PROTECTING PRIVACY IN OUR FINANCIAL TRANSACTIONS: AN ALTERNATIVE METHOD TO THINKING ABOUT OUR PRIVACY IN THE DIGITAL ERA

Dina Moussa*

CITE AS: 1 GEO. L. TECH. REV. 342 (2017)
https://perma.cc/5LSY-RD7S

INTRODUCTION

Mobile banking, digital payments, peer-to-peer lending, and e-commerce are no longer ideas drawn from science fiction. The rise of the internet has disrupted our notion of financial payments; we can now shop, invest, and manage our payments online. The emerging industry of financial technology ("fintech") deepens and broadens the range of financial services that customers can use over the internet, whether through a desktop computer, laptop, or smartphone. Fintech participants include start-ups and other companies that use technology to conduct the fundamental functions provided by financial services, impacting how consumers store, save, borrow, invest,

* GLTR Staff Member; Georgetown Law, J.D. expected 2017; Wesleyan University, B.A. 2012. © 2017, Dina Moussa.
move, pay, and protect money. Examples of fintech products include the ability for individuals with checking accounts to use Apple Pay, a payment platform linking their debit and credit cards to their Apple devices. Android users can use Android Pay, a similar app, which links users’ financial information to their devices. To make a payment with either of these, users simply hold their device near a payment reader. Drivers can pay tolls by simply having E-Z Pass devices on their vehicles while driving through toll gates. The E-Z Pass system allows drivers to purchase small electronic transponders, which correspond to their pre-paid accounts. When drivers travel a toll-paying road, the antennas at the tolls will read the transponders and debit the accounts for the appropriate amount.

Fintech has also attracted attention beyond Silicon Valley. Governments and policy-makers are also invested in its progress and success. Fintech’s proponents also promise that fintech will make financial services cheaper, more readily available, and more efficient. For example, the World Bank Group, through its Universal Financial Access 2020 initiative, aims to ensure that communities who have poor access to mainstream financial services normally offered by retail banks, have access to traditional financial platforms, like checking accounts, by 2020. Once previously unbanked individuals have something as simple as a checking account, the fintech movement aims to dramatically expand and ease their abilities to make payments.

As new technologies emerge and the global economy expands, individuals will continue to rely on the use of cryptocurrency, data analytics,
and online transactions. Every action one takes on a fintech platform leaves what computer programmers and app developers call “digital breadcrumbs.” Digital breadcrumbs refer to all the recorded information we share while shopping, investing, or browsing online: purchasing histories, visited websites, and IP addresses, are all stored. Fintech companies store customer information as a matter of course, and often use the information to improve their products or offer new ones. Because companies store this information, and the government can subpoena much of this information, the government in turn will have increased access to our whereabouts, spending habits, and behaviors as individuals increasingly rely on new technology allowing the government access to more sensitive information.

The Fourth Amendment protects individuals from unwarranted searches and seizures conducted by the government. However, under the third-party doctrine, the Fourth Amendment does not afford protection for information turned over to third parties, as individuals surrender a reasonable expectation of privacy in that information by entrusting it to someone else. Depending on the type of data requested, the government is often not required to obtain a particularized warrant or subpoena when requesting user information that was given to a third party. These parties can legally provide their users’ information, which can be used as evidence in a criminal proceeding. While the Supreme Court strives to uphold Fourth Amendment values of protecting individuals and their right to privacy, it has not reconciled

---

6 See Miklos Dietz et al., supra note 1.
7 See United States v. Miller, 425 U.S. 435, 440 (1976) (noting that individuals have no reasonable expectation of privacy in their bank records because they are business records created and kept by the bank).
8 There are some statutory legal protections on information provided to a third party, such as the Stored Communications Act, which prohibits disclosure of customer information under some circumstances and permits it in others. Stored Communications Act (SCA), 18 U.S.C. §§ 2701-2711 (1986). The Gramm-Leach-Bliley Act, codified in 15 U.S.C. §§ 6801-6810 (1999), also protects customer information and requires financial institutions to provide their information-sharing practices to their customers. However, the Act is an insufficient protection given that it only applies to “financial institutions” and it is not clear whether these new fintech platforms are “financial institutions” as defined by the statute.
the current third-party doctrine with the new practical realities imposed by the
digital age.\footnote{The Court has tried to reconcile the third party doctrine with new technologies, such as GPS, but it is not clear whether its application can accommodate future cases with different technologies. \textit{See, e.g.}, United States v. Jones, 565 U.S. 400, 412 (2012).}

Skeptics argue there is no reason to worry about government searches of our digital footprints because existing Fourth Amendment doctrine prevents the government from unfairly accessing digital breadcrumbs.\footnote{\textsc{Jennifer Granick}, \textit{American Spies: Modern Surveillance, Why You Should Care, and What to Do About It} 220 (Cambridge Univ. Press, 2017) (arguing that the third party doctrine does not apply to network providers).} However, this Note will argue that financial data handed over by users to these third parties is not sufficiently protected under the Fourth Amendment, and that Fourth Amendment jurisprudence has not kept up with technological developments that have made an individual’s financial information increasingly accessible.

First, this Note will explain that financial information in particular requires Fourth Amendment protection in order to sufficiently safeguard individual privacy, as the fintech industry expands and our economy increasingly relies on digital payment methods. It will then argue that current jurisprudence is insufficient to protect an individual’s privacy in his or her financial information given the evolution of modern technology, and that the Supreme Court has made compelling arguments as to why the third-party doctrine is outdated and should not be applied to financial data. This Note will also provide an overview of other existing privacy protections that are insufficient for protecting financial privacy. It will then suggest a solution to protecting the privacy of an individual’s financial information by proposing a new jurisprudential framework that better reconciles the fintech revolution with existing Fourth Amendment values by distinguishing between sensitive and intrusive data. It will conclude with a hypothetical, illustrating how the framework may be used to better uphold Fourth Amendment values in the digital age.

