Seattle Journal of Technology, Environmental & Innovation Law

Volume 10 | Issue 1 Article 6

5-6-2020

Cryptocurrencies' Revolt Against the BSA: Why the Supreme Court Should Hold that the Bank Secrecy Act Violates the Fourth Amendment

Jeremy Ciarabellini
jciarabellini@gmail.com

Cryptocurrencies' Revolt Against the BSA: Why the Supreme Court Should Hold that the Bank Secrecy Act Violates the Fourth Amendment

*Jeremy Ciarabellini**

"It may be that it is the obnoxious thing in the mildest and least repulsive form; but illegitimate and unconstitutional practices get their footing first in that way, namely, by silent approaches and slight deviations from legal modes of procedure. This can only be obviated by adhering to the rule that constitutional provisions for the security of person and property should be liberally construed."[1]

"In the new economy, it is as important to have access to a basic bank account and financial services as it is to have access to electricity, running water, and a telephone.[2]

I. INTRODUCTION

The Bank Secrecy Act (BSA) creates a Hobson's choice: one must either struggle to function in modern society without a bank account or submit to financial surveillance by the government. Both

* Jeremy Ciarabellini is a graduate of Seattle University School of Law where he earned both a Juris Doctor (2015) and an L.L.M in Innovation and Technology Law (2018). He specializes in electric transmission law and finds additional academic interests in privacy law and brain–computer interface law. Jeremy thanks his family, professors, and SJTEIL for their depthless support as he wrote this article.

[1] Boyd v. United States, 116 U.S. 616, 635 (1886).

[2] Michael A. Stegman, *Banking the Unbanked: Untapped Market Opportunities for North Carolina's Financial Institutions*, 5 N.C. BANKING INST. 23 (2001) (citing Lawrence H. Summers, *Helping Americans To Save More*, Remarks at the Choose to Save Forum (April 2, 2000)).

choices result in drastic consequences. The following two stories illustrate these consequences.

A. Story One

Ariel Schwartz tried to live without a bank account for a single day.[3] As part of a simulation to determine what it is like to function without a bank account, Ariel had two hours to purchase and load a prepaid card, cash both a payroll and a personal check, send those checks, pick up a money transfer, and finally pay rent.[4] Ariel described this simulation as an "exhausting experience."[5]

The first payday loan and cash advance business Ariel tried to use refused to cash her checks. The business turned her down because it could not readily verify that the checks were legitimate. A second business was willing to cash the checks but for a "significantly higher fee;" however, that same business refused to let her pay $10 of the rent bill for "unspecified reasons."[6]

Ariel then went to Western Union to send and receive her money transfers. There, she could not receive funds, being told by Western Union that part of its system was down.[7] However, while Western Union did allow Ariel to send a money transfer of $30, it concurrently imposed a $5 fee.[8] In the two-hour deadline, these were all of the tasks that Ariel was able to complete.[9]

B. Story Two

Ken Quran immigrated to America to provide for his family.[10] Over the next seventeen years, Ken owned and worked in his convenience store.[11] Despite working seventy hours per week, Ken and his family had time to become American citizens.[12]

During his seventeen-year career, Ken saved $150,000 for his retirement, "[b]ut his American dream [became] a legal

---

[3] Ariel Schwartz, *What It's Like to Live Without A Bank Account For A Day*, FAST CO. (Dec. 15, 2014), https://www.fastcompany.com/3039201/what-its-like-to-live-without-a-bank-account-for-a-day [https://perma.cc/XYS8-JT5G].
[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] Nick Sibilla, *How An Obscure Banking Law Let The IRS Seize Bank Accounts From Innocent Americans*, FORBES (July 17, 2015), https://www.forbes.com/sites/instituteforjustice/2015/07/17/how-an-obscure-banking-law-let-the-irs-seize-bank-accounts-from-innocent-americans/#300b06f95361 [https://perma.cc/Z2MS-YM7Y].
[11] *Id.*
[12] *Id.*

nightmare."[13] Ken's bank reported him to the government because it believed that he was violating the anti-structuring provision of the Bank Secrecy Act (BSA) because of how Ken was withdrawing cash from his account.[14] Ken did not know that his actions could be seen as violations of the BSA. Ken also did not know that he was reported to the government until the day government agents stormed his store, prevented customers from entering, searched the area with a dog, and interrogated him.[15] According to Ken, the government agents coerced him to sign a civil forfeiture form, and the government agents then seized all of his cash.[16] The government never charged Ken with a crime.[17]

C. The Bank Secrecy Act Created This Reality

The intersection of these two stories begs the question: Does the Fourth Amendment protect United States citizens' banking information against warrantless searches and seizures by the government? "No," declared Congress by enacting the BSA and the Supreme Court in holding that the BSA is constitutional.

According to the Office of the Comptroller of the Currency, the purpose of the BSA is to combat money laundering, terrorism, and other criminal activities.[18] Undoubtedly, this aim is legitimate. However, in the pursuit of protecting its citizens under the Bank Secrecy Act, Congress gave law enforcement the power to search citizens' private bank records without obtaining a warrant. After the BSA's enactment, the Supreme Court upheld these warrantless searches as constitutional under the Fourth Amendment.

The Court came to that holding in *United States v. Miller*, where it applied the "third-party doctrine."[19] Broadly, this doctrine holds that information voluntarily disclosed to a third party is not subject to Fourth Amendment protections.[20] Applying the third-party doctrine, the Court reasoned that the Fourth Amendment does not demand an authorized search warrant before the government can search an individual's bank records because there is no constitutionally protected privacy interest in such records. By voluntarily providing their financial information to a bank, individuals abandon their privacy interests in that information,

---

[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] Bank Secrecy Act (BSA), OFFICE OF THE COMPTROLLER OF THE CURRENCY, https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html [https://perma.cc/VMQ5-V2K3].
[19] *See* United States v. Miller, 425 U.S. 435 (1976).
[20] *Id.* at 443.

accepting the risk that the bank may not keep their information confidential.

The Court was wrong. It inappropriately applied the third-party doctrine in its original form—as an outgrowth of a previously overruled Fourth Amendment jurisprudence. This form of the third-party doctrine excludes all voluntarily disclosed information from Fourth Amendment protections. Instead, the Supreme Court should have examined the third-party doctrine though the lens of the *Katz* test. The *Katz* test provides Fourth Amendment protection where society would consider it reasonable.[21] This test is more flexible and would have allowed the Court to strike down the BSA as unconstitutional.

The Supreme Court's mistake in *Miller* should render that opinion with little precedential value and invite the Court to re-examine the constitutionality of the BSA. Applying the *Katz* test to modern financial practices strongly suggests that the BSA is anathema to the Fourth Amendment because modern living requires the use of a bank account for active participation in society. Thus, the assertion that an individual's choice to have a bank account is wholly voluntary can hardly be argued. Further, the emergence of cryptocurrencies provides evidence that society expects financial privacy, as financial privacy and autonomy are core values in cryptocurrency theory. For these reasons, the Court should rule that the BSA's allowance of warrantless disclosure of financial information to the government violates the Fourth Amendment protection against warrantless searches and seizures.

This article proceeds in analyzing the constitutionality of the BSA as to banks in light of the emergence of cryptocurrencies. For this analysis, this article will specifically apply the *Katz* test to the banking industry. However, as stated in Part II.B.1, the BSA's mandatory reporting provisions apply to a wide range of businesses, consequently providing a broad impact on citizens' privacy expectations against their government far beyond banks. The broader societal impact of the BSA thus deserves attention, but it is beyond the scope of the present article.

Within the stated scope, this article proceeds as follows: Section II details the creation of the BSA and explains its reporting requirements as specific to banks. This section intends to show that the BSA is a strict criminal statute that leaves banks with no choice but to over-report their customers' transactions to the government. Section III transitions to Fourth Amendment principles. Arguing that the Supreme Court in *Miller* misconceptualized the third-party doctrine Section III begins with a careful look at the line of cases developing the third-party doctrine. It then shows how the Court failed to recognize that the later emergence of the *Katz* test undercut

[21] Katz v. United States, 389 U.S. 347, 361 (1967).

the reasoning of the third-party doctrine. Section III concludes by describing and critiquing the *Miller* opinion itself. Section IV looks at the BSA in the context of the modern era. It argues that society would now recognize as reasonable an individual's privacy expectation in banking information—an indicator of constitutional protection under the *Katz* test. Arguing that the BSA violates the Fourth Amendment, the final section looks to bank accounts as involuntary realities of society and cryptocurrencies as a refute to the BSA's constitutionality.

II. THE BANK SECRECY ACT: HISTORY, FORM, & FUNCTION

Congress enacted the BSA "in 1970 following extensive hearings concerning the unavailability of foreign and domestic bank records of customers thought to be engaged in activities entailing criminal or civil liability."[22] Congress intended the BSA to address two major areas related to law enforcement-assisted banking: (1) financial recordkeeping by domestic banks and (2) United States citizens' use of foreign banks to hide their money.[23]

Specific to laws and regulations aimed at domestic banks, the BSA enabled a wholesale financial surveillance regime. Because banks must report all transactions above $5,000 and any transaction that looks "suspicious" to the government, "banks are paying attention to even the smallest of . . . transactions."[24] Indeed, "anti-money laundering" software allows banks to automatically monitor approximately 50 million financial transactions per day looking for suspicious or unordinary activity.[25] While Congress's intent in passing the BSA may have been altruistic, the specific provisions of the BSA fail to follow a core constitutional principle: If criminal activity "is to be fought, those who fight it must respect the rights of individuals, whether or not those individuals are suspected of having committed a crime."[26]

---

[22] California Bankers Ass'n v. Shultz, 416 U.S. 21, 26 (1974).
[23] H.R. Rep. 91-975 (1970).
[24] John Borland, *The Technology That Toppled Eliot Spitzer*, MIT TECHNOLOGY REVIEW (Mar. 19, 2008), https://www.technologyreview.com/s/409766/the-technology-that-toppled-eliot-spitzer/ [https://perma.cc/26XP-JCMS].
[25] *Id.*
[26] Florida v. Bostick, 501 U.S. 429, 439 (1991).

A. Historical Development

The origins of the BSA are unique, beginning with Switzerland's defiance against Adolf Hitler.[27] During World War II, Hitler sought to seize assets that German Jews deposited into Swiss bank accounts for safekeeping.[28] To prevent Hitler's plundering of those assets and for the protection of "legitimate business secrets," Switzerland passed a series of statutes criminalizing the release of depositors' identities.[29]

While the Swiss banking system attempted to overcome Hitler's evil intentions, it quickly became a place where Nazi leaders themselves would deposit valuables stolen during their conquests.[30] Subsequently in the 1960s, the United States became deeply concerned that its citizens were using the same system for illegal purposes.[31] As the "jet age" facilitated increased travel, the Swiss banking system became available to more people.[32] Some of these individuals took advantage of Swiss banks' strict secrecy laws to avoid culpability for several crimes, from illegal securities participation to organized crime's laundering of money "skimmed" from Las Vegas casinos.[33]

In 1968, Congress began looking into these issues in earnest.[34] Congress invited numerous government agencies to speak at hearings documenting the relationship between crime and secrecy havens. Multiple law enforcement agencies testified to Congress that the United States lacked the necessary legal framework to identify and prosecute individuals involved in financial crimes linked to secret bank accounts.[35] The combination of time-consuming foreign legal processes and secrecy laws often prevented law enforcement from obtaining admissible evidence of financial crimes.[36] Domestically, the government estimated that the use of secret bank accounts cost the government loss of tax revenues in the

---

[27] *Legal and Economic Impact of Foreign Banking Procedures on the United States: Hearings Before the House Comm. on Banking and Currency*, 90th Cong., 2nd Sess. 6 (1968), https://babel.hathitrust.org/cgi/pt?id=uc1.$b654959;view=1up;seq=9;size=150 [https://perma.cc/4RX3-K5YK] [hereinafter *Legal and Economic Impact*].

[28] *Id.*; *see also* James E. Eldridge, *The Bank Secrecy Act; Privacy, Comity, and the Politics of Contraband*, 11 N.C. J. INT'L L. & COM. REG. 667, 668 (1986).

[29] *Legal and Economic Impact*, *supra* note 27.

[30] *Swiss banks and Nazi gold*, THE ECONOMIST (July 2, 1998), http://www.economist.com/node/139987 [https://perma.cc/LMR4-565C].

