OKLAHOMA CITY UNIVERSITY
LAW REVIEW

VOLUME 44 NUMBER 3 SPRING 2020

NOTES

PROTECTING FINANCIAL PRIVACY IN THE FINTECH ERA: A NEW CATEGORY OF FINANCIAL RECORDS THAT DESERVE PROTECTION

Matt Andrus*

I. INTRODUCTION

Technology, as is true with death, waits for no one. Technology is constantly pushing forward regardless of whether society can keep pace. The ever-expanding gap between technology and law is perhaps the starkest reminder of how quickly technology grows and, on the other hand, how slowly the law adapts. While the system of governance in which we live is inherently incompatible with rapid change, the race with technology is nonetheless one the judiciary must run. Perhaps one of the most pressing and evolving forums for the race is that in the context of data privacy in the FinTech era.

Banking itself is nothing new and intriguing; the way in which banking is done, however, is incomparable to when the Continental Congress established the Bank of North America in 1782.[1] Cash is

* Juris Doctor Candidate, Oklahoma City University School of Law, May 2020. First, I would like to thank God for His providence and blessings in my life over these past

arguably no longer king of the wallet—giving way to convenience by way of plastic.[2] In fact, studies have shown that "the share of transactions using cash has fallen steadily in recent years."[3] Cash versus card is only the beginning of the changed landscape—online banking, peer-to-peer lending, blockchain, and bitcoin have all emerged onto the scene. Financial technologies, or FinTech, such as these have driven the banking industry into a rapid revolution—disrupting the way consumers transact their financial needs.[4]

While many of the advancements bring great benefits to consumers, they also may be stripping the consumer of privacy and exposing their financial information. For example, a consumer that once would have simply made a cash payment to a merchant may now choose to swipe her debit card, thereby creating a record that contains the when, where, and how much around the purchase. The Fourth Amendment seeks to protect individuals from unreasonable searches and seizures conducted by the government; however, because of a legal concept called the third-party doctrine, bank records may not be covered since this information is shared with the bank—a third party.[5] A consequential byproduct of the modern banking landscape is the increased quality and quantity of data being shared with third parties. Data collected in the information age is fundamentally different and more revealing than what was collected in

three years and for surrounding me with a supportive and loving family. I'd like to thank my wife for her support, motivation, patience and for being the best mom to our beautiful daughter, Merritt. I would also like to thank my parents for instilling in me a strong work-ethic and a love for education. Thank you to my sister for being my first teacher and holding classes for me before I was old enough to go to school. Special thank you to Professor Greg Eddington for helping me refine my writing and for the guidance and commentary throughout this process. Finally, I would like to thank my friends and law school community for all their prayers and support.

1. FED. DEPOSIT INS. CORP., HISTORICAL TIMELINE (2014), https://www.fdic.gov/about/history/timeline/1700s.html [https://perma.cc/2QJH-2N3E].

2. 2012 Fed. Res. Bank of San Francisco Ann. Rep. at 5. John C. Williams, Case Is Dead! Long Live Cash!, 7 (Fed. Reserve Bank of San Francisco 2012 Annual Report), https://www.frbsf.org/our-district/about/annual-report/annual-report-2012/2012-annual-report-essay-cash-is-dead-long-live-cash/ [https://perma.cc/3UZ6-N5Y7].

3. *Id.* at 10.

4. Daniel Newman, *Exploring 5 Trends Driving the Fintech Revolution*, FORBES (Jul. 3, 2018, 10:16 AM) https://www.forbes.com/sites/danielnewman/2018/07/03/exploring-5-trends-driving-the-fintech-revolution/#636d2c9b12c7 [https://perma.cc/6RY7-SE7C].

5. United States v. Miller, 425 U.S. 435, 443 (1976) (stating there is no expectation of privacy when information is shared with a third party).

past years, thereby providing the government with significant personal information by way of the third-party doctrine.

The question must now be raised as to whether the third-party doctrine remains applicable in the context of modern banking. Recently, the Supreme Court in *Carpenter v. United States* faced a similar question in the context of modern communications.[6] In *Carpenter*, the Supreme Court refused to extend the third-party doctrine into the realm of geolocation technology embedded into cell phones.[7] In doing so, the Court recognized modern technology and the need to reconcile it with historically recognized notions of privacy.[8] It may be well past due to reevaluate the third-party doctrine in the context of modern banking and whether it adequately provides consumers with the notion of privacy as intended by the framers and set forth in the Fourth Amendment.

First, this Note will establish the current legal framework of consumer financial privacy and the judicially created third-party doctrine. It will then explore how, in light of the advancements in technology, modern financial records should be redefined because they are incomparable to those discussed in *United States v. Miller*.[9] Specifically, the argument will be made that modern financial records should follow the recent Supreme Court cases of *United States v. Jones*,[10] *Riley v. California*,[11] and *Carpenter*.[12] Finally, this Note will argue that modern financial records cannot be evaluated by the third-party doctrine, but rather should be analyzed by, and successfully pass, the *Katz v. United States* reasonable expectation of privacy test.

II. FINANCIAL PRIVACY: BANK SECRECY ACT AND THIRD-PARTY DOCTRINE

A. The Bank Secrecy Act

Discussions of financial privacy must begin with the enactment of the Bank Secrecy Act (BSA) in 1970.[13] The purpose of the BSA was

6. *See* Carpenter v. United States, 138 S. Ct. 2206 (2018).
7. *Id*. at 2220.
8. *Id*. at 2220-23.
9. *Miller*, 425 U.S. at 442-43.
10. United States v. Jones, 565 U.S. 400 (2012).
11. Riley v. California, 573 U.S. 373 (2014).
12. *See Carpenter*, 138 S. Ct. at 2206.
13. Dean Galaro, *A Reconsideration of Financial Privacy and* United States v.

centered around the prevention of money laundering and required financial institutions "to generate information helpful in investigating money laundering."[14] The primary method of information generation was through the Currency Transaction Report (CTR).[15] CTRs are required to be completed by financial institutions for transactions involving more than $10,000.[16] The legislature extended the reporting requirements of financial institutions through the enactment of the Money Laundering Control Act in 1986[17] and the Annunzio-Wylie Anti-Money Laundering Act.[18] Importantly, the Annunzio-Wylie Anti-Money Laundering Act created an additional obligation for financial institutions to file a Suspicious Activity Report (SAR) upon activity deemed suspicious by the institution.[19]

In 1974, only four years after the enactment of the BSA, the plaintiffs in *California Bankers Association v. Shultz* challenged the constitutionality of the BSA's recordkeeping and reporting requirements.[20] The challenge was brought by individual depositors and financial institutions, among others.[21] Ultimately, the Court upheld the BSA's requirements pertaining to financial institutions[22] finding that an institution could not maintain the same level of Fourth Amendment protection as an individual.[23] Additionally, the Court noted the regulations as reasonable and particularized to only "abnormally large transactions in currency."[24] However, the Court refused to address the question of whether the BSA infringes on the privacy rights of individual depositors because no depositor had suffered any harm, and the Court was unwilling to assume that because someone is a depositor at a bank, they will engage in a transaction requiring reporting and, therefore, be

Miller, 59 S. TEX. L. REV. 31, 34 (2017).