As the automation of the global economy grows and online payment practices proliferate, the Supreme Court will need to adapt the current legal structure to adequately protect Fourth Amendment values governing financial information. If the Court does not, its jurisprudence will abandon many core Fourth Amendment values in the face of technological innovation.
OUR FINANCIAL INFORMATION REQUIRE PRIVACY PROTECTION

Fintech has increased the digitalization of financial transactions making financial data more accessible and easier to store for longer periods of time. Detailed and sensitive user data can now often be stored indefinitely in one or several centralized locations, generally only protected by privacy policies instituted by the company holding the data. Mobile payments, peer-to-peer lending, virtual investing, and connected devices now allow instant transactions through the internet and apps rather than by bank clerks and investment brokers. The internet and new technological products are establishing new norms in banking and lending, which allow individuals to conduct financial transactions more independently. These new norms also allow individuals to have one app to conduct all of their financial transactions—which was previously unheard of. As convenient payment and investment methods become cheaper and more readily available, many of us will use them. For example, many people already prefer to use credit or debit cards rather than cash; many banks and investment companies are slowly eliminating bank branches, and encouraging users to do their banking online.11 The global market trend is toward increasingly digital financial transactions.12

As fintech proliferates, users will centralize their transactions and financial information. Unlike transactions conducted with cash or, to a lesser degree, checks and credit cards, fintech transactions create a holistic digital fingerprint of an individual, which is kept indefinitely by the company processing the transaction. Before the digitization of financial transactions, individuals used cash or personal checks, which allowed individuals to purchase items or services without revealing much about the purchases or

---


services themselves. Historically, paper receipts and checkbooks were used to prove that particular transactions took place. If an individual used a personal check to make a purchase, the bank had the check recipient’s name, which revealed some information about the purchase (the date and the store name) but not as much as what a digital transaction reveals. The individual also had the option to include more details in his or her checkbook surrounding the actual purchase, like the time, location, and the item or service purchased.\(^{13}\) A purchaser could discard the receipt or keep it with his or her financial records. Now, with the increased digitization of financial transactions, financial platforms and apps have immense storage capacity to keep an individual’s digital records indefinitely, without allowing users the ability to delete the information.\(^ {14}\) While users may believe they have simply moved the functions of their checkbooks to the cloud, the legal impacts are profound. While checkbooks are considered a protected “effect” under the Fourth Amendment,\(^ {15}\) online records maintained by a third party may have no such protection depending on the type of data they contain.\(^ {16}\)

These platforms store an immense amount of data, calling into question what, if any, privacy protections their consumers hold. For instance, with the centralization of large amounts of financial and transaction information, law enforcement no longer needs to investigate and search for individual’s separate bank accounts: this data may now plausibly be stored by a single company along with credit card and transaction information. Mint, a web-based personal financial management service, allows users to input information about their bank accounts, physical location, shopping preferences, household budget, investments, and debts and loans. Since all this information is stored by Mint online, law enforcement no longer needs to spend time and energy searching for and obtaining access to different services, greatly reducing individual privacy protections from the government in a way

\(^ {13}\) An individual’s checkbook is an effect protected under the Fourth Amendment. *United States v. Wilson*, 36 F.3d 1298, 1306 (5th Cir.1994).

\(^ {14}\) The Privacy Act of 1974, 5 U.S.C. § 552a, was enacted to protect the privacy rights of individuals by reducing the federal government’s ability to have a centralized computer database with all their information.

\(^ {15}\) *Wilson*, 36 F.3d 1298, 1306.

\(^ {16}\) See *United States v. Miller*, 425 U.S. 435, 440 (1976) (noting that individuals have no reasonable expectation of privacy in their bank records because they are business records created and kept by the bank); *see also* Stored Communications Act (SCA), 18 U.S.C. §§ 2701-2711 (1986).
that could not be the case if this information were stored in the physical realm.\textsuperscript{17}

Online financial transactions can also reveal much about a person from the transaction’s date, time, item purchased (including its image) and its cost. These records create a story explaining where and when an individual was present, and whom was in that particular vicinity when that purchase was made. Additionally, an individual’s purchases can reveal a lot about his or her preferences, needs, and lifestyle.

Even social media can store, track, and reveal users’ preferences, interests, and movements. If an individual uses Facebook’s platform to make purchases or engage in financial transactions with his or her Facebook friends or through Facebook’s apps (like buying a product or service from a friend, making a purchase for a Facebook-hosted game, or making a donation on Facebook), the platform collects and retains information about the transaction. This information includes the user’s payment information and the individual’s name, billing, shipping and contact details.\textsuperscript{18} Users may not expect this information to be revealed to anyone, including the government.

Even when individuals are not using fintech services, their financial and transaction data may be held by third parties, with or without the individual’s knowledge. Many companies now also require individuals to submit a credit report for anything from employment to residential applications. To avoid credit report costs, individuals now use services such as Credit Karma, to generate free updated credit scores and reports from national credit bureaus like TransUnion.\textsuperscript{19} To sign up, individuals must create a user profile, which includes personally identifiable information. Although these services do not acquire payment information, they look into a user’s credit history from multiple sources, including his or her banks, credit card companies, collection agencies, and the government.\textsuperscript{20} This information

\textsuperscript{17} The Supreme Court has noted diminishing privacy protections due to the ease of accessing digital personal information. See, e.g., United States v. Jones, 565 U.S. 400, 412 (2012) (Sotomayor, J., concurring that the mosaic theory, whereby government can obtain a lot of information easily, changes the relationship between the government and citizens).


\textsuperscript{20} While the Fair Credit Reporting Act, 15 U.S.C. § 1681, provides privacy and notice rights for consumers, such as the right to know what information is contained in their credit reports, it does not prevent third parties from obtaining such information without their consent.
reveals the individual’s spending habits, payment history, and yearly income. This type of data can identify certain life events or categorize an individual based on his or her credit history.

When the Bill of Rights was added to the Constitution in 1791, it is unlikely (to say the least) that its drafters envisioned a world where the government would have nearly unlimited access to citizens’ financial information through a blanket rule called the third-party doctrine. In the Fourth Amendment, the Founders codified what they believed was essential to individual liberty: protection from unlawful government intrusion, barring particularized warrants and probable cause. In 2017, hardly anyone goes a day without passing information through a third party, leaving that information vulnerable to exactly the type of warrantless intrusion the Fourth Amendment was written to protect against. As the fintech movement continues, financial data is more accessible to law enforcement because it can be centrally stored and kept for longer periods of time without giving users the ability to delete their records.

