MERCATUS CENTER
George Mason University

TESTIMONY

AVOIDING MISUSE OF AMERICANS' FINANCIAL RECORDS

BRIAN KNIGHT
Senior Research Fellow, Director of Innovation and Governance

House Judiciary Committee, Select Subcommittee on the Weaponization of the Federal Government
The Weaponization of the Federal Government

March 7, 2024

Chairman Jordan, Ranking Member Plaskett, and members of the Subcommittee:

My name is Brian Knight. I am a senior research fellow at the Mercatus Center at George Mason University, although my testimony does not necessarily reflect the views of my employer. My research focuses on financial regulation, including its use as a tool of broader policy. It is an honor to be asked to testify.

In the wake of the events of January 6, 2021, law enforcement and financial firms collaborated to scan the accounts of an unknown number of Americans, using what appear to have been very broad criteria touching upon certain constitutional rights—of speech, of political and religious beliefs, of assembly, of owning and bearing a firearm—to identify potential suspects as well as to preempt future violence. The implications of this effort are troubling. The use of financial records as a dragnet or tool of surveillance violates the privacy of the American people with little likely benefit. It is incumbent upon Congress to identify how financial records are being used for these purposes and, if necessary, to reform the system to protect Americans' privacy and liberty.

As a threshold matter, I want to make clear that my comments today are based on what information is publicly available, which is limited. Additional information, whether inculpatory or exculpatory, may materially change any analysis. However, the lack of information itself speaks to one of the major problems with the current financial surveillance regime—that it is opaque to both citizens and members of Congress. We know so little about how it works, how well it works, if it works at all, and what it costs, that the American people cannot make an informed assessment of whether it is a policy worth continuing.

I also want to make clear that my comments are not intended to deny that financial information can be useful to law enforcement. Nor are they meant to impugn anyone's motives. The events of January 6 constitute an extremely serious crime. The threat of violence at the inauguration was a credible risk.

For more information or to meet with the scholar, contact
Mercatus Outreach, 703-993-4930, mercatusoutreach@mercatus.gmu.edu
Mercatus Center at George Mason University, 3434 Washington Blvd., 4th Floor, Arlington, Virginia 22201

Trying to prevent acts of extreme violence such as terrorist attacks and mass shootings is laudable. That law enforcement would consider using every tool available in the face of such serious threats is not surprising.

However, it is in the face of serious threats that the rights of the American people are in the most danger. Our history is unfortunately replete with examples of Americans' civil rights being compromised in the name of security, often for no real benefit. Fear is toxic to liberty. Based on what is known publicly, I fear that we risk going down a dangerous path, where, in a likely futile effort to obtain security, we sacrifice further freedom.

America was founded on the idea that the interest of the state must be balanced by, and often yield to, the rights of the individual. The American tradition is not that law enforcement gets a blank check. Nor is it generally that law enforcement cannot access information at all. Rather, the American model looks to due process to balance the two legitimate interests. Unfortunately, in the case of financial records, that balance is badly askew.

My testimony will discuss the following: the current regime for government access to Americans' financial records; recent allegations and other emerging efforts at financial surveillance and their troubling implications; reasons why using the tools of financial surveillance, such as Merchant Category Codes, are likely constitutionally suspect; reasons why we should be skeptical of their use even if such use is constitutional; and finally, ideas for reform.

THE CURRENT REGIME

Americans write the story of their lives in their bank accounts. Modern economic realities require people to interact with financial intermediaries such as banks, credit card companies, and many other money services businesses to accomplish the most basic transactions. Yes, one could use only the cash they keep in their mattress, but only if they were willing to forgo many common activities such as having a mortgage, shopping online, or being employed by one of the increasing number of employers that uses automatic payroll deposit.

Those interactions all leave a trail of records created by the financial firms, and those records are obtainable by the government without a warrant or any need to get outside approval. The Bank Secrecy Act[1] (BSA) allows, and in some cases requires, covered financial firms to report "suspicious" activities to the government, but suspicious is not meaningfully defined.

As a result, financial firms are providing a massive amount of information to the government. For example, in fiscal year 2022, they submitted approximately 4.3 million suspicious activity reports (SARs).[2] The current regime also permits and encourages collaboration between financial firms and the government to craft data exchanges. Rather than an arm's length transaction, financial firms have become assistants to government surveillance.

[1] Bank Secrecy Act, 12 U.S.C. §1829b; 12 U.S.C §1951–1960; 31 U.S.C §5311 et seq.

[2] Financial Crimes Enforcement Network, *FinCEN FY 2022 Year in Review*, April 21, 2022.

This generally occurs outside the public's view—by design. The law prohibits the target of a SAR from being notified.[3] Even the Right to Financial Privacy Act (RFPA), which was intended to allow people to challenge the provision of financial records to the government in court under most circumstances, exempts SARs.[4] The only time a person is likely to know they were the target of a SAR is if they are being prosecuted.

Congress is being kept in the dark. In the 2021 National Defense Authorization Act, Congress ordered that reports on how SARs are used, how effective they are, how long it takes for a SAR to be used, and other essential data be provided to Congress on a yearly basis, beginning in 2022.[5] To date, that information has not been provided. In fact, there is reason to believe that the responsible agencies themselves do not know this information. According to a 2022 Government Accountability Office report, most law enforcement agencies said they lacked the necessary systems to track and report such information and that spending the resources necessary to obtain the information may prevent them from fulfilling the agency's "core mission."[6]

In a recent hearing before the House Financial Services Committee[7] FinCEN Director Andrea Gacki acknowledged that FinCEN did not know how SARs were used and was only now beginning to collect the necessary statistics to determine this.[8] In short, a massive amount of information is being collected on Americans' financial lives without even understanding how useful it is.

This situation is permitted because the Supreme Court has ruled that Americans lack a privacy interest in their financial records.[9] According to the rulings, either Americans share this information during commerce, such as a check, or the records don't belong to them in the first place, instead belonging to the financial intermediary.[10] This is perhaps ironic, since federal law otherwise treats financial records as something customers have a significant privacy interest in and even quasi-ownership of.

Federal law requires financial firms to protect customer data from outside theft, limits how firms can use the data, and even requires firms to share a customer's data with a competitor if the customer so orders.[11] There is, therefore, considerably inconsistency in the ways the law represents customer privacy, in effect telling customers, "It's your data, and it should be private, but not from the government."

---

[3] 31 U.S.C. § 5318(g)(2).

[4] 12 U.S.C. § 3413(d).

[5] Public Law 116-283 § 6201.

[6] Government Accountability Office Report, *Bank Secrecy Act: Action Needed to Improve DOJ Statistics on Use of Reports on Suspicious Financial Transactions*, August 25, 2022.

[7] House Financial Services Committee Hearing, "Oversight of the Financial Crimes Enforcement Network (FinCEN) and the Office of Terrorism and Financial Intelligence (TFI)," Video, February 14, 2024, https://www.youtube.com/watch?v=HAlGmDhq-tI.

[8] House Financial Services Committee Hearing, "Oversight of the Financial Crimes Enforcement Network (FinCEN) and the Office of Terrorism and Financial Intelligence (TFI)," 1:07:25.

[9] See e.g. California Bankers Association v. Shultz, 94 S. Ct. 1494, 1525–1526 (1974); United States v. Miller, 96 S. Ct. 1619 (1976).

[10] See *Miller*, 96 S. Ct. 1619.

[11] See e.g. Gramm–Leach–Bliley Act, 15 U.S.C. § 6801 et seq; Dodd-Frank Act 12 U.S.C. § 5533.

However, as discussed further below, recent Supreme Court precedent may signal a changing perception that would call into question the constitutionality of the Bank Secrecy Act, at least in situations like those currently alleged. But we should not wait on the Court. Congress must critically reassess for itself whether the current regime is appropriate and make any necessary changes.

