The Right to Financial Privacy

Crafting a Better Framework for Financial Privacy in the Digital Age

By Nicholas Anthony

October 14, 2022

CATO WORKING PAPER
No. 69

The Right to Financial Privacy

Crafting a Better Framework for Financial Privacy in the Digital Age

Nicholas Anthony

Nicholas Anthony is a policy analyst at the Cato Institute's Center for Monetary and Financial Alternatives.[1]

Financial privacy in the United States has been in disrepair for over 50 years, and it's getting worse. Not only are decades-old beliefs (e.g., the third-party doctrine) outdated for the digital age, but the merits of those beliefs are also highly questionable. Efforts, both new and old, to surveil and collect data on American's financial activity show that now is time to craft a better framework for financial privacy. But Congress may not need to look far for ideas on how to protect American's financial privacy.

The Right to Financial Privacy Act, originally enacted in 1978 in response to how the Bank Secrecy Act and the third-party doctrine weakened the protections of the Fourth Amendment, has already set a foundation for some of the protections needed today. However, it is largely due to a long list of exceptions for law enforcement and other government agencies in the Right to Financial Privacy Act that much of the financial surveillance over the past 50 years has not only been permitted to occur away from the public eye, but also to expand.

Part of the challenge is due to the fact that the "right to financial privacy goes to the heart of the tension between an individual's right to conduct [his or her] business without governmental

intrusion and the government's legitimate need for information in law enforcement."[2] But striking this balance is not an insurmountable task. While critics point to curbing criminal activity to justify invading the public's financial privacy,[3] there should be stronger protections so long as the U.S. justice system maintains that the public is innocent until proven guilty. Neither fishing expeditions nor thread pulling that *may* lead to investigations should be considered a sound justification when financial information can reveal a person's relationships, profession, religion, political leanings, locations, and so much more.[4] Law enforcement still has a role to play in a future with stronger financial privacy protections, but that role would be, and should be, restricted by the Fourth Amendment to the Constitution.

To restore Americans' financial privacy, Congress should amend the Right to Financial Privacy Act to remove the list of exceptions to its protections. Removing the exceptions will not bar law enforcement and other government agencies from access to financial information. Instead, it will merely require that government agencies acquire a warrant through the judicial process. During the last few years, Americans have seen time and time again how financial privacy can be violated by unchecked government authorities.[5] Now is the time to establish the protections that should have been in place from the beginning, and especially now amidst the digital age.

Trouble in the Wake of the Bank Secrecy Act: A Brief History Leading to the Right to Financial Privacy Act

The Bank Secrecy Act was signed into law by President Richard Nixon on October 26, 1970.[6] At the time, the Bank Secrecy Act—a response to concerns over the use of secret foreign

bank accounts[7]—made two major changes to the U.S. financial system: (1) the requirement that U.S. financial institutions maintain records "where such records have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings," and (2) the requirement that U.S. financial institutions report certain financial transactions to the U.S. Treasury.[8] In other words, the Bank Secrecy Act deputized American financial institutions as de facto law enforcement investigators. And although this initial form of the Bank Secrecy Act was only a fraction of what can be seen today, it did not take long for people to recognize how the law conflicted with the Fourth Amendment to the U.S. Constitution considering it forced financial institutions to report information that the government would otherwise need a warrant to obtain.

By 1972, a group including the American Civil Liberties Union (ACLU), California Bankers Association, and Security National Bank applied for a temporary restraining order in the United States District Court for the Northern District of California in an effort to stop the enforcement of the Bank Secrecy Act.[9] The group principally argued that the Bank Secrecy Act violated the Fourth Amendment's protection from unreasonable search and seizure as well as the protections in the First and Fifth Amendments. In response, the District Court issued a temporary restraining order to halt the Bank Secrecy Act's enforcement while the complaint could be reviewed.[10] However, the order was lifted after the District Court held that most of the Bank Secrecy Act was constitutional. Yet efforts to stop the Bank Secrecy Act did not stop there.