CURRENT FOURTH AMENDMENT JURISPRUDENCE IS INSUFFICIENT TO PROTECT AN INDIVIDUAL’S PRIVACY IN HIS OR HER FINANCIAL INFORMATION

A Fourth Amendment search takes place when the government violates a person’s subjective expectation of privacy through an examination of “persons, places [or] effects,” when that subjective expectation is one that society recognizes as objectively reasonable. The third party doctrine, established by United States v. Miller21 and Smith v. Maryland,22 removes Fourth Amendment protection for information handed over by individuals to third parties. The Court reasoned that turning over information to another party undermines any reasonable expectation of privacy, such that the government’s accessing of such information is not a search. While once a sensible accommodation of the underlying technological landscape, the third-party doctrine is no longer a reasonable approach to individual privacy, given current and upcoming technological developments. Historically, the third-party doctrine concerned targeted and limited government investigations

21 See 425 U.S. 435 (1976) (holding that individuals have no reasonable expectation of privacy in their bank records because they are business records created and kept by the bank).
22 See 442 U.S. 735 (1979) (holding that when an individual dials telephone numbers, he or she has no reasonable expectation of privacy in his or data because it was handed over to a telephone provider, a third party.).
directed at specific individuals for which the government could show grounds for suspicion.\footnote{Id.} Neither of these cases from the 1970s addressed our current reality in which digital data storage contains almost all of our private information.

More recently, the Supreme Court has recognized the need to update the third-party doctrine. It has opened up exceptions to the third-party doctrine in order to update it for the digital age, such as in a recent opinion banning government search of information stored on an arrestee’s cell phone without a warrant.\footnote{See Riley v. California, 134 S. Ct. 2473 (2014).} But the fundamental problems with the third-party doctrine remain, and cannot be dealt with by anything less than abandoning the doctrine and replacing it with a more modern and nuanced approach to privacy in the digital age.\footnote{See id.}

**Overview of the Third-Party Doctrine**

The leading case discussing privacy rights in information given to third parties is *Smith v. Maryland*, where the Supreme Court held that the defendant who voluntarily provided his data to a phone company had no reasonable expectation of privacy in the information.\footnote{Smith v. Maryland, 442 U.S. 735, 755 (1979).} The Court dismissed the Fourth Amendment claim against the government for using a pen register, with the phone company’s authorization, to track the numbers dialed by the defendant.\footnote{Id. at 745.}

The Court held that when an individual dials numbers on a phone, he willingly uses a telephone company’s service in order to make the call and understands that using the service includes providing certain information to the company.\footnote{Id. at 742.} Therefore, when an individual dials these numbers, he has no reasonable expectation of privacy in his data because he handed it over to the telephone provider, a third party.\footnote{Id.} Individuals should reasonably know that companies have the capability and incentive to make permanent records of the numbers that their customers dial.\footnote{Id.} The *Smith* Court reasoned that if an individual takes the risk of “revealing his affairs to another, that . . .
information will be conveyed by that person to the Government . . . even if the information is revealed on the assumption that it will be used only for a limited purpose.”31 Since Smith, the third-party doctrine applies not just to telephone numbers, but to any information handed over to third parties, such as purchase history, invoices, and online banking transactions.

Similarly, in United States v. Miller, the police connected the defendant to a bootlegging conspiracy by subpoenaing his bank for checks written from his business account.32 The Court held that checks are not confidential because they are a business instrument, rather than a private document.33 Additionally, the Court noted that bank customers have no reasonable expectation of privacy in their bank records because they voluntarily hand over this data to third parties and the bank employees are able to view these documents.34

In addition, under the current third-party doctrine, when individuals use fintech (e.g., sending payments online, investing online, banking through their bank’s website, or lending money to a friend) and download the corresponding apps that allow them to conduct these transactions, individuals will have no reasonable expectation of privacy in this data. From financial transactions between friends using Venmo35 to a bank record tracking the whereabouts of an individual at all times through their debit card use, some fintech apps and methods used to facilitate these virtual transactions may allow companies and the government to access a variety of personal data, which may be voluntarily handed over by the third parties to the government without a warrant.36 In many cases, courts may conclude that individuals voluntarily used these devices and apps and willingly chose to disclose to third parties the data collected, analyzed, stored, and synced by these apps. Therefore, in some situations where the government requests this information

31 Id. at 744.
33 Id. at 440.
34 Id. at 442.
36 There are some statutory legal protections on information provided to a third party, such as the Stored Communications Act (“SCA”), 18 U.S.C. §§ 2701-2712. The SCA permits voluntary disclosure, requires disclosure, and prohibits disclosure of customer information in varying circumstances. See, e.g., 18 U.S.C. §§ 2701 (defining “offense,” and establishing punishments and exceptions for the purposes of the SCA), 2702 (“Voluntary Disclosure of Customer Communications or Records”), 2703 (“Required Disclosure of Customer Communications or Records”), 2711 (defining relevant terms for purposes of the SCA).
from a third party, courts may hold that this is not an unlawful search under the Fourth Amendment, and the evidence may be admissible against an individual in a criminal proceeding. This depends on the specific type of financial data at issue and whether other statutory protections apply to its disclosure.

*The Third-Party Doctrine, as Developed in Smith and Miller, No Longer Adequately Protects Core Fourth Amendment Values*

Although well-reasoned for their times, the holdings in *Smith* and *Miller* simply do not provide relevant guidance for today’s highly networked world. Nearly all of the vast volumes of information that individuals generate about themselves is filtered through a third party, which robs those holdings of their original logic. The way information was created and used in 1970’s America is enormously different from how it is created and used today. As the financial industry becomes digitized, the financial data of individuals will be increasingly gathered and stored electronically by the third parties that run these financial apps and platforms. An individual’s privacy in this data may be vulnerable and at risk depending on the type of financial data he or she is handing over.\(^{37}\)

In *Smith*, the police requested a list of the defendant’s dialed phone numbers from his telephone company in order to determine his whereabouts during the robbery.\(^{38}\) The police were led to the defendant because a witness had written down his license plate number when his vehicle was spotted during the robbery. Here, the police had two justifications to collect the defendant’s data: (1) the date of the robbery; and (2) “particularized suspicion” that the defendant was the robber because he was spotted fleeing the scene shortly after the crime.