[31] *Id.*

[32] *Id.* at 9-10.

[33] *Id.*

[34] James E. Eldridge, *The Bank Secrecy Act; Privacy, Comity, and the Politics of Contraband*, 11 N.C. J. INT'L L. & COM. REG. 667, 669 (1986).

[35] *Id.* at 669-72.

[36] California Bankers Ass'n v. Shultz, 416 U.S. 21, 29 (1974).

hundreds of millions of dollars.[37] A former U.S. Attorney described the use of secret bank accounts "as the largest single tax loophole permitted by American law."[38]

As Congress intended to close criminals' use of foreign bank accounts, it also believed that it needed to increase law enforcement's access to domestic bank accounts to investigate criminal activity. As the Internal Revenue Service (IRS) puts it, Congress passed the BSA "in response to increasing reports of people bringing bags full of currency of doubtful origin" for deposit into banks."[39] In response to these problems, Congress enacted the BSA.[40]

Yet, Congress did not pass the BSA in a vacuum; it came in the greater context of President Richard Nixon's war on drugs.[41] In 1970, President Nixon signed a suite of additional laws designed to provide law enforcement with multiple avenues of criminal prosecution of drug crimes,[42] including the Controlled Substances Act (CSA), the Organized Crime Control Act (OCCA), and the Racketeer Influenced and Corrupt Organizations Act (RICO).[43] The CSA criminalized actions such as drug manufacturing and distribution.[44] Nevertheless, when a law enforcement agency fails to gather sufficient evidence for prosecution under the CSA, that agency may still have sufficient evidence to prosecute under OCCA, RICO, or the BSA. Both OCCA and RICO target criminal activity, while the BSA criminalized entry of ill-gotten money into the banking system.[45]

Therefore, the BSA emerged as a tool to combat criminal activity. The specific provisions of the BSA cast a wide net to achieve its goals. In its original form, the Supreme Court recognized that there was "no denying the impressive sweep of the authority conferred upon the Secretary [of the Treasury] by the [BSA]."[46]

---

[37] *Id.* at 28.
[38] *Id.* at 29.
[39] *4.26.5 Bank Secrecy Act History and Law*, INTERNAL REVENUE SERVICE, INTERNAL REVENUE MANUALS (2012), https://www.irs.gov/irm/part4/irm_04-026-005#idm139674414931904 [https://perma.cc/R7HH-8QB4].
[40] Eldridge, *supra* note 34.
[41] Steven Wisotsky, *Exposing The War On Cocaine: The Futility And Destructiveness of Prohibition*, 1983 WIS. L. REV. 1305, 1306 (1983).
[42] *Id.* at 1353-54.
[43] *Id.*
[44] *See, e.g.*, 21 U.S.C. §§ 841(a)(1), 802(6), 812(c).
[45] Patrick A. Tighe, *Underbanked: Cooperative Banking as a Potential Solution To The Marijuana-Banking Problem*, 114 MICH. L. REV. 803, 808-10 (2016).
[46] California Bankers Ass'n v. Shultz, 416 U.S. 21, 30 (1974).

B. Rules

The current version of the BSA is codified at 31 U.S.C. §§ 5311-5332. Throughout its existence, Congress has expanded the scope of the BSA. As currently enacted, the purpose of the BSA is "to require certain reports or records where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism."[47] The law enforcement arm of the BSA says that the act

> requires U.S. financial institutions to assist U.S. government agencies to detect and prevent money laundering. Specifically, the act requires financial institutions to keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding $10,000 (daily aggregate amount), and to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities.[48]

To avoid these penalties, a broad range of institutions must be prepared to follow precise rules.

In general, "financial institutions" must maintain a variety of records, including their customers' identities, copies of certain checks, and reports on certain domestic and foreign currency transactions, all as proscribed by the Secretary of the Treasury.[49] Additionally, the BSA considers a broad array of businesses as "financial institutions." Organizations designated as "financial institutions" include banks, private bankers, credit unions, brokers or dealers in securities or commodities, currency exchanges, operators of credit card systems, insurance companies, pawnbrokers, loan and finance companies, travel agencies, car dealerships, certain casinos, and more.[50] To accomplish the BSA's domestic law enforcement goals, these financial institutions must follow detailed requirements under the threat of severe punishment for noncompliance.

---

[47] 31 U.S.C. § 5311. The Secretary of the Treasury has also determined that the reports required under the BSA "have a high degree of usefulness in criminal, tax, [and] regulatory investigations or proceedings." 31 C.F.R. § 1010.301.

[48] *FinCEN's Mandate from Congress*, U.S. DEP'T OF TREAS., https://www.fincen.gov/resources/fincens-mandate-congress [https://perma.cc/VBW7-2X54].

[49] 31 U.S.C. §§ 5313(a), 5314(a); California Bankers Ass'n v. Shultz, 416 U.S. 21, 30 (1974).

[50] 31 U.S.C. § 5312(a)(2) (2004).

1. Domestic Bank Reporting Requirements

Banks carry a particularly heavy regulatory burden under the BSA. To begin, they must file a report for every deposit, withdraw, exchange, payment, transfer, or other type of transaction involving more than $10,000.[51] These reports must "verify and record the name and address of the individual presenting a transaction, as well as record the identity, account number, and the social security or taxpayer-identification number, if any, of any person or entity on whose behalf such transaction is to be effected."[52]

Moreover, the BSA limits distributing specific monetary instruments in amounts of over $3,000,[53] whereby banks may not "issue or sell a bank check, cashier's check, traveler's check, or money order to any individual in connection with a transaction or group of such contemporaneous transactions involving United States coins or currency (or such other monetary instruments as the Secretary may prescribe) in amounts or denominations of $3,000 or more . . . ."[54] The only exceptions to this rule require banks to verify the identity of the purchaser and keep records of the transaction, which they must provide to the federal government upon request of the Secretary of the Treasury.[55]

Whenever any of these conditions are met, banks must send their reports directly to the Secretary of the Treasury.[56] While these provisions of the BSA may seem mechanical in their nature of action and response, the BSA also requires banks to actively monitor for suspicious activity—a much vaguer and, ultimately, far-reaching mandate.

2. Suspicious Activity Reporting Requirements

In addition to the bright-line reporting requirements mentioned above, banks must also submit Suspicious Activity Reports (SARs) under certain circumstances.[57] The BSA empowers the Secretary of the Treasury to decide the parameters of this rule, stating that "The Secretary may require any financial institution, and any director, officer, employee, or agent of any financial institution,

[51] 31 C.F.R. § 1010.311. For purposes of reaching the $10,000 threshold, the Secretary of the Treasury aggregates all transactions made during a single business day by or on behalf of any person. 31 C.F.R. § 1010.313.
[52] 31 C.F.R. § 1010.312 (2011).
[53] 31 U.S.C. § 5325 (1988).
[54] 31 U.S.C. § 5325(a) (1988).
[55] 31 U.S.C. § 5325(a)-(b) (1988).
[56] 31 U.S.C. § 5312(c)(1)(C) (2004).
[57] 31 U.S.C. § 5318(g)(1) (2014).

to report any suspicious transaction relevant to a possible violation of law or regulation."[58]

For banks, the BSA delineates two types of SARs: required SARs and voluntary SARs. Required SARs can be broken into two categories: illegal-transaction SARs and unexplainable-activity SARs. Banks are required to file illegal-transaction SARs anytime they know, suspect, or have reason to suspect that a transaction of $5,000 or more involves money "derived from illegal activity or are intended to hide funds from illegal activities . . . as part of a plan to violate or avoid any Federal law or regulation…" or other reporting requirement of the BSA.[59] For unexplainable-activity SARs, a bank must file a report on any transaction that the bank feels "has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction."[60]

On the other hand, banks have quite a bit of discretion for voluntary SARs. For any activity that does not require reporting, a bank may still file a SAR on a transaction if "it believes [the information would be] relevant to the possible violation of any" federal mandate.[61]

For both types of SARs, the reporting bank must file the SAR with the Financial Crimes Enforcement Network (FinCEN) no later than thirty calendar days after discovering the facts that constitute the basis of the SAR and must make the supporting documentation available for inspection at the federal government's request.[62] The bank must maintain the supporting documentation for five years.[63] Moreover, SARs are strictly confidential, and a bank many not disclose its existence to the individual to whom the transaction pertains.[64]

3. Incentives to Report

The BSA imposes significant legal consequences on banks for noncompliance, and also conversely provides civil immunity on compliant banks as well as a potential reward for reporting. To avoid violations in the first instance, the BSA requires that banks

---

[58] *Id.*
[59] 31 C.F.R. § 1020.320(a)(2)(i)-(ii) (2011).
[60] 31 C.F.R. § 1020.320(a)(2)(iii) (2011).
[61] 31 C.F.R. § 1020.320(a)(1) (2011).
[62] 31 C.F.R. § 1020.320(b)(3), (d) (2011).
[63] 31 C.F.R. § 1020.320(b)(1), (d) (2011).
[64] 31 U.S.C. § 5318(g)(2) (2014); *see also* 31 C.F.R. § 1020.320(e) (2011) (regulation specific to banks).

"maintain appropriate procedures to ensure compliance with [the BSA] . . . to guard against money laundering."[65]

If a BSA violation does occur, the potential civil fines are quite large. For example, a bank that willfully violates a reporting requirement of a domestic transaction can be held liable for a civil penalty of at least $25,000 and up to $100,000 per violation per day.[66] If BSA violations are the result of negligence rather than willfulness, the Secretary of the Treasury has the discretion to impose no more than $500 on the bank. If that negligent action is part of a pattern of negligent activity, the maximum fine the Secretary of the Treasury can impose is increased to $50,000.[67]

In addition to civil liabilities, BSA violations can give rise to criminal culpability.[68] A single violation of a domestic transaction reporting requirement of the BSA by an individual carries a fine of up to $250,000, up to five years of imprisonment, or both.[69] If that individual's violation is part of additional illegal activity or a pattern of illegal activity that involves more than $100,000 in one year, the mandatory sanctions are increased to a fine of up to $500,000, up to 10 years of imprisonment, or both.[70]

On the other hand, the BSA does provide a degree of compliance immunity and incentives to banks and individuals. First, banks may not be held civilly liable by customers for revealing their banking information in SARs.[71] Second, if an individual employee of a bank reports to the government that the bank, or any of its employees, is "possibly" in violation of the BSA, the bank is prohibited from retaliating against the whistleblowing employee.[72] Finally, any individual that provides original information leading to a recovery of a criminal fine, civil penalty, or forfeiture, for a violation of the BSA in excess of $50,000 is eligible for an award of either 25% of the money collected by the government or $150,000, whichever is less.[73]

In sum, the BSA requires banks to closely monitor their customers, resulting in banks filing of a considerable number of SARs over fear of governmental enforcement actions. The banks must file these reports to FinCEN, which in turn uses the reports for criminal investigations.

---

[65] 31 U.S.C. § 5318(a)(2) (2014).
[66] 31 U.S.C. § 5321(a)(1) (2004).
[67] 31 U.S.C. § 5321(a)(6)(B) (2004).
[68] 31 U.S.C. § 5321(d) (2004) (emphasis added).
[69] 31 U.S.C. § 5322(a) (2001).
[70] 31 U.S.C. § 5322(b) (2001).
[71] 31 U.S.C. § 5318(g)(3)(A) (2014).
[72] 31 U.S.C. § 5328(a) (2001).
[73] 31 U.S.C. § 5323(a)-(b) (1984); 31 C.F.R. § 1010.930(a)-(b) (2011).