In 1973, Representative Fortney Stark (D-CA) led a separate effort in Congress to enact legislation—a first draft of what would later be enacted as the Right to Financial Privacy Act—seeking to better protect financial privacy.[11] Representative Stark argued that the Bank Secrecy Act undermined the long-held tradition of confidentiality between bankers and customers.[12] Although there does not exist a binding expectation of confidentiality like one has with doctors

or lawyers, Representative Stark's bill was designed in part to protect and preserve the long unwritten expectation of confidentiality between bankers and customers.[13]

In 1974, Congress made a step forward with the passage of a separate piece of legislation, titled the Privacy Act.[14] The Privacy Act established requirements for government agencies disclosing, handling, accessing, and maintaining information. More so, should a federal agency fail to adhere to these standards, the Privacy Act gave American citizens grounds to sue the agency. Nonetheless, the Privacy Act included many exceptions, resulting in privacy protections that do not apply consistently with law enforcement or even at all under circumstances deemed as "routine use."[15]

Also in 1974, the question of financial privacy reached the Supreme Court after a series of appeals—from both the plaintiffs and the government—in *California Bankers Association v. Schultz*. After reviewing the case, the Supreme Court held at the time that the Bank Secrecy Act did not violate the First, Fourth, or Fifth Amendments. In the majority opinion, the Supreme Court held that the Bank Secrecy Act was not an undue burden considering it applied to "abnormally large transactions," those of $10,000 or more.[16] For instance, at the time, one could purchase two brand new Corvettes for that price.[17] However, Justices Lewis Powell and Harry Blackmun warned in a concurring opinion that, "A significant extension of the regulations' reporting requirements, however, would pose substantial and difficult constitutional questions for me… At some point, governmental intrusion upon these areas would implicate legitimate expectations of privacy."[18]

In 1976, the question of financial privacy was again brought to the Supreme Court in *United States v. Miller*. When considering a case in which the U.S. Treasury Department's Bureau of Alcohol, Tobacco, and Firearms presented grand jury subpoenas to collect the records of a

suspected bootlegger's (Mitchell Miller's) financial activity, the Court argued that Americans do not have a right to privacy when they share information with a third party (e.g., a bank or other financial institution). The Court wrote, "The depositor takes the risk, in revealing his [or her] affairs to another, that the information will be conveyed by that person to the Government."[19] This decision came to be known as the "third-party doctrine."[20] As described by the Electronic Privacy Information Center (EPIC), so long as the "records are developed or maintained during the course of an ordinary business relationship by a person other than the subject of those records, the subject has no expectation of privacy and thus, no constitutional protection."[21] With that, after years of citizens trying to push back against the Bank Secrecy Act, the Court seemingly made it stronger than ever before.

In 1977, the Privacy Protection Study Commission (PPSC)—a commission created by Congress with the passage of the Privacy Act of 1974—issued a report titled, "Personal Privacy in an Information Society."[22] The commission argued that "as records continue to supplant face-to-face encounters in our society, there has been no compensating tendency to give the individual the kind of control over the collection, use, and disclosure of [his or her] information."[23] They noted that many challenged the Bank Secrecy Act because of the questions it raises regarding not only the confidentiality between customers and financial institutions, but also the "relationship between government and citizens in a free society."[24] More so, the commission argued that the 1974 Privacy Act "had not resulted in the general benefits of the public that either its legislative history or the prevailing opinion as to its accomplishments would lead one to expect…"[25] So while the 1974 Privacy Act may have been a step forward, it did not do enough to protect Americans' privacy broadly and it certainly did not protect American's financial privacy.

In 1978, the Right to Financial Privacy Act was finally enacted after being first drafted at least 5 years earlier. And at first glance, the Right to Financial Privacy Act appeared to be a much needed solution to the concerns born out of the Bank Secrecy Act. A deeper read of the legislation, however, shows that Americans were left with much to be desired.

The Right to Financial Privacy Act of 1978

Although financial privacy took many heavy hits from the Bank Secrecy Act, Americans did not leave the 1970s completely defenseless against government intrusions. Just two years after the Supreme Court established the third-party doctrine,[26] Congress passed the Right to Financial Privacy Act—an act that was "essentially designed to reverse the [Supreme Court's] decision in [*United States v. Miller*] in the context of financial records and provide standing for individuals to complain about the improper release of information about them in records maintained by financial institutions."[27] With that said, both in practice and on paper, the Right to Financial Privacy Act did not offer the privacy protections its name suggests.