*Smith* is obsolete today because the volume and sensitivity of the information gathered in *Smith* is significantly less than the data that is and will be collected by banks and apps. The *Smith* investigation had a set duration, and collected only three days’ worth of numbers. However, the certain financial data collection from banks and apps will be endless and easier to analyze if the information is not protected under other statutory or regulatory

\(^{37}\) However, the Stored Communications Act prohibits disclosure of customer information under some circumstances and permits it in others. *See*, e.g. 18 U.S.C. §§ 2701, 2702, 2703, 2711.

\(^{38}\) *See Smith*, 442 U.S. at 737.
schemes. The government will have the ability to gather a tremendous volume of financial data that may be stored indefinitely and acquired at any time without cause or justification. Mass surveillance increases the number of targets available to track at any given time and decreases the cost of tracking to zero as data is collected and stored in the course of our day. Because the facts in *Smith* and society’s current reliance on technology are no longer analogous, *Smith* and the third-party doctrine should no longer be used to analyze whether individuals have a reasonable expectation of privacy in the financial data they hand over to third parties.

Similarly, *Miller* is inapplicable today because the amount of data that banks, and other financial and investment companies acquire from their customers can be sorted and analyzed to create a full profile of an individual and his or her behaviors and patterns. For example, companies now use algorithms and computer models to analyze massive pools of information to make inferences about a user’s health, personality traits, and even mood in real time, in order to help the companies predict, and ultimately influence, the user’s next purchase. In the aggregate, law enforcement could learn this information as well as a user’s private thoughts and interests from this data or a company’s analysis of the user and his or her preferences.

Additionally, *Miller*’s holding is too archaic to apply to today’s fintech landscape because banking practices and the financial industry have changed since the Supreme Court decided the case in 1978. Bank tellers, financial advisors, and brokers are being replaced by apps, online banking websites, and financial planning services. These individuals who once played essential roles in processing our checks, transferring our money, and investing in our retirements are no longer acting as intermediaries to facilitate our transactions. Individuals are now capable of engaging in these transactions—transferring funds, sending virtual checks, peer-to-peer lending—instantly and on their own without stepping foot outside their homes. Because the intermediary component (the tellers, the brokers, the financial planners) has been eliminated from these transactions, we should no longer consider financial

---


records and transactions as business records belonging to the banks or the apps used to engage in these transactions.

When the Supreme Court issued the Miller and Smith holdings, it was both unanticipated and unforeseeable that technology would reach the level of sophistication and accessibility that it has today. We are now able to lend money and make payments at the click of a button, \textsuperscript{41} refinance debts online, \textsuperscript{42} and have robot investors execute our investment choices. \textsuperscript{43} Technology is now an inherent part of society, and the amount of data that is passed through third parties is “so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression,” thus increasing an individual’s reasonable expectation of privacy in this data. \textsuperscript{44} Additionally, some of the data handed over by individuals to third parties is not “voluntary.” For example, the use of some banking apps, like Charles Schwab’s online app, is mandatory—the company only has eleven physical bank locations, which are all in California and Nevada. \textsuperscript{45} Most individuals perform their transactions through the Charles Schwab online app. \textsuperscript{46} Similarly, when individuals purchase apps, like the Charles Schwab app, they are required to accept the terms and conditions before receiving that product or service. Individuals are forced to sign these contracts in order to receive these apps. Courts apply traditional contract law to determine whether users had reasonable notice and provided consent to a service’s privacy policy. \textsuperscript{47}

\begin{footnotesize}


\footnote{44 City of Ontario v. Quon, 560 U.S. 746, 760 (2010).


\footnote{46 See Schwab Mobile Deposits, CHARLES SCHWAB, http://www.schwab.com/public/schwab/investing/pricing_services/mobile/schwab_mobile_deposit (last visited Mar. 27, 2017) [https://perma.cc/SK9W-Y48N] (many across the country use Charles Schwab. However, the company only has banking branches in California and Nevada meaning its users are required to use the online app for financial transactions).

\footnote{47 Alison S. Brehm & Cathy D. Lee, \textit{From the Chair: “Click Here to Accept the Terms of Service,”} 31 AM. BAR ASS’N. COMM’C’N LAWYER 1 (Jan. 2015),}
speaking, the terms and conditions usually are not enough to provide actual notice of what data the app collects about the individuals, or what the companies can do with that information. These agreements are generally way too long and wordy. Individuals also do not have any bargaining power and cannot negotiate the terms of service with the financial company or platform. Lastly, individuals may not have viable alternatives to using a particular financial service or product because it may be the most popular or most of their friends and family members use a particular platform. Users may be forced to agree to these terms and conditions without fully understanding the agreements. The volume of information individuals generate and necessarily ‘hand over’ to third parties makes the underlying logic of Smith and Miller inapplicable in the digital age.

The Supreme Court Has Made Compelling Arguments for Why the Third-Party Doctrine is Outdated and Should Not Be Applicable to an Individual’s Financial Data

Recently, the Court provided several strong arguments for why an individual’s right to privacy in the emerging digital age should not be limited by the third-party doctrine. In Riley v. California, the Court unanimously concluded that the government must obtain a warrant to search a cell phone confiscated during an individual’s arrest because arrestees have a reasonable expectation of privacy in the digital information stored on their cell phones. Writing for the Court, Chief Justice Roberts explained that “cell phones differ in both a quantitative and qualitative sense from other objects that might be kept on an arrestee’s person.” He listed several factors explaining why searching a cell phone implicates individual privacy to a degree that is categorically distinct from searching other closed containers; their “immense storage capacity” which can hold and transfer “millions of pages of text, thousands of pictures, or hundreds of videos” and the quantity of information individuals store on these devices. The Court acknowledged ninety percent of Americans carry cell phones and “use them to keep a digital record of nearly every aspect of their lives.” Some of this personal information includes

49 Id. at 2479.
50 Id.
where and when they travel, whom they spoke to and what they said, and what they were thinking about as they searched a question on their phone.51