PRESENT ALLEGATIONS AND OTHER EMERGING EFFORTS AT FINANCIAL SURVEILLANCE

The recent allegations of the government's using Americans' financial data as a tool of surveillance has troubling implications for Americans' privacy. It is even more distressing when one realizes that these efforts aren't necessarily unique but may simply be uniquely visible owing to the work of whistleblowers and the efforts of this Subcommittee.

Unfortunately, the present allegations are not the only emerging example of efforts to use financial information as a tool to surveille Americans engaged in legal, and in some cases constitutionally protected, activities. Both government and private actors are increasingly seeking to use financial records to track Americans. While justified by its proponents as a way of preventing violence, which is a noble cause, there are reasons to be skeptical of how effective these efforts will be and reasons to fear they will further erode individual privacy and public trust.

The highest-profile recent example is the federal government, in conjunction with banks, such as Bank of America, and other financial firms, apparently soliciting and obtaining financial records based on broad criteria, including location on and surrounding January 6; the purchase of a firearm, or at least from a vendor associated with firearms, within a certain period; the purchase of certain items associated with "extremism," including religious texts; and the contents of messages associated with Venmo payments.[12] The government did not have identified suspects it was investigating; it was trying to identify suspects via mass data collection.

These efforts also included FinCEN sharing "typologies" and "methodologies" previously developed to help financial firms identify other illegal activities, such as mass shootings, based on what was presented as a series of large purchases in a short period of time from multiple vendors associated, at least tangentially, with firearms in a manner inconsistent with previous customer behavior.[13] This presumably included the methodology created by KeyBank and shared by FinCEN that purported to be of a narrow focus (implying broader typologies were also shared) but that relied on merchant category codes (MCCs), vendor names, including popular stores such as Dick's Sporting Goods and Cabela's, and spending thresholds that are likely to be both significantly over- and underinclusive.[14]

Another notable revelation in the KeyBank methodology is that KeyBank used several non-standard MCCs related directly to firearms manufacture. These MCCs are not part of the standard developed by the International Organization for Standardization (IOS), but rather are assigned by individual banks

---

[12] See US House of Representatives, *Interim Staff Report*, *Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government*, May 18, 2023; Chairman Jim Jordan, letter to Christopher Wray, Director, Federal Bureau of Investigation (Wray letter), January 17, 2024; Chairman Jim Jordan, House Committee on the Judiciary, letter to Noah Bishoff, AML Officer, Plaid Inc., (Bishoff letter), January 17, 2024.

[13] Secretary Corey Tellez, Letter to Senator Tim Scott, (Scott letter), February 9, 2024.

[14] Bishoff Letter. For a more detailed discussion and critique of the KeyBank methodology please see Brian Knight, "(Updated) MCCs and Financial Privacy, Again," *FinRegRag*, January 18, 2024; Brian Knight "More Thoughts on the Use of MCCs for Law Enforcement Tracking," *FinRegRag*, January 24, 2024.

and other users, which means that there may be other MCCs relating to sensitive, and perhaps constitutionally protected, activities that are unknown to the public.

MCCs are assigned based on the merchant's general business and do not reveal what specific items were purchased, but they can provide greater detail of a customer's activities the more tailored they are. This reality prompted recent efforts by Amalgamated Bank, the City of New York, and certain pension funds to get the ISO to create an MCC specifically for gun stores.[15] This move has been justified as a way to allow banks to detect suspicious activity that may indicate an imminent crime, especially a mass shooting, and allow them to alert law enforcement.[16] While some states have banned the use of the gun store MCCs, California has mandated it, explicitly for the purpose of surveillance.[17]

In summation, we have recent evidence that indicates that law enforcement sought payment information to help determine, at a minimum, Americans' whereabouts, political and religious views, and whether they own a firearm. We also know that there are efforts to increase the granularity and expand the collection of similar information, all of which is highly sensitive and personal.

In other contexts, the Supreme Court has ruled that Americans have a constitutionally protected expectation of privacy for much of this information. And yet the government and banks, perhaps with the best of intentions, can share it without any due process.

As discussed further below, there are significant reasons we should be both skeptical of the efficacy of these efforts and worried about their constitutionality and the damage they may cause.

QUESTIONS ABOUT CONSTITUTIONALITY

The current BSA system assumes that Americans lack a constitutionally protected right to privacy in their financial records. This assumption is based, in turn, on the belief that people do not have a privacy right in data they share with others or the records of another. Since it is the financial firm's records that the government receives, the customer cannot claim a privacy right in them. This assumption comes from a series of Supreme Court cases in the 1970s.[18] *United States v. Miller*, a case involving bootlegging and tax evasion, is particularly relevant. In that case the Court held that law enforcement can obtain a suspect's financial records without a warrant because the records are not the suspect's papers, and therefore, the suspect lacks a protectable privacy interest.

However, more recent Supreme Court precedent, especially the 2018 case of *Carpenter v. United States*[19] calls that into question and may indicate that warrantless financial surveillance, especially of the type of collection alleged in the Subcommittee's reporting and being recently advocated and implemented in California, may be constitutionally suspect.

---

[15] See Associated Press, "Visa, Mastercard, AmEx to Start Categorizing Sales from Gun Shops," *NBC News*, September 10, 2022; Leah Collins, "Amalgamated Bank CEO on Why We Can and Should Track Gun Purchases on Cards," *CNBC*, July 13, 2022.

[16] Kate Fitzgerald, "Will New Merchant Code for Gun Sales Turn Issuers into Morality Police?" *American Banker*, September 16, 2022.

[17] Caitlin Mullen, "States Split Over Gun Merchant Category Code," *Payments Dive*, October 2, 2023.

[18] See *Shultz*, 94 S. Ct. 1494; *Miller*, 96 S. Ct. 1619.

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

Briefly, in *Carpenter*, the Court declined to extend the reasoning of *United States v. Miller* to the context of cell-tower location data. While acknowledging that the cell phone data belonged to the phone company, not the customer, the Court found that wireless customers had a Fourth Amendment privacy interest in cell-tower records showing their location. The Court reasoned that the sensitivity of the information, the ubiquity and necessity of cell phones in modern life, and the inability to not create the information because it was generated automatically as a condition of using the phone required finding a privacy interest. Failing to do so, the Court reasoned, would allow the government "near perfect surveillance, as if it had attached an ankle monitor to the phone's user" as well as information about the user's past movements in a way that traditional observation does not.[20]

As I have discussed in greater detail elsewhere,[21] the logic of *Carpenter* matches the present situation better than that of the 1970s cases. To be sure, the Court did not overturn *Miller*, but when one considers the sensitivity, ubiquity, and necessity of electronic financial records and their power to give the government sweeping and retrospective surveillance of peoples' movements, beliefs, and the most intimate details of their lives, it is hard to believe there are no constitutional concerns. It is possible that were the Court presented with facts like those alleged, it might overturn or distinguish *Miller* and follow the logic of *Carpenter*.

REASONS FOR SKEPTICISM

Even if one discounts the constitutional argument, the potential costs of this type of surveillance likely outweigh any potential benefit. Further embracing financial surveillance, especially directed at sensitive and constitutionally protected activities, threatens Americans' privacy and trust in our system of law enforcement. It also risks further straining what appears to be an already overburdened system, harming its ability to perform legitimate functions. Further, there are reasons to be deeply skeptical that using this type of financial surveillance of Americans to preempt violence will even be effective.

The threat to Americans' privacy is obvious. As mentioned previously, the examples of financial surveillance that have recently come to light involve searching Americans' financial records to gain information about private and sensitive matters. It was the very sensitive nature of the data that made it attractive to law enforcement. Such an action should be subject to due process and transparency, but it isn't. Instead, it appears that law enforcement and financial firms can simply collaborate over email without the targets ever finding out.