14. *Id.* at 34-35.
15. *Id*. at 35.
16. 31 C.F.R. § 1010.311 (2017).
17. *See generally* 18 U.S.C. §§ 1956-57 (2012) (The Money Laundering Control Act criminalized the structuring of financial transactions done by the consumer with the purpose of avoiding the filing of a CTR).
18. Galaro, *supra* note 13, at 35.
19. *Id.*
20. California Bankers Ass'n v. Shultz, 416 U.S. 21, 37 (1974).
21. *Id*. at 41.
22. *Id*. at 54.
23. *Id.* at 65.
24. *Id.* at 67.

imminently harmed in the future.[25] With no standing for individual depositors, the Court did not discuss the Fourth Amendment in the context of an individual.[26] This question was left unresolved until 1976 when *United States v. Miller* reached the Supreme Court.

B. Miller *and the Establishment of the Third-Party Doctrine*

Before discussing *Miller*, it is important to outline the history of the third-party doctrine. The concept of the third-party doctrine began with *Katz v. United States*. In *Katz*, the Supreme Court decided that evidence obtained "by FBI agents who had attached an electronic listening and recording device to the outside of the public telephone booth from which [Katz] had placed his calls"[27] was unconstitutionally obtained.[28] In his concurrence, Justice Harlan set forth his view that there is a two-part test as to how the Constitution should be interpreted in regard to the government's access to private communications[29]: "My 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.'"[30] After *Katz*, "courts have analyzed whether defendants have had a 'reasonable expectation of privacy' in information or things."[31] The Court in *Miller* extended this analysis outside the realm of the government obtaining personal communications and into the realm of government oversight of an individual's financial information.

In *Miller*, Defendant Mitchell Miller was convicted of several crimes including the possession of 175 gallons of untaxed whiskey.[32] The prosecutor attempted to introduce as evidence checks and other bank records that had been maintained by the banks pursuant to the BSA.[33]

25. *Id.* at 68.
26. Galaro, *supra* note 13, at 38.
27. Katz v. United States, 389 U.S. 347, 348 (1967).
28. *Id.* at 359.
29. Jim Harper, *A Twenty-First Century Framework for Digital Privacy: Balancing Privacy and Security in the Digital Age*, 3 (Nat'l Const. Ctr., White Paper Series), https://constitutioncenter.org/digital-privacy/The-Fourth-Amendment-in-the-Digital-Age#footnote-1 [https://perma.cc/A77U-M6JL].
30. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).
31. Harper, *supra* note 29, at 1-3.
32. United States v. Miller, 425 U.S. 435, 436 (1976).
33. *Id.* at 436.

Miller moved to suppress these records on the basis that the subpoena used to collect the information was defective.[34] The United States Court of Appeals for the Fifth Circuit agreed with Miller, finding that "a depositor's Fourth Amendment rights are violated when bank records maintained pursuant to the Bank Secrecy Act are obtained by means of a defective subpoena."[35] In recognizing the need for a valid subpoena to access an individual's checks and other bank records, the Fifth Circuit established that these personal financial records were indeed worthy of Fourth Amendment protections. The Supreme Court, however, found that Miller "had no protectable Fourth Amendment interest in the subpoenaed documents . . . ."[36]

In the Supreme Court's analysis, the issue of whether the subpoena was defective was regarded as irrelevant.[37] The Court held there can be no Fourth Amendment violation because bank records are not within a "protected zone of privacy"; therefore, there is no need for a warrant.[38]

In concluding that bank records were outside of the "protected zone of privacy," the Court first applied the "reasonable expectation of privacy" test as established in *Katz*.[39] Miller argued that he maintained a subjective and reasonable expectation of Fourth Amendment privacy protection for his bank records because "they are merely copies of personal records that were made available to the banks for a limited purpose."[40] Although the Court did recognize that a government's search and seizure may be found unreasonable when it violates "the privacy upon which (a person) justifiably relie[s,]"[41] it also stressed that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[42] Therefore, in denying Miller's financial information any Fourth Amendment protection, the Court entirely rejected the notion that the bank records are the depositor's "private papers"[43] that carry a justifiable reliance of privacy and held instead that

34. *Id.* at 437.
35. *Id.*
36. *Id.*
37. *Id*.
38. *Id.* at 440 (citing Hoffa v. United States, 385 U.S. 293, 301-02 (1966)).
39. *Id.* at 442.
40. *Id.*
41. *Id.* (quoting Katz v. United States, 389 U.S. 347, 353 (1967) (alterations in original)).
42. *Id*. (quoting *Katz*, 389 U.S. at 351).
43. *Id*. at 440.

"the business records of the banks" are voluntarily exposed to the public.[44]

In reaching the conclusion that a depositor does not maintain a subjective reasonable expectation of privacy, the Court analyzed the "nature of the particular documents sought" to determine if the documents were indeed protected by the Fourth Amendment.[45] The Court found the checks that were obtained could not have a legitimate expectation of privacy because they were "not confidential communications but negotiable instruments to be used in commercial transactions[, a]ll of the documents obtained, including financial statements and deposit slips contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[46] The Court concluded Miller maintained no reasonable expectation of privacy because the documents contained only information that was voluntarily shared—failing the first prong of the *Katz* test.[47]

The Court then analyzed the second prong of the *Katz* test—whether society is ready to recognize an expectation of privacy in financial information as reasonable.[48] The Court found in the negative, holding that "any legitimate expectation of privacy concerning the information kept in bank records was assumed by Congress in enacting the Bank Secrecy Act."[49] This loss of Fourth Amendment protections due to the sharing of financial information with a third party became known as the third-party doctrine.

In his dissent, Justice Brennan advocated for many of the arguments in favor of financial privacy that are still made today. First, he argued that an individual's disclosure of financial information is not entirely volitional because of the necessity of a bank account for the participation in economic life.[50] As will be discussed below, the concept of voluntary disclosure should be viewed in an even dimmer light in the context of the modern economy. Second, he recognized that financial transactions "can reveal much about a person's activities, associations, and beliefs" and

44. *Id*.
45. *Id.* at 442.
46. *Id*.
47. *Id.* at 443.
48. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
49. *Miller*, 425 U.S. at 442.
50. *Id.* at 447 n.1 (Brennan, J., dissenting) (comparing Couch v. United States, 409 U.S. 322 (1973) with California Bankers Assn. v. Shultz, 416 U.S. 21, 52-54 (1974)).

that "[a]t some point, governmental intrusion upon these areas would implicate legitimate expectations of privacy."[51] The argument made today is that this point has been reached.

