a warrant.[140] While transaction data usually

134 Norbert Michel & David Burton, *Financial Privacy in a Free Society*, HERITAGE FOUND. (Sept. 23, 2016), https://www.heritage.org/markets-and-finance/report/financial-privacy-free-society [https://perma.cc/5HVA-FCK2].

135 How to Fix the Internet, *Podcast Episode 108: How Private Is Your Bank Account?*, ELEC. FRONTIER FOUND., at 08:40 (Jan. 18, 2022), https://www.eff.org/deeplinks/2021/12/who-peering-your-bank-account [https://perma.cc/GWK3-PYKX].

136 Swire, *supra* note 127, at 473–75.

137 Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 85 (1974) (Douglas, J., dissenting).

138 Michel & Schulp, *supra* note 55, at 14.

139 Walter Olson, *Canada: In a Blow to Liberty, Government Invokes Emergencies Act Against Domestic Protests*, CATO INST. (Feb. 16, 2022), https://www.cato.org/blog/canada-invokes-emergencies-act-against-domestic-protests [https://perma.cc/S4T4-M9KS].

140 Ron Lieber & Tara Siegel Bernard, *Payment Data Could Become Evidence of Abortion, Now Illegal in Some States*, N.Y. TIMES (June 29, 2022), https://www.nytimes.com/2022/06/29/business/payment-data-abortion-evidence.html [on file with the Columbia Business Law Review]; CHRIS

does not show the exact item purchased, the inference may be simpler when payment is to an online medication abortion service.[141] The examination of financial records does not need to prove conclusive either—related purchases or location evidence could be used to build probable cause for a more sweeping search.[142] In the wake of *Dobbs v. Jackson Women's Health Organization*,[143] many bank executives and healthcare spending account administrators declined to comment on whether they would respond to subpoenas for such information.[144] Others claimed they would "not comply with requests for medical expense data—including from law enforcement and other governmental entities—unless we are specifically compelled by law to do so."[145] But the law as currently written and interpreted does indeed compel them to comply with "simple subpoena[s]" from law enforcement.[146] While some financial institutions may attempt to fight these subpoenas harder than in the past, "prosecutors may not say exactly what they're investigating when they ask for transaction records," making real pushback more unlikely.[147]

In response to concerns about access to bank accounts and credit cards, some major cities such as Philadelphia, San Francisco, and New York City "have passed legislation

D. LINEBAUGH, CONG. RSCH. SERV., LSB10786, ABORTION, DATA PRIVACY, AND LAW ENFORCEMENT ACCESS: A LEGAL OVERVIEW 1 (2022).

141 Maggie Koerth & Amelia Thomson-DeVeaux, *As States Banned Abortion, Thousands More Americans Got Pills Online Anyway*, FIVETHIRTYEIGHT (Nov. 1, 2022), https://fivethirtyeight.com/features/medication-abortion-after-dobbs/ [https://perma.cc/ZTJ9-8FXY]. *See* David W. Chen & Pam Belluck, *Wyoming Becomes First State to Outlaw the Use of Pills for Abortion*, N.Y. TIMES (Mar. 17, 2023), https://www.nytimes.com/2023/03/17/us/wyoming-abortion-pills-ban.html [on file with the Columbia Business Law Review].

142 The Fourth Amendment has been incorporated against the states. *See, e.g.*, Mapp v. Ohio, 367 U.S. 643, 655 (1961); Ker v. California, 374 U.S. 23, 30–31 (1963).

143 Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228 (2022).

144 Lieber & Siegel Bernard, *supra* note 140.

145 *Id.*

146 *Id.*

147 *Id.*

forbidding most merchants from refusing to accept cash."[148] These laws also protect privacy. However, no such law exists at the national level, and some scholars even argue that more should be done by policymakers to eliminate cash completely.[149] While financial exclusion could be alleviated by ensuring all Americans have bank accounts, such as through the looming possibility of a Central Bank Digital Currency or Central Bank retail accounts,[150] privacy advocates are rightly worried about the potential implications of a cashless society.

2. *Carpenter*'s Growing Inconsistencies

From the outset, critics noted that much of *Carpenter*'s reasoning is inconsistent with the Court's precedents. In dissent, Justice Kennedy lamented that the majority had injected confusion into the doctrine by rejecting a "straightforward application of *Miller*."[151]

Instead, the *Carpenter* majority attempted to leave standing much of the prior case law, while also creating a new class of digital data to which the third-party doctrine would not

---

148 Pamela Paul, *The Cost of Going Cashless*, N.Y. TIMES (Nov. 13, 2022), https://www.nytimes.com/2022/11/13/opinion/cashless-pay-problem.html [on file with the Columbia Business Law Review].

149 James J. McAndrews & Kenneth S. Rogoff, *Should We Move to a Mostly Cashless Society?*, WALL ST. J. (Sept. 24, 2017), https://www.wsj.com/articles/should-we-move-to-a-mostly-cashless-society-1506305220 [on file with the Columbia Business Law Review]; Lawrence H. Summers, *It's Time to Kill the $100 Bill*, WASH. POST (Feb. 16, 2016), https://www.washingtonpost.com/news/wonk/wp/2016/02/16/its-time-to-kill-the-100-bill/ [https://perma.cc/5KV8-T8MF].

150 *See* Donna Fuscaldo, *Postal Service Gets into Banking, Again*, AARP (Mar. 22, 2022), https://www.aarp.org/money/investing/info-2022/restarting-postal-banking-services.html [https://perma.cc/JS25-EYDA]; John Crawford, Lev Menand & Morgan Ricks, *FedAccounts: Digital Dollars*, 89 GEO. WASH. L. REV. 113, 125–27 (2021); BD. OF GOVERNORS OF THE FED. RSRV. SYS., MONEY AND PAYMENTS: THE U.S. DOLLAR IN THE AGE OF DIGITAL TRANSFORMATION 14-20 (Jan. 2022), https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf [https://perma.cc/5CAP-MJ9Z].