We don't know the full scope of what is being searched. We don't know who has access to that information or how reasonable their determinations are. We don't know how securely the information is being stored. We don't know how common coordination between government and firms is. We don't know what other types of search criteria are being used and what other legal activities may be seen as red flags.

[20] *Carpenter*, 138 S. Ct. at 2219–2220.

[21] Brian Knight, "Is the Bank Secrecy Act Vulnerable to Constitutional Challenge over Post-January 6th Data Collection?," *FinRegRag* February 26, 2024.

This all raises important concerns about the protection of Americans' legitimate privacy issues, from their government, financial firm employees, and potential malicious actors who would seek to compromise government and private systems to access that information. This concern is not unique to the present allegations and is by no means limited to conservatives. For example, after the Supreme Court's decision in *Dobbs vs. Jackson Women's Health Organization*, many women realized that their financial records could indicate whether they had pursued an abortion.[22] Nothing says that if we stay on the current path, we won't see increasing escalation of financial surveillance directed at disfavored groups and activities across the political spectrum.

Not only is Americans' privacy threatened, but so is their trust in both law enforcement and the financial system. Already, innocent Americans are worried they may be put on a list for performing constitutionally protected activity. They already believe that big banks and the government are hostile to them, even though they have not committed a crime. Further coopting the financial system as a tool of surveillance would only deepen and spread this distrust.

While the privacy costs are high, it is not clear how useful the information is. For example, the information reported to have been provided by Bank of America, which was given to at least two FBI field offices, was ultimately pulled from the FBIs system because the "leads lacked allegations of federal criminal conduct."[23] Likewise, given the broad scope of the search criteria shared by FinCEN, it is likely that search results swept in far more innocent people than guilty.

Efforts to use financial surveillance to prevent crimes such as mass shootings are also unlikely to be effective. To do so, the bank would need to be able to correctly identify suspicious activity and report it promptly; FinCEN would need to triage it promptly; and then law enforcement would need to respond promptly.

On what basis do we believe this will occur? How will banks identify suspicious activity with the limited, though still sensitive information they have access to? Remember, banks don't know what is being purchased, only what store it is being purchased from. Cabela's sells firearms, but they also sell bass boats and pellet grills. If Cabela's is a "gun store," a lot of non-gun purchases will be swept up; if they aren't, a lot of gun purchases will be missed.

Further, what confidence do we have that banks will be able to identify suspicious activities at a rate better than random? For example, the spending thresholds recommended in the KeyBank methodology are much more than it takes to commit a terrible act of violence but less than it takes to buy a really nice hunting rifle and scope. Banks are faced with the problem that the stricter the criteria they use, the fewer legitimate threats will get flagged, but the looser the criteria, the more false positives will be submitted to law enforcement.

[22] Alejandra Caraballo, "Payment Data Could Become Evidence of Abortion, Now Illegal in Some States," *New York Times*, June 29, 2022.

[23] US House of Representatives, *Interim Staff Report*, *Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government*, May 18, 2023; Wray letter.

False positives would not only harm innocent Americans but would also place more strain on the BSA system, whose effectiveness is already highly questionable. Adding potentially millions of false positives will require resources and manpower that could go to pursuing legitimate reports to be spent instead on wild goose chases. This will likely result in longer turnaround times and lower quality responses overall.

Apparently, nobody knows how quickly FinCEN triages SARs or how quickly law enforcement responds to SARs on average, despite Congress having asked for this information years ago. Advocates of financial surveillance need to answer the critical threshold question of how quickly law enforcement would realistically act on a threat. Yet that information isn't publicly available. What is known is that large numbers of false positives will only impede the system's legitimate operation.[24]

IDEAS FOR REFORM

The need for BSA reform generally is obvious, and much good work has already been done to propose changes.[25] I will limit my proposals to what I think are most directly relevant to the issues raised by the Subcommittee's reporting and by recent efforts to use MCCs as a tool of surveillance.[26]

First, Congress should consider mandating that a customer be notified, after a reasonable period, if they are the target of a SAR. If a compelling reason exists, such as an ongoing criminal investigation, law enforcement could petition a court to delay that notification. Otherwise, citizens should eventually know if and why a report was filed on them. Doing so will help the public and Congress better understand how the current SAR system works and assess whether it is worth the cost.

Second, Congress should obtain from FinCEN, other relevant agencies, and financial institutions a complete and up-to-date list of all MCCs and other criteria used by financial services firms to categorize customer transactions and how that information is reported to the government. The level of possible intrusiveness of financial surveillance is inherently linked to the granularity of the data available.

Third, Congress should investigate the nature of interactions between financial institutions and the government around data sharing. The BSA and RFPA originally appeared to contemplate a largely arm's-length relationship; however, the relationships are now far more collaborative. Given this situation, changes to the law may be appropriate.

Fourth, Congress should investigate how relevant government agencies and financial institutions view their powers and limitations under the law. Given the secrecy of information sharing, those whose information has been shared find it almost impossible to challenge the exchange in court. This means that the judiciary may not be able to correct mistaken views of the law that government and industry

[24] The extent of the legitimacy of the BSA is beyond the scope of this testimony.

[25] See e.g. Norbert Michel and Jennifer Schulp, "Revising the Bank Secrecy Act to Protect Privacy and Deter Criminals" (Policy Analysis No. 932, Cato Institute, Washington, DC, July 26, 2022); Nicholas Anthony, "The Right to Financial Privacy" (Policy Analysis No. 945, Cato Institute, Washington, DC, May 2, 2023); David Burton and Norbert J. Michel, "Financial Privacy in a Free Society" (The Heritage Foundation, Report, Washington, DC, September 23, 2016). (Note: I am not endorsing every idea in these papers. Rather, I refer the Subcommittee to them as resources.)

[26] Many of these ideas are also included in my statement for the record entitled "Financial Privacy: Limits, Developments, and Ideas for Reform" (Statement for the Record submitted to the House Financial Services Committee, Mercatus Center at George Mason University, Arlington, VA, February 14, 2024).

may have. Congress's assessment of whether the understanding of government and industry conforms with both the law and congressional intent will help inform whether reform is necessary.

Fifth, financial institutions should be granted greater legal protection for pushing back in good faith on government requests that they consider outside the law or for failing to file SARs when they deem them unreasonable. This protection would need to shield institutions from regulators' informal efforts to punish them through procedural and formal actions.

Sixth, Congress should explicitly include a reasonableness requirement for all transfers of information, whether voluntary or—owing to a compulsive reporting requirement—obligatory. Law enforcement is limited to reasonable suspicion in other contexts, and it should not be different here. That standard should at a minimum prevent dragnet style mass requests or transfers based on nothing more than location or constitutionally protected activity. It should also allow for the suppression of evidence obtained or derived from unreasonable transfers in a subsequent trial as well as for a customer's private right to action against the government, the financial institution, or both.

Failing this, FinCEN should be required to define "suspicious" via regulation in a way that is consistent with the reasonableness requirement imposed on law enforcement in other contexts and that explicitly precludes dragnet style mass requests as well as reports based solely or primarily on constitutionally protected activity.

Seventh, Congress may wish to consider prohibiting the use of MCCs or other classifying criteria that directly relate to, or seek to identify, constitutionally protected activities. The most obvious is the purchase of firearms, but criteria that focus on political, religious, or other core constitutional rights could also endanger privacy. Congress may also wish to expand this restriction beyond constitutional rights to other highly sensitive issues such as healthcare.

Eighth, Congress should create or enhance a body—either within or outside of the relevant agencies—to investigate privacy issues and advocate for the protection of consumer privacy from excessive intrusion. This body should have the ability to access all necessary records, be able to compel testimony, and be insulated from pressure from agency management. Inspector generals could be one option, and an independent body could be another.[27]

Ninth, Congress should establish a clear statutory right to allow its members and staffers to promptly access relevant data from government agencies. Their access would be subject to proper handling requirements and necessary customer privacy protections but without the agencies' ability to prevent or unduly impede access. This is essential to meaningful oversight.