Aside from bank records and financial transactions, the Supreme Court has recognized the third-party doctrine in other contexts. For example, in *Smith v. Maryland*, the Supreme Court found the installation and use of a pen register on petitioner's phone without a warrant did not violate the Fourth Amendment.[52] Writing the opinion of the Court, Justice Blackmun reasoned that because telephone users willingly share the numbers they dial with the phone company, and these users know the phone company has permanent records of the numbers they dial, the users in general cannot "entertain any actual expectation of privacy in the numbers they dial."[53] In *Smith*, the Court found, "even if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation [was] not 'one that society is prepared to recognize as reasonable.'"[54] This argument of society having no expectation of privacy in whom they contact with their private phones was arguable at the time of the decision[55] and is perhaps a weaker argument now given the amount of information that can be exposed through phone records.

C. A Response to Miller*: The Right to Financial Privacy Act of 1978*

The decision in *Miller* caused a significantly negative reaction.[56] Aside from his dissent, Justice Brennan also voiced his displeasure with *Miller* and the decision's deterioration of due process and equal protection under the Bill of Rights in his 1977 Harvard Law Review article titled *State Constitutions and the Protection of Individual Rights.*[57]

51. *Id.* at 453 (Brennan, J., dissenting) (quoting Burrows v. Superior Court, 529 P.2d 590, 595 (Cal. 1974) (en banc)).

52. Smith v. Maryland, 442 U.S. 735, 742-43 (1979).

53. *Id*.

54. *Id.* at 743 (quoting Katz v. United States, 389 U.S. 347, 361 (Harlan, J., concurring)) (internal quotation marks omitted).

55. *Id.* at 748 (Stewart, J., dissenting) ("I doubt there are any who would be happy to have broadcast to the world a list of local or long distance numbers they have called. This is not because such a list might in some sense be incriminating, but because it easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life.").

56. Galaro, *supra* note 13, at 40.

57. *Id.* at 40. *See generally* William J. Brennan, Jr., *State Constitutions and the*

Furthermore, in 1979, Judge Hufstedler of the Ninth Circuit voiced her concern that after *Miller*, using a bank now means assuming the risk of government surveillance.[58] Given the disunion between *Miller* and the technologically modern world recognized in the years after *Miller*, it seems obvious how much more archaic *Miller* and the third-party doctrine is in today's data-filled financial landscape.[59]

Attacks on *Miller* also came from outside of academia as Congress responded directly to the holding with the enactment of the Right to Financial Privacy Act of 1978 (RFPA).[60] The RFPA was enacted to provide customers with a reasonable amount of privacy in their financial records held by their financial institutions.[61] The RFPA generally requires that the government first obtain either authorization from the customer, an administrative subpoena or summons, a search warrant, judicial subpoena, or a formal written request by the government agency.

While intentions of the RFPA were centered around the privacy of consumers' information, the application falls short of the intentions. Several exceptions found in the RFPA leave the consumer with minimal protection:

> (1) disclosures that do not identify a particular customer; (2) disclosures that benefit the financial institution, including its security interests, government loans, and other disclosures relevant to possible violations of the law; (3) disclosures in connection with supervisory investigations and proceedings; (4) disclosures under the tax privacy provisions; (5) disclosures pursuant to other federal statutes or rules, administrative or judicial proceedings, and legitimate functions of supervisory agencies; and (6) emergency disclosures and disclosure to federal agencies charged with foreign intelligence or counter

Protection of Individual Rights, 90 HARV. L. REV. 489, 495-97 (1977).

58. Galaro, *supra* note 13, at 40 n.75 (citing Shirling M. Hufstedler, *Invisible Searches for Intangible Things: Regulation of Governmental Information Gathering*, 127 U. PA. L. REV. 1483, 1504-05 (1979)).

59. *See* Robert S. Peck, *Extending the Constitutional Right to Privacy in the New Technological Age*, 12 HOFSTRA L. REV. 893, 907 (1984) (recognizing the *Miller* decision as "illustrat[ing] the judicial reluctance to expand the privacy to modern needs").16.4, 1]

60. Galaro, *supra* note 13, at 43.

61. Fed. Reserve Bd., Right to Financial Privacy Act (Jan. 2006), https://www.federalreserve.gov/boarddocs/supmanual/cch/priv.pdf [https://perma.cc/2TDW-X9GZ].

intelligence or other national security protective functions.[62]

Most alarming to FinTech customers is the exception for disclosures in accordance with any federal statute.[63] This exception permits both the BSA and *Miller* to allow financial institutions to disclose its users' financial data outside of the protections afforded by the RFPA.[64]

The RFPA is also weakened by more recent legislation such as the PATRIOT Act. As a direct response to the 9/11 terrorist attacks, the government enacted the PATRIOT Act which increased the recordkeeping and reporting requirements for financial institutions.[65] Presumably, this too would fall under the exception for disclosure in accordance with any federal statute and leave customer information outside the RFPA. These inherent exceptions have rendered legislators' attempts to curtail the impact of *Miller* as largely ineffective.

III. TREND TOWARD PROTECTION: RECOGNITION OF DIGITAL AGE REQUIRING DIFFERENT ANALYSIS

Recently, the Supreme Court has decided three cases that provide grounds for an argument in favor of the proposition that modern financial records require Fourth Amendment protections. Although these cases have not dealt directly with the financial records, they provide the beginnings of a framework for how the Court will analyze Fourth Amendment cases in the digital age.

A. United States v. Jones

First, in *United States v. Jones*, the Court was faced with the issue of "whether the attachment of a Global-Positioning-System (GPS) tracking device to an individual's vehicle, and subsequent use of that device to monitor the vehicle's movements on public streets, constitutes a search or seizure within the meaning of the Fourth Amendment."[66] Justice Scalia delivered the holding for the Court stating "the Government's

62. Dina Moussa, *Protecting Privacy in Our Financial Transactions: An Alternative Method to Thinking About Our Privacy in the Digital Era*, 1 GEO. L. TECH. REV. 342, 360 (2017).
63. *Id.*
64. *Id.*
65. Galaro, *supra* note 13, at 44.
66. United States v. Jones, 565 U.S. 400, 402 (2012).

installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'"[67]

There are three key points from *Jones* that can transfer into the realm of financial records. First, the holding established *Katz* extended Fourth Amendment protections beyond the exclusively property-based approach.[68] This is a key factor for financial privacy because it re-establishes the argument that financial records, although a business record of the bank, should be protected because "the Fourth Amendment protects people, not places."[69]

Second, in their separate concurring opinions, Justice Sotomayor and Justice Alito noted that advancement in technologies will affect the *Katz* test by shaping the evolution of societal privacy expectations.[70] As more people become aware that the government can essentially store or access copious amounts of personal records, the societal expectation of privacy will change.[71] In *Jones*, it was the Government's use of GPS—a technological form of physically trailing a suspect.