151 Carpenter v. U.S., 138 S. Ct. 2206, 2230 (2018) (Kennedy, J., dissenting).

apply.[152] It did so by identifying several key factors, including "intimacy, comprehensiveness, expense, retrospectivity, and voluntariness."[153] The Court distinguished the records in *Miller* from CSLI, but the financial tools of 1976 are misleading when analogized to modern technology. While those factors aptly distinguish CSLI from checks and deposit slips, they further muddle Fourth Amendment law when one considers modern financial records.

The majority thoroughly explored the comprehensiveness of the location tracking that CSLI provides, since "individuals have a reasonable expectation of privacy in the whole of their physical movements."[154] While favorably comparing CSLI to GPS tracking, they stated "cell phone location information is detailed, encyclopedic, and effortlessly compiled."[155] Although financial records may not produce location data points as frequently as CSLI, they may be more precise and reveal more intimate information. Additionally, the cell data at issue in *Carpenter* was only collected "at call origination and at call termination for incoming and outgoing calls," which for many people would produce hits less frequently than transaction data.[156] CSLI was also accurate to "one-eighth to four square miles,"[157] which in a city could cover "several hundred city blocks."[158] A credit card swipe will place you at a particular subway station, or a precise business on a crowded street or in a mall.

In *Carpenter*, CSLI was seen as even more invasive than a GPS monitor placed on a car because a "cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales."[159] But a credit card is not left in the car either—it will follow a user into each of those locales.

152 *Id.* at 2217.

153 *Id.* at 2234 (Kennedy, J., dissenting).

154 *Id.* at 2217.

155 *Id.* at 2216.

156 *Id.* at 2212.

157 *Id.* at 2218.

158 *Id.* at 2225 (Kennedy, J., dissenting).

159 *Id.* at 2218.

While the card will only 'ping' when used, the cell phone in *Carpenter* only transmitted location data when used for calls.[160] Increases in online shopping and donations, and peer-to-peer transfers, mean financial records also provide information on users who never even leave their homes.[161]

Furthermore, the majority was concerned with the retrospectivity of CSLI data. Privacy concerns were higher because the government could "travel back in time to retrace a person's whereabouts subject only to the [5-year] retention policies of the wireless carriers."[162] Financial data is also kept for years, and like CSLI it can reveal more than just a person's whereabouts. Similarly, authorities do not need to "know in advance whether they want to" investigate an individual using financial records because they can later "call upon the results of that surveillance without regard to the constraints of the Fourth Amendment."[163] While Sprint and Verizon are "[u]nlike the nosy neighbor who keeps an eye on comings and goings, [since] they are ever alert, and their memory is nearly infallible," so too are Visa and Wells Fargo.[164] The *Carpenter* majority relied on distinguishing the financial records in *Miller* as "limited types of personal information," but that description no longer holds true.[165]

The majority also cited the ease of access to those records. They explained that "cell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense."[166] The same can be said for financial records. When the BSA was created, it was "estimated that a minimum of 20 billion checks—and perhaps 30

160 *Id.* at 2214.

161 *See supra* Section III.A.1.

162 Carpenter v. U.S., 138 S. Ct. 2206, 2218 (2018).

163 *Id.*

164 *Id.* at 2219.

165 *Id.*; *see supra* Section III.A.1.

166 *Carpenter*, 138 S. Ct. at 2217–18.

billion—[would] have to be photocopied . . .a year."[167] Now, government authorities can acquire nearly limitless digital financial data with simple requests to financial institutions.[168] The equivalent records used to be physical papers that a bank possessed or, to get a comprehensive view of someone's finances, personal records kept at home.[169] Additionally, much of the data that is present in modern financial records simply would not have existed in the past, since many transactions were in cash.[170]

Finally, the Court distinguished CSLI from other third-party doctrine cases because the "inescapable and automatic nature of its collection" made it difficult to call the sharing voluntary.[171] Since the use of a cell phone was "indispensable to participation in modern society," it became exempt from the traditional third-party doctrine.[172] But having a bank account should "not mean that one has waived all right to the privacy of the papers" either.[173] Today, having a bank account is just as essential an activity as owning a cell phone. In 2021, 3% of Americans did not own a cell phone and 4.5% did not have a bank account.[174] Even "unbanked" individuals complete transactions that are picked up by our surveillance infrastructure, such as those done through money orders and check cashing. Importantly, in *Carpenter* the user could not opt out of sharing CSLI, so "there [was] no way to avoid leaving

167 Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 84 (1974) (Douglas, J., dissenting).

168 *See supra* Section II.A.

169 "The fact that someone could have tucked a paper bank statement in a pocket does not justify a search of every bank statement from the last five years." Riley v. California, 134 S. Ct. 2473, 2493 (2014).

170 *See supra* Section III.A.1.

171 *Carpenter*, 138 S. Ct. at 2223.

172 *Id.* at 2220.

173 *Cal. Bankers Ass'n*, 416 U.S. 21 at 96 (Marshall, J., dissenting).

174 Pew Research Center, *Mobile Fact Sheet*, PEW RSCH. CENTER (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/ [https://perma.cc/YN8J-NA3R]; Federal Deposit Insurance Corporation, *2021 FDIC National Survey of Unbanked and Underbanked Households*, FDIC (Jul. 24, 2023), https://www.fdic.gov/analysis/household-survey/index.html [https://perma.cc/5R4K-2P9B].

behind a trail of location data."[175] If a user could opt out of the BSA's record retention requirements, surely the option would have been exercised by cartel leaders, fraudsters, and sanctioned oligarchs.

In 1974, Justice Powell noted that "[a]t some point, governmental intrusion upon [financial records] would implicate legitimate expectations of privacy."[176] If one focuses on the logic of *Carpenter,* that time has come.