[27] The US Privacy and Civil Liberties Oversight Board presents one model, though any new outside agency should have its own subpoena power rather than relying on the Department of Justice.

CONCLUSION

Americans should not have to choose between having meaningful privacy and engaging with the modern economy. Recent efforts to use financial surveillance to prevent crime, while understandable, highlight a growing danger that our current financial privacy regime will effectively eliminate the ability of Americans to keep their movements, faith, political beliefs, and other sensitive activities private from the government without any meaningful protections or due process. This is not a conservative or liberal problem; it is not a Democrat or Republican problem. It is a problem that faces all of us, and we must be willing to enact necessary reforms to restore the proper balance between liberty and security. Otherwise, we risk ending up with neither.

Attachment: Brian Knight, "Financial Privacy: Limits, Developments, and Ideas for Reform," (Statement for the Record, Submitted to the House Financial Services Committee, Mercatus Center at George Mason University, Arlington, VA, February 14, 2024); Brian Knight, "Is the Bank Secrecy Act Vulnerable to Constitutional Challenge Over Post-January 6th Data Collection?" *FinRegRag*, February 26, 2024.

MERCATUS CENTER
George Mason University

STATEMENT FOR THE RECORD

FINANCIAL PRIVACY: LIMITS, DEVELOPMENTS, AND IDEAS FOR REFORM

BRIAN KNIGHT
Director of Innovation and Governance and Senior Research Fellow, Mercatus Center at George Mason University

US Congress, House Financial Services Committee
Oversight of the Financial Crimes Enforcement Network (FinCEN) and the Office of Terrorism and Financial Intelligence (TFI)

February 12, 2024

Thank you, Chairman McHenry and Ranking Member Waters, for the opportunity to submit this statement. My name is Brian Knight, and I am a senior research fellow at the Mercatus Center at George Mason University. My research is on financial services and financial services regulation as a tool of broader regulation, and I also study financial privacy. This statement is intended to help inform the committee of certain issues relevant to its jurisdiction and is not intended to support or oppose any given piece of legislation.

Americans' financial records contain some of the most personally sensitive information available. Yet, under current Supreme Court jurisprudence, Americans lack constitutional privacy protections. Through people's financial records, you could trace—with strong, though not perfect, accuracy—their movements, relationships, health, religion, political views, and activities.

As the Cato Institute's Nicholas Anthony points out,[1] threats to financial privacy have become increasingly ubiquitous as more and more Americans embrace electronic services such as credit and debit cards, automatic deposit, and apps like PayPal, leading to more data collection by financial services providers. This, in turn, has led these same providers to create data types, such as Merchant Category Codes (MCC), on top of consumer-provided information to help manage these transactions. As a collective result, people are being forced to leave a more and more detailed trail of their lives as a condition of engaging with the modern economy.

The very sensitivity and completeness of this data has made it attractive to law enforcement officials and others who hope to use it to surveil, interdict, and prosecute criminals. While these motives are laudable, the United States has long recognized that assisting law enforcement does not grant an

[1] Nicholas Anthony, "The Right to Financial Privacy" (Policy Analysis No. 945, Cato Institute, Washington, DC, May 2, 2023).

For more information or to meet with the scholar, contact
Mercatus Outreach, 703-993-4930, mercatusoutreach@mercatus.gmu.edu
Mercatus Center at George Mason University, 3434 Washington Blvd., 4th Floor, Arlington, Virginia 22201

unlimited justification to use sensitive data, and that precedence must be given to the right of its citizens to meaningful protection from "arbitrary invasions" of their privacy.[2] Additionally, for reasons discussed below, our current financial system may be sacrificing far too much privacy for limited benefit, making itself subject to abuse as a law enforcement tool intending to accomplish by financial regulation what cannot be accomplished by other means.

The remainder of this statement presents the following:

1. A sketch of the limits of financial privacy enjoyed by Americans
2. An overview of recent distressing developments regarding the use of financial records as tools of broad surveillance, including the use of personal data directly related to core constitutional rights
3. Ideas for reform that may inform Congress as it wrestles with how to allow legitimate law enforcement activity while protecting American citizens' privacy in a rapidly evolving world
4. Conclusion

1. LACK OF SUFFICIENT PROTECTION OF CUSTOMER PRIVACY

It is a bitter irony that federal law simultaneously prizes and denigrates the financial privacy of Americans. While laws such as the Gramm–Leach–Bliley Act impose significant duties on financial firms to protect customers' sensitive data from being compromised by outsiders,[3] laws such as the Bank Secrecy Act (BSA) not only enable but often require financial firms to share data with law enforcement without meaningful recourse by the customer.[4] It is as if government is telling customers, "your financial data should be safe and private, except from us." The problem is evident in reporting thresholds and requirements, the emergence of the "third-party doctrine," and informal pressuring by the government.

THE EROSION OF REPORTING THRESHOLDS AND THE EXTENSION OF REPORTING REQUIREMENTS

The problem of privacy infringements has exacerbated over time, as the scope of the BSA has expanded and as inflation has eroded the thresholds that initially limited reporting to relatively large sums. For example, when in 1974 the Supreme Court originally ruled in *California Bankers Association v. Shultz* that the BSA did not violate the Constitution, Justices Powell and Blackmun, who were the margin of victory, noted in their concurrence that because the Department of the Treasury had imposed a $10,000 threshold for reporting, the BSA did not impose an impermissible infringement on privacy.[5] While that threshold for reporting has not changed, the value of the dollar has. The worth of $10,000 in 1974 is approximately $63,900 today.[6] Further, the threshold for mandatory suspicious-activity reporting by banks is currently only $5,000 in aggregate.[7]

[2] See Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018).

[3] Gramm–Leach–Bliley Act, 15 U.S.C. §6801 *et seq.*

[4] Bank Secrecy Act, 12 U.S.C. §1829b; 12 U.S.C §1951–1960; 31 U.S.C §5311 *et seq.*

[5] California Bankers Association v. Shultz, 94 S. Ct. 1494, 1525–1526 (1974).

[6] US Bureau of Labor Statistics, CPI Inflation Calculator (database), accessed February 8, 2024, (https://www.bls.gov/data/inflation_calculator.htm).

[7] 31 C.F.R. §1020.320.

The justices also noted, however, that "a significant extension of the regulations' reporting requirements. . . would pose substantial and difficult constitutional questions."[8] Since 1974 there has been a significant extension of reporting requirements. Today, banks are permitted to voluntarily make reports on any "possible violation of law or regulation" and enjoy protection from liability.[9]

THE EMERGENCE OF "THIRD-PARTY DOCTRINE"

Consumer privacy has been further undercut by the emergence of the "third-party doctrine." For example, in *United States v. Miller*, the Supreme Court found that bank customers lack a privacy interest in their bank records.[10] In the case of checks and similar instruments, the Court reasoned that the customer shared those documents with recipients and banks, and therefore lacked a privacy interest. In the case of the banks' own records, the Court found that those records belonged to the bank, not the customer; therefore, the customer could not have a privacy interest in them.

Even laws to restrain the sharing of information and provide customers with recourse to protect their privacy, such as the Right to Financial Privacy Act (RFPA), provide, at best, extremely limited protection.[11] The RFPA contains so many exceptions to its provisions,[12] including for the reporting of "suspicious activities" under the BSA,[13] as to be almost meaningless. As such, extremely intimate details of a person's life are readily available to the government without substantial due process.