In the context of financial information, it could be the difference between writing a check or swiping a card. In either case, an argument can be made that technology has altered the scenario and therefore has altered the societal expectation of privacy. Society would likely view the government obtaining this kind of financial record—where you swiped your debit card, when you were at the location making the purchase, and for how much—as worthy of more reasonable privacy expectations than a copy of a check written to your landlord.

Finally, Justice Sotomayor proposed, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[72] She continued that, "[t]his approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[73] The third-party doctrine was created around the assumption that because one shares their information with a third party, they cannot be said to maintain an

67. *Id.* at 404.
68. *Id.* at 405-06.
69. Katz v. United States, 389 U.S. 347, 351 (1967).
70. *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring).
71. *Id.*
72. *Id.*
73. *Id.*

expectation of privacy.[74] The discussion that the sharing of financial information can no longer be deemed *voluntary* is discussed below.[75] Here, it suffices to say that banking is so entrenched into our economy and households that it is no longer, assuming that it ever was, a voluntary practice.

B. Riley v. California

Second, in *Riley v. California*, the Court addressed "whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested."[76] The Court found that a warrant was required because the information accessible through one's cell phone is both quantitatively and qualitatively different than the information available in a search of other items that may be kept on an arrestee's person.[77]

In addressing the qualitative difference, the Court acknowledged the privacy concerns implicated by a modern cell phone's ability to store vast amounts of data is simply not present with the search of a cigarette pack, a wallet, or even a purse.[78] The Court found that cell phones were more of a miniature computer than merely a phone; therefore, a search of a modern cell phone is more akin to the search of a person's camera, rolodex, personal calendar, tape recordings, library history, diary, album collection, television history, maps of places traveled, or preferred newspapers.[79] Making all of this information available in a handheld device broadens the risk of an intrusion into one's sphere of privacy.[80] Indeed, the storage capacity on a modern cell phone allows a person to carry around every piece of mail, every picture taken, and every book or article read.[81] Because of the immense amount of available storage, law enforcement is no longer limited to physical search limitations that previously protected individuals.

The increased storage capacity of cell phones was found to have

74. United States v. Miller, 425 U.S. 435, 443 (1976). *See also* Smith v. Maryland, 442 U.S. 735, 742 (1999).
75. *See* discussion *infra* Section IV.
76. Riley v. California, 573 U.S. 373, 378 (2014).
77. *Id.* at 393.
78. *Id.*
79. *Id*.
80. *Id.*
81. *Id.*

"several interrelated consequences for privacy."[82] First, the cell phone will allow for the collection of several distinct types of information from one location.[83] Second, a single type of information will be able to convey much more than previously possible.[84] Third, the cell phone can create a full history back to the date the cell phone was purchased.[85] Finally, as discussed above, an element of pervasiveness is presented by cell phones that is not present with physical records.[86]

Aside from the quantity of data accessible on cell phones, the Court also distinguished physical records from cell phone data as qualitatively different.[87] A cell phone often contains an internet search and browsing history that may reveal data otherwise thought of as private, such as a recent search of medical symptoms.[88] A cell phone may also reveal a history of a person's location that can be used to reconstruct someone's specific movements.[89] Cell phones often contain applications specifically selected by the owner that can provide law enforcement with an array of information such as a person's political party affiliation, past medical history, religious affiliations, family planning, financial planning, and many other uniquely revealing identifiers.[90]

Riley signifies an important step in the Court's recognition of the privacy concerns implicated by the digital age. The Court's recognition that cell phone data is quantitatively and qualitatively different shows the Court's understanding of the increased risk technology has become to an individual's privacy. This recognition should extend into the realm of financial records. As will become apparent below in section IV, the quantity and quality of data available in a cell phone is not unreasonably different from the data modern financial records may reveal. The way in which the data is handled, however, is unreasonably different. In *Riley*, the Court required a warrant before the information would be accessible

82. *Id*. at 394.
83. *Id.*
84. *Id.* ("The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet.").
85. *Id*. at 394-95 ("A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.").
86. *Id.* at 395.
87. *Id.*
88. *Id*.
89. *Id.* at 396.
90. *Id*.

to law enforcement.[91] On the other hand, because of *Miller*, financial records are completely outside the scope of the Fourth Amendment.

C. Carpenter v. United States

The Court's most recent decision regarding the third-party doctrine is *Carpenter v. United States*. The opinion issued in *Carpenter* has several implications, including perhaps the signaling of the beginning of the end for the third-party doctrine. Although *Carpenter* is a narrow decision, and more a progeny of *Smith* than *Miller*, the implications of the Court's decision seem to attack the third-party doctrine as a whole.

In *Carpenter*, law enforcement suspected Defendant, Timothy Carpenter, of participating in several robberies in the Detroit area.[92] Police obtained cell-site location information (CSLI)[93] from Carpenter's cell-service provider as a means of showing that Carpenter was in the vicinity when the robberies took place.[94] In doing so, "the Government obtained 12,898 location points cataloging Carpenter's movements—an average of 101 data points per day."[95] Carpenter was ultimately charged with "six counts of robbery and an additional six counts of carrying a firearm during a federal crime of violence."[96] Before trial began, Carpenter moved to suppress the location information provided to law enforcement from his cell-service provider.[97]

The issue for the Court was whether Carpenter maintained a legitimate expectation of privacy under the Fourth Amendment in his physical movements recorded as CSLI. The Sixth Circuit relied on the third-party doctrine in finding that Carpenter had no reasonable expectation of privacy in his location data because he voluntarily revealed this information to a third party—his cell-service provider.[98] The Supreme Court overturned this ruling and "decline[d] to extend

91. *Id.* at 403.
92. Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).
93. *Id.* at 2211-12 (Cell phones are continually searching for a signal. In doing so, the cell phone is continuously updating the service provider of location information that the service provider then stores for business purposes.).
94. *Id*. at 2212.
95. *Id.*
96. *Id.*
97. *Id.*
98. *Id*.

Smith and *Miller* to the collection of CSLI."[99]

The Court began its analysis by setting the case in the historical purpose of the Fourth Amendment and the Court's role in preserving the right to privacy in this technological era.[100] The expansion of technology was recognized by the Court as "enhanc[ing] the Government's capacity to encroach upon areas normally guarded from inquisitive eyes."[101] Indeed, many of the Fourth Amendment issues facing the Court today could not have been imagined at the time of the Fourth Amendment's drafting. In *Carpenter*, the Court acknowledged that "when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements."[102] Recognizing CSLI as a new technology, the Court declined to mechanically lump it in with *Smith* or *Miller* and evaluated it as a new category of information.[103] In doing so, the Court found that two fundamental principles of the third-party doctrine could not be extended into the modern data context of CSLI.