B. The Law Enforcement Tradeoff

The financial surveillance infrastructure was built to serve law enforcement purposes and limit the "heavy utilization of our domestic banking system by the minions of organized crime."[177] While that structure undoubtedly raises privacy and constitutional concerns, completely eliminating the BSA and broad subpoena powers for financial information would make "a good deal of white-collar crime" nearly impossible to prosecute.[178]

In many cases, such as in *Miller* itself, the government likely had the probable cause required for a warrant.[179] A warrant requirement in those circumstances is simply a procedural hurdle. Like any procedural protection, one consequence is added inefficiency. While inefficiency is a feature and not a bug in the domain of the Fourth Amendment,[180] law enforcement would point to the marginal costs of such a change as a reason to oppose it. Presenting your evidence to a judge for a warrant application takes time—"police must draft affidavits

175 *Carpenter*, 138 S. Ct. at 2220.

176 *Cal. Bankers Ass'n*, 416 U.S. at 79 (Powell, J., concurring).

177 *Id.* at 30; *see supra* Section II.A.

178 Stuntz, *supra* note 22, at 863.

179 In *Miller*, prior to the subpoena for bank records, law enforcement received an informant's tip that the defendant operated an unlicensed distillery, found incriminating material in a car driven by his coconspirators, and discovered "a 7,500-gallon-capacity distillery, 175 gallons of nontax-paid whiskey, and related paraphernalia" after a fire in his building. United States v. Miller, 425 U.S. 435, 437 (1976).

180 Riley v. California, 573 U.S. 373, 401 (2014).

and wait around courthouses."[181] Given that complex white-collar investigations can take months or years, it is hard to see how any short procedural delay would have significant effects on such an investigation. But the effect could be cumulative, with countless additional hours spent completing paperwork.

More importantly, a probable cause standard for accessing financial records could prevent many white-collar investigations from beginning at all.[182] In those cases, authorities heavily use subpoenas and "often must examine documents and question witnesses" before establishing probable cause.[183] Law enforcement often "subpoena[s] credit card statements to develop probable cause to prosecute" a wide range of crimes, such as "drug trafficking… healthcare fraud [and] tax evasion."[184] If warrants were required for digital financial data, it "would be a massive sea-change with untold consequences on investigative possibilities (and a significant disturbance of the equilibrium in favor of the individual)."[185] Instead, the government "must have the power to subpoena witnesses and documents before it knows whether those witnesses and documents will yield incriminating evidence" if it is to regulate much of modern business and political affairs.[186]

For crimes like drug trafficking, where there are often witnesses or physical evidence which create suspicion, the subpoena power may be less necessary. Traditional physical evidence and witnesses, along with CTRs and SARs, can alert law enforcement to unusual transaction patterns of cash-based illegal operations. Additionally, "raising the cost of searching" for small-time crimes may be a good idea anyway,

181 Stuntz, *supra* note 22, at 848. *But see Riley*, 573 U.S. at 401 (noting that technological advances have also made the process of obtaining a warrant itself more efficient).

182 Stuntz, *supra* note 22, at 860.

183 *Id.* at 859.

184 Carpenter v. U.S., 138 S. Ct. 2206, 2229 (2018) (Kennedy, J., dissenting).

185 Rosenzweig, *supra* note 24.

186 Stuntz, *supra* note 22, at 860.

as it could "improve the allocation of police resources."[187] The subpoena power can also be dangerous because it can allow "prosecutors to invade the privacy of suspects and witnesses without sufficient cause," and permit "white-collar investigations to run amok."[188] The "almost limitless subpoena power" means overzealous investigators can intrude on "the privacy, time, and energy of suspects and witnesses."[189] Because prosecutorial discretion and federal law are so expansive, "if prosecutors look hard enough, they can find nearly anyone to have violated" some law.[190]

While critics of the larger BSA framework contend "money laundering charges *tend to be* simply added to the main offense rather than providing any independent benefit," this concedes there are added benefits to affirmative reporting.[191] Indeed, FinCEN highlights examples of CTRs or SARs which began or expanded investigations resulting in significant criminal sanctions.[192] Multiple fraud schemes against the pandemic Paycheck Protection Program unraveled after the filing of single SARs.[193] Further investigation led authorities to recover millions of dollars and charge multiple individuals.[194] Other notable cases involved BSA reports starting investigations into securities fraud, drug trafficking, and

187 *Id.* at 849.

188 *Id.* at 843.

189 *Id.* at 861, 864.

190 *Id.* at 864. *See also* Robert H. Jackson, *The Federal Prosecutor*, ROBERT H. JACKSON CTR., https://www.roberthjackson.org/speech-and-writing/the-federal-prosecutor/ [https://perma.cc/LYG6-2H5U] (last visited Sept. 15, 2023).

191 Michel & Schulp, *supra* note 55, at 10 (emphasis added).

192 *Annual FinCEN Program Recognizes Law Enforcement Cases Supported by BSA Data*, FINCEN (Dec. 7, 2022), https://www.fincen.gov/news/news-releases/annual-fincen-program-recognizes-law-enforcement-cases-supported-bsa-data [https://perma.cc/24C2-MZ6P].

193 *Compilation of Award Recipient & Nominated Cases*, FINCEN (Jan. 9, 2023), https://www.fincen.gov/sites/default/files/shared/Compilation%20of%20Award%20Recipient%20and%20Nominated%20Cases%20FINAL%20508C.pdf [https://perma.cc/MR5K-RWZS].

194 *Id.*

healthcare fraud.[195] The reports also proved vital in prosecuting firearms trafficking, Ponzi schemes, and violations of non-proliferation sanctions.[196] After using financial information to build probable cause, search warrants were executed in many of these cases to gather physical evidence of the crimes.