It is worth noting that the Supreme Court has recently refused to expand the logic of *Miller* to cell phone location data.[14] The Court reasoned that the reality of modern life and technology means that people inevitably leave a record of their movements by carrying their phone.[15] The Court also found that allowing the government unfettered access to that data would amount to "near perfect surveillance, as if it had attached an ankle monitor to the phone's user" as well as information about the user's past movements in a way traditional observation does not.[16] The Court also distinguished *Miller* on the grounds that, unlike checks, cell phone data isn't so much shared by the user as much as created automatically.[17]

To be clear, the Court did not overrule *Miller* but rather distinguished it. But when one considers the scope of information that law enforcement can access through modern financial records, the records' retrospective nature, and the need for people to interface with modern forms of financial services to survive, it is not hard to think that *Shultz* and *Miller* have become outdated.

---

[8] *Shultz*, 94 S. Ct. at 1526.

[9] 31 U.S.C. §5318(g); 31 C.F.R. §1020.320(f); see also 12 U.S.C. §3403(c).

[10] United States v. Miller, 96 S. Ct. 1619 (1976).

[11] 12 U.S.C. §3401 *et seq.*

[12] 12 U.S.C. §3413.

[13] 12 U.S.C. §3413(d).

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

[15] *Carpenter*, 138 S. Ct. at 2218.

[16] *Carpenter*, 138 S. Ct. at 2219–2220.

[17] *Carpenter*, 138 S. Ct. at 2220.

OPACITY AND GOVERNMENT PRESSURE

In addition to the formal, black-letter law obligations of financial firms under the BSA, there is also the possibility of informal pressure by the government on financial firms to share more information than may be required. Financial services firms are strongly incentivized to file suspicious activity reports (SARs) defensively, even if there is little reason to file them. This is because failure to file a SAR could result in being penalized, whereas excessive filing has no penalty beyond the burden of filing.

Financial services firms, especially banks, are also strongly incentivized to not push back on government requests. Because banks rely on their regulators' good graces to function, and are subject to regular and potentially burdensome supervision as well as a regulatory regime in which perfect compliance is impossible, they are uniquely vulnerable to being punished through informal means.[18] As such, while firms may voluntarily, perhaps even enthusiastically, share data, they may also do so to avoid both formal and informal government sanction.

It is important to recognize how limited the data available to the public and Congress is, regarding the use of SARs and other information sharing. The BSA prohibits notifying a customer if they become the target of a SAR.[19] Moreover, federal and state open records laws do not apply to such reports.[20] While FinCEN will periodically release some information about SARs,[21] it is by no means comprehensive, and it fails to provide insight into how many SARs actually result in meaningful leads or prove essential to preventing serious crimes. This opacity makes it impossible for Congress and the public to meaningfully assess whether the benefits of the system outweigh its burdens, or even what the benefits and burdens actually are.

2. ALLEGATIONS INVOLVING THE USE OF FINANCIAL RECORDS FOR SURVEILLANCE

Recent efforts to explicitly use financial records as a tool of surveillance and mass data collection raise troubling implications for Americans' privacy. These efforts have emerged from both the government and private sector, and while these efforts are at least purported to serve a worthy cause, they also risk producing significant damage for only limited benefit.

The most high-profile use of financial services records are the allegations raised by the House Judiciary Committee's Select Subcommittee on the Weaponization of the Federal Government. The subcommittee alleged that the FBI worked with banks to obtain records based on broad criteria, such as whether the customer had purchased a firearm and been in Washington, DC, around the January 6 riots.[22] Evidence presented by the subcommittee indicates that law enforcement collaborated with

[18] For a more detailed discussion of this dynamic, please see Julie Hill, "Regulating Bank Reputation Risk," *Georgia Law Review* 54, No. 523 (2020). See also Nicholas R. Parrillo, "Federal Agency Guidance and the Power to Bind: An Empirical Study of Agencies and Industries," *Yale Journal on Regulation*, No. 165 (2019); The Financial and Business Law Scholars as Amici Curiae, 3–27, The National Rifle Association of America v. Maria T. Vullo.

[19] See e.g. 31 U.S.C. §5318(g)(2); 31 C.F.R. §1020(e).

[20] 31 U.S.C §5319.

[21] See e.g. Financial Crimes Enforcement Network, *FinCEN FY 2022 Year in Review*, April 21, 2022.

[22] See US House of Representatives, *Interim Staff Report, Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government*, May 18, 2023; Chairman Jim Jordan, letter to Christopher Wray, Director, Federal Bureau of Investigation (Wray letter), January 17, 2024; Chairman Jim Jordan, House Committee on the Judiciary, letter to Noah Bishoff, AML Officer, Plaid Inc., (Bishoff letter), January 17, 2024.

banks on shaping data requests and used criteria that was both broad and tied directly to constitutionally protected activity, such as the purchase of firearms and religious and political activity.

As a threshold matter, it is important to note that there is limited information publicly available regarding the subcommittee's recent allegations that the FBI, FinCEN, and financial services firms collaborated to obtain large amounts of customer information based on broad and sensitive criteria. As more information is released, the picture may change significantly. Based on what is now available, however, the implications are troubling.

One of the subcommittee's allegations is that Bank of America (BoA) provided, either at the request of the FBI or on its own initiative,[23] a list of customers who (1) used a BoA card in the Washington, DC, area on the days surrounding January 6, (2) purchased a firearm with the card, and (3) traveled to or rented lodging in the DC area at the relevant time.[24] While a significant number of customer records were allegedly provided, it is also alleged that those records were ultimately removed from FBI systems because they "lacked allegations of federal criminal conduct."[25]

The subcommittee also claims that FinCEN circulated materials to financial services firms that recommended using search terms directly related to political activity, such as "MAGA," the purchase of books—including religious books—or the consumption of media that espoused "extremist views."[26] It is not clear what would constitute an extremist view for these purposes, but the potential use of the financial system to monitor Americans' political activity, speech, and religious pursuits is troubling.

FinCEN also allegedly distributed material created by KeyBank discussing ways to identify potential violent extremists using a combination of MCCs, vendor names, and purchase thresholds.[27] Many of the MCCs and other criteria were inherently and dramatically overinclusive, such as those covering sporting-goods stores, pawn shops, or popular retailers like Dick's Sporting Goods and Bass Pro Shops. Of note, some of the MCCs KeyBank used were attached to arms manufacturing. These MCCs were not established by the International Organization for Standardization (ISO) and are not in use by all banks.[28] While many MCCs are standardized, MCC 3000-3999 are "reserved for private use."[29] Therefore, it is possible that banks have established MCCs that may relate to sensitive and constitutionally protected activities that are not publicly known. This would allow banks and the government to more easily search for economic activity that, while controversial, is constitutionally protected or extremely sensitive.[30]

---

[23] There are discrepancies between witness testimony and documents as to whether the FBI or BoA initiated the data exchange.

[24] Wray letter.

[25] Wray letter.

[26] Bishoff letter.

[27] Bishoff letter.

[28] For a greater discussion of the KeyBank MCCs please see Brian Knight, "(Updated) MCCs and Financial Privacy, Again," *FinRegRag*, January 18, 2024.

[29] Knight, "(Updated) MCCs and Financial Privacy, Again."

[30] This concern is by no means shared only by conservatives. After the Supreme Court ruled that there was no right to an abortion under the US Constitution, many were concerned that their banking records could be used to identify them having an abortion. See e.g. Alejandra Caraballo, "Payment Data Could Become Evidence of Abortion, Now Illegal in Some States," *New York Times*, June 29, 2022.