C. FinCEN and BSA Effectiveness

As required under regulation, banks send their SARs to FinCEN. Established in 1990, FinCEN operates under the Assistant Secretary for Enforcement of the Department of the Treasury.[74] The stated mission of FinCEN "is to provide a governmentwide, multisource intelligence and analytical network in support of the detection, investigation, and prosecution of domestic and international money laundering and other financial crimes by Federal, State, local, and foreign law enforcement agencies."[75] To achieve its mission, FinCEN is tasked with "analyzing and disseminating" all the data it collects to federal and state law enforcement agencies to "[i]dentify possible criminal targets" and to support ongoing criminal financial investigations.[76] FinCEN's reports to law enforcement agencies include instances of banks' non-compliance with the BSA.[77]

Statistics from recent years suggest that FinCEN contributes to high rates of successful prosecutions under the BSA but investigates a relatively low percentage of SARs. According to the IRS, from 2009 to 2016, the total number of BSA anti-money laundering investigations, indictments, and successful convictions has remained relatively constant. For example, in the fiscal year 2009, FinCEN initiated 624 investigations, which led to 289 indictments and a conviction rate of 75.5%.[78] In 2011, there were 795 money laundering investigations initiated, resulting in 462 indictments and a 75.3% conviction rate.[79] The most recent data set available is from 2016, showing 504 investigations, 399 indictments, and a conviction rate of 74.8%.[80] These statistics include "investigations from Suspicious Activity Report (SAR) Review Teams, violations of BSA filing requirements, and all" other related requirements."[81]

However, the total number of SARs reported compared to the total number of investigations and indictments suggests a massive problem of overreporting. In 2009, FinCEN received

---

[74] Organization, Functions, and Authority Delegations, 55 Fed. Reg. 18, 433-03, § 1 (1990).
[75] *Id.* at § 2.
[76] *Id.* at § 4(d)(1)-(2).
[77] *Id.* at § 4(d)(3).
[78] *Statistical Data – Money Laundering and Bank Secrecy Act (BSA)*, INTERNAL REVENUE SERV., https://www.irs.gov/compliance/criminal-investigation/statistical-data-money-laundering-bank-secrecy-act-bsa [https://perma.cc/9P8J-V3TL].
[79] *Id.*
[80] *Id.*
[81] *Id.*

720,309 SARs from depository institutions alone.[82] That number increased to 798,688 SARs in 2011[83] and 958,537 in 2016.[84]

One cannot deny that society benefits from the Federal Government's pursuit of eliminating money-laundering, especially in the context of drugs, organized crime, and terrorism. However, the expansiveness of the BSA's directives and resulting investigations raises significant Fourth Amendment issues. Justice William Brandeis stated:

> Experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent. [Individuals] born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by [individuals] of zeal, well-meaning but without understanding.[85]

Yet, the Supreme Court failed to evaluate the BSA under the proper Fourth Amendment standards. Thus, the Supreme Court allowed Congress to encroach upon its citizens' constitutional rights.

III. THE BANK SECRECY ACT AND THE FOURTH AMENDMENT

In *United States v. Miller,* the Supreme Court held that the BSA's requirement that banks report suspicious customer activity did not violate the Fourth Amendment's guarantee against unreasonable searches and seizures.[86] In its conclusion, the Supreme Court relied on the third-party doctrine, stating that individuals do not retain privacy interests in information shared with banks.[87] Based on the underlying policy of the third-party doctrine and then-recent developments in Fourth Amendment conceptions, the Supreme Court erred in its ruling.

More precisely, the Supreme Court developed the third-party doctrine in an era when Fourth Amendment protections were

---

[82] FINANCIAL CRIMES ENFORCEMENT NETWORK, THE SAR ACTIVITY REVIEW – BY THE NUMBERS, FINCEN.GOV, https://www.fincen.gov/sites/default/files/sar_report/sar_by_numb_18.pdf [https://perma.cc/GCH5-RRT6].
[83] *Id.*
[84] FINANCIAL CRIMES ENFORCEMENT NETWORK, SAR STATS – ISSUE 3 – DEPOSITORY INSTITUTIONS, SAR STATS TECHNICAL BULLETIN, FINCEN.GOV (Mar. 2017), https://www.fincen.gov/sites/default/files/sar_report/2017-03-09/SAR%20Stats%203.pdf [https://perma.cc/4AUK-LL2L].
[85] Olmstead v. United States, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting).
[86] *See* U.S. v. Miller, 425 U.S. 435 (1976).
[87] *Id.*

based on trespass principles.[88] However, shortly before *Miller*, the Supreme Court held that Fourth Amendment rights protected "people, not places."[89] Thus displacing the traditional trespass-based analysis, the Supreme Court looked, in part, at whether society would consider a particular search reasonable in the absence of a warrant. Nevertheless, the Supreme Court did not analyze *Miller* in this new fashion and instead reverted to the traditional trespass-based analysis of the Fourth Amendment under the guise of the third-party doctrine.[90]

A. Fourth Amendment Protection Against Unreasonable Searches and Seizures

The United States Constitution does not have a general provision protecting privacy. Instead, it grants only a few, specific privacy rights. For example, the Fourth Amendment prevents the government from unreasonably peering into the lives of its citizens:

> 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.[91]

Fourth Amendment protections are currently analyzed under the *Katz* test.[92] Broadly, the *Katz* test states that a court must analyze and determine whether the actions taken by the government are considered a search or seizure under the Fourth Amendment.[93] If the court does not find a reasonable "objective" privacy interest implicated by the government's action, the Fourth Amendment is not implicated.[94] Similarly, the Fourth Amendment is not implicated if the court cannot find that the defendant had a "subject" privacy interest invaded by the government's action.[95]

Then, if the Fourth Amendment applies, the court will determine whether the search or seizure was "reasonable."[96] If the search was for law enforcement purposes, "reasonableness"

---

[88] *See infra* Part III.A.1.
[89] Katz v. United States, 389 U.S. 347, 351 (1967).
[90] *See* Miller, 425 U.S. 435.
[91] U.S. CONST. amend. IV.
[92] *See* Katz, 389 U.S. at 361 (Harlan, J., concurring).
[93] *See id.*
[94] *See id.*
[95] *See id.*
[96] *See, e.g.*, Riley v. California, 573 U.S. 373, 381 (2014).

generally requires the government to have first obtained a warrant authorized by a neutral magistrate that is supported by probable cause.[97] In the absence of a warrant, the search is only reasonable if it "falls within a specific exception to the warrant requirement" and is supported by probable cause.[98]

However, the *Katz* test is relatively new. Until the 1960s, the court used a "trespass" test: if the government was not physically trespassing in a private space, it was not violating the Fourth Amendment.[99] The third-party doctrine developed from this view of the Fourth Amendment, and its strict application became a powerful tool for law enforcement. With the emergence of the *Katz* test, on the other hand, the justifications supporting the strict application of the third-party doctrine have been severely diminished.

Two years after it adopted the *Katz* test, the Supreme Court had the opportunity to apply it to the BSA in *United States v. Miller*.[100] But, instead of providing a robust analysis of the BSA under the *Katz* test, the Supreme Court defaulted to the anachronistic conceptions of the third-party doctrine.[101] Specifically, the Court in *Miller* mistakenly relied on the line of cases which created the third-party doctrine without recognizing how *Katz* undercut its reasoning in those cases.[102]

This and other missteps in analysis provides grounds for the Supreme Court to revisit the question of the BSA's constitutionality. The following sections explain (1) the evolution of the third-party doctrine, the *Katz* test, and how the Supreme Court initially tried to reconcile the two; (2) the *Miller* case; and (3) why the Court's decision in *Miller* was wrong.

1. Historical Development of the Third-Party Doctrine

The Fourth Amendment does not apply where the third-party doctrine does.[103] The third-party doctrine states that "a person has no legitimate expectation of privacy in information he voluntarily

---

[97] *See, e.g.*, *Id.* at 382.
[98] *See, e.g.*, *Id.*
[99] *See, e.g.*, Gouled v. United States, 255 U.S. 298 (1921).
[100] *See* U.S. v. Miller, 425 U.S. 435 (1976).
[101] *See infra* Part III.B.
[102] *Id.*
[103] *E.g.*, Smith v. Maryland, 442 U.S. 735, 743-44 (1979). For ease of reading, I use the common description of the doctrine as being an "exception" to the Fourth Amendment. However, the use of "exception" is imprecise—it assumes that the Fourth Amendment initially applies to a particular situation and then the third-party doctrine functions as a reprieve. In fact, the third-party doctrine is the initial consideration; if it applies to a particular situation, then that situation is outside the realm of Fourth Amendment law.

turns over to third parties."[104] Over time, the Supreme Court expanded the third-party doctrine into a binary inquiry "in which any information disclosed to a third party for any reason is public and does not merit Fourth Amendment protection."[105] The third-party doctrine was the result of the Court's trespass-based interpretation of the Fourth Amendment; therefore, a detailed analysis of the line of cases establishing the third-party doctrine is necessary in order to evaluate the third-party doctrine under the later *Katz* test. The result of the analysis of the third-party doctrine's lineage shows that an "all or nothing" approach to the third-party doctrine is inextricably attached to the trespass doctrine. Thus, the *Katz* test demands a retooling of the third-party doctrine.

The Supreme Court first recognized the third-party doctrine in *Gouled v. United States*.[106] In *Gouled*, the United States Army suspected that the defendant was part of a conspiracy to defraud the government through contracts for clothing and equipment, so it sent an undercover private to obtain information from the defendant.[107] The private, a former business acquaintance of the defendant, travelled to the defendant's office for a "friendly" visit.[108] The defendant allowed the private to enter his office; when the defendant momentarily stepped out, the private took and carried away several documents from the defendant.[109] The private did not have a warrant.[110] The government used the seized documents as evidence at trial, which ultimately resulted in the defendant's conviction.[111]

On appeal, the defendant argued that the private's warrantless seizure of his documents violated his Fourth Amendment rights, and that the court should have suppressed that evidence at trial.[112] The Supreme Court agreed with the defendant, finding that it was significant that the private took the papers outside the presence of the defendant.[113] The Court reasoned that a secret taking of an object, despite being voluntarily invited into office, is analogous to a forced or coerced entry and seizure prohibited by the Fourth Amendment.[114] In its conclusion, the Supreme Court declared:

---

[104] *Id.*
[105] Note, If These Walls Could Talk, 130 HARV. L. REV. 1924, 1931 (2017).
[106] *See* Gouled v. United States, 255 U.S. 298 (1921).
[107] *Id.* at 304.
[108] *Id.*
[109] *Id.*
[110] *Id.*
[111] *Id.* at 303.
[112] *Id.*
[113] *Id.* at 306.
[114] *Id.* at 305-06.

> [w]hether entrance to the home or office of a person suspected of crime be obtained by a representative . . . of the government . . . and whether the owner be present or not when he enters, any search and seizure subsequently *and secretly made in his absence*, falls within the scope of the prohibition of the Fourth Amendment . . . . [115]

This ruling, while favorable for the defendant, implicitly endorsed governmental subterfuge. The Court's endorsement came from the Court's pure reliance on the voluntariness of the defendant's actions.[116] In this case, the idea of voluntariness only manifested when the private took the papers outside of the defendant's presence because the defendant was not present to give consent, and the Court assumed that he would not have if he were.[117] The fact that the private gained the defendant's permission to enter the office under false pretenses was of no regard—that still counted as voluntary consent.[118]

Seven years later, in *Olmstead v. United States*, the Supreme Court emphasized voluntariness and trespass as a part of Fourth Amendment considerations.[119] In *Olmstead*, the government suspected that the defendant was involved in a "conspiracy of amazing magnitude"[120] to violate the National Prohibition Act.[121] The government wiretapped the defendant's home and office telephones without a warrant to conduct its investigation.[122] The government accomplished this by attaching wires to the telephone lines across the street from his home and in the basement below the defendant's office.[123] The government was thus able to listen to the defendant's conversations without any act of trespass.[124] Therefore,

---

[115] *Id.* at 306 (emphasis added).
[116] *See id.*
[117] *See id.* at 305-06.
[118] *See id.* at 306.
[119] Olmstead v. United States, 277 U.S. 438, 462-66 (1928).
[120] "The evidence in the records discloses a conspiracy of amazing magnitude to import, possess, and sell liquor unlawfully. It involved the employment of not less than 50 persons, of two sea-going vessels for the transportation of liquor to British Columbia, of smaller vessels for coastwise transportation to the state of Washington, the purchase and use of a branch beyond the suburban limits of Seattle, with a large underground cache for storage and a number of smaller caches in that city, the maintenance of a central office manned with operators, and the employment of executives, salesmen, deliverymen dispatchers, scouts, bookkeepers, collectors, and an attorney. In a bad month sales amounted to $176,000; the aggregate for a year must have exceeded $2,000,000." *Id.* at 455-56.
[121] *Id.*
[122] *Id*.
[123] *Id.* at 456-57.
[124] *Id.* at 457.

the government used evidence gained from the wiretaps in the defendant's trial which lead to his conviction.[125]