First, the Court held CSLI data is fundamentally different from the information at issue in *Smith* and *Miller*. When the Court compared CSLI to the phone records of *Smith* and the bank records of *Miller*, it held that CSLI was a "qualitatively different category"[104] of information because "cell phone location information is detailed, encyclopedic, and effortlessly compiled."[105] Additionally, the negotiable instruments of *Miller* and the telephone call logs of *Smith* were found to have self-limiting capabilities because of the minimal personal information they actual reveal.[106] CSLI in *Carpenter*, however, contains no comparable limitations on the information it can reveal.[107]

Second, the Court found "the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."[108] The Court recognized that activities

99. *Id.* at 2220.
100. *Id.* at 2214.
101. *Id.*
102. *Id*. at 2217.
103. *Id.* at 2214-15.
104. *Id*. at 2216-17.
105. *Id.* at 2216.
106. *Id.* at 2219.
107. *Id.*
108. *Id*. at 2217.

entrenched into society inherently negate the volunteerism that is assumed by the third-party doctrine.[109] Because cell phones have become so pervasive and insistent in society, "[c]ell phone location information is not truly 'shared' as one normally understands the term."[110] Therefore, CSLI was found not to satisfy the voluntary exposure rationale underlying the third-party doctrine.[111]

These two principles from *Carpenter* also hold true beyond CSLI and into the context of modern financial information. As will be made clear, modern financial information is a new category apart from *Miller* and *Smith*, and the necessity of modern banking negates the voluntary exposure rationale behind the third-party doctrine.

IV. A NEW CATEGORY: MODERN FINANCIAL INFORMATION IS SIMILAR TO *CARPENTER* AND SHOULD NOT BE SUBJECT TO THE THIRD-PARTY DOCTRINE OF *MILLER*.

Justice Kennedy, in his dissent, made clear that the logic of many of the key decisions made by the majority in *Carpenter* could also be extended to financial information. He recognized "[t]he troves of intimate information the Government can and does obtain using financial records . . . dwarfs what can be gathered from cell-site records" and that "[b]anks and credit card companies keep a comprehensive account of almost every transaction an individual makes on a daily basis."[112] Simply put, the modern financial information is fundamentally different from the bank records at issue in *Miller*, and the entrenchment of banking into our society negates the notion of voluntary sharing. Therefore, the consumer can show a subjective and reasonable expectation of privacy that society is ready to accept as reasonable.

As long as *Katz* is good law, financial information must be found to carry a reasonable expectation of privacy before it can be deemed protected under the Fourth Amendment. Financial information failed this test in *Miller*, but with the Supreme Court's ruling in *Carpenter* and the technological changes that have taken place since, the issue may be ripe for judicial review.

109. *Id.* at 2220.
110. *Id*.
111. *Id.*
112. *Id.* at 2232 (Kennedy, J., dissenting).

A. Modern financial information is fundamentally different than the bank records discussed in Miller.

In *Carpenter*, the Court recognized that as technology advances and the information obtained enhances, the Court's role is to recognize this change and "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[113] In doing so, the Court found the information in CSLI is qualitatively different from the information in *Miller* and *Smith*,[114] but the rationale of the holding blurred the line between cell-site location and financial records.[115] In his dissent, Justice Kennedy found the majority's opinion "illogical" in respects to the Government being able to:

> acquire a record of every credit card purchase . . . over months or years without upsetting a legitimate expectation of privacy . . . [b]ut . . . crosses a constitutional line when it obtains a court's approval to issue a subpoena for more than six days of cell-site records in order to determine whether a person was within several hundred city blocks of a crime scene.[116]

The Court may soon face the issue of reconciling the blurred line between *Carpenter* and financial records. The decision will be whether modern financial information continues down the path of *Miller* and falls unprotected, or perhaps is more similar to *Carpenter* and receives protection. In deciding, the Court should re-evaluate what financial records actually are in modern society. The analysis will reveal that, like the difference between a pen register in *Smith* and the CSLI in *Carpenter*, the bank records at issue in *Miller* are fundamentally different from the financial records of today.

1. Continual Location Tracking

The information at issue in *Carpenter* is not so dissimilar than the information obtained by financial institutions today. In *Carpenter*, the Court found issue with the fact that the location tracking continually runs

113. *Id*. at 2214 (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001) (majority opinion).
114. *Id*. at 2220.
115. *Id.* at 2224 (Kennedy, J., dissenting).
116. *Id.*

against everyone regardless of whether any suspicion exists and that the "[g]overnment can now travel back in time to retrace a person's whereabouts . . . ."[117] The *Carpenter* Court realized the "seismic shifts in digital technology" and the "world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information" collected today.[118] Although no reasonable expectation of privacy was found in *Miller* and *Smith*, the fundamental difference in the information led the Court to conclude "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI."[119]

Modern financial records include tracking information similar to the CSLI data in *Carpenter*. When a person swipes their card at a point of sale, the bank immediately records when and where that sale took place.[120] In some respects, this information is more intrusive than CLSI because, instead of placing a suspect "within a wedge-shaped sector ranging from one-eighth to four square miles[,]"[121] financial transactions are detailed down to the specific store and exact time.[122] Therefore, the holding that "when the Government accessed CSLI from the wireless carriers, [they] invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements"[123] can logically extend to bank records that may also retrospectively reveal an individual's physical movements. For example, in April 2018, law enforcement around the country were trying to track down suspected murderer Lois Riess.[124] Reiss was charged with murdering her husband in Minnesota and 59-year-old Pamela Hutchinson in Florida.[125] After the Florida killing, Reiss took off with Hutchison's credit card.[126] Authorities were able to track

117. *Id*. at 2218.
118. *Id.* at 2210.
119. *Id.* at 2217.
120. Consumer.gov, *Using Debit Cards*, https://www.consumer.gov/articles/1004-using-debit-cards#!what-to-know (last visited Jan. 31, 2020) [https://perma.cc/T4F7-EDC8].
121. *Carpenter*, 138 S. Ct. at 2218.
122. Consumer.gov, *supra* note 120.
123. *Carpenter*, 138 S. Ct. at 2219.
124. John Egan, *How Credit Cards Can Lead Law Officers to Criminals*, (Sept. 18, 2018), https://www.creditcards.com/credit-card-news/credit-cards-track-criminals.php [https://perma.cc/Z8ZZ-9PFZ].
125. *Id.*
126. *Id.*

Reiss after she used Hutchison's credit card to pay for a hotel room.[127] A private investigator familiar with the use of credit card data as a means of tracking individual's movements acknowledged that "[w]hen you're paying for something, you're leaving a trail, you're leaving tracks."[128] In essence, technology has transformed financial records into a category of information that communicates almost a complete locational track to law enforcement.