KeyBank is not the only firm that wished to use MCCs as part of a surveillance program. At the prompting of Amalgamated Bank, the City of New York, and various pension funds, ISO established an MCC for gun stores.[31] The justification was that the MCC allowed banks to potentially detect activity that could indicate an imminent crime, especially a mass shooting, and alert law enforcement via a suspicious activity report.[32]

While the desire to prevent violence is laudable, the use of MCCs for this purpose is unlikely to be effective.[33] The data would be both over- and underinclusive, because it would capture information on merchants rather than purchased items. It would also rely on bank personnel being able to assess what was truly suspicious, which is unlikely. Finally, it would add numerous additional SARs, most of which are unrelated to any crime, to a system that already receives over four million SARs per year.[34] It is not clear how many SARs are followed up on, but a small study by the Bank Policy Institute in 2018 found that a median of 4 percent of SARs resulted in a law enforcement follow-up.[35]

While such preemptive surveillance would be unlikely to provide much benefit, it would be expensive to administer and would subject Americans to even more intrusive surveillance. These concerns prompted several states to prohibit the use of the gun store MCC, though California has recently mandated its use.[36] California explicitly justified its law as using financial services as a surveillance tool to preempt crime.[37]

In summary, there is evidence of ongoing—and increasing—efforts to use financial data as a tool of preemptive and sweeping surveillance. These efforts directly target constitutionally protected activities—an outcome that risks significant threat to Americans' rights. It is critical that Congress have a complete picture of how financial surveillance is being used and ensure it conforms to the American model of constitutional self-governance.

3. AREAS OF POSSIBLE REFORM

Efforts to reform the BSA and other data-sharing laws are long-standing. Much excellent work has already been done, and I commend the committee to consider it. For example, the scholars at the Cato Institute have written extensively about ways to more broadly reform the BSA.[38] I will limit my ideas

[31] See Associated Press, "Visa, Mastercard, AmEx to Start Categorizing Sales from Gun Shops," *NBC News*, September 10, 2022; Leah Collins, "Amalgamated Bank CEO on Why We Can and Should Track Gun Purchases on Cards," *CNBC*, July 13, 2022.

[32] Kate Fitzgerald, "Will New Merchant Code for Gun Sales Turn Issuers into Morality Police?" *American Banker*, September 16, 2022.

[33] For a more detailed discussion of why using MCCs to prevent mass shootings would be unlikely to be effective please see Brian Knight, "More Questions about Credit Card MCCs for Gun Stores," *FinRegRag*, September 22, 2022; Brian Knight, "More Thoughts on the Use of MCCs for Law Enforcement Tracking," *FinRegRag*, January 24, 2024.

[34] *FinCEN FY 2022 Year in Review*.

[35] Bank Policy Institute, *Getting to Effectiveness—Report on US Financial Institutions Devoted to BSA/AML and Sanctions Complications* (Washington, DC, October 29, 2018).

[36] Caitlin Mullen, "States Split Over Gun Merchant Category Code," *Payments Dive*, October 2, 2023.

[37] Mullen, "States Split Over Gun Merchant Category Code."

[38] See e.g. Norbert Michel and Jennifer Schulp, "Revising the Bank Secrecy Act to Protect Privacy and Deter Criminals," (Policy Analysis No. 932, Cato Institute, Washington, DC, July 26, 2022); Nicholas Anthony, "The Right to Financial Privacy," (Policy Analysis No. 945, Cato Institute, Washington, DC, May 2, 2023).

primarily to areas mentioned in the recent allegations and the efforts to increase the use of the payments system as a tool of preemptive surveillance.

First, greater transparency is essential. FinCEN and other relevant agencies should be required to report to Congress and the public not only the number of SARs and other reports they receive but also the number of SARs and reports that are (1) followed up by law enforcement, (2) used to open new investigations that result in prosecutions and convictions, and (3) not used. The relevant agencies should also report on the time it takes for SARs to be used by law enforcement. This last point is relevant to how effective SARs could be at preempting a crime rather than simply assisting in a post-crime investigation.

Second, Congress should consider mandating that a customer be notified, after a reasonable period, if they are the target of a SAR. If a compelling reason exists, such as an ongoing criminal investigation, law enforcement could petition a court to delay that notification. Otherwise, citizens should eventually know if and why a report was filed on them. This will help the public and Congress better understand how the current SAR system works and assess whether it is worth the cost.

Third, Congress should obtain from FinCEN, other relevant agencies, and financial institutions a complete and up-to-date list of all MCCs and other criteria used by financial services firms to categorize customer transactions, and how that information is reported to the government. The level of possible intrusiveness of financial surveillance is inherently linked to the granularity of the data available.

Fourth, Congress should investigate the nature of interactions between financial institutions and the government around data sharing. The BSA and RFPA appeared to contemplate a largely arm's-length relationship; however, there are indications that the relationship is far more collaborative. If this is the case, changes to the law may be appropriate.

Fifth, Congress should investigate how relevant government agencies and financial institutions view their powers and limitations under the law. Given the secrecy of information sharing, those whose information has been shared find it almost impossible to challenge the exchange in court. This means that the judiciary may not be able to correct mistaken views of the law that government and industry may have. Congress's assessment of whether the understanding of government and industry conforms with both the law and congressional intent will help inform whether reform is necessary.

Sixth, financial institutions should be granted greater legal protection for pushing back in good faith on government requests they believe to be outside the law, or for failing to file SARs when they deem them unreasonable. This protection would need to shield institutions from regulators' informal efforts to punish them through procedural, as well as formal, actions.

Seventh, Congress should explicitly include a reasonableness requirement for all transfers of information, whether voluntary or—due to a compulsive reporting requirement—obligatory. Law enforcement is limited to reasonable suspicion in other contexts, and it should not be different here. That standard should at a minimum prevent "dragnet-style" mass requests, or transfers based on nothing more than location or constitutionally protected activity. It should also allow for the suppression of evidence obtained or derived from unreasonable transfers in a subsequent trial, as well as a customer's private right to action against the government, the financial institution, or both.

Eighth, Congress may wish to consider prohibiting the use of MCCs or other classifying criteria that directly relate to constitutionally protected activities. The most obvious is the purchase of firearms, but criteria that focus on political, religious, or other core constitutional rights could also endanger privacy. Congress may also wish to expand this restriction beyond constitutional rights to other highly sensitive issues such as health care.

Ninth, Congress should create or enhance a body—either within or outside of the relevant agencies—to investigate privacy issues and advocate for the protection of consumer privacy from excessive intrusion. Inspector generals could be one option, and an independent body could be another.

Finally, Congress should establish a clear statutory right to allow its members and staffers to access relevant data from government agencies. Their access would be subject to proper handling requirements and necessary customer privacy protections, but without the agencies' ability to prevent or unduly impede access. This is essential to meaningful oversight.

4. CONCLUSION

Americans' lives are written in their bank accounts. Engaging with the modern economy necessitates that Americans leave a trail of information that can be used to build a reasonably accurate and complete picture of a person's travels, interests, beliefs, and problems. This information is regarded by the government as extremely sensitive, yet it enjoys severely limited protection from government intrusion.

While sharing information on consumers may, at times, be useful to law enforcement, it also poses serious risks of abuse and excessive intrusion into the private lives of Americans. This country was founded on the notion that the government should not have a general warrant to surveil its citizens, and that even the legitimate needs of law enforcement must be balanced against, and often subsumed by, the need to protect reasonable privacy.

Recent events and allegations raise concerns that this balance is increasingly slighted. Congress should mandate greater transparency, examine the current system, and initiate reforms as appropriate to preserve legitimate law enforcement capabilities within the limits of meaningful privacy protections.

Is the Bank Secrecy Act Vulnerable to Constitutional Challenge over post January 6th Data Collection?

Recent allegations raise the question of whether the Bank Secrecy Act is ripe for challenge, and may provide the vehicle to do so.

BRIAN KNIGHT

FEB 26, 2024

Share

Source

Important caveat: There is limited information available publicly about what banks and law enforcement did post January 6th, or how they operate the Bank Secrecy Act generally. New information may materially change this analysis.

The Federal Government's use of financial records to attempt to identify suspects and preempt potential violence after the January 6th riots is, to put it mildly, controversial.