However, those narratives from FinCEN are still akin to the anecdotes of pre-BSA activity which supposedly necessitated its creation.[197] Individual cases are necessarily limited in providing information on the overall value of the financial surveillance system. It is difficult to do a more thorough cost-benefit analysis on affirmative reporting because law enforcement agencies do not track the usefulness of SARs and CTRs.[198] Scholars have attempted to do so without much success,[199] and some in Congress have "repeatedly asked the Treasury and FinCEN for evidence—not merely anecdotes about enforcement actions—that the AML regime provides a *net* benefit."[200] This regime's compliance costs, excluding enforcement by the Department of Justice and Internal Revenue Service, "are estimated to be between $4.8 billion and $8

195 *Id.*

196 *Id.*

197 Michel & Schulp, *supra* note 55, at 4.

> Both the 1968 and 1969 hearings relied on little more than government officials' anecdotes and assurances that access to more information was essential to effective law enforcement. None of the witnesses provided data to support the prevalence of the ostensible money laundering problems through either domestic or foreign financial institutions. Moreover, the witnesses barely discussed how the specific legislative proposals for domestic transactions might improve the ability to prosecute crimes.

198 U.S. GOV'T ACCOUNTABILITY OFF., GAO-22-105242, BANK SECRECY ACT: ACTION NEEDED TO IMPROVE DOJ STATISTICS ON USE OF REPORTS ON SUSPICIOUS FINANCIAL TRANSACTIONS 2 (2022).

199 Lanier Saperstein, Geoffrey Sant & Michelle Ng, *The Failure of Anti-Money Laundering Regulation: Where is the Cost-Benefit Analysis?*, 91 NOTRE DAME L. REV. ONLINE 1, 1–2, 11 (2015); Ronald F. Pol, *Anti-Money Laundering: The World's Least Effective Policy Experiment? Together, We Can Fix It,* 3 POLICY DESIGN AND PRACTICE 73 (2020).

200 Michel & Schulp, *supra* note 55, at 10 (emphasis added).

billion annually." [201] If, as Congressman McHenry argues, the benefits provided "[do] not justify the [financial] burden placed on small businesses," how do they justify the privacy consequences for individuals?[202]

As discussed in Section III.A, the transition to a cashless society is likely inevitable, raising concerns about government agents' access to the data produced by mass surveillance. Privacy advocates are right to push back on the constant ratcheting up of financial surveillance and question its benefits. But without strong evidence that it is wholly ineffective, we must also keep in mind the real public interest in combatting organized crime, terrorist financing, and other illicit activities. While law enforcement's unrestricted access to the products of financial surveillance should be limited, a complete warrant requirement could allow financial records to "become a protected medium that dangerous persons will use to commit serious crimes."[203]

C. "No Single Rubric" will Resolve these Issues in the Courts

Two alternate approaches to Fourth Amendment cases are originalism and the mosaic theory. Originalism has been applied widely to issues facing federal courts, but it has not been prevalent in this space. Meanwhile, the mosaic theory, which understands quantitative privacy in ways categorical tests do not, could offer an interesting framework for modern, data-driven searches. However, for reasons both doctrinal and practical, neither provides a sweeping solution to privacy concerns about searches of financial records.

---

201 Norbert Michel and David Burton, *Financial Privacy in a Free Society*, THE HERITAGE FOUND. (Sept. 23, 2016), https://www.heritage.org/markets-and-finance/report/financial-privacy-free-society/#_ftn1 [https://perma.cc/KV6V-RRUW].

202 Michel & Schulp, *supra* note 55, at 10.

203 Carpenter v. U.S., 138 S. Ct. 2206, 2230 (2018) (Kennedy, J., dissenting).

1. Differing Originalist Conceptions of the Fourth Amendment

While originalism may currently reign supreme as a constitutional interpretive method, it is not quite clear what originalism as applied to searches of financial records would look like. In separate dissents in *Carpenter*, Justices Thomas, Alito, and Gorsuch offered their approaches to the Fourth Amendment issues raised.

The main issue with applying originalism to Fourth Amendment cases is that there is "limited source material."[204] A committed originalist cannot look to debates in Congress over the amendment because there were "virtually [none]."[205] "[T]he Supreme Court did not directly address the meaning of searches for nearly 100 years," so looking to early case law is also unhelpful.[206] The way courts approached broader Fourth Amendment cases has changed too, limiting their use for insight into the original meaning of the text. Since "early cases involved a physical violation of the home or other property," there was obviously a search and courts were concerned with reasonableness.[207] Now, when the whole question is whether something is a search or not, those cases "[do] not give meaningful guidance for the myriad technological advances in investigatory techniques."[208]

In *Carpenter*, Justice Thomas argued for a property-based reading of the Fourth Amendment, which would be incompatible with the existence of the *Katz* test.[209] He stated that the Fourth Amendment aims to protect property, and it protects

204 Michael Gentithes, *Rulifying Reasonable Expectations: Why Judicial Tests, Not Originalism, Create A More Determinate Fourth Amendment*, 59 HOUS. L. REV. 1, 18 (2021).

205 *Id.* at 19.

206 *Id.*

207 *Id.* at 17.

208 *Id.*

209 Carpenter v. U.S., 138 S. Ct. 2206, 2238–39 (2018) (Thomas, J., dissenting).

privacy only in a derivative manner.[210] To him, *Katz* distorts the original meaning of the Fourth Amendment.[211] The second *Katz* prong, whether society is prepared to recognize the subjective privacy belief as reasonable, can of course change over time, even by government influence.[212] He argued that a search should not be defined by whether an expectation of privacy was violated, but by its ordinary definition of looking or examining "for the purpose of finding something."[213]

From this starting point, financial records requests could qualify as searches. Government authorities surely request them for the purpose of examining their contents for traces of illegal activity. However, Justice Thomas also noted that "a subpoena for third-party documents" is not a search.[214] On that point, Justice Alito agreed, writing separately that "an order to produce" is wholly different than a search, and that "the Fourth Amendment, as originally understood, did not apply to the compulsory production of documents at all."[215] Furthermore, he concluded that the Fourth Amendment focused on the means of production, and records requests to third parties are not nearly as invasive as physical searches.[216] For financial records, the inquiry would seem to end there. Both justices would likely agree that judicial subpoenas for financial records do not count as searches and therefore the Fourth Amendment is not implicated.