Through its discussion of cell phones, the Court stressed the importance of protecting an individual’s right to privacy in the digital era. It acknowledged that possible “intrusion[s] on privacy [are] not physically limited in the same way when it comes to cell phones” and other digitally stored information.52 The storage capacity of cell phones has several interrelated consequences for privacy. First, cell phones collect many distinct types of information from a single location. This information combined can reveal much more than any isolated record.53 Second, their capacities allow “even just one type of information to convey far more than previously possible.” Many details about an individual's private life can be “reconstructed through a thousand photographs labeled with dates, locations, and descriptions.” This would not have been the case if an individual had a single photograph or two of loved ones stored in his or her wallet.54 Third, the phone’s metadata can date back to the purchase of the phone or earlier. The Court compared this capability to an example predating cell phones: a person may carry a slip of paper in his pocket reminding him to call an individual. However, he would not carry a record of all his communications with this individual for the past several weeks, months, or years.55

Similarly, the most compelling argument that the Court gave in protecting the digital data of individuals was the “element of pervasiveness that characterizes cell phones but does not exist with physical records.”56 The Court noted prior to the Internet age, individuals did not carry a collection of their sensitive personal information with them “as they went about their day.”57 It also noted that certain types of data are also qualitatively different. It acknowledged internet searches and browsing histories can reveal an individual's private interests, concerns, worries, thoughts, or feelings. Coupled with a search for disease symptoms, they can reveal an individual's sensitive

51 Id.
52 Id. at 2489.
53 Riley v. California, 134 S. Ct. 2473, 2489 (2014). For example, if law enforcement accesses a cell phone containing an address, a note, a prescription, a bank statement, and a video, they can gather a lot more information about an individual than having one of these in isolation.
54 Id.
55 Id.
56 Id. at 2490.
57 Id.
medical information or symptoms they may be experiencing.\textsuperscript{58} Additionally, the Court acknowledged information contained on a cell phone can also reveal a person’s whereabouts and current location. It can even be used to “reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.”\textsuperscript{59}

The Court also discussed another example of why the digital data of individuals requires additional protections: society’s pervasive use of apps. The average smartphone user installs and uses thirty-three apps.\textsuperscript{60} These apps offer a range of convenient tools for managing detailed information about all aspects of a person’s life—such as drug recovery addictions, pregnancy, budgeting, hobbies, dating, and buying and selling just about anything and the records of such transactions may be accessible on the phone indefinitely.\textsuperscript{61}

Together, this information “reveal[s] a montage of the user's life” and “not only contains in digital form many sensitive records previously found in the home” but “also contains a broad array of private information never found in a home in any form—unless the phone is [there].”\textsuperscript{62} The Court acknowledged the flaw in comparing a cell phone to a digital container because the information may not only be stored on the device itself, like information stored on clouds or remote servers but left us with no clear guidance on how to analyze the reasonable expectation of privacy in our data.\textsuperscript{63}

The Court’s decision in Riley was consistent with its view in United States v. Jones where the government attached a Global Positioning System (“GPS”) tracking device to the defendant’s vehicle to monitor the vehicle’s movements on public streets.\textsuperscript{64} The Court used the reasonable expectation of privacy test and held that the government’s actions constituted a search under the Fourth Amendment and were an invasion of the defendant’s privacy. Specifically, the Court determined that when the Government engages in physical intrusion of a constitutionally protected area or effect in order to obtain information, that intrusion constitutes a violation of the Fourth Amendment.\textsuperscript{65} Here, the officers encroached on the defendant’s vehicle, which

\textsuperscript{58} Riley v. California, 134 S. Ct. 2473, 2490 (2014).
\textsuperscript{59} Id.
\textsuperscript{60} Id.
\textsuperscript{61} Id.
\textsuperscript{62} Id.
\textsuperscript{63} Id.
\textsuperscript{64} United States v. Jones, 565 U.S. 400 (2012).
\textsuperscript{65} Id. at 407.
the Court considered a protected space and effect, in order to monitor the vehicle’s movements.\footnote{66}{Id. at 412.}

In \textit{Jones}, the Court noted that “achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but [that] the present case [did not] not require [them] to answer that question.”\footnote{67}{Id.} Nonetheless, the Court noted that “situations involving merely the transmission of electronic signals without trespass would remain subject to \textit{Katz} analysis and would likely need to be resolved at a later time.”\footnote{68}{Id. at 411.}

Justice Alito and Justice Sotomayor agreed with the Court’s holding but took it a step further in their concurrences alluding to additional privacy concerns as technologies become more sophisticated. Justice Alito’s concurrence noted that advancements in technology are making it easier for the Government to monitor criminal activity and that the “‘[t]raditional surveillance’ of \textit{Jones} for a 4-week period ‘would have required a large team of agents, multiple vehicles, and perhaps aerial assistance.’”\footnote{69}{United States v. Jones, 565 U.S. 400, 412 (2012) (quoting Alito, J., concurring at 429).} He added that while short-term monitoring of an individual’s movements on public streets accords with expectations of privacy, longer term GPS monitoring in investigations impinges on expectations of privacy.\footnote{70}{Id. at 430 (Alito, J., concurring).} He acknowledged that he could not answer the question of when short term surveillance became long term surveillance.

Justice Sotomayor took Justice Alito’s concurrence a step further and cautioned about the implications of wireless surveillance and its effects on privacy, including questions about the constitutionality of warrantless short-term GPS surveillance.\footnote{71}{Id. at 413-9 (Sotomayor, J., concurring).} She argued that even short-term GPS monitoring could reveal an individual's every movement, divulging a great deal about a person's daily actions, interests, and private destinations.\footnote{72}{Id. at 415.}

Additionally, new technologies have made individuals especially vulnerable to government surveillance. As new technologies develop, surveillance will become cheaper and easier than it has ever been before, which facilitates greater surveillance.\footnote{73}{United States v. Jones, 565 U.S. 400, 428-29 (2012) (Alito, J. concurring).} Under the current third-party doctrine,
law enforcement can simply ask a cooperative third party, such as a cell phone provider, for cell tower information to determine the vicinity and movements of a suspect. Judge Richard Allen Posner\textsuperscript{74} made a similar point discussing the implications of mass surveillance, GPS, and advances in technology:

The new technologies enable, as the old (because of expense) do not, wholesale surveillance . . . It would be premature to rule that such a program of mass surveillance [of public movements] could not possibly raise a question under the Fourth Amendment—that it could not be a search because it would merely be an efficient alternative to hiring another 10 million police officers to tail every vehicle on the nation’s roads.\textsuperscript{75}

Given that the Court has acknowledged society’s pervasive reliance on technology, particularly cell phones as a means of storing personal information, there is a strong argument to be made that the third-party doctrine should be revisited given that many of our financial transactions are done through apps and stored in cyberspace. Individuals now use fintech (e.g., send payments, shop, invest, bank through their bank’s website, or lend money to a friend—all online) and download the corresponding apps that allow them to conduct these transactions.