On appeal, the defendant argued that the government's warrantless interception of his private conversations violated the Fourth Amendment.[126] The Supreme Court held that the defendant's Fourth Amendment rights were not violated because the government did not trespass upon his property or seize any physical objects.[127] In addition to a lack of physical trespass or seizure, the Court regarded the voluntariness of the defendant's conversations as an essential consideration: "Here we have testimony only of *voluntary* conversations secretly overheard."[128] The Court viewed that a "well-known historical purpose of the Fourth Amendment" is to prevent the government from compelling suspects to agree to searches or seizures against their will.[129] Without government coercion, the defendant's conversations were voluntary.[130]

Therefore, the Court built upon *Gouled* by allowing for more than knowing and voluntary disclosure, but also for a defendant's complete unawareness of the eavesdropping of another party. Unlike the Court in *Gouled*, the Court in *Olmstead* did not assume what the defendant would have done had he known the government was listening to his conversations.[131] This distinction highlights the connection of voluntariness to a physical location or tangible object. Without trespass, the Court assumed voluntariness.[132]

The Supreme Court further expanded this "voluntariness" reasoning in the 1960s as it decided a series of Fourth Amendment cases which evaluated defendants' statements to undercover government agents.[133] For example, in *Lopez*, the defendant was convicted for attempted bribery of an Internal Revenue Service agent.[134] The agent was initially investigating whether the defendant was evading taxes in the operation of his hotel.[135] At the defendant's hotel, the agent asked the defendant if the hotel provided entertainment in the evenings, such as singing or dancing.[136] The defendant stated the hotel did not.[137] But when the agent returned later that same evening and again the next day, the agent discovered

---

[125] *Id.* at 455, 457.
[126] *Id.* at 455.
[127] *Id.* at 466.
[128] *Id.* at 464.
[129] *Id.* at 463.
[130] *Id.* at 463-69.
[131] *See id.*
[132] *See id.* at 463.
[133] *See, e.g.*, Lopez v. United States, 373 U.S. 427 (1963); Hoffa v. United States, 385 U.S. 293 (1966); Lewis v. United States, 385 U.S. 206 (1966).
[134] Lopez, 373 U.S. at 428.
[135] *Id.* at 429.
[136] *Id.*
[137] *Id*.

that the hotel was indeed hosting dancing.[138] The agent again confronted the defendant, stating that he believed that the defendant might be liable for a cabaret tax and requested to inspect the defendant's books.[139] The defendant took the agent back to his office and offered the agent $420 to "drop this case."[140]

After the bribe, the agent took the money and reported the event to his supervisor.[141] The IRS equipped the agent with a secret recording device and sent the agent back to the hotel to get the defendant to discuss the previous bribery event.[142] The plan worked; the agent returned to the hotel and recorded a conversation with the defendant in which the defendant recognized the previous bribe and set up a system for continuing payments in order to avoid taxes.[143]

The court admitted the recording as evidence and allowed the agent to testify in the trial despite the defendant's objections under the Fourth Amendment, which led to the defendant's conviction.[144] The defendant appealed, and the issue reached the Supreme Court.[145] The Supreme Court decided that admission of the recording at trial did not violate the defendant's Fourth Amendment rights.[146] Similar to the Court in *Olmstead*, the Supreme Court employed the trespass doctrine for its analysis.[147] The court held that the agent did not violate the defendant's Fourth Amendment rights because the defendant invited the agent into his office and because the agent did not furtively seize any evidence.[148] The Supreme Court specifically harkened back to *Gouled* and emphaisized that the linchpin of its holding was trespass, not the nature of the defendant's statement.[149] Therefore, the recording and the fact that the defendant likely would not have made any incriminating statements had he known of the recording were immaterial in the Supreme Court's decision.[150]

The Supreme Court subsequently expanded the *Lopez* principles simultaneously in *Hoffa v. United States* and *United States v. Lewis* by disregarding whether the defendant knew the true identity of the listener.[151] Put another way, the third-party doctrine now allowed for the government's intentional deception of the

---

[138] *Id.*
[139] *Id.*
[140] *Id.* at 430.
[141] *Id.*
[142] *Id.*
[143] *Id.* at 431-32.
[144] *Id.* at 432-33.
[145] *Id.* at 427.
[146] *Id.* at 439.
[147] *Id.* at 438-39.
[148] *Id.* at 430.
[149] *Id.* at 438.
[150] *Id.*
[151] *See* Hoffa v. United States, 385 U.S. 293 (1966).

defendant. The facts in *Hoffa* begin with the defendant on trial for violation of the Taft-Hartley Act.[152] During the trial, the defendant stayed in a hotel suite and was frequently visited by two associates.[153] The defendant had voluntary conversations with the associates in multiple locations around the site of the trial.[154] During the conversations, the defendant discussed his efforts to bribe the jurors in his trial.[155] However, unbeknownst to the defendant, one of the associates was reporting the contents of their conversations to a federal agent.[156] In fact, the reporting associate was acting as a government agent.[157]

With this information, the government indicted the defendant for attempting to bribe jurors.[158] The court admitted that the reporting associate's disclosures and testimony at the defendant's trial "unquestionably contribut[ed]" to the defendant's conviction.[159] The defendant appealed his conviction and argued that the court violated the Fourth Amendment when it admitted the evidence derived from the reporting associate in his trial.[160] More specifically, the defendant called upon the Supreme Court to determine whether the reporting associate's "failure to disclose his role as a government informer vitiated the consent that [the defendant] gave to [the reporting associate's] repeated entries into the suite, and that by listening to [his] statements [the reporting associate] conducted an illegal 'search' for verbal evidence."[161] The Supreme Court found the defendant's argument that his voluntary statements to and around the associate unconvincing.[162] The defendant "was not relying on the security of the hotel room; he was relying on his misplaced confidence that [the reporting associate] would not reveal his wrongdoing."[163] Citing *Lopez*, the Supreme Court affirmed that the Fourth Amendment does not "protect[] a wrongdoer's misplaced belief that a person to whom he voluntarily

---

[152] *Id.* at 294.
[153] *Id.* at 296.
[154] *Id.*
[155] *Id.*
[156] *Id.*
[157] *Id.* at 298-99. The parties in this case disagreed on the incentives of the reporting associate, as he was himself facing separate criminal charges before being approached by the government to be an informer. *Id.* The Supreme Court rendered its opinion on the assumption that the reporting associate as a government agent—acting in the interests of the government—for the entire course of events. *Id.*
[158] *Id.* at 294-95.
[159] *Id.* at 296-97.
[160] *Id.* at 300.
[161] *Id.* at 300-01 (citing United States v. Jeffers, 342 U.S. 48 (1951); Silverman v. United States, 365 U.S. 505 (1961)).
[162] *Id.* at 301-03.
[163] *Id.* at 302.

confides his wrongdoing will not reveal it."[164] Indeed, the Supreme Court went as far as to quote the *Lopez* opinion's reasoning, which cited *Gouled*, to highlight that the associate did not seize anything not freely given to him: "He was in the office with [the defendant's] consent, and while there [the reporting associate] did not violate the privacy of the office by seizing something surreptitiously without petitioner's knowledge."[165]

The Supreme Court released its opinion in *Lewis v. United States* the same day as *Hoffa,* emphasizing its holding that government subterfuge does not make a statement involuntary.[166] In *Lewis*, the defendant invited an undercover law enforcement officer into his home and sold the agent unlawful narcotics.[167] The trial court convicted the defendant because he violated various narcotics laws in a trial where his interactions with the undercover officer were admitted into evidence over his objection.[168] On appeal, the defendant argued that the admission of such evidence violated his Fourth Amendment rights because he could not have waived his privacy protections inside his home when he invited the officer inside because "the invitation was induced by fraud and deception."[169]

However, the Supreme Court disagreed.[170] The Supreme Court noted that the "pretense resulted in no breach of privacy" and focused on the defendant's voluntary statements and the defendant freely invited the officer into his home.[171] Further the Supreme Court noted that pretense "merely encouraged the [defendant] to say things which he was willing and anxious to say to anyone who would be interested in purchasing [narcotics]."[172]

This line of cases shows that up until 1966, the Supreme Court interpreted the Fourth Amendment as only protecting unreasonable physical trespass and seizures. The third-party doctrine emerged under this interpretation. On these terms, voluntariness was a defendant-centric inquiry. The Court did not evaluate whether the defendant knew he was speaking to a government agent or whether one was secretly listening. Then, the *Katz* test was created and undercut the line of cases behind the third-party doctrine.

---

[164] *Id.* (citing Lopez v. United States, 371 U.S. 471 (1963)).
[165] *Id.* at 303.
[166] Lewis v. United States, 385 U.S. 206 (1966).
[167] *Id.* at 206-07.
[168] *Id.* at 208.
[169] *Id.*
[170] *Id*. at 212.
[171] *Id*.
[172] *Id.*

2. Emergence of the Katz Test

The Supreme Court recognized a different Fourth Amendment paradigm in *Katz v. United States* when it held that the Fourth Amendment protects people but does not protect places.[173] Under this new standard, Justice Harlan articulated the test that would henceforth guide Fourth Amendment inquiry.[174] As this case displaced the trespass doctrine, the Supreme Court also redefined the third-party doctrine as it was then understood.

In *Katz*, the defendant was convicted in federal court for various crimes after he "transmit[ted] wagering information by telephone" across state lines.[175] The trial court allowed the government to introduce recordings of the defendant's end of a telephone conversation into evidence despite the defendant's objection, which contributed to the defendant's conviction.[176] The government obtained the defendant's conversation by placing "an electronic listening and recording device to the outside of the public telephone booth from which he had placed his calls."[177]

Following conviction, the defendant appealed, contending that the government's listening and recording of his phonebooth conversation violated his Fourth Amendment rights.[178] The Court of Appeals disagreed; it held that the government did not violate the defendant's Fourth Amendment rights because the government did not "physical[ly enter] into the area occupied by" the defendant.[179]

The defendant then appealed to the Supreme Court, which granted certiorari.[180] At the Supreme Court, the defendant argued that a public telephone booth was a constitutionally protected area and that physical penetration was necessary before the government violated the Fourth Amendment.[181] In essence, the defendant challenged the trespass doctrine.

Initially, the Supreme Court took exception to the defendant's formulation of the issues.[182] The Supreme Court rejected both the defendant's and the government's strict reliance on the physical location of the putative search because such analysis was not a "talismanic solution to every Fourth Amendment problem."[183] Instead, the Supreme Court declared that "[w]hat a

---

[173] *See* Katz v. United States, 389 U.S. 347 (1967).
[174] *Id.* at 361 (Harlan, J., concurring).
[175] *Id.* at 348.
[176] *See id.*
[177] *Id.*
[178] *Id.*
[179] *Id.* at 348-49.
[180] *Id.* at 349.
[181] *Id.* at 349-50.
[182] *Id.* at 350.
[183] *Id.* at 350-51, 351 n.9.

person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[184]

The Supreme Court applied these principles and concluded that the defendant's actions demonstrated that he sought to preserve his privacy.[185] The government argued that the defendant could not have expected any privacy because phone booths are made out of glass, but the court couched the defendant's privacy expectation in terms of audio privacy.[186] Specifically, the court held that the defendant had an expectation that his conversation would be private because he shut the phonebooth door behind himself and paid the toll to make his call.[187]

Then, the Supreme Court then considered whether Fourth Amendment searches require the government's physical presence during a search.[188] Indeed, the Supreme Court recognized that its previous jurisprudence limited Fourth Amendment application to instances of the government's physical trespass and seizure of material items, specifically citing *Olmstead* and *Goldman*.[189] However, the Court also recognized that such an approach had "been discredited."[190] The Supreme Court accomplished this by citing *Warden, Md. Penitentiary v. Hayden*, which recognized that Fourth Amendment jurisprudence has decoupled from the common-law understanding of property to the broader concept of personal privacy.[191] As such, the Supreme Court announced that the so-called "trespass doctrine" was no longer valid.[192]

Thus, the Supreme Court disregarded the absence of the government's physical presence in the phonebooth and concluded that the government violated the defendant's justified expectation of privacy while using the phonebooth.[193] Therefore, the government's electronic eavesdropping on the defendant constituted a "search and seizure" within the meaning of the Fourth Amendment because of the defendant's reasonable privacy expectation.[194] In finding that the government's actions constituted a "search and seizure" under the Fourth Amendment, the Supreme Court ultimately held that

---

[184] *Id.* at 351 (citations omitted).
[185] *Id.* at 352.
[186] *Id.*
[187] *Id.*
[188] *Id.*
[189] *Id.* at 352-53 (citing Olmstead v. United States, 277 U.S. 438, 457, 466 (1928); Goldman v. United States, 316 U.S. 129, 134-36 (1942)).
[190] *Id*. at 353.
[191] *Id.* at 353 (*citing* Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 304 (1967)).
[192] *Id.*
[193] *Id.*
[194] *Id.*

eavesdropping on the defendant was unreasonable because the government failed to get a warrant and no exception to the Fourth Amendment warrant requirement existed.[195]

Beyond the facts of the case, *Katz* became significant for Justice Harlan's test to judge whether a government action constitutes a Fourth Amendment "search and seizure."[196] Precisely, Justice Harlan stated that his "understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[197] Henceforth, Justice Harlan's "*Katz* test" became the controlling interpretation of Fourth Amendment jurisprudence.[198]

Looking at the reasoning of *Katz*, the principles underlying the third-party doctrine were necessarily shaken. First, the Court expressly renounced the trespass doctrine. The government could now be found to have violated the Fourth Amendment without any physical trespass or seizure. Secondly, the Court's reasoning overruled any case stating that the government could eavesdrop on a defendant through wiretaps and without the use of a confederate, such as in *Olmstead*. Furthermore, in the bigger picture, the third-party doctrine could no longer be viewed as a binary, all or nothing analysis because the *Katz* test requires an evaluation of what the defendant and society would deem to be reasonably private, regardless of how the defendant made the statement. Unfortunately, the Supreme Court struggled to fully apply the *Katz* test in the cases preceding *Miller*, falling back upon old conceptions of the Fourth Amendment instead.