Based on disclosures made by the House Judiciary Committee's Select Subcommittee on the Weaponization of the Federal Government (Subcommittee) it appears that after the events of January 6th law enforcement and financial institutions collaborated to search financial records, including credit and debit card transactions and Venmo payments, as well as the notes the customers wrote on Venmo.

These searches were allegedly based on certain broad criteria, including whether they involved merchants that might sell firearms, as well as certain religious and political affiliations and geographic locations. The searches were conducted to identify potential suspects or people who may be planning violence in the future. It is also implied by the evidence released that law enforcement and financial firms have been using, or at least considering using financial surveillance to preempt other crimes, such as mass shootings.

This was and is presumably done under the auspices of the Bank Secrecy Act (BSA) which provides the government with broad powers to access financial records and firms broad powers and protections from liability for sharing records, either at the request of the government or on their own motion via a Suspicious Activity Report (SAR). In theory only records indicating "suspicious" transactions should be shared, but suspicious isn't meaningfully defined. The Supreme Court has previously upheld the Bank Secrecy Act as constitutional and ruled that customers don't have a privacy interest in their bank records.

However, I wonder if the current controversy provides an opportunity to challenge the BSA, at least as applied in cases like the current allegations, where financial data isn't used to support a prosecution of a previously identified suspect, but rather as a dragnet

to try to find suspects, perhaps before a crime has even occurred. To be sure, a challenge would not be easy to win, but the current facts as alleged and recent Supreme Court precedent may combine to provide a unique chance.

Below I will discuss some of the reasons why this may be an especially good opportunity to challenge the BSA. First however, I want to throw myself on the mercy of the readership and acknowledge that while I am a lawyer and an active member of a state bar this is meant to be a "quick and dirty" analysis and I am not an expert on litigation procedure or the Fourth Amendment. As such, it won't cover everything, and I may have missed something important. Constructive feedback is very much appreciated! With that out of the way let's get going.

Plaintiffs

One advantage of the current situation is that it may be easier to find plaintiffs. Finding plaintiffs in BSA suits is challenging. First, transfers of information like Suspicious Activity Reports are supposed to be kept secret from the target by law. Even the Right to Financial Privacy Act (RFPA), which was passed to provide customers notice of their records being shared with the government and in most cases to be able to challenge the transfer in court, excludes reports made pursuant to the BSA. This means that most targets of SARs likely never know their information was sent to the government, which makes it impossible to be able to sue over it.

Second, while there is one group who learn they were the subject of a SAR, that group is defendants. If the government uses bank records obtained via the BSA in a prosecution the defendant will likely find out about it, but that is a suboptimal place to start from.

The current situation is unique. Due to the Subcommittee's work, we know of at least some criteria used to identify records the government wanted to obtain. A customer who meets those criteria (and didn't participate in the attack on the Capitol or another serious violent crime) could potentially argue that they have a reasonable basis to believe their information was shared in violation of the Fourth Amendment.

The Legal Argument

Skipping over other procedural issues let's assume that ultimately the Supreme Court must look at the legal and constitutional argument that as applied to the current allegations the BSA violates the Constitution. How could that argument be made?

The first challenge the plaintiffs will face is that existing precedent mentioned earlier, especially the 1976 case, United States v. Miller which held that a person lacks a privacy interest in their bank records, either because the person shared those records with others in the course of commerce or because the person doesn't own the records, the bank does.

To briefly explain Miller, after getting a tip from an informant on possible bootlegging and a fire at a warehouse rented by Miller revealing a still and a large amount of untaxed whiskey law enforcement requested Miller's bank records from his banks via subpoena. Miller sought to have the records suppressed because they weren't obtained with a warrant, violating the Fourth Amendment. The Supreme Court ruled against Miller, finding that he lacked a privacy interest in his checks, because he shared those with others through commerce. The Court also ruled Miller lacked an interest in the other bank records because they weren't his papers, they belonged to the bank.

The bad news is that it is not great to have existing Supreme Court precedent on the very topic at issue that goes against you. The good news is that there is a more recent precedent that may provide a roadmap for distinguishing, if not outright overturning Miller.

That case is Carpenter v. United States, a 2018 case where the Court declined to extend Miller and related cases to the context of cell phone tower location tracking. To have the best chance of success the plaintiffs will need to convince the court that the current facts and interests at play are sufficiently different from those in Miller, and close enough to Carpenter, that the Court should distinguish Miller. (There are some other arguments outside the Miller/Carpenter tension that could be made, and we will address them briefly later.)

In Carpenter a 5-4 Court, in an opinion written by Chief Justice Roberts, found that law enforcement accessing cell phone location data was a search for Fourth Amendment purposes and therefore generally required a warrant. The Court ruled that while the cell

phone company, not the customer, owned the records, the information they contained was so sensitive and violative of privacy that Fourth Amendment protections needed to apply.

To come to this conclusion the Court held that a person generally has a reasonable expectation of privacy in their movements and cited the ubiquity and necessity of cell phones to function in modern life, with them becoming "a feature of human anatomy" that rarely leaves a person's side and therefore can create a very robust trail of a person's movements. The scope of information the records could provide as to one's location, including the retrospective nature of the records, would allow law enforcement to obtain information it could never obtain by mere observation. The Court also noted how creating these records isn't voluntary because they are created automatically whenever the phone is on.

Distinguishing Miller

So how could the plaintiffs distinguish Miller? And how could they get the Court to think that Carpenter is a better fit?

First, to distinguish Miller the plaintiffs could argue that unlike Miller, where the financial records were only obtained after a suspect was identified by traditional law enforcement techniques, the current situation is more like a dragnet, where law enforcement uses broad criteria to sweep in the records of many innocent people without necessarily finding a legitimate suspect. What's more, the criteria law enforcement used touched on highly sensitive information like a customer's speech, religion, location, political affiliation, and use of Second Amendment rights. It is possible that the search was so overinclusive as to be an unreasonable search under the Fourth Amendment.

The plaintiffs could also argue that in Miller the financial records were necessary to prove the allegations Miller was accused of, since they were financial crimes. In the present case, the records are primarily used to build a pool of suspects for non-financial crimes.

Finally, plaintiffs could argue that at least Miller's records were obtained via subpoena. In the present case it appears that financial firms collaborated with law enforcement

before any requests were formally made and then the information was conveyed via SAR. This process prevented any outside check or review prior to the information being turned over.

Of course, the main effort should be to persuade a court that the sharing of Jan. 6 information is more like Carpenter than Miller; it may not be enough to just distinguish Miller. Plaintiffs will need to convince the Court that the Fourth Amendment should apply in this case. To follow Carpenter plaintiffs will need to show that they have a reasonable expectation of privacy, that the information in the records is highly sensitive, and that its creation is necessary and inevitable as a condition of modern life. There are good arguments for this.

Privacy

First, American law creates a reasonable expectation of privacy, and to some degree ownership, in one's financial records.

The Right to Financial Privacy Act places at least some restrictions on the government's access of financial records and the ability of financial firms to share such records with the government. While there are so many exceptions, they arguably swallow the rule, the RFPA at least shows a legislative policy that people have a privacy interest in their records not being shared with the government without process.

Other federal laws like Gramm-Leach-Bliley require financial firms to safeguard a customer's sensitive data and govern how that data can be used and shared. If that data is illegally accessed by a third party due to the firm's negligence, or misused by the firm itself, the government will punish the firm.

It isn't just liability either. Section 1033 of Dodd-Frank grants consumers data access rights to certain records held by a financial firm. The Consumer Financial Protection Bureau has proposed a rule based on this provision that would require covered firms to make their covered records available to the customer or their agent, with an eye to facilitating greater competition by making it easier for customers to switch providers.