Through the pervasive use of fintech platforms, individuals will generate millions of data points through their financial transactions ranging from the bank records tracking the whereabouts of individuals at all times through their debit card use to the apps that store transaction information, such as purchases, dates, and times. The information generated through the use of these technologies reveals many intricate details pushing in favor of reevaluating the third-party doctrine as it applies to financial transactions.

\textbf{OTHER PRIVACY PROTECTIONS ARE INSUFFICIENT FOR FINANCIAL PRIVACY}

Besides case law lagging behind technological advancement, the existing statutory protections for financial information are insufficient to protect an individual’s privacy in an age of pervasive data collection. The Right to Financial Privacy Act of 1978 (“RFPA”) protects the confidentiality of personal financial records by attempting to create a statutory Fourth

\textsuperscript{74} Former Chief Judge of the United States Court of Appeals for the Seventh Circuit from August 1, 1993–August 1, 2000.

\textsuperscript{75} United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007).
Amendment protection for bank records. The RFPA requires the government to provide an individual with notice and an opportunity to object before his or her bank or other financial institution discloses an individual’s financial information to the government for law enforcement purposes.

The RFPA was enacted as a response to Miller, and was meant to protect against unwarranted and unrestricted government access. However, the RFPA contains several exceptions that the government can use to sidestep the statute’s safeguards. These exceptions are (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 intelligence or other national security protective functions. As a result of these exceptions, there are hardly powerful restrictions on the government’s ability to obtain an individual’s financial records.

To fintech users, the most jarring of these exceptions is disclosures in accordance with any federal statute. This exception allows banks and other financial institutions to disclose its users’ financial data under the Bank Secrecy Act. This Act, initially at issue in Miller, allowed the Court to justify its holding that individuals have no reasonable expectation of privacy in their bank information because their banks and other financial institutions are required to keep records under this federal statute. Other glaring issues under the RFPA include the exception allowing the disclosure of this data

---

78 Id.
80 See Michael W. Price, Rethinking Privacy: Fourth Amendment “Papers” and the Third-Party Doctrine, 8 J. NAT’L SEC. L. & POL’Y 247, 265 (2015) (explaining how congressional alarm over the implications of the third party doctrine has resulted in legislation affording privacy to some categories of third-party records yet these efforts have been undermined by changing technologies).
81 FED. RESERVE Bd., supra note 77.
when foreign intelligence investigations are at issue. This exception has the potential to be applied indefinitely without a way to limit its reach.

A SOLUTION TO PROTECTING THE PRIVACY OF AN INDIVIDUAL’S FINANCIAL INFORMATION

The Court should consider modifying—but not abandoning—the third-party doctrine to better reconcile the privacy interests that individuals have in their financial information and metadata today. Specifically, the current third-party doctrine does not separate situations where the government obtains information that is intrusive or sensitive.

I. Intrusive: This category describes situations where the government encroaches on an individual’s physical space or goes through a third party to acquire an individual’s data. An example of this category of data is if the government receives access to an individual’s financial records from his/her bank without his/her consent; and

II. Sensitive: Several scholars disagree as to the nuances of the definition of sensitive information but most agree that the definition describes information that can be used to enable privacy or security harm when placed in the wrong hands.82 Presumably, this category involves information that individuals would not knowingly broadcast to the world and would not want others to see because of the harm it may cause if the information is spread. The category includes inherently sensitive information and inferentially sensitive information.83

a. Inherently sensitive information: describes “information that causes concrete harm merely by being known to another”, such as information we often regard as embarrassing, humiliating or abasing, like health information.84

82 See generally Paul Ohm, Sensitive Information, 88 S. Cal. L. Rev. 1125 (2015) (concluding that different categories of sensitive information need more protection than others depending on the privacy harms they bring individuals, and devising a taxonomy for information of varying sensitivity). Since there is considerable debate as to how sensitive information is defined, I use Professor Ohm’s definitions because they are in line with the type of information intended to be protected under the Fourth Amendment. However, in my proposed framework, I do not distinguish between the two types of sensitive information he defines because I leave it up to the courts to determine whether a distinction is warranted depending on the factual situations at issue.

83 Id. at 1170.

84 Id.
b. *Inferentially sensitive information*: describes information “connected to harm through at least one inferential or predictive step” like past criminal conduct, “not only for the inherent shame sometimes associated with criminal activity but also for the possibility of future danger or recidivism.” An example of this type of data is data from an offender’s Amazon account, including all of his or her search and purchase history, that law enforcement uses in a sentencing memorandum to predict his or her rate of recidivism.

Under this model, data is divided into four groups: 1) sensitive, intrusive; 2) non-sensitive, intrusive; 3) non-sensitive, non-intrusive; and 4) sensitive, non-intrusive. This would allow judges to classify which category the data falls into. This section will explain each of the categories under the following diagram and provide examples of each of these groups of data.

**Figure I: Categories of Data**

<table>
<thead>
<tr>
<th>Sensitive</th>
<th>Non-Sensitive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intrusive</td>
<td></td>
</tr>
<tr>
<td>Non-Intrusive</td>
<td></td>
</tr>
</tbody>
</table>

A. **Intrusive, Sensitive Data**

The top left-hand corner represents sensitive and intrusive data. The “sensitive” aspect of this category involves information that individuals do not knowingly broadcast to the world and would not want others to see because of its potential to cause privacy or security harm when placed in the wrong hands. The “intrusive” component of this category involves law enforcement impeding into an individual’s physical or digital space to obtain this information.

---

85 *Id.*
86 *Id.*
An example of intrusive, sensitive data is personal financial records on Angie’s computer, including mortgage paperwork citing her earning potential, debt, and bank statements that tell a story of where she has traveled and what she purchased over time, that law enforcement obtained without her consent. In this category, law enforcement accessed Angie’s digital space, without consent, to acquire information (the financial records) that Angie did not want the world to see. In the wrong hands, the release of Angie’s financial records can lead to identity theft, fraud, and embarrassment. Angie did her best to store this information in a place where she would not expect anyone to have access to unless the intruder broke into her home or personal computer, which are Angie’s “home” and “effects” respectively for purposes of the Fourth Amendment.