An originalist reading of the Fourth Amendment would also focus on "*whose* property was searched."[217] In *Carpenter*, the originalists argued there was not a property interest because the defendant "did not create the records, he does not maintain them, he cannot control them, and he cannot destroy them."[218] This is similar to the third-party doctrine and would

210 *Id.* at 2240.

211 *Id.* at 2238, 2241–43.

212 *Id.* at 2245.

213 *Id.* at 2238.

214 *Id.* at 2244.

215 *Id.* at 2247–50 (Alito, J., dissenting).

216 *Id.* at 2251–52.

217 *Id.* at 2235 (Thomas, J., dissenting) (emphasis in original).

218 *Id.*

also likely cut against protection for modern financial records. Justice Thomas wrote that the Court has "not acknowledged that individuals can claim a reasonable expectation of privacy in someone else's business records."[219] Justice Alito added that the third-party doctrine simply effectuates the "their" in the Fourth Amendment, which concentrates the inquiry on who owns the item being searched.[220]

While Justice Gorsuch agreed that subpoenas should be allowed for "ordinary business records," he was more receptive to an individual having property rights in certain data entrusted to third parties.[221] In signaling a desire to scrap the third-party doctrine altogether, he commented that if the *Katz* test is still good law, "no one believes that" we don't actually have expectations of privacy in our private documents residing with third parties.[222] While also applying a property-based conception to the Fourth Amendment, he concluded that related law has not developed a sufficient answer for when digital data is "yours."[223]

The originalists may therefore proceed differently in a property-interest analysis of financial records. All three of these Justices concurred that positive law can be used to create a property interest and therefore a Fourth Amendment interest.[224] But Justice Gorsuch noted third-party access need not eliminate one's property interest in their papers and effects, and that exclusive control or ownership may not be needed to create a Fourth Amendment interest.[225] He pondered whether the "demands of modern life" mean that the

219 *Id.* at 2242.

220 *Id.* at 2260 (Alito, J., dissenting).

221 *Id.* at 2271 (Gorsuch, J., dissenting).

222 *Id.* at 2262.

223 *Id.* at 2268. "Just because you entrust your data—in some cases, your modern-day papers and effects—to a third party may not mean you lose any Fourth Amendment interest in its contents." *Id.* at 2269.

224 *Id.* at 2240–42 (Thomas, J., dissenting), 2251–52, 57–60 (Alito, J., dissenting), 2267–71 (Gorsuch, J., dissenting).

225 *Id.* at 2268–70. "Where houses are concerned, for example, individuals can enjoy Fourth Amendment protection without fee simple title . . . tenants and resident family members—though they have no legal title—have standing to complain about searches of the houses in which they live."

way "we store data with third parties may amount to a sort of involuntary bailment too."[226]

Therefore, in *Carpenter*, Justice Gorsuch thought it possible that the CSLI did belong to the defendant.[227] The "substantial legal interests" he had through positive law could be enough to create a property right, even though the corporation held the information.[228] Applying Justice Thomas's reasoning, any statutory hook for a property interest in financial records would be limited by the RFPA itself, which allows warrantless requests for financial records. Additionally, Justice Alito specifically noted that many statutes, including the RFPA, grant rights to customers "without creating any property right."[229] The BSA's rules also show that "customers do not create the records; they have no say in whether or for how long the records are stored; and they cannot require the records to be modified or destroyed."[230]

But Justice Gorsuch further noted "there may be some circumstances where positive law cannot be used to defeat" property interests.[231] For example, Congress could not defeat Fourth Amendment interests of individuals by requiring the post office to read every letter.[232] Justice Gorsuch, therefore, would not give Congress's creation of the BSA as much weight in considering the Fourth Amendment interests in our financial transactions.[233] In not only protecting "the specific rights known at the founding," but "their modern analogues too," Justice Gorsuch may be sympathetic to the idea that modern

226 *Id.* at 2270.

227 *Id.* at 2272.

228 *Id.*

229 *Id.* at 2257 n.3 (Alito, J., dissenting).

230 *Id.* at 2229 (Kennedy, J., dissenting).

231 *Id.* at 2270 (Gorsuch, J., dissenting).

232 *Id.*

233 *See* United States v. Miller, 425 U.S. 435, 442–43 (1976).

The lack of any legitimate expectation of privacy concerning the information kept in bank records was assumed by Congress in enacting the Bank Secrecy Act, the expressed purpose of which is to require records to be maintained because they "have a high degree of usefulness in criminal tax, and regulatory investigations and proceedings." (internal citation omitted).

financial transactions contain information that was traditionally within one's papers.[234] If so, he explained that subpoenas could not then be used to evade constitutional protections.[235]

At the moment, there does not appear to be a consensus originalist approach to this issue that would have the necessary votes at the Supreme Court, if the Court were to even take another Fourth Amendment case soon. As such, the methodology does not currently solve the "indeterminacy" in Fourth Amendment jurisprudence.[236] Additionally, an originalist approach that considers traditional property rights and other positive law may simply end up back at *Miller*, proving unhelpful for privacy advocates' policy goals.

2. Mosaic Theory and Judicial Line Drawing

The mosaic theory is the approach most apt to protect privacy interests in financial records. However, its critics contend that the approach would, at best, sacrifice consistency and efficiency for accuracy.

The mosaic theory rejects a categorical approach to searches and instead focuses on the amount and type of information collected.[237] It argues that, at a certain point, a large quantity of data paints a picture that is "qualitatively different" than the same search technique in smaller doses.[238] In this way, it aligns best with the privacy interests at issue in large volumes of financial records. Unlike a search of a house on one occasion, a query of an individual's financial transactions from one day may not reveal copious information. However, that same financial records search could reveal a detailed view of an individual's life if sufficiently expanded, as "[a]ggregations of data create information beyond their

234 *Carpenter*, 138 S. Ct. at 2271 (Gorsuch, J., dissenting).

235 *Id.* Justice Gorsuch notes that even if the Fourth Amendment did not cover this issue, the Fifth Amendment would likely be implicated as a right against self-incrimination was recognized at the time of the founding.