3. Early Tension Between The Katz Test And The Third-Party Doctrine

The Supreme Court struggled to harmonize *Katz* with the third-party doctrine in subsequent cases.[199] In *United States v. White*, the Court failed to analyze the third-party doctrine under the *Katz* test; rather, it reapplied the third-party doctrine as conceptualized under the trespass doctrine.[200] In *White*, the government was investigating a defendant for illegal drug transactions.[201] To gather incriminating evidence on the defendant,

---

[195] *See id.* at 354-59.
[196] *See id.* at 361 (Harlan, J., concurring).
[197] *Id.* (Harlan, J., concurring).
[198] *See, e.g.*, U.S. v. Miller, 425 U.S. 435 (1976); United States v. White, 401 U.S. 745, 749 (1971).
[199] *See* United States v. White, 401 U.S. 745 (1971).
[200] *See id.*
[201] *Id.* at 746.

the government used an informant who had several conversations with the defendant regarding illegal drug transactions.[202] The locations of these conversations included a restaurant, a car, the informant's home, and the defendant's home.[203] During all of these conversations, the informant was secretly wearing a radio transmitter that allowed government agents to listen to the conversations through radio equipment in real-time.[204] The conversations that took place at the informant's home were also listened to by an agent concealed in a closed kitchen (with the informant's consent).[205]

When it came time for trial, the government could not locate and produce the informant as a witness.[206] Instead, the government introduced the testimony of the agents who had listened to the defendant's conversations via the radio transmitter.[207] The defendant objected to the agents' testimonies which the court overruled.[208] At the end of the trial, the jury found the defendant guilty.[209]

The defendant appealed his conviction on the ground that the agents' testimonies violated his Fourth Amendment rights.[210] The Court of Appeals ruled that the agents' statements were inadmissible under the principles outlined in *Katz*.[211] The court stated that there was no substantive legal difference between the bug used in *Katz* and an informant wearing a wire.[212] However, the Court of Appeals reasoned by analogy to *Katz* rather than employing the *Katz* test.[213] In doing so, the court held that *Katz* stands for the per se rule that all covert, warrantless eavesdropping by the government violates the Fourth Amendment.[214] Additionally, the court concluded that the listener's consent was "irrelevant."[215] The court emphasized that the Fourth Amendment required such a rule for efficacy:

> That amendment's search and seizure protection is lost to a person when his actions as a matter of law can be said to constitute a waiver of his right. Since the Fourth Amendment protects a speaker's right to

---

[202] *Id.* at 746-47.
[203] *Id.* at 747.
[204] *Id.* at 746-47.
[205] *Id.* at 747.
[206] *Id.*
[207] *Id.*
[208] *Id.*
[209] *Id.*
[210] *Id.*
[211] United States v. White, 405 F.2d 838, 840 (1969).
[212] *Id.* at 843-44.
[213] *Id.* at 844.
[214] *Id.*
[215] *Id.* at 843-44, 844 n.5.

> privacy, this right would be illusory if it could be waived by other individuals.[216]

In this sentence, the Court of Appeals took *Katz* as obliterating the third-party doctrine without using the *Katz* test in its analysis.[217]

The Supreme Court took a position opposite that of the Court of Appeals, holding that *Katz* did not implicate the third-party doctrine whatsoever because the defendant could neither show that he had any constitutionally protected right to expect, nor prevent those to whom he spoketo not later reveal that converstion to the police.[218]

In analyzing the issue, the Supreme Court considered the third-party doctrine and traced it through *Hoffa*, *Lewis*, and *Lopez*, and determined that these cases "remained unaffected by Katz [sic]."[219] The Court took those cases as creating a per se rule that a person can never have an expectation of privacy in the information disclosed to another;[220] though on its surface, it appeared as if the Court used the *Katz* test to reach this decision. However, the Court's opinion was actually driven by the trespass doctrine version of the third-party doctrine, which only analyzes the volition of the defendant's statements in the absence of a physical search or seizure.

This is seen in how the Court viewed the defendant's thought process in sharing information with a third party:

> If he sufficiently doubts their trustworthiness, the association will very probably end or never materialize. But if he has no doubts, or allays them, or risks what doubt he has, the risk is his. In terms of what his course will be, what he will or will not do or say, we are unpersuaded that he would distinguish between probably informers on the one hand and probable informers with transmitters on the other.[221]

But, this hypothetical thought process leaves no room for a person to share information and retain a privacy expectation in that information. The Court in *White* focused on the defendant's free will whether to share was determinative—the binary choice associated

---

[216] *Id.* at 845.
[217] *Id.* at 843-48.
[218] United States v. White, 401 U.S. 745, 749 (1971).
[219] *Id.* at 749-50.
[220] *See id.*
[221] *Id.* at 752.

with the trespass doctrine, not the *Katz* test. Upon this reasoning,[222] the Court held that the government did not violate the defendant's Fourth Amendment rights and denied his motion. [223]

Thus, *White* laid the groundwork for the Supreme Court to adhere to the trespass doctrine version of the third-party doctrine despite the *Katz* decision. To the extent that the Court's decision was result-driven, the Court could have fully performed the *Katz* test in *White* to find that the defendant had no expectation of privacy. Society would unlikely accept a defendant's expectation of privacy in a conversation with a police informant as reasonable in that limited context and for the public good. Unfortunately, the Court's flawed reasoning laid the groundwork for future faulty decisions. By using the third-party doctrine as valid per se rule, the Court left room for the possibility that society could consider a privacy expectation in the information given to a third party to be reasonable in circumstances substantially different from those in *White*. Indeed, that is what happened when the Court decided the constitutionality of the BSA.

B. The Supreme Court Applies the Third-Party Doctrine to the Bank Secrecy Act

Finally, in 1976, the Supreme Court had the opportunity to evaluate the BSA in light of the relatively new *Katz* test. Unfortunately, the Court only gave a cursory nod to the *Katz* test and reverted back to the pre-*Katz* conception of the third-party doctrine[224] from the case of *U.S. v. Miller*.[225] In *Miller*, law enforcement's ultimate warrantless search of the defendant's bank records stemmed from when the defendant first came to law enforcement's attention.[226] That attention came as a consequence of an informant's tip to law enforcement, which led to a traffic stop of two of the defendant's co-conspirators.[227] During the stop, law enforcement found illegal distillery equipment and raw materials in the vehicle.[228] A few weeks later, a warehouse rented to the defendant caught on fire, and during the response to the fire, law

---

[222] Actually, the Supreme Court ruled that the Court of Appeals erred by applying *Katz* retroactively. White, 401 U.S. at 753-54 (citing Desist v. United States, 394 U.S. 244 (1969)). This raises interesting precedential issues. Since the Supreme Court's purported *Katz* reasoning was unnecessary to denying the defendant's motion, it could be regarded as dicta.
[223] White, 401 U.S. at 754.
[224] *See* U.S. v. Miller, 425 U.S. 435 (1976).
[225] *Id.*
[226] *Id.* at 437.
[227] *Id.*
[228] *Id.*

enforcement found "a[n illegal] 7,500-gallon-capacity distillery, 175 gallons of nontax-paid whiskey, and related paraphernalia."[229]

As law enforcement officials investigated the defendant, they issued grand jury subpoenas to the presidents of two separate banks where the defendant maintained accounts.[230] The particular subpoenas used in this case were issued in blank by the clerk of the trial court and completed by the United States Attorney's office.[231] These subpoenas required the bank presidents to appear before the grand jury on a specific date and produce "all records of accounts, i. e., savings, checking, loan or otherwise, in the name of" the defendant from approximately two months prior through the present.[232] The banks already kept the requested records under the requirements of 12 U.S.C. § 1829b(d).[233] The bank presidents provided the requested information to law enforcement and were therefore excused from appearing before the grand jury.[234] Throughout this process, the banks never notified the defendant about the subpoenas.[235]

Eventually, the grand jury indicted the defendant for various financial crimes and the defendant's case went to trial.[236] At trial, the defendant moved to suppress the documents provided by the bank presidents, arguing that they were illegally seized because they were the product of a non-judicially ordered subpoena.[237] The trial court denied the defendant's motion, but the Court of Appeals reversed.[238] The Court of Appeals held that the defendant had a Fourth Amendment privacy interest in the bank records.[239] As such, the subpoena violated the defendant's Fourth Amendment rights for not being obtained through an "adequate 'legal process.'"[240] The government then appealed the case to the Supreme Court.[241]

In its decision, the Supreme Court ultimately held that "there was no intrusion into any area in which [the defendant] had a protected Fourth Amendment interest," and thus reversed the Court of Appeals.[242] The Supreme Court began its analysis by affirming the Court of Appeals's holding that "'no interest legitimately protected by the Fourth Amendment' is implicated by governmental

---

[229] *Id.*
[230] *Id.* at 437-38.
[231] *Id.* at 437.
[232] *Id.* at 437-38.
[233] *Id.* at 436.
[234] *Id.* at 438.
[235] *Id.*
[236] *Id.*
[237] *Id.* at 438-39.
[238] *Id.*
[239] *Id.* at 439.
[240] *Id.*
[241] *Id.*
[242] *Id.* at 440.

investigative activities unless there is an intrusion into a zone of privacy, into 'the security a man relies upon when he places himself or his property within a constitutionally protected area.'"[243] The Supreme Court diverged from the Court of Appeals in its belief that the bank documents did not "fall within a protected zone of privacy."[244]

"On its face," the Supreme Court said the bank documents were not the defendant's "private papers" because they were the business records of the banks.[245] Although the records contained personally identifiable information of the defendant, the records belonged to the banks because the banks created the records themselves as a party in the defendant's banking transactions.[246] As the Court put it, the banks had a "substantial stake" in dealing with negotiable instruments with the defendant.[247]

The Supreme Court also rejected the defendant's argument that the unique combination of the BSA's recordkeeping requirements and the government's access to those records through a subpoena was "the functional equivalent of a search and seizure" of his "private papers," thus implicating his Fourth Amendment rights as if the government sought the bank records" directly from his custody.[248] The Supreme Court framed this issue as "whether the compulsion embodied in the [BSA] as exercised in this case creates a Fourth Amendment interest in the depositor where none existed before."[249]

Disposing of the defendant's argument, the court gave a passing nod to the *Katz* test by parroting the rule's language in the context of what the defendant was arguing.[250] However, the Supreme Court immediately countered that *Katz* "also stressed that '[w]hat a person knowingly exposes to the public . . . is not subject of Fourth Amendment protection."[251] The Court further included the rule that it is necessary to "examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents."[252]

Under these rules, the Court only looked to the second part of the *Katz* test—whether society would recognize a privacy