Test

In situations like these, the courts should use the tangible invasion of privacy standard reaffirmed in Jones to determine whether the government committed a digital trespass to acquire private information. This means the court must assess whether there was a tangible invasion of privacy to acquire the data at issue. In the example above, after applying the Jones test, a court would hold that law enforcement committed a digital trespass to acquire Angie’s financial records because they accessed Angie’s computer without a warrant or her consent.

B. Intrusive, Non-Sensitive Data

The top right-hand corner is intrusive, non-sensitive data. This is data that individuals voluntarily broadcast to the world but which can still be obtained by law enforcement hacking into an individual’s physical or digital space or effects. Intrusive, non-sensitive data includes Nora’s past or present locations from her Fitbit87 GPS tracker, which law enforcement obtains on the app, through a third party without a warrant. Because law enforcement went through a third party, and did not have a warrant, to obtain this data and intruded in Nora’s digital space to obtain this information, the data was collected in an intrusive manner. The information itself was not private

---

87 Fitbits are wireless, activity trackers that measure number of steps walked, heart rate, sleep quality, steps climbed, and other personal metrics involved in fitness. Who We Are, FITBIT, https://www.fitbit.com/about (last visited Apr. 1, 2017) [https://perma.cc/MJF6-5BEV].
because Nora was recording it for her personal use but, at the same time, she was protecting this data in her digital space.

**Test**

When law enforcement invades an individual’s digital space or effects, the test should be the tangible invasion of privacy standard reaffirmed in *Jones* in order to determine whether law enforcement had probable cause or a warrant to enter, or trespassed into an individual’s space. In the example above, after applying the *Jones* holding, a court would hold that law enforcement trespassed into Nora’s digital space because it accessed her password-protected Fitbit account to obtain her past and present location information without a warrant or her consent.

**C. Non-Sensitive, Non-Intrusive Data**

The bottom right-hand corner is non-intrusive, non-sensitive data: data that individuals voluntarily reveal to the world or would not mind sharing. To acquire this type of data, law enforcement need not hack into a website, app, or personal device. Non-private, non-intrusive data is a list of all timestamps from Leith’s Venmo payments which are displayed on his public Facebook profile. Law enforcement neither hacked into Facebook nor went through a third party to obtain this information, and they did not collect data that was meant to be private. The individual voluntarily posted this information for the public to access and see.

**Test**

When law enforcement obtains data that is neither sensitive nor obtained in an intrusive way, the court should use the third-party doctrine as it exists to evaluate whether law enforcement conducted an unreasonable search. In the example above, a court would hold that law enforcement was rightfully permitted under the third-party doctrine to obtain the time stamps, including the financial payment information, from Leith’s public Facebook posts because Leith posted the information publicly and did nothing to protect it. Additionally, law enforcement did not impede on Leith’s digital space or personal effects. A government agent merely viewed Leith’s public profile.

**D. Sensitive, Non-Intrusive Data**

Sensitive, non-intrusive data is the most difficult category to analyze. In these situations, law enforcement collects sensitive information but does so
in a non-intrusive, non-trespassory manner. This could arise if law enforcement used a public library computer to view the search history of a previous patron.

This scenario is the most challenging because law enforcement does not commit a trespass: the tangible invasion of privacy standard reaffirmed in *Jones* would not apply. The Court would have to use the *Katz* test to determine whether an individual had a subjective expectation of privacy in the sensitive data he or she accessed and whether there was an objective expectation of privacy in the individual’s data. When applying the test, the Court should consider the following factors:

1. Whether this information is considered “personal” (meaning, whether a reasonable person would feel that law enforcement intruded on his or her personal privacy such that he or she would be embarrassed, uncomfortable, or vulnerable should this data be revealed to the public);
2. Whether the government used readily-available mechanisms to access the information (i.e. was there a technology used to access information on the computer or did the government simply look at the readily available search history); and
3. What type of analysis could be conducted on that data.

The first factor upholds the longstanding notion that an individual has a right to intellectual privacy, both under the Fourth Amendment’s protection of privacy interests,\(^88\) and the First Amendment’s protection of free expression and association.\(^89\) The second factor allows the courts to balance whether the government had other means to obtain the information that it did. This can help the courts determine whether the government could have obtained a search warrant, used technology unavailable to the public or obtained the information simply due to the individual’s negligence. The third factor allows the courts to determine how much information the data reveals about the

---


\(^{89}\) The Court has supported the concept that an individual not only has the ability to think freely, but also express him or herself freely from government interference. See Stanley v. Georgia 394 U.S. 557 (1969) (holding that law enforcement exceeded the scope of a warrant to search the defendant's home by viewing a defendant's videos and that protecting the individual's intellectual privacy rights under the First Amendment were more important in this case than prosecuting the defendant for a crime outside the scope of the warrant).
individual and whether a narrow or broad analysis can be conducted on this data. This will help the courts balance an individual’s privacy interests with the government’s interests.

**Overview**

The Court should use this data classification system to carve out additional Fourth Amendment protections to an individual’s right to privacy in the digital age. By classifying data using a sensitive/intrusive distinction, the Court will be able to reconcile the existing tangible invasion of privacy standard reaffirmed in *Jones*, the reasonable expectation of privacy test, and the third-party doctrine. This data classification system will be better suited to protect individuals and their financial communications and transactions passing through certain spaces or transmitted through certain activities. The third-party doctrine will no longer have a blanket application and will restrict law enforcement’s ability to obtain data passed through to third parties. This restriction will protect certain types of data—data containing private communications by payment and retail platforms, other financial platforms, and apps—and consider any precautions individuals took to protect this information.

The following is an example demonstrating how the proposed classification system would apply to analyze whether the government’s conduct constitutes an unreasonable search of an individual’s financial data.