236 Gentithes, *supra* note 204, at 28.

237 *See* Rosenzweig, *supra* note 24.

238 *Id.* "[A] single piece of tile in a mosaic is just a single tile with a single color, that tells you nothing. But if you collect enough tiles, put them in a pattern, and step back, you can see a beautiful Roman mosaic."

individual value."[239] Advertisers and political campaigns already believe this to be true—they target outreach based on it.[240] Applying the mosaic theory to financial records searches could protect against warrantless reviews that are long-term and reveal particularly sensitive information. At the same time, smaller pieces of financial data would still be accessible without a warrant.

While the mosaic approach has not been accepted by many courts, in recent years some have experimented with applying it to new technologies.[241] In *Commonwealth v. Henley* and *Commonwealth v. McCarthy*, the Massachusetts Supreme Court openly embraced the mosaic theory.[242] *McCarthy* concerned cameras on a Cape Cod bridge, which created a comprehensive record of vehicles traveling over it.[243] Police used the cameras to track a drug trafficking suspect's car in real-time, and they also searched the historical data.[244] The court reasoned that widespread use of such technology could certainly constitute a search, but the use of four cameras on two bridges was limited surveillance that did not capture "sufficiently detailed" information to require a warrant.[245] Deploying similar logic, in *Henley* the court rejected the wholesale application of the third-party doctrine to metro cards and decided that an extensive search of those records for location history could constitute a search under the mosaic theory.[246] However, "whether the aggregation of data collected by police implicates the mosaic theory depends on how much data police

239 *Id.*

240 *Id.*

241 It was also used by the D.C. Circuit in the case that became *United States v. Jones*, but the Supreme Court upheld that ruling on a property-based conception of the Fourth Amendment. *See* United States v. Maynard, 615 F.3d 544, 562–63 (D.C. Cir. 2010) (finding that the "whole of one's movements over the course of a month . . . reveals far more than the individual movements it comprises.").

242 Commonwealth v. Henley, 488 Mass. 95 (2021); Commonwealth v. McCarthy, 484 Mass. 493 (2020).

243 *McCarthy*, 484 Mass. at 495.

244 *Id.* at 494–97.

245 *Id.* at 505–09.

246 *Henley*, 488 Mass. at 95.

retrieved and the time period involved," and two days' worth of data was not a search.[247]

In another transit-related case, police used video surveillance to determine which metro card an armed robber was associated with.[248] They then set up an alert for that card's future access to the system, which later notified them of his location and lead to his arrest.[249] The court relied on *Henley* and concluded that the information gathered during this two-day tracking was limited, so the use of the subject's location data was not a search in this case.[250] Meanwhile, the Seventh Circuit walked through an application of the mosaic theory in a drug trafficking case where long-term video surveillance was employed, but it cautioned that it was not accepting the approach yet.[251] The court determined that even if it accepted a mosaic approach, 18 months of video surveillance directed at a subject's home would not be a search because it was targeted and did not reveal the "businesses he frequented, with whom he interacted in public, or whose homes he visited, among many other intimate details of his life."[252]

The mosaic theory is not without its critics, however.[253] The theory would be quite hard to administer, especially as technological changes move faster than judges can "resolve how to regulate them."[254] Law enforcement would lack clear guidance to know when they need to request a warrant. Judges would be left to individually weigh duration, content, platform, and other considerations, with results that may vary greatly between courts. This contrasts with criminal

247 *Id.* at 110, 113–14.

248 Kelly v. United States, 281 A.3d 610, 613 (D.C. Cir. 2022).

249 *Id.*

250 *Id.* at 614–15.

251 United States v. Tuggle, 4 F.4th 505 (7th Cir. 2021), *cert. denied*, 142 S. Ct. 1107 (2022).

252 *Tuggle*, 4 F.4th at 524.

253 Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012).

254 *Id.* at 347.

law's usual prioritization of certainty for police, who "must act before they know whether they have guessed right."[255]

Uncertainty is especially bad in the Fourth Amendment context because of exclusionary and immunity rules—if police err innocently, our legal system generally does not want them liable for significant damages or for defendants to be unjustly freed.[256] Regarding the exclusionary rule, there are questions of whether it would even apply to mosaic theory cases and, if not, whether that would lead to more inconsistencies.[257] Additionally, courts applying "mosaic protection complicate the legislative picture" by effectively preempting action which would regulate new technologies' capability for privacy infringement.[258] If a court imposes "an arbitrary and outside limit," it "closes off further legislative debate on these issues."[259] While certainty is favored, courts in criminal procedure have almost always avoided setting bright-line *durational* limits.[260]

Fourth Amendment jurisprudence should protect values besides consistency, but critics are ultimately correct that the mosaic approach is not a sustainable method of Fourth Amendment jurisprudence. If the theory is effectively "more legislating than interpreting anything in the Constitution," it would make more sense for Congress to take the reins.[261]

255 Stuntz, *supra* note 22, at 867.

256 Gentithes, *supra* note 204, at 37–38.

257 Kerr, *supra* note 253, at 340–42, 346.

258 *Id.* at 351.

259 Carpenter v. U.S., 138 S. Ct. 2206, 2233 (2018) (Kennedy, J., dissenting).

260 *See* Rosenzweig, *supra* note 24.

261 Orin Kerr, *Four Thoughts on the Briefing in Carpenter v. United States*, LAWFARE (Nov. 17, 2017), https://www.lawfaremedia.org/article/four-thoughts-briefing-carpenter-v-united-states [https://perma.cc/2UL3-EPLN]. *See also Carpenter*, 138 S. Ct. at 2233 (Kennedy, J., dissenting).

IV.

A. Congressional Checks on Financial Records Searches

> It would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment. Legislatures, elected by the people, are in a better position than we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future.[262]

While, even after *Carpenter*, courts are very unlikely to overturn *Miller*,[263] the reality of easy government access to increasingly comprehensive financial records should spur Congressional action. Vast databases of financial data are available on nearly all Americans,[264] and the constitutional rationales for that data being unprotected are now doctrinally weak.[265] This Note does not purport to resolve the complicated issue it recognizes. Rather, it discusses the real tradeoffs and merely offers a few potential mitigating policies below.