---

[243] *Id.* (citing Hoffa v. United States, 385 U.S. 293, 301-02 (1966)).
[244] *Id.*
[245] *Id.*
[246] *Id.*
[247] *Id.* (citing California Bankers Assn. v. Shultz, 416 U.S. 21, 48-49 (1974)).
[248] *Id.* at 441.
[249] *Id.*
[250] *Id.* at 442.
[251] *Id.* (citing Katz v. United States, 389 U.S. 347, 351 (1967)).
[252] *Id.* (citing Couch v. United States, 409 U.S. 322, 335 (1973)).

expectation in bank records as being reasonable.[253] The Supreme Court answered in the negative by looking to the third-party doctrine as well as the pronouncements of Congress. For the third-party doctrine, the Court looked primarily to *White* and its predecessor cases, stating,

> This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[254]

In this, "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[255]

In regard to Congressional intent, the Court justified a societal lack of expectation of privacy in bank records through the mere existence of the BSA.[256] Explaining Congress's intent, the Court articulated,

> 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."[257]

Further, neither did the Courtbelieve that the BSA's record-keeping mandate impacted its Fourth Amendment analysis.[258] Here, the Court first avowed that such requirements do not transform the banks into government agents.[259] The Court then said that even if it were to consider the banks as "acting solely as Government agents," there would still be no Fourth Amendment violation because the banks recorded the information and provided it pursuant to the subpoena "without protests."[260]

---

[253] *See id.*
[254] *Id.* at 443.
[255] *Id.*
[256] *See id.* at 442-43.
[257] *Id.* (citing 12 U.S.C. § 1829b(a)(1); Couch v. United States, 409 U.S. 322, 335 (1973)).
[258] *Id.* at 443.
[259] *Id.* (citing California Bankers Assn. v. Shultz, 416 U.S. 21, 52-53 (1974)).
[260] *Id.*

In the end, the Court held that the BSA did not violate the Fourth Amendment. In its reasoning, the Court relied on the trespass-doctrine formulation of the third-party doctrine as well as wrongly deferring to congressional opinion. Because of these errors, the constitutionality of the BSA must be reevaluated.

C. Criticism of the Supreme Court's Opinion

In *Miller*, the Supreme Court's analysis erred in two respects: (1) it did not apply the *Katz* test to its rightful extent, but reverting to outmoded concepts of the third-party doctrine, and (2) let Congress define constitutional law. Without these errors, the Court would have likely held that the BSA violated the Fourth Amendment. At a minimum, these flaws should cause *Miller* to have little precedential value.

First, the Court failed to reconcile the third-party doctrine with the *Katz* test. As discussed in section III.A.1, the third-party doctrine evolved out of the Court's trespass doctrine. The strict policy supporting the trespass doctrine was that if an individual does not control a location or relinquishes control of a location by inviting the government in, then that individual can expect no Fourth Amendment privacy rights. This reasoning has necessarily influenced the third-party doctrine—by relinquishing control of a piece of information, an individual can no longer expect any control over that information.

It was the trespass doctrine-based understanding of the third-party doctrine that the Supreme Court applied in *Miller*. The Court first showed its use when it quoted *Hoffa* to analyze the constitutionality of the BSA—that there is no Fourth Amendment violation unless the government violates "the security a man relies upon when he places himself or his property within a constitutionally protected area."[261] This pre-*Katz* language focuses Fourth Amendment protections on locations, the hallmark of the trespass doctrine.[262] Next, the Court emphasized that the banks had possession of the records supplied to the government. Again, this is a trespass doctrine-based analysis because it looks solely to the physical location and ownership of records.[263] This analysis is a direct appeal to the traditional third-party doctrine because it asserts that the defendant could not have privacy interest in the information that he voluntarily gave to the banks.

Still, the Supreme Court purported to apply the *Katz* test, but it did so in name only.[264] The Court merely restated that the bank

---

[261] *Id.* at 440.
[262] *See supra* Part III.A.
[263] *Id.* at 440-41.
[264] *Id.* at 442.

documents "contain[ed] only information voluntarily conveyed to banks and exposed to their employees in the ordinary course of business," rather than asking the right *Katz* question: Does society expect privacy in bank records?[265] Finally, the Court solidified its trespass doctrine-based third-party doctrine analysis by string-citing *White*, *Hoffa*, and *Lopez*.[266] From these cases, the Court struck the final blow to the defendant:

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. . . . This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[267]

Therefore, as seen by the cases it cited and the analyses it utilized, the Supreme Court applied the third-party doctrine under the trespass-doctrine of the Fourth Amendment.

If the Court looked at the third-party doctrine though the lens of the *Katz* test, it would have seen that the strictness of the third-party doctrine has eroded. Under the *Katz* paradigm, "the Fourth Amendment protects people, not places."[268] Moreover, while an individual may still lose Fourth Amendment protection in information purposefully exposed to third parties, "what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[269] By asking if the defendant exhibits a subjective privacy interest that society would objectively recognize as reasonable (the *Katz* test), it is evident that there is room for privacy in the information disclosed to third-parties. Yet, the Supreme Court in *Miller* did not go into this particular analysis.

By not recognizing the full extent of the *Katz* test, the Court failed to analyze its specific components. Indeed, the Supreme Court only touched upon societal expectations while discussing subpoena requirements, not *Katz*'s substantive analysis.[270] Specifically, the Supreme Court stated,

---

[265] *Id.*
[266] *Id.* at 443.
[267] *Id.*
[268] Katz v. United States, 389 U.S. 347, 351 (1967).
[269] *Id.*
[270] U.S. v. Miller, 425 U.S. 435, 444 (1976).

> Many banks traditionally kept permanent records of their depositors' accounts, although not all banks did so and the practice was declining in recent years. By requiring that such records be kept by all banks, the Bank Secrecy Act is not a novel means designed to circumvent established Fourth Amendment rights. It is merely an attempt to facilitate the use of a proper and longstanding law enforcement technique by insuring that records are available when they are needed.[271]

However, this statement does not explain why banks were moving away from keeping permanent records of their customers. Perhaps it was merely for procedural efficiency; perhaps it was because customers considered such records a privacy threat. Moreover, the Court's statement only looks back at past practices but not current, and potentially different, realities. Regardless, this is not sufficient analysis for the *Katz* test.

Second, the Supreme Court erred by interpreting the pure existence of the BSA as relevant to its constitutional analysis. Allowing statutes to determine constitutional law is anathema to the American system. As stated in *Marbury v. Madison*, "the particular phraseology of the Constitution of the United States confirms and strengthens the principle, supposed to be essential to all written constitutions, that a law repugnant to the constitution is void . . . ."[272] This has been a fundamental principle throughout the United States' existence. As the Supreme Court stated much later in 1997, "Congress does not enforce a constitutional right by changing what that right is. It has been given the power 'to enforce,' not the power to determine what constitutes a constitutional violation."[273] Stated plainly, Congress does not decide what is constitutional, the Supreme Court does.

However, that is what the Supreme Court allowed when it called to congressional intent to justify a lack of privacy interests in bank documents:

> 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

---

[271] *Id.*
[272] Marbury v. Madison, 5 U.S. 137, 180 (1803).
[273] City of Boerne v. Flores, 521 U.S. 507, 519 (1997).

> degree of usefulness in criminal tax, and regulatory investigations and proceedings."[274]

The Court's line of reasoning here is inappropriate because it allows Congress to dictate citizens' Fourth Amendment protections. This system is akin to the fox in the henhouse analogy because Congress could abrogate any Fourth Amendment protection by merely passing a statute declaring that individuals no longer have a privacy interest in the subject matter.

Interestingly, the Supreme Court began this line of thinking regarding the BSA not in *Miller*, but three years earlier in *Shultz*. While describing the "sweeping" effect of the BSA in *Shultz*, the Court said,

> While an Act conferring such broad authority over transactions such as these might well surprise or even shock those who lived in an earlier era, the latter did not live to see the time when bank accounts would join chocolate, cheese, and watches as a symbol of the Swiss economy. Nor did they live to see the heavy utilization of our domestic banking system by the minions of organized crime as well as by millions of legitimate businessmen.[275]

Here, the court implied that individuals should give up privacy for the sake of criminal investigations.

These errors in reasoning call into doubt the Court's holding in *Miller*. If the Court avoided these errors, it may have determined that the BSA was unconstitutional under the Fourth Amendment—or at least it would have been a much closer case. Either way, these errors severely limit *Miller*'s precedential value and calls for the Court to revisit the issue. In 2017, ruling that the BSA in its current form violates the Fourth Amendment seems unavoidable.

Nevertheless, such a ruling would not necessarily ring the BSA's death-bell; it only means that the BSA is unconstitutional to the extent that it allows the government to collect personal information to investigate criminal acts, determined by a *Katz* analysis, without a warrant. The Court would have to strike provisions such as the mandatory reporting of SARs for the BSA to be constitutional. Further, any information-collecting portions of the BSA that are not specifically geared towards criminal investigation would not even fall under the purview of the Fourth Amendment in the first place.[276]

---

[274] Miller, 425 U.S. at 442-43.
[275] California Bankers Ass'n v. Shultz, 416 U.S. 21, 30 (1974).
[276] *See supra* Part III.A.

IV. REEVALUATING THE BSA UNDER THE FOURTH AMENDMENT IN THE MODERN ERA

Regardless of whether the Supreme Court correctly decided *Miller* in 1976, society has since sufficiently changed to demand that the Supreme Court now overturn *Miller*. Particularly in the digital age, the third-party doctrine should not operate to deny Fourth Amendment protection of banking information categorically. "It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advances of technology."[277] The expectation that Fourth Amendment protections can change over time is supported by how the Supreme Court describes its *Katz* decision as a rejection of a "mechanical interpretation of the Fourth Amendment" because "that approach would leave [individuals] at the mercy of advancing technology . . . "[278] Under this approach to constitutionally protected privacy rights, the Supreme Court should not rigidly apply Fourth Amendment doctrines developed in historically dissimilar contexts in modern cases.

Several realities of modern society and technological advances support a finding that society has a reasonable expectation of privacy in banking records. In the modern era, a person's bank account can reveal the intimacies of that person's life.[279] As one scholar has noted, the depth of this information is great:

> With access to an individual's financial records, interested parties can easily determine the groups and associations to which the individual belongs (*e.g.*, through membership dues or contributions) and the social causes the individual supports (*e.g.*, through contributions). With access to banking records, interested parties can identify the books and publications an individual buys (*e.g.*, through subscription payments or receipts) and the material items an individual purchases (*e.g.*, through receipts or credit charges). Prying eyes with access to bank records can even identify the political party and causes supported by the individual (*e.g.*, through

[277] Kyllo v. United States, 533 U.S. 27, 33-34 (2001).
[278] *Id.* at 35.
[279] Matthew N. Kleiman, *The Right to Financial Privacy Versus Computerized Law Enforcement: A New Fight In An Old Battle*, 86 NW. U. L. REV. 1169, 1176 (1992).

> contributions to an election campaign or to a lobbying group).[280]

Moreover, this reasoning is not restricted to that of academics—the Supreme Court has previously echoed such sentiments.

The Supreme Court has already recognized that it is precisely this type of information and activity that the Constitution protects. In *National Ass'n for Advancement of Colored People v. State of Ala. ex. rel. Patterson*, the Supreme Court reiterated the "[i]nviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs."[281] Similarly, in *Talley v. California*, the Supreme Court recognized that anonymity in personal participation in political discourse and activities is necessary to the freedom of people from governmental tyranny.[282] This principle is ingrained in the rise of our nation—anonymous distribution of literature critical of the British, which the British considered a criminal act, was part of the prelude to the Revolutionary War.[283] Further, the Supreme Court has recognized significant privacy expectations barring governmental intrusion into individuals' sexual and family lives, such as privacy in marriage, procreation, family relationships, child-rearing, child education, possession of pornography in the home, and contraceptive use.[284]

Moreover, as the United States moves closer to a cashless society where all financial transactions are conducted by computer recordkeeping, debit and credit card transactions can be used to map an individual's physical movements.[285] This tracking capability can be expanded to identify groups of people meeting together.[286]

Under these realities, there are two reasons to hold that the BSA is unconstitutional. First, banks have become government agents. In a society that both requires banking and government disclosure of banking records, banks are *de facto* arms of the federal government engaged in continuous surveillance of its citizens.[287]

---

[280] *Id.*

[281] National Ass'n for Advancement of Colored People v. State of Ala. ex. rel. Patterson, 357 U.S. 449, 462 (1958).

[282] *See* Talley v. California, 362 U.S. 60, 64-65 (1960).