**A. Example: Amazon iCloud Hack**

Assume the Amazon iCloud hacked. The Amazon iCloud platform contains all of the financial information, purchase history, and past searches of its users, all of which is stolen by hackers. The information particularly at issue is information acquired by Echo assisting individuals in their financial transactions, including purchasing personal items and gifts for family members and friends. Assume, law enforcement is able to track down this information. Based on the current third-party doctrine, there would be no expectation of privacy in this data because users consented to the terms and conditions of Amazon and gave their information to the company via the data platform. They also consented to bringing Amazon Echo into their homes. However, under this Note’s new framework, the data would first be classified by the criteria explained above.
First, a court must determine whether the government was intrusive when collecting this data. Because law enforcement did not obtain this information by hacking into the Amazon iCloud directly or accessing an individual’s Echo device, it inadvertently received the information directly from a third party (the hackers who put it online). Arguably, it found this information once the platform was hacked so arguably, no intrusion occurred. Since this data is non-intrusive, we move from row 1 to row 2.

The court must now move on to the question of whether the data acquired was sensitive or non-sensitive. A reasonable person likely would not want to reveal the information contained in his or her Amazon Echo search or browsing and purchase history, which is why these accounts are password-protected. This information can also be considered sensitive because it may be embarrassing (depending on which products an individual is browsing), could be inherently shameful, could reveal private information about an individual’s life or preferences, and could also lead to future recidivism. A court could move away from classifying the data from non-sensitive to the sensitive category.

Because law enforcement accessed an Amazon user’s information without the user’s consent, and did so to obtain sensitive information, the Court could apply the non-intrusive-sensitive standard. Considering the Amazon Echo device was in an intimate location, the individual’s home, a reasonable person is likely to feel that the government intruded on his or her personal privacy by snooping around as to his or her thoughts and needs by viewing their browsing history and purchase history, organized by the data and time of these actions. Furthermore, a reasonable person in their home would be embarrassed if the government obtained information regarding the intimate and confidential details of their actions in the privacy and comfort of their own homes. With this information and the quantity of data, the government will have information as to an individual's discussions, behaviors, habits, and location. A court would rule that this information is extremely personal and an individual has a reasonable expectation of privacy in this data, particularly because of the data’s contents, quantity, and the place it was collected from. Therefore, the government conducted an unreasonable search by obtaining this information from the third party.

In this example, this classification system reaffirms core Fourth Amendment values by upholding Katz’s reasonable expectation of privacy standard and examining the totality of circumstances surrounding the data. This includes the type of data obtained, the place from which the information was acquired, and an individual's attempt to protect access to the information.
Here, the analysis hinges on what information is revealed and how law enforcement obtained access to this information.

B. Addressing Counter-Arguments

Critics may argue that this classification system does not adequately balance law enforcement’s interests and an individual’s right to privacy because it creates too high a bar for government investigation. However, this classification system does not eliminate the current third-party doctrine. It merely limits its applicability to particular types of financial data and considers the realities of digital spaces used to store data. The classification system also considers the existing Katz and Jones doctrines and their applications to an individual’s digital effects in the modern age.

Several administrability arguments can be made against the imposition of this classification system, such as the increased burden on the government to obtain warrants and the lack of flexibility in obtaining information from third parties. Law enforcement currently uses the third-party doctrine as a general warrant, allowing the government access to certain financial information passed through to third parties. However, a core value of the Fourth Amendment is to ensure that the government does not have sweeping authority to collect a citizen’s information or property, which is what is currently done under the third-party doctrine. When the Founding Fathers added the Bill of Rights to the Constitution in 1791, the country codified what society believed was essential to an individual’s liberty: the notion that individuals should be protected from unlawful government intrusions without particularized warrants and probable cause. This Amendment was created to protect American citizens from the type of government invasions rampant under King George that allowed British soldiers to invade the colonists’ homes in search of anti-monarchists. 90 The classification system above takes the Founders’ values into account by considering the nature of the financial information and whether the data can be used to harm the individual and considers where the government obtained the information to determine whether it encroached on an individual’s physical or digital space.

Critics may also argue that this classification system itself is too flexible, less predictable, and prone to judicial abuse. However, this test is narrower than the reasonable expectation of privacy test in that it groups data

---

into particular categories and puts the government on notice as to what categories a court will use to determine whether an unreasonable search has occurred. This system will be more responsive to a defendant’s individual circumstances and will be more likely to promote fairness to the parties—unlike the current third-party doctrine, which allows the government to obtain an individual’s information, which he or she voluntarily hands over to third parties, without a warrant.

Finally, critics may argue that well-informed consumers can choose a company or service with better privacy policies if they do not agree with a company’s terms of service. However, even if individuals agree to a company’s terms of service, individuals expect that companies will keep their financial information in their password-protected accounts private and will not reveal it to the government without a warrant. Consumer expectations of this privacy have come to the spotlight since the Snowden and San Bernardino incidents.91 Today, creating a password-protected account to store information is comparable to storing papers in a lock box where only the owner has the key.92 In this scenario, the government is required to obtain a warrant to compel an individual to hand over the key. The government should be required to acquire a particularized warrant to obtain the information stored in a password-protected digital account in the same way they are required to obtain the key to a physical lock box.

**CONCLUSION**

As fintech platforms increase, it will fall to the Supreme Court to ensure that Fourth Amendment jurisprudence continues to uphold society’s values of an individual’s financial privacy in the digital age. The current doctrines are ill-equipped to incorporate the modern Fourth Amendment


92 See People v. Snipe, 841 N.Y.S.2d 763, 770-772 (N.Y. Sup. Ct. 2007) (holding that the defendant’s mother had no authority to consent to the defendant’s closet, containing a lock, because the defendant did not provide his mother with a key.) This is similar to how a third party cannot consent on behalf of its user to provide the contents of a password-protected account. The difference is he had not entrusted the care of the contents of the box to his mother. She still probably could not just guess passwords until she got it right or reset it or whatever. See also David D. Thomas, *Dangerously Sidestepping the Fourth Amendment: How Courts Are Allowing Third-Party Consent to Bypass Warrants for Searching Password-Protected Computer*, 57 CLEV. ST. L. REV. 279 (2009).
values of protecting an individual’s privacy in their financial data with today’s fintech landscape. Given the pervasiveness and reliance on digital financial services and apps, the financial privacy of individuals is at risk. It is time for the Supreme Court, and the broader legal community, to revise Fourth Amendment jurisprudence for the modern digital age.