Moreover, law enforcement agencies have obtained "hot watch" orders to coordinate directly with financial institutions "to monitor in real-time the ongoing and future bank transactions involving customer accounts, including date, time and location of such transactions."[129] The discovery of the use of hot watch orders began when a United States District Attorney from New York's Eastern District argued in a court filing that because the government permits law enforcement officials to secretly spy on American's financial transactions, it should also be able to have the same secretive access to people's cell phone location records.[130] In effect, this argument exposed that the government had been covertly spying on American's financial transactions and quickly caught the attention of privacy experts.[131] One expert, Christopher Soghoian, filed a Freedom of Information Act (FOIA) Request to learn more.[132] One and a half years went by before the FOIA Request was granted, and the Department of Justice (DOJ) released a ten-page document outlining law enforcement's guidelines for spying on American's financial transactions.[133] The document revealed that the government was using this hot watch order to track real-time activity on American's credit and debit card transactions without obtaining a warrant and without the individual's knowledge.[134]

127. *Id.*

128. *Id.*

129. Craig Denney and Carrie Parker, Snell & Wilmer L.L.P., *Bankers Beware of So-Called "Hotwatch" Orders—Are They Even Legal?*, A.B.A. SEC. CRIM. JUST. W.C.C. COMM., Winter/Spring 2015, at 1.

130. Tim Chen, *Is the Government Tracking Your Credit Card Purchases?*, (Jan. 26, 2011, 3:10 PM), https://www.forbes.com/sites/moneybuilder/2011/01/26/is-the-government-tracking-your-credit-card-purchases/#69f1c66f6701 [https://perma.cc/L9LV-VDRW]. *See also* Brief of U.S. Attorney, *In re Application of the U.S. for an Order* (1), 396 F. Supp. 2d 294 (E.D.N.Y. 2005) (No. 2:05-mj-01093-JO).

131. *Id*.

132. *Id.*

133. *Id.*

134. *Id.* (Hotwatch is also used to watch real time activity of airline and hotel

In December 2010, the DOJ revealed details of the practice of federal law enforcement agencies obtaining credit cards, member cards, and travel reservations in real-time surveillance without a warrant.[135] The released presentation outlined the methods of how to obtain a hot watch order.[136] These methods, listed in preferential order, are: (1) obtain an administrative subpoena with a court order for non-disclosure; (2) obtain an administrative subpoena with Ex Parte Order to allow for a 90-day delay of notice; (3) obtain a search warrant; and (4) grand jury subpoena for past records only.[137] Once the preferred administrative subpoena is obtained, the steps used to initiate real-time tracking are simply: (1) contact the credit card security department; and (2) send the administrative subpoena with court order for non-disclosure.[138]

The simplistic process to obtain such intrusive records seems starkly anti-ethical to the founding fathers' desires of ensuring individual privacy with the Fourth Amendment; therefore, hot watch orders seem to stand on shaky legal ground. Hot watch orders have been purported to rely on federal statutes for wiretaps, pen registers, trap and trace devices, and section 1651 of the All Writs Act.[139] Wiretap and Stored Communication statutes are inapplicable to the hot watch orders because of the heavier burden of detail required in Title III electronic surveillance orders and the fact that financial institutions simply are not electronic communication service providers.[140] Federal statutes for pen register and trap-and-trace devices are written for use on telephone calls and allow only for the collection of information related to times and numbers of calls made and received.[141] In the U.S. Attorney's brief that exposed the hot watch scheme, the attorney claimed the hot watch orders were granted pursuant to the All Writs Act.[142] The All Writs Act states that

reservations, cell phone calls, and rental car activities.).

135. U.S. Dept. of Just., PowerPoint Presentation on Hotwatch Surveillance Orders of Credit Card Transactions (Dec. 2, 2010), http://www.scribd.com/doc/44542244/DOJ-powerpoint-presentation-on-Hotwatch-surveillance-orders-of-credit-card-transactions [https://perma.cc/3TN6-NMGW]. *See also* Brian Davis, Abstract, *Prying Eyes: How Government Access to Third-Party Tracking Data May Be Impacted* United States v. Jones, 46 NEW ENG. L. REV. 843, 851-52 (2012).

136. *Id*.

137. *Id*.

138. *Id.*

139. Denney and Parker, *supra* note 129, at 2.

140. *Id.* at 3.

141. *Id.*

142. Brief of U.S. Attorney, *supra* note 130.

federal courts may "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[143] Federal courts have begun to rely on the All Writs Act for the authority to compel technology companies to provide them with information.[144] For example, the American Civil Liberties Union (ACLU) found the government had used the "All Writs Act at least 63 times to compel tech companies to assist in accessing information on locked smartphones."[145] The most well-known instance is the fight between the FBI and Apple for access to the locked cell phone of one of the San Bernardino terrorists in 2015.[146] The FBI eventually dropped the case after finding an alternative way into the phone, but the high-profile case brought attention to the government's use of the All Writs Act.[147]

Although no court has directly addressed the legality of the hot watch orders under the All Writs Act,[148] it is hard to reconcile the legality of ongoing real-time surveillance of financial transactions with a mere administrative subpoena with the Court's ruling in *Carpenter*. Furthermore, the records obtained through hot watch orders are categorically different from those at issue in *Miller* and are taken without the ordinary checks and constraints for abusive law enforcement practices.

2. Personal Information

Modern banks collect data for two main reasons: first, to comply with government regulations and, second, as a means of business survival.[149] The latter reason has drastically increased the type and amount of information the bank gathers on its customers.[150] Banks obtain

143. 28 U.S.C. § 1651(a) (2012).

144. Elizabeth Weise, *ACLU Finds More Than 63 Uses of All Writs Act*, (Mar. 30, 2016, 4:25 p.m.), https://www.usatoday.com/story/tech/news/2016/03/30/aclu-finds-close-100-uses-all-writs-act/82437408/ [https://perma.cc/GBC5-YGXQ].

145. *Id.*

146. *Id.*

147. *Id.*

148. *In re Application of the United States*, 396 F. Supp. 2d. 294, 326 n.24 (E.D.N.Y. 2005).

149. Steven Lewis, *For Banks, Customer Data Is the New King*, RETAIL BANKER INT'L (Sept. 2013), https://www.ey.com/Publication/vwLUAssets/EY_-_The_upside_of_compliance/$FILE/EY-The-upside-of-compliance-Steven-Lewis.pdf [https://perma.cc/3V5K-RTH9].