1. Time Constraints

Currently, subpoenas and other procedures for government access to financial records are not limited in scope by statute.[266] Congress can mimic the intent of a mosaic theory, while providing certainty to law enforcement, through a bright-line durational rule.

---

262 Riley v. California, 573 U.S. 373, 408 (2014) (Alito, J., concurring).

263 *See supra* Section II.B.

264 *See supra* Section III.A.1.

265 *See supra* Section III.A.2.

266 While summonses and subpoenas can be ruled overbroad, defendants often do not have an incentive or opportunity to challenge them, as noted in Section IV.A.2. Additionally, due to the long-term nature of many alleged schemes, financial records requests that span months or years may actually be relevant to an investigation.

Courts have a "general preference to provide clear guidance to law enforcement through categorical rules,"[267] and the rule from *Miller* is undoubtedly clear. However, the Fourth Amendment's other values are now in sharp conflict with that rule. As Professor Kerr notes, "when technology is new or in flux, and its use may have privacy implications far removed from property law, Fourth Amendment rules alone will tend not to provide adequate privacy protections."[268] While financial records are not a wholly new data form, the technologies which feed into them are new and still developing.

Accordingly, Congress should enact a durational limit for requests of financial records under The Right to Financial Privacy Act.[269] Sections that authorize access through consent,[270] administrative subpoena,[271] judicial subpoena,[272] and written request [273] already contain criteria for their applicability. A limit set between two to four weeks would protect against long-term surveillance access, which produces the most serious privacy concerns.[274] "The potential for abuse is particularly acute where" there is access to financial "information without invocation of the judicial process," and current law does not require any invocation of such process.[275] By requiring that "a neutral magistrate" scrutinize every request for probable cause once it goes beyond the durational limit, Congress would restore some balance between the "societal and individual interests" at play here.[276]

267 *Riley*, 573 U.S. at 398.

268 Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 809 (2004).

269 Search warrants under § 3406 would not be impacted.

270 12 U.S.C. § 3404.

271 12 U.S.C. § 3405.

272 12 U.S.C. § 3407.

273 12 U.S.C. § 3408.

274 *See supra* Sections III.A, III.B.

275 Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 79 (1974) (Powell, J., concurring).

276 *Id.*

While some advocate for a total warrant requirement,[277] limited-duration financial records searches are not as invasive. Shorter collection periods limit the privacy consequences of data aggregation, as fewer inferences can be drawn from less encyclopedic information.[278] Surely, even one day of financial transactions could reveal very private information. But even in the pre-digital age, a member of law enforcement may have seen what religion a target belongs to, who their friends are, which political party they support, and various purchases they make just by shadowing them. A time constraint on warrantless review of financial data would allow authorities to build probable cause over a period when privacy concerns are less implicated. More extreme measures, such as a warrant requirement or a much shorter duration requirement, would make prosecuting many white-collar crimes nearly impossible.[279]

This change would not impact the filing of BSA reports. Law enforcement would still receive SARs and CTRs and use them to begin or augment investigations. Probable cause for a wide-ranging search of financial records may exist at that stage. If not, financial data gathered during the circumscribed request period and traditional evidence from confidential informants, anonymous tips, and direct observation would supplement each other. If probable cause for a search of physical properties or email contents is not met at that point, a comprehensive search of a target's financial records should not proceed either. This framework could limit fishing through an individual's financial records in search of a crime. Additionally, this change only protects individuals—the RFPA would still not cover corporations or partnerships of more than five individuals.[280]

277 Michel & Schulp, *supra* note 55.

278 *See* James G. McLeod, *All Things in Aggregation: Reassessing the Fourth Amendment's Third-Party Doctrine and the Fourth Circuit's Approach to Cell Site Location Information in* United States v. Graham, 96 N.C. L. REV. 1203, 1213 (2018); *see also* Kerr, *supra* note 253, at 313.

279 *See supra* Section III.B.

280 12 U.S.C. § 3401(4)-(5).

There are certainly other issues to be worked out with this approach. Would law enforcement be able to string together one-month subpoenas in order to get a comprehensive look at one's records? Or, if they request a subpoena against an individual any time after they already used the one-month look, does the bar still apply years later? What if coordinating authorities get subpoenas that cover different time periods, and then share information? This Note does not purport to craft a perfect solution but merely offers one proposal that attempts to assuage privacy concerns while realizing that "privacy comes at a cost."[281]

2. Suppression as a Remedy under the RFPA

Alternatively, or in conjunction with the above proposal, Congress should add suppression as a remedy for violations of the RFPA and similar statutes. If we are to accept lesser statutory protections in place of full Fourth Amendment coverage for financial data, there need to be real consequences for breaches of such protections.

Suppression of evidence is not a remedy for violations of the RFPA.[282] The statute provides for monetary damages,[283] injunctive relief,[284] and, in cases of willful or intentional violations, disciplinary action.[285] Since exclusion is not explicitly included, when defendants have tried to challenge the use of seized financial records under the RFPA, courts have plainly held that any statutory violation "is insufficient to justify the

[281] Riley v. California, 573 U.S. 373, 401 (2014).

[282] United States v. Kington, 801 F.2d 733, 737 (5th Cir. 1986); United States v. Davis, 953 F.2d 1482, 1496 (10th Cir. 1992); *see also* U.S. Dep't of Just., Crim. Res. Manual § 440.

[283] 12 U.S.C. § 3417(a). Plaintiffs are entitled to $100, plus actual damages.

[284] 12 U.S.C. § 3418. Note that injunctive relief consists of an order that the government, for example, provide notice the *next time* it requests a *specific defendant's* financial records. Botero-Zea v. United States, 915 F. Supp. 614, 620 (S.D.N.Y. 1996).