The way the law treats consumer financial records not only shows that the government thinks consumer financial privacy is important, but also that the records a financial firm

creates aren't like other records. It would be odd for the government to punish a firm who suffered a breach of its own information or used its own information to increase profits, or make the firm share information with its rivals to its detriment. Yet this is done as a matter of course in the financial space because we recognized how sensitive that information is for customers and have given them an enhanced interest in the records made about them.

Further, banks and other financial firms trumpet how secure they are, priming customers to expect their data to be private. Yes, there is no doubt fine print in the privacy statements explaining how it will be shared and is at risk, but the message firms are trying to have stuck in people's heads is that *their* data is safe.

Sensitivity

Arguing that financial information is sensitive is probably the easiest part of a plaintiff's argument. Americans' lives are written in their bank records. What makes the data sensitive is also what made it attractive to law enforcement in the current case, it can provide a very rich, though not perfect, portrayal of a person's life, interests, beliefs, health, and yes, location. In fact, in his dissent in Carpenter, Justice Kennedy noted that financial records were if anything *more* sensitive than the cell cite location data at issue because unlike that data financial records could reveal not just location but the person's medical history, sexual orientation, friends and family.

Justice Kennedy was exactly right. The data at issue in the current situation related to Jan. 6 is potentially far more sensitive than what was at stake in Carpenter. Banks and the government allegedly sought to use financial data to identify people with certain political and religious beliefs, who engaged in certain constitutionally protected activities like buying a firearm (or at least something at a store affiliated with firearms) or participating in a political rally, and who were in certain locations at certain times. In using these broad criteria, they almost certainly swept in far more innocent people who had the intimate details of their lives exposed to the government than guilty parties.

Further, like the information in Carpenter bank records are retrospective in nature, allowing law enforcement to not just observe a person in public at a given moment, but

pour over the history of their lives for years. In fact, the law requires the banks preserve records for a period of years to ensure they are available for law enforcement to access.

Finally, the fact that technology makes these records relatively easy to access, and query, and the fact that the firms, rather than the government pay for their upkeep and complying with the law, means it allows for a scope and persistence of surveillance that was unthinkable in the past. The police at the time of Miller had to reckon with resource limitations far greater than those currently faced by law enforcement, limiting the use of financial surveillance as a tool.

Necessity

The next question will be whether it is necessary to make such records, or if people choose to do so, and therefore could choose not to. Here the plaintiffs can point out that to engage in the modern economy one must interact with a financial intermediary who will create the type of records at issue and be bound to provide them to law enforcement. Living by cash alone simply isn't possible unless one is willing to separate from mainstream society.

Living by cash alone also isn't safe, economically, or physically. Electronic finance via intermediaries is frequently safer, often due to public policy. Card transactions have certain fraud protections. Bank deposits have insurance. Wires provided by the Federal Reserve are faster, cheaper, and more secure than moving large amounts of money around via truck. The government makes electronic finance safer than cash; can it then hold that against people when it comes to privacy?

It isn't just economic safety though. Not carrying cash makes one less attractive to potential muggers. It is not surprising that cannabis firms who face impediments to bank accounts cite safety as a major reason they should get access.

Under the law financial firms *must* create and maintain certain records, so people can't "shop around" to find the most privacy friendly, at least vis-à-vis the government, bank, or credit card. The reality is that if one wishes to engage with the modern economy, one must leave a copious stream of records currently accessible to the government without Fourth Amendment protections.

Other Arguments

The plaintiffs could also consider arguing that the government's actions in this case impeded other constitutional rights. It is alleged that the government and banks used terms relating to political and religious activities and gun ownership, and asked for messages created by customers, rather than just the financial firms, in other words their speech, to be searched. It may be worth considering an argument that this activity could chill other constitutionally protected activities.

Plaintiffs could also argue that federal law in effect gives them an ownership right in their financial data. The laws discussed above that give rise to an expectation of privacy also give customers certain ownership-like rights and treat financial firms as less than pure owners of the data. As discussed below, the law has changed in this regard since Miller, and this might help swing over at least one justice who dissented in Carpenter.

These arguments would be outside the Carpenter road map. But that may be a good thing because Carpenter was a close case and the textualist wing of the Supreme Court were the dissenters.

Headwinds

A successful challenge is by no means certain. Plaintiffs will face serious headwinds. One of the most obvious is that the textualist wing of the Supreme Court disagreed with the holding in Carpenter. The primary reason is that they reject the formulation of the Fourth Amendment as a right to privacy. Instead, they believe the Fourth Amendment provides a right to not have one's home, papers, and effects ransacked. Yes, this has a benefit for privacy, but what matters is ownership. To the dissenters it is hard to see how a person has a protectable interest in someone else's records.

However, not all is lost. Justice Gorsuch is no fan of Miller, and his dissent lays out an alternative method of getting to the Fourth Amendment that could be relevant here. Gorsuch, like the other dissenters, believes that the Fourth Amendment is about ownership, not a general expectation of privacy. To Gorsuch the question is whether something is "yours under law." However, he does not believe that total or exclusive ownership is necessary.

Instead, Gorsuch believes that law can grant sufficient ownership rights in others' records to prompt Fourth Amendment protection. In his Carpenter dissent he points to federal law that gives customers certain rights over cell-site location and limits the ability of the cell-phone company to use or share the data.

This sounds like how federal law treats customer financial records, even going so far as to require certain firms to make certain data available to their competition if requested by the customer. Of course, the law may cut both ways. The Right to Financial Privacy Act for example explicitly permits things like SARs, and while the law has expanded consumers' interest in the privacy of their financial records against private actors since Miller was decided, it has eroded it against the government. On the other hand, Gorsuch might argue that the Government can't slice the salami that finely, and that once the law grants someone a certain type of interest in an item, the constitutional protection is inseparable from that interest.

The Circumstances around the Request

Another impediment is the reality that the requests at issue arose to respond to the extremely serious crimes of Jan. 6 and to prevent violence at the presidential inauguration or other types of extreme violence like mass shootings and terrorist events. Preventing events like these is a legitimate role of government.

This reality may make it hard for the Court to second guess the likely claim from law enforcement that even if *these* inquiries weren't terribly useful, the tools law enforcement used are too important to be taken away. The argument will be made that requiring a warrant would delay things too much and prevent serious crimes from being interdicted.

That claim should not go untested. We don't know how quickly the government tends to react to a SAR, or how many SARs are useful, or really anything about the effectiveness of this system. Just because it is *possible* using the BSA in this manner could prevent serious crimes, that doesn't make it plausible. And it is prevention on which the government's argument must rest. If the government is investigating a crime that has already occurred a warrant should be no impediment.

Beyond the practical, there is also an important philosophical reason to be skeptical of the government's likely necessity argument. While it is undeniable that law enforcement was responding to serious threats, that is not a blank check. The Bill of Rights is intended to protect people against government excesses, and it is in the face of serious threats that those excesses are most likely to occur. If the American people would prefer to tilt the balance in favor of government power, they could amend the Constitution to modify or remove the Fourth Amendment. They haven't done so.

Further, as the Chief Justice notes in Carpenter, there are certain exceptions to the Fourth Amendment's warrant requirement for exigent circumstances. While one hopes these exceptions do not swallow the rule, it is at least unlikely those exceptions would cover the type of wide-ranging collection of customers' data based on broad terms currently alleged.

Conclusion

The allegations of government surveillance are troubling, as is the lack of protection for consumers' financial privacy. The current situation may present a unique opportunity to challenge the BSA and restore at least some strictures around the government's access to some of the most sensitive data around. If nothing else, it might force the Court to reevaluate its holding in Miller considering the reality of the modern economy. Whether it will be attempted, and whether any attempt will work, remains to be seen, but it might be worth a try. If nothing else, raising more awareness of how the system currently operates will help voters and Congress make more informed policy choices.