150. *Id.*

personal information beyond simple debits and credits in order to stay afloat in the information-driven business environment.[151] The days of the teller asking whether you would like to open an additional savings account are over; instead, the bank now studies you to determine what you need without asking. Banks are now able to create a behavioral profile for each customer that "continuously studies [the customer's] quirks and idiosyncrasies, learning where, when and how much [the customer] spend[s]."[152] "For example, asking behavioral questions about a new customer's future plans—funding a college education or buying a home—can help a bank design and sell more targeted products."[153] Banks can collect employment information, asset information and even the level of your investment experience.[154] Banks recognize that the "reams of data" provided by the customer can help the bank create a "front-to-back view of each customer."[155] A front-to-back view that may also be available to law enforcement without the protections of a warrant.

The online financial platform Mint provides consumers with the ability to consolidate all their financial information into a single platform.[156] Mint allows consumers to track bills, create budgets, pull their own credit, and even link their bank accounts to the site for a single point of access.[157] While convenient, this platform may, unbeknownst to the consumer, be providing law enforcement with a single point of entry into a complete view of their financial life. This single port of entry into a vast amount of financial information is similar to the enhancements in modern cell phones that was found in *Riley*, and discussed above, as increasing the pervasiveness of the search.

Obtaining this full-customer view allows banks to predict customer's needs and market directly to those needs. It also helps to counter-act

151. *U.S. Consumer Policy Notice*, BANK OF AM. (Jan. 2018), https://www.bankofamerica.com/content/documents/privacy/us-consumer-privacy-notice-en.pdf [https://perma.cc/F7TD-V44E]. ("All financial companies need to share customers' personal information to run their everyday business.").

152. Jeremy Olshan, *How My Bank Tracked Me to Catch a Thief: Inside the Secret 'Signature' File that Banks Keep on Every Customer*, MARKET WATCH (Apr. 18, 2015 8:00 a.m.), https://www.marketwatch.com/story/how-my-bank-tracked-me-to-catch-a-thief-2015-04-14 [https://perma.cc/3EMQ-6AV7].

153. Lewis, *supra* note 149.

154. U.S. Consumer Policy Notice, *supra* note 151.

155. Lewis, *supra* note 149.

156. *See It's All Coming Together*, INTUIT MINT, https://www.mint.com [https://perma.cc/EK4N-W8DF] (last visited Jan. 31, 2020).

157. *See id.*

fraud by tracking spending patterns and alerting the customer to possible fraudulent transactions that take place outside of that spending pattern.[158] But what if the government wanted to obtain this detailed personal information? Is the government able to obtain information that I created, such as a budget goal for a vacation to the Bahamas through my bank's online banking feature? What if law enforcement wanted to use my proposed trip to the Bahamas against me? Can that be classified as a financial record—placing it under the precedent of *Miller*? It very well could. The RFPA defines a financial record broadly as "an original of, a copy of, or information known to have been derived from, any record held by a financial institution pertaining to a customer's relationship with the financial institution."[159] In this hypothetical, the government may not only be able to see where you have been but possibly where you are planning on going.

D. Because maintaining a bank account is a necessity, modern financial information cannot be subject to the third-party doctrine.

The creation of the third-party doctrine by the Court in *Miller* was largely based on the idea that a depositor cannot maintain a reasonable expectation of privacy because bank records "contain only information voluntarily conveyed."[160] Essentially, the Court established two paths for consumers. Either benefit yourself with the banking system and expose yourself to the government's gaze or remain wholly unbanked. In other words, the Court contends that a depositor either maintain complete control over their information or none at all. One of the effects of *Miller* was the categorization of information as either totally private or freely accessible to the government.[161] Pushing consumers out of the banking industry is counterproductive for the economy as a whole and economically disadvantages those wishing to maintain their privacy.[162] In fact, this would work against long-standing efforts of the federal

158. Olshan, *supra* note 152.
159. *E.g.*, 12 U.S.C. § 3401(2) (2012).
160. United States v. Miller, 425 U.S. 435, 442 (1976).
161. Stephen E. Henderson, *Fourth Amendment Time Machines (And What They Might Say About Police Body Cameras)*, 18 U. PA. J. CONST. L. 933, 959 (2016).
162. *See* Eric Robbins & Patrick Contreras, *Strategies for Banking the Unbanked*: *How Banks are Overcoming Entrance Barriers*, FIN. INDUSTRY PERSP. (Fed. Res. Bank of Kan. City) (Jan. 2006).

government to reach the unbanked and encourage market participation.[163]

As mentioned above, in Justice Sotomayor's concurring opinion in *Jones*, she admitted "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties" and "[t]his approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[164] In *Carpenter*, the Court echoed this contention that an act can hardly be voluntary when alternatives are non-existent. The Court found that the pervasiveness of cell phones in modern life make them "indispensable to participation in modern society" and "in no meaningful sense does the user voluntarily [share] his physical movements."[165] Like cell phones, banking is entrenched in our society and indispensable to participation in modern society.

Maintaining a bank account to participate in economic life has long been recognized as a necessity. Justice Brennan dissented in *Miller* because, "[f]or all practical purposes, the disclosure by individuals . . . 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."[166] While true in 1974, it is even truer today. For example, hotels often require a credit card before reserving a room,[167] some employers require payroll be paid with direct deposit into an employee's bank account,[168] and it may not be possible to purchase a home without an established banking fingerprint because most lending guidelines require a credit history or financial transaction history.[169]

163. *See id.*

164. United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

165. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018). *See also* Riley v. California, 573 U.S. 373 (2014).

166. United States v. Miller, 425 U.S. 435, 451 (Brennan J., dissenting) (quoting Burrows v. Superior Court, 529 P.2d 590, 593-96 (Cal. 1974) (en banc)).

167. Hilton Reservation Rules and Restrictions, https://www.hilton.com/en/hi/info/reservation_rules.jhtml [https://perma.cc/3DZS-P645] (last visited Jan. 31, 2020).

168. Direct Deposit Pay Programs, Payroll Mgmt. Guide ¶ 3593A (2019) ("Under federal law, employers may require direct deposit if employees are given a choice of financial institutions . . . .").

169. John Kuo, *7 Documents You Need When Applying for a Home Loan*, CREDIT KARMA (Apr. 20, 2017), https://www.creditkarma.com/home-loans/i/home-loan-documents/ [https://perma.cc/UVN4-9ZAU].

Even if a consumer decides to open a bank account for limited purposes, technology is eliminating his or her choice of how much information to share with their bank.[170] Banks are now realizing that it is much more profitable to close satellite branches and offer online services.[171] "For example, the use of some banking apps, like Charles Schwab's online app, is mandatory—the company has eleven physical bank locations, which are all in California or Nevada."[172] Forcing individuals into online services increases the information disclosed by an individual and forces the individual into agreeing to the terms and conditions before use.