[283] *See id.* at 65.

[284] Kleiman, *supra* note 279, at 1181.

[285] *Id.* at 1176.

[286] *Id.*

[287] Although beyond the scope of this article, there are numerous other reporting requirements imposed by the federal government upon banks—many of which provide punishment for noncompliance. *See e.g.*, 26 U.S.C. §§ 7602(a), 7604(b) (stating that the IRS may demand to inspect bank records, and any noncompliance can result in contempt of court). Such mandatory reporting requirements and

Second, recent financial developments demonstrate that citizens demand privacy in banking. Specifically, the massive rise of cryptocurrencies[288]—a financial mechanism designed to protect privacy—is society's revolt against the BSA.

A. To Participate in Society, the BSA Effectively Requires Individuals to Give the Federal Government Private Information.

The combination of detailed and vague reporting requirements for banks within the BSA forces banks to overreport on the transactions of their customers. This is out of fear of sanctions for noncompliance. Concurrently, in the modern age, banking is necessary for individuals to participate in society effectively. The result of this paradigm requires citizens to give the government free access to their financial records—such revelations are anything but voluntary. Consequently, the third-party doctrine under the *Katz* test is inapplicable. The *Katz* test recognizes that the Fourth Amendment may protect some third-party disclosures. A court cannot hold that individuals voluntarily relinquish privacy expectations in the information given to third parties when the government requires those disclosures.

1. Banks as Government Agents

The Fourth Amendment applies to agents of the federal government.[289] The circuit courts have identified "two critical factors" in determining whether a private entity acts as a government agent: "(1) whether the government knew of or acquiesced in the intrusive conduct, and (2) whether the party performing the search intended to assist law enforcement efforts or to further his own ends."[290] The courts also consider other cicrumstances, such as whether a search is performed at the request of the government or whether the government offered a reward for the search.[291]

---

applicable punishments only serve to bolster the argument that the federal government has coopted banks as its agents.

[288] *See infra* Part IV.B; "Cryptocurrency" is defined by Merriam-Webster as "any form of currency that only exists digitally, that usually has no central issuing or regulating authority but instead uses a decentralized system to record transactions and manage the issuance of new units, and that relies on cryptography to prevent counterfeiting and fraudulent transactions."

[289] Oliver v. United States, 466 U.S. 179, 177 (1984).

[290] United States v. Blocker, 104 F.3d 720, 725 (5th Cir. 1997); United States v. McAllister, 18 F.3d 1412, 1417 (7th Cir. 1994); United States v. Malbrough, 922 F.2d 458, 462 (8th Cir. 1990); United States v. Miller, 688 F.2d 652, 657 (9th Cir. 1982).

[291] Malbrough, 922 F.2d at 462 (citing United States v. Koenig, 856 F.2d 843, 847 (7th Cir. 1988)).

Under these rules, the BSA turns banks into government agents. Not only does the government know banks are keeping customers' banking records for use in criminal investigations, but the government also requires it.[292] In this same manner, the banks are keeping transaction records and sending many of those records, including SARs, to FinCEN expressly for the criminal-investigation ends of the BSA.[293] To ensure compliance with the BSA, the government both offersrewards and threatens punishment.[294] These "critical" factors all point to banks as being government agents.

In *Shultz*, the Supreme Court rejected the notion that the BSA turns banks into government agents.[295] The Court reasoned because the records that the BSA requires banks to keep were already being kept voluntarily by the banks for their business purposes and that it is a party in banking transactions, a statute requiring banks to keep the same records does not transform the banks into government agents.[296] The Supreme Court determined that this situation was not any different from its prior holding that the IRS summons directed at banks for records did not violate the customers' Fourth Amendment protections.[297] Further, in *Miller*, the Supreme Court insisted that even if it assumed the banks were acting as government agents under the BSA, there could be no Fourth Amendment violation due to the third-party doctrine.[298]

The Supreme Court's arguments do not follow. As the Supreme Court itself admitted in *Miller*, the banks' practice of keeping permanent records was on the decline in recent years.[299] Moreover, SARs are reports designed for the benefit of the government—banks do not create them during standard business practices of banking.[300] Since the BSA requires banks to keep records they may not have otherwise kept and then requires that the records be available to the government for criminal investigations, the BSA squarely imparts government agency onto banks. Banks acting as government agents is particularly troublesome when individuals must choose between disclosing information to the government or forego full participation in society.

---

[292] *See supra* Part II.B.1-2.
[293] *See supra* Part II.
[294] *See supra* Part II.B.3.
[295] California Bankers Ass'n v. Shultz, 416 U.S. 21, 52-53 (1974); *see also* Miller, 425 U.S. at 443.
[296] *Id.*
[297] *Id.* (citing First National Bank v. United States, 267 U.S. 576 (1925); Donaldson v. United States, 400 U.S. 517, 522 (1971)).
[298] Miller, 425 U.S. at 443.
[299] *Id.* at 444.
[300] *See supra* Part II.B.2.

2. No Option but to Bank

Technological progress in modern society gives the public no option but to hold bank accounts. The third-party doctrine emerged in a society that was then mostly cash-based. In that system, an individual did not necessarily have (much less need) a bank account. It was easier to believe that individuals giving information to banks were doing so voluntarily. Today, individuals primarily receive and send payments electronically—an act that requires banks to function as necessary intermediaries. As highlighted in Airel's story,[301] it is unduly burdensome to function in modern society without a bank account.[302]

The Supreme Court of California recognized the need for bank accounts in 1975, declaring "[f]or all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional since it is impossible to participate in the economic life of contemporary society without maintaining a bank account."[303] For those choosing to live without bank accounts, there are limited options for making and receiving payments. These options are restricted to using prepaid cards or paper currency, and each of these options comes with its own disadvantages.[304] While prepaid cards do allow for individuals to make online purchases just like bank-issued credit and debit cards, money stored in accounts for prepaid cards are not necessarily insured by the Federal Deposit Insurance Corporation (FDIC).[305] One of the requirements for insurance is that the owner of the prepaid card must be identified.[306] For individuals seeking to avoid the BSA's reporting requirements, they must forego FDIC insurance as the requisite identification would result in BSA surveillance.[307] Further, assuming the operators of these prepaid cards are money transmitters, the amount of money loaded onto the card can itself trigger a required SAR under the BSA.[308]

The sole use of paper currency also comes with disadvantages. First, possessing only paper currency can pose a safety issue. Homes and people are subject to burglary. Money kept

---

[301] *See supra* Part I.A.
[302] *See supra* Part I.
[303] Burrows v. Superior Court, 529 P.2d 590, 596 (Cal. 1975).
[304] Justin Pritchard, *How to Live with No Bank Account, Common Money Tasks Without a Bank Account*, THE BALANCE (Mar. 19, 2019), https://www.thebalance.com/how-to-live-with-no-bank-account-3861031 [https://perma.cc/24QN-AEDV].
[305] *Prepaid Cards and Deposit Insurance Coverage*, FED. DEPOSIT INS. COMMISSION, https://www.fdic.gov/deposit/deposits/prepaid.html [https://perma.cc/PQ4Q-EZJY].
[306] *Id.*
[307] Pritchard, *supra* note 304.
[308] 31 U.S.C. § 5312(a)(2).

at home is additionally subject to destruction, such as from fires. If paper currency is stolen by an unknown individual or destroyed, there is no getting it back. Even if an individual has a method to safeguard his or her cash, it still does not accrue interest as it would when locked in a bank's vault.

Users of only paper currency are also disadvantaged in receiving and making payments. Without a bank account and unless an employer pays in cash, these individuals will require check cashing services.[309] These services typically charge fees above what one would have to pay when receiving a direct deposit into their bank account.[310] For example, an individual wishing to cash a check at a non-bank entity is usually charged "between 1.5% and 3.3% of [the] check's face value."[311] If that same individual wants to send a money order, for amounts under $500, that individual will typically face fees ranging from $0.50 to $10, or up to ten percent of the money order's value.[312]

Likewise, if a debtor, such as a utility company, does not have a local office that accepts cash payments, the individual must get and send a money order, which also comes with fees.[313] Furthermore, payments made by paper currency do not help improve an individual's credit score.[314] This is significant because credit scores do not only affect an individual's ability to make large purchases, but employers are entitled to look at credit scores to make hiring and promotion decisions.[315]

Still, individuals remain "unbanked." The FDIC considered a household to be "unbanked" when "no one in the household had a checking or savings account." In response, the Government has taken multiple steps to get unbanked individuals signed up for banking services. The Government has been trying this even before the FDIC began its survey program in 2009 where it tried to quantify the number of unbanked and underbanked households in the United

---

[309] *Id.*
[310] *Id.*
[311] Mehrsa Baradaran, *How The Poor Got Cut Out Of Banking*, 62 EMORY L.J. 483, 492 (2013).
[312] Gerald Morales, *Compare Fees To Find Where You Should Get A Money Order*, MYBANKTRACKER (Feb. 4 2020), https://www.mybanktracker.com/news/comparing-post-office-bank-western-union-money-order-fees [https://perma.cc/86DG-9PTH].
[313] *See, e.g.*, *Sending Money Orders*, U.S. POSTAL SERV., https://www.usps.com/shop/money-orders.htm [https://perma.cc/W4EB-7D6Q] (a money order of up to $500 comes with a $1.25 fee).
[314] *See* LaDonna Hadley, *The Pros and Cons of Living Cash-Only*, QUICKEN LOANS (Apr. 17, 2017), https://www.quickenloans.com/blog/pros-cons-living-cash [https://perma.cc/R7S3-QDXF].
[315] 15 U.S.C. § 1681b(a)(3)(B).

States.[316] For example, in 1998, Congress passed the Assets for Independence Act (AFIA), which provided $125 million in federal funds to local programs aimed at getting individuals to sign-up for Individual Development Accounts.[317]

Statistical analysis on the number of individuals who do not have bank accounts is a recent development but does provide some interesting insights. Starting in 2011, The World Bank estimated that 22% of United States citizens over fifteen years old did not have a bank account.[318] In that same year, the Board of Governors of the Federal Reserve System estimated that 10.8% of United States citizens were unbanked.[319] Four years later in 2015, a national survey by the Federal Deposit Insurance Corporation (FDIC) found that 7% of United States households were unbanked.[320] The 2015 survey results demonstrated only a small decrease in unbanked households since the FDIC's 2013 survey, and found that 7.7% of households were unbanked.[321]

Nevertheless, the 2015 survey also asked the unbanked individuals why they do not have bank accounts. The following were respondents most stated reasons: (1) they do not have enough money to keep in a bank account by 57.4% of respondents, (2) avoiding banks provides more privacy by 28.5% of respondents, and (3) they do not trust banks by 28% of respondents.[322]

The government's success in this endeavor is demonstrated by the shrinking numbers of unbanked Americans. However, the desire for financial privacy is demonstrated by the high number of

---

[316] *2009 FDIC National Survey of Unbanked and Underbanked Households*, FED. DEPOSIT INS. COMMISSION, https://www.fdic.gov/householdsurvey/2009/index.html [https://perma.cc/XT6V-Y5CQ]. This survey found that 7.7% of United States houeholds—that is nearly nine-million hosehoulds—did not have checking or savings accounts.

[317] Michael A. Stegman, *Banking the Unbanked: Untapped Market Opportunities for North Carolina's Financial Institutions*, 5 N.C. BANKING INST. 23, 33 (2001) (citing Community Opportunities, Accountability and Training, and Educational Services Act of 1998, Pub. L. No. 105-285, §416, 112 Stat. 2772 (1999)).

[318] THE WORLD BANK, GLOBAL FINANCIAL DEVELOPMENT REPORT 2014: FINANCIAL INCLUSION, 171 tbl. B.1 (2014), http://siteresources.worldbank.org/EXTGLOBALFINREPORT/Resources/8816096-1361888425203/9062080-1364927957721/GFDR-2014_Complete_Report.pdf. [https://perma.cc/B3EZ-HBTW].

[319] BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, CONSUMERS AND MOBILE FIN. SERVICES 2014, 5 (Mar. 2014), http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201403.pdf [https://perma.cc/2SXV-AQVY].

[320] FEDERAL DEPOSIT INSURANCE COMMISSION, 2015 FDIC NATIONAL SURVEY OF UNBANKED AND UNDERBANKED HOUSEHOLDS 1, 11 (Oct. 20, 2016), https://www.fdic.gov/householdsurvey/2015/2015report.pdf [https://perma.cc/S66G-5L6C].