[285] 12 U.S.C. § 3417(b). There appear to be no reported cases where a party was disciplined under this provision.

exclusion of any evidence."[286] Similarly, the Patriot Act's financial records request provisions provide only damages as a remedy for violations.[287]

Since exclusion of evidence is not a remedy under the RFPA, a defendant must show that the government's request "violated the Fourth Amendment to warrant suppression of evidence."[288] But according to current case law,[289] searches of financial records never violate the Fourth Amendment. Therefore, evidence obtained illegally under the RFPA may still be used at a criminal trial or regulatory hearing. As a result, defendants have little incentive to litigate the scope of their rights under the RFPA.[290]

To summarize, an administrative subpoena or written request for financial records can be issued under a standard of "relevant" to an investigation.[291] Such subpoena or request does not require sign-off by a neutral magistrate, and notice can be delayed to the target of the investigation.[292] Then, even if a defendant successfully challenges any deviation from those already thin procedural protections, the evidence may still be used against them.[293] While subjects have a right to

286 United States v. Thompson, 936 F.2d 1249, 1251 (11th Cir. 1991).

287 Brantley v. Fla. Att'y Gen., No. 19-13214, 2021 WL 3077017, at *7 (11th Cir. July 21, 2021), *cert. denied sub nom.* Brantley v. Moody, 142 S. Ct. 2723, 2723 (2022), *reh'g denied*, 143 S. Ct. 57, 57 (2022). This was a child exploitation case where agents used the Patriot Act, likely Section 314, to discover the defendant used an American Express account, and then invoked it again to request the defendant's financial information from American Express. This Note's proposed changes would not result in suppression in this case, as a judge viewing the facts could determine that exigent circumstances necessitated prompt discovery of the defendant's hotel rooms. 12 U.S.C. § 3417(c), which provides for a good-faith defense to RFPA violations, would also remain.

288 United States v. Cray, 450 F. App'x 923, 931 (11th Cir. 2012).

289 *See supra* Section II.B.

290 *See supra* notes 282–85.

291 12 U.S.C. §§ 3405, 3408. Investigators only need a reason to believe the records are relevant, which would "permit access where the only information available is an anonymous tip." U.S. Dep't of Just., Crim. Res. Manual § 413.

292 12 U.S.C. § 3409.

293 *See supra* note 282.

challenge a subpoena if notified,[294] when notice is not given before the subpoena is completed, the ability to quash it is moot.[295] So, if the delay provision is invoked, the subject loses any ability to stop their financial records from being turned over and used by the government. Congress should close this loophole by adding suppression of evidence as a remedy under 12 U.S.C. § 3417.[296]

3. Reforming Mandatory Reporting

The heart of the BSA is the system of mandatory retention and reporting by financial institutions. While reforming the reporting of CTRs and SARs is a complicated issue that is much too large for detailed discussion within this student Note, addressing it would reduce the privacy concerns discussed here.

Some advocates have questioned whether CTRs are even necessary because truly suspicious information should be covered by the SAR process.[297] Other advocates urge that SAR reporting itself be discontinued.[298] The government receives many more SARs than are needed; institutions are incentivized to over-file, and in the process, they effectively accuse their customers of wrongdoing to the government.[299] Mandatory reporting has become much more extensive because reports have not been adjusted for inflation, regulators' aggressive stance has encouraged defensive filings, and laws have

294 12 U.S.C. § 3410. They must move to challenge within 10 days from receipt of notice or 14 days from its mailing date. 12 U.S.C. § 3405(3).

295 *See* Botero-Zea v. United States, 915 F. Supp. 614, 614 (S.D.N.Y. 1996).

296 The RFPA only applies to federal investigations. As such, the proposals in this Section and Section IV.A.1 are inapplicable at the state and local level, which is concerning because of the larger volume of investigations and higher likelihood of politicization there. However, Congress may be able to preempt state law on this issue in regard to interstate financial institutions.

297 Michel & Burton, *supra* note 40.

298 Michel & Schulp, *supra* note 55.

299 *See supra* note 44.

brought more businesses under the umbrella of "financial institution."[300]

However, law enforcement does use SARs to hold bad actors accountable.[301] Scrapping the whole system, even if the evidence is unclear as to its effectiveness, would not be prudent. Reforming the SAR process to discourage defensive filing is a complicated issue that would likely necessitate leniency from regulators. If it can be accomplished, it would limit the regulatory burden on financial institutions, reduce innocent transactions reported to the government, and better focus law enforcement's resources.

V. CONCLUSION

Since the BSA was enacted, successive laws have marched forward in one direction, adding new reports, covered institutions, and other requirements. At the same time, changes in technology and consumer habits have greatly increased the proportion of transactions that are recorded and retained. The resulting financial surveillance system contains comprehensive and intimate information about nearly every American.

While a complete warrant requirement to view any financial data would end many legitimate investigations before they begin, a measured approach would allow law enforcement to build support for a finding of probable cause. Access to a subject's comprehensive financial information, spanning years across all platforms, should be restricted until a standard higher than "relevant" is met and approved by a judge. Breaches of these lesser statutory protections should still come with the exclusionary rules that accompany Fourth Amendment violations.

Congress can balance the competing concerns in this area and, for the first time in decades, turn back the dial on financial surveillance.[302] In a cashless society where massive troves

300 *See supra* Section II.A.

301 *See supra* Section III.B.

302 While a Central Bank Digital Currency is rightly feared for its potential surveillance capabilities, a legislative push to implement one may be a unique opportunity for privacy advocates to leverage their votes to raise

of financial data can reveal our most intimate matters, we should reconsider the procedures for access and use by government agents. To wait to do so risks keeping the door open "to a vast and unlimited range of very real abuses of police power."[303]

the standards for law enforcement access of financial data. Substantial protections on existing financial records, which already enable troubling surveillance possibilities, may be unlikely to be independently imposed.

[303] United States v. Miller, 425 U.S. 435, 451 (1976) (Brennan, J., dissenting) (quoting Burrows v. Sup. Ct., 13 Cal. 3d 238 (1974)).