Furthermore, requiring individuals to end their relationship with a bank that has moved online to retain the privacy lost by sharing additional information is unreasonable. Opening a new banking relationship requires an individual to disclose financial information to a new third party. Additionally, banks maintaining physical locations often charge higher fees to counteract the cost of operations or offer lower interest rates on savings accounts.[173] Therefore, many may be forced into transacting their business fully online and accepting the diminished privacy. This can hardly be deemed volitional.

V. MODERN FINANCIAL RECORDS SATISFY THE *KATZ* TEST FOR REASONABLE EXPECTATION OF PRIVACY.

As established, the financial records of today are of a category of non-volitionally conveyed information that is completely different from the financial records at issue in *Miller*; therefore, courts should not apply the *Miller* third-party doctrine when dealing with this new category. Under current law, the new category of financial records should be subject to the *Katz* test. The *Katz* test is applied in situations involving technology rather than the traditional physical trespass concept originally established by the Court.[174] *Katz*, as reaffirmed in *Jones*, extends Fourth

170. Moussa, *supra* note 62, at 354 ("Additionally, some of the data handed over by individuals to third parties is not 'voluntary.'").

171. Ron Shevlin, *Do Banks Still Need Branches? (The Answer is No)*, (Mar. 11, 2019, 5:00AM), https://www.forbes.com/sites/ronshevlin/2019/03/11/will-bank-branches-go-the-way-of-retail-stores/#3c31c4a5a72d [https://perma.cc/S2DQ-Q4CH].

172. Moussa, *supra* note 62, at 354.

173. *See* Shevlin, *supra*, note 171.

174. United States v. Jones, 565 U.S. 400, 405-06 (2012) (citing Katz v. United States, 389 U.S. 347, 351 (1967)).

Amendment protections to people rather than property and has added to Fourth Amendment protections.[175] The following analysis focuses on applying the two elements of the *Katz* expectation of privacy test to modern financial records.

A. Depositors maintain an actual expectation of privacy because of the quantity and quality of modern financial records and the nature of banking relationships.

First, the *Katz* test requires "that a person have exhibited an actual (subjective) expectation of privacy."[176] The Court in *Miller* found that, when applied to the *Katz* test, checks and deposit slips were merely "negotiable instruments" and not communicative—unworthy of an expectation of privacy.[177] Modern financial records, however, are communicative. As discussed above, a financial record with a transaction history of my credit card provides law enforcement with a near complete picture of my recent locations. Since financial records have become more communicative and portray a more complete view to law enforcement, the expectation of privacy is greater than the era of *Miller*.[178]

Second, the banking relationship is a relationship built on confidentiality and trust. Handling another's money is a unique role society has entrusted to banks. Although most commercial relationships are viewed as contractual, the relationship between bank and depositor is debtor-creditor and oftentimes that of fiduciary.[179] Banks are often found to be fiduciaries because of society's perception of banks as a place of special trust.[180] As cash transactions decline, modern banks play an even larger role than ever before. Modern banks offer much more than a place to deposit money. Banks accumulate mass amounts of consumer information and then act on this information as an adviser—promoting financial products they feel best serve the depositor's financial situation.[181]

175. *Id.* at 406 (quoting *Katz*, 389 U.S. at 351).
176. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).
177. United States v. Miller, 425 U.S. 435, 442 (1976).
178. Again, this was a recognized point in *Jones* by both Justice Sotomayor and Justice Alito. *See Jones*, 565 U.S. at 413-431.
179. Edward L. Symons, Jr., *The Bank-Customer Relation: Part 1—The Relevance of Contract Doctrine*, 100 BANKING L.J. 220, 224 (1983).
180. *Id*.
181. *Id.* at 225.

B. The depositor's expectation of privacy is one that society will recognize as reasonable.

To gain needed protection, the depositor's expectation of privacy must also be one that society will recognize as reasonable.[182] The second *Katz* element requires that the individual's expectation of privacy, when viewed objectively, is "one that society is prepared to recognize as 'reasonable.'"[183] Society certainly seems to value privacy—perhaps now more than ever.[184] "Fifty-four percent of Americans disapprove of collecting telephone and internet data for counterterrorism purposes."[185] Ninety-three percent "of Americans [also] want to control *who* can see their personal information, and 90% want to control *what* information the government collects about them."[186]

Although it seems society is ready to recognize a depositor's expectation of privacy as reasonable, the ultimate authority lies with the Court. There is often a disconnect between society's expectations and that of the Justices.[187] Although surveys show the courts "are often not in tune with commonly held attitudes about police investigative techniques[,]"[188] the gap seems to be closing. *Riley*, *Jones*,[189] and *Carpenter* all seem to signify a shift in the Court's understanding of Fourth Amendment privacy implications of modern technology. In *Jones*, Justice Alito recognized that technology can change society's privacy expectations and "[d]ramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes."[190] This is a stark

182. Katz v. United States, 389 U.S. 361 (Harlan, J., concurring).
183. *Id.*
184. NSA leaks and recognition of bulk data collection has made Americans more aware of the privacy risk associated with technology. *See* A.W. Geiger, *How Americans Have Viewed Government Surveillance and Privacy Since Snowden Leaks*, PEW RESEARCH, (June 4, 2018), https://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/ (last visited Mar. 6, 2020).
185. Galaro, *supra* note 13, at 55.
186. *Id.* (emphasis in original).
187. *Id*. at 54.
188. *Id*. (quoting Christopher Slobogin & Joseph E. Schumaker, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted in Society"*, 42 DUKE L. J. 727, 738-39 (1993)).
189. *See* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).
190. *Id.* at 427 (Alito, J., concurring).

contrast from *Miller*, which did not discuss societal expectations of privacy.[191] *Miller* simply argued that in passing the BSA, Congress found there was no expectation of privacy.[192] This argument, however, was subsequently rebutted by Congress with the enactment of the RFPA.

Modern financial records are fundamentally different from those discussed in *Miller* and should not be evaluated under the *Miller* third-party doctrine framework. Financial privacy in the twenty-first century has reached a level of invasiveness to pass both the subjective and objective elements of the *Katz* test.

VI. CONCLUSION

As society becomes digitalized, individuals should not be expected to forfeit their privacy protections as a prerequisite to community participation. Likewise, technology should not be forgone as a viable tool simply because it may expose an individual's private information. The Supreme Court should evaluate each case based on the facts of the previously unknowable technology and not be quick to mechanize the Fourth Amendment analysis. The increased quantity and quality now collected by financial institutions has far exceeded the bank records at issue in *Miller* and should be evaluated as a new category of personal information. In light of *Carpenter*, this new category of information should receive Fourth Amendment protection.

191. *See* United States v. Miller, 425 U.S. 435 (1976). *See also* Galaro, *supra* note 13, at 54.

192. *See Miller*, 425 U.S. at 444.