[321] *Id.* at 13.

[322] *Id.* at 3, Fig. ES.2, 20-21, Fig. 3.8.

unbanked individuals reporting that their unbanked status was due to privacy concerns and a lack of trust in banks. Technological advances are allowing these individuals (and even the currently banked) to take advantage of services traditionally provided by banks while foregoing the use of banks and incurring lower fees. The rise of these technologies supports society's reasonable expectation for privacy in banking. Of all these technologices, cryptocurrencies make a particularly strong case.

B. Cryptocurrencies and the Rise Of Privacy Coins

Cryptocurrencies—and the more secrecy-focused "privacy coins"—provide a large degree of anonymity to their users.[323] While critics of cryptocurrencies argue that they are merely a vehicle for illegal activity such as money-laundering, cryptocurrency adopters assert that "embracing privacy and anonymity doesn't mean you're a criminal; it just simply means that you're redeeming your rights to have absolute control over your own privacy.[324] If this is the case, the BSA cannot survive the *Katz* test.

1. Cryptocurrency Technology and Privacy Coins

FinCEN defines "currency" as "the coin and paper money of the United States or of any other country that [i] is designated as legal tender and that [ii] circulates and [iii] is customarily used as a medium of exchange in the country of issuance."[325] Conversely, FinCEN defines "virtual" currency as "a medium of exchange that operates like a currency in some environments but does not have all the attributes of real currency. Virtual currency does not have legal tender status in any jurisdiction."[326] Cryptocurrencies fall under the latter category as they are a type of encrypted, electronic semi-currencies that act as a medium of exchange in a largely anonymous environment. The public's rapidly increasing adoption of cryptocurrencies is a significant sign that individuals want—and in practice, expect—privacy in their financial transactions.

---

[323] Tom Wilson, *Explainer: 'Privacy coin' Monero Offers Near Total Anonymity*, REUTERS (May 14, 2019), https://www.reuters.com/article/us-crypto-currencies-altcoins-explainer/explainer-privacy-coin-monero-offers-near-total-anonymity-idUSKCN1SL0F0 [https://perma.cc/2KG5-59DW].

[324] Aziz, *Guide on Privacy Coins: Comparison of Anonymous Cryptocurrencies*, MASTER THE CRYPTO, https://masterthecrypto.com/privacy-coins-anonymous-cryptocurrencies/ [https://perma.cc/9F97-AK5T].

[325] *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN. CRIMES ENFORCEMENT NETWORK (Mar. 18, 2013), https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering [https://perma.cc/5AY9-8WH9] (quoting 31 CFR § 1010.100(m)).

[326] *Id.*

The first major cryptocurrency introduced to the public was Bitcoin in 2009, and as of 2019, it remains the most valuable cryptocurrency on the market.[327] Bitcoin, like all other cryptocurrencies, is a virtual currency that only exists in electronic form.[328] Cryptocurrencies are unique in that financial transactions are not recorded in a central location, and users' identities are kept anonymous.[329] Rather, the transactions are processed and logged on a decentralized public ledger—many independent computers and servers working in parallel, each keeping a separate, immutable copy of each transaction.[330] These independent computers and servers are incentivized to lending their processing power to this system by having a chance to earn fees for their participation.[331]

On the users' end, cryptocurrency transfers may be made without having to reveal any personally identifiable information.[332] The transactions recorded on the public ledger only include the amounts involved in that transaction and an equivalent of an account number for each party involved.[333] These account numbers are a randomly generated set of numbers and letters—they do not in and of themselves identify the account's owner.[334] However, because the ledger is public, account numbers are available to anyone so inclined to look up a particular account's full history of money sent and received.[335] Thus, a user risks identification by using cryptocurrencies to purchase traceable goods, which then can reveal that users' entire transactional history.[336] Several alternative cryptocurrencies have emerged to solve this identification problem.

Improving upon this privacy, several cryptocurrencies have been developed to ensure anonymity in cryptocurrency-based financial transactions; these cryptocurrencies have earned the moniker "privacy coins."[337] Notable privacy coins include Monero,

---

[327] At the time of writing this sentence, a single Bitcoin was valued at $7,297.80 and had a market cap of approximately $132 billion.

[328] Matthew Kien-Meng Ly, *Coining Bitcoin's "Legal-Bits": Examining The Regulatory Framework For Bitcoin And Virtual Currencies*, 27 HARV. J.L. & TECH. 587, 590 (2014).

[329] *Id.* at 590-93.

[330] *Id.* at 590.

[331] *Id.*

[332] *Id.* at 593.

[333] *Id.*

[334] Wilson, *supra* note 323.

[335] Aaron Mangal*, Privacy Coins – What Are They, How Do They Work and Why Are They Needed*, COIN CENTRAL (Sept. 25, 2017), https://coincentral.com/privacy-coins-what-are-they-how-do-they-work-and-why-are-they-needed/ [https://perma.cc/U7PP-5YB4].

[336] Tyler G. Newby & Ana Razmaza, *An Untraceable Currency? Bitcoin Privacy Concerns*, FINTECH WEEKLY (Apr. 7, 2018), https://www.fintechweekly.com/magazine/articles/an-untraceable-currency-bitcoin-privacy-concerns [https://perma.cc/SA5W-2AJX].

[337] *Id.*

Zcash, Dash, Verge, PIVX, and Hush, each taking advantage of different technologies to shield their users' identities.[338] For example, Monero arguably offers the highest degree of financial anonymity.[339] In a brief explanation of its technologies, Monero uses Ring Confidential Transactions (RCT) and Stealth Addresses to mask the accounts of both senders and receivers as well as the amount involved.[340] RCT anonymizes the identities of senders by comingling a number of senders for any one particular transaction, so it is impossible to distinguish the actual sender for a particular transaction.[341]

Further, RCT hides the actual amount being sent by requiring the sender to transfer more than required and receiving back the excess amount as "change."[342] This is done through "a cryptographic proof that the sum of the input amounts is the same as the sum of the output amounts, without revealing the actual numbers."[343] Finally, the Stealth Address component of Monero works by publishing the sender's side of a transaction on the blockchain—the receiver is not specified.[344] Rather, each transfer is routed to a unique, one-time-use address on the blockchain.[345] A receiver wishing to use the received money gains a one-use private key to identify his or her funds on the public ledger and send them to a new address.[346] This whole process is done without the receiver ever having to publish any information on the publicly-viewable ledger.[347] The technology advanced by Monero is but one example of innovation looking to keep financial transactions private.

2. Cryptocurrencies As A Sign Of Expectations To Privacy In Financial Transactions

While some try, estimating the number of cryptocurrency holders is difficult.[348] Still, the explosive growth of cryptocurrencies in such a short time and on a global scale is a sign that individuals are seeking financial privacy. Certainly, other factors, such as price

---

[338] *Id.*
[339] *Id.*
[340] *Id.*
[341] *Id.*
[342] *Id.*
[343] Aziz, *supra* note 324.
[344] Mangal, *supra* note 335.
[345] Aziz, *supra* note 324.
[346] Mangal, *supra* note 335.
[347] *Id.*
[348] Brandon Hurst*, Here's How Many People Actually Own Bitcoin*, BUS. INSIDER (Mar. 19, 2014), https://www.businessinsider.com/heres-how-many-people-actually-own-bitcoin-2014-3 [https://perma.cc/FZ8K-CVFK].

speculation, have contributed to the rise of cryptocurrencies,[349] but the promise of financial privacy cannot be overlooked—privacy was one of Bitcoin's founding principles after all.[350]

On a global scale, Bitcoin's number of users has drastically increased over the past five years.[351] In January 2015, there were approximately 2.8 million users; by the end of 2019, that number was approaching 50 million.[352] For all types of cryptocurrencies, a 2017 University of Cambridge, Judge Business School study estimated that there are between 2.9 million and 5.8 million unique cryptocurrency users.[353] Yet, even since the release of this study, the number of cryptocurrency users are likely to drastically increase as cryptocurrency exchanges report ever-growing numbers of accounts. After the Cambridge study was released, Coinbase, one of the world's biggest cryptocurrency exchanges, announced that on a single day it saw the registration of 40,000 additional customers.[354] Even ancillary services for cryptocurrencies are emerging. For example, by September 1, 2019, there were 3,571 Bitcoin ATMs located in the United States.[355] Monero has seen gains even more impressive than Bitcoin. In 2016, the price of Bitcoin doubled; that same year, the price of Monero grew by 2,760%.[356]

The trend towards cryptocurrencies is undeniable and there is a proven market for privacy coins. Individuals require banking services, but those services disclose private financial information to the government because of the BSA. If need is the mother of all inventions, the rise of cryptocurrencies shows that society is trying

---

[349] Charles Bovaird, *Why The Cryptocurrency Market Has Reached A New Record High*, FORBES (Aug. 31, 2017), https://www.forbes.com/sites/cbovaird/2017/08/31/why-the-cryptocurrency-market-has-reached-a-new-record-high/#47d818d44038 [https://perma.cc/X69V-Y4ED].

[350] SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM, BITCOIN 6, https://bitcoin.org/bitcoin.pdf [https://perma.cc/27W3-GE35].

[351] *Blockchain Wallet Users,* BLOCKCHAIN, https://www.blockchain.com/en/charts/my-wallet-n-users?timespan=all [https://perma.cc/HVY9-YGT4].

[352] *Id.*

[353] DR. GARRICK HILEMAN & MICHEL RAUCHS, GLOBAL CRYPTOCURRENCY BENCHMARKING STUDY, UNIV. OF CAMBRIDGE: CTR. FOR ALTERNATIVE FIN. 8 (2017), https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-04-20-global-cryptocurrency-benchmarking-study.pdf [https://perma.cc/DN4J-DG45].

[354] *Coinbase CEO Claims the Company Saw 40,000 User in One Day*, NEWS BTC (May 27, 2017), http://www.newsbtc.com/2017/05/27/coinbase-ceo-claims-company-saw-40000-user-registrations-one-day/ [https://perma.cc/2E4Q-MY2N].

[355] M. Szmigiera, *Number of Bitcoin ATMs Worldwide 2020, By Country*, STATISTA (Apr. 2, 2020), https://www.statista.com/statistics/343147/number-of-bitcoin-atms-countries/ [https://perma.cc/3M52-BWFN].

[356] Andy Greenberg, *Monero, The Drug Dealer's Cryptocurrency Of Choice, Is On Fire*, WIRED (Jan. 25, 2017), https://www.wired.com/2017/01/monero-drug-dealers-cryptocurrency-choice-fire/ [https://perma.cc/B4HF-8FEM].

to reclaim financial privacy. Under the *Katz* test, this means that society recognizes financial privacy as reasonable, thus, requiring the BSA conform with Fourth Amendment principles. A foundational principle of the Fourth Amendment is that warrantless searches and seizures are unreasonable. The BSA allows the government to obtain financial information from banks in the absence of a warrant. Accordingly, the BSA violates the Fourth Amendment.

V. CONCLUSION

The Supreme Court should reevaluate the BSA under the Fourth Amendment and provide a robust *Katz*-test analysis. In *Miller*, the Court erroneously reasoned that the BSA's reporting requirements did not violate Fourth Amendment privacy expectations. The court erred by misinterpreting the line of cases creating the third-party doctrine and therefore applied the rule as constructed under the overruled trespass-doctrine. This error has caused the Court to view an individual's disclosure of information to a third party as a bright-line rule: because individuals voluntarily provide information to banks, they forfeit any privacy expectation in that information. Instead, the Court should have given full consideration to the *Katz* test, which allows for the possibility of Fourth Amendment protection over information shared with third parties.

Regardless of the Court's decision in *Miller*, the *Katz* test open parameters provide changing Fourth Amendment protections over time. Applying the *Katz* test to the BSA in the modern era shows that the BSA is unconstitutional. Certainly, society should recognize an individual's privacy expectation in banking information as reasonable. The individual is not strictly "voluntarily" providing that information to his or her bank because the burden of living without a bank account is extreme. Moreover, the rise of cryptocurrencies is an indicator that society expects privacy in banking information. A central vision of cryptocurrencies is user anonymity and autonomy in financial information. Society's desire for anonymity and autonomy excludes its acceptance of the BSA. Therefore, the Supreme Court should take the opportunity to reexamine the BSA and hold that its reporting requirements violate the Fourth Amendment.