At its core, the Right to Financial Privacy Act established a process for notifying the public of when the government requests their financial information and providing the public the opportunity to challenge said requests.[28] More so, it established clear requirements for government officials seeking information.[29] These protections cover information held by depository institutions; money service businesses, money order issuers, sellers, and redeemers; travelers check issuers, sellers, and redeemers; the U.S. postal service; securities and futures industries; futures commission merchants; commodity trading advisors; and casinos and card

clubs. In short, the Right to Financial Privacy Act tried to strengthen privacy protections through new requirements.

Unfortunately, the Right to Financial Privacy Act has a major weakness: 12 U.S. Code Section 3413, or the list of exceptions.[30] Taken broadly, the exceptions provide *particular* situations or conditions in which the law does not apply.[31] In practice, the exceptions provided for government access to financial records apply to some of the most routine instances of financial data collection. Each item is broken down into more general terms in Appendix A, but the full list of exceptions as written in the law is as follows:

1. Disclosure of financial records not identified with particular customers;
2. Disclosure to, or examination by, supervisory agency pursuant to exercise of, regulatory, or monetary functions with respect to financial institutions, holding companies, subsidiaries, institution-affiliated parties, or other persons;
3. Disclosure pursuant to title 26[, or the Internal Revenue Code];
4. Disclosure pursuant to federal statute [(e.g., the Bank Secrecy Act)] or rule promulgated thereunder;
5. Disclosure pursuant to federal rules of criminal procedure or comparable rules of other courts;
6. Disclosure pursuant to administrative subpoena issued by administrative law judge;
7. Disclosure pursuant to legitimate law enforcement inquiry respecting name, address, account number, and type of account of particular customers;
8. Disclosure pursuant to lawful proceeding, investigation, etc., directed at financial institution or legal entity, or consideration or administration respecting government loans, loan guarantees, etc.;
9. Disclosure pursuant to issuance of subpoena or court order respecting grand jury proceeding;
10. Disclosure pursuant to proceeding investigation, etc., instituted by government accountability office and directed at a government authority;
11. Disclosure necessary for proper administration of programs of certain government authorities;
12. Crimes against financial institutions by insiders;

13. Disclosure to, or examination by, employees or agents of board of governors of federal reserve system or federal reserve banks;
14. Disclosure to, or examination by, resolution trust corporation or its employees or agents;
15. Disclosure to, or examination by, federal housing finance agency or federal home loan banks;
16. Access to information necessary for administration of certain veteran benefits laws;
17. Disclosure pursuant to federal contractor-issued travel charge card; and
18. Disclosure to the bureau of consumer financial protection.[32]

While the scope of the list of exceptions is in and of itself objectionable, the exceptions are particularly objectionable given the broad authority that these exceptions supply to law enforcement and other government agencies that routinely act as the most common collectors of financial information. As noted by the Financial Crimes Enforcement Network (FinCEN),

> The Right to Financial Privacy Act (RFPA) **generally prohibits** financial institutions from disclosing a customer's financial records to a Government agency without service of legal process, notice to the customer and an opportunity to challenge the disclosure. **However, no such requirement applies when the financial institution provides the financial records or information to FinCEN or a supervisory agency in the exercise of its "supervisory, regulatory or monetary functions.**[33] (Emphasis added)

Other than FinCEN, the other supervisory agencies considered relevant and appropriate for these purposes include the criminal investigative services of the armed forces; the Bureau of Alcohol, Tobacco, and Firearms; the attorney general, district attorney, or state's attorney at the

state or local level; the Drug Enforcement Administration; the Federal Bureau of Investigation; the Internal Revenue Service or tax enforcement agencies at the state level; the Office of Foreign Assets Control; state or local police departments; the United States Attorney's Office; Immigration and Customs Enforcement; the U.S. Postal Inspection Service; and the U.S. Secret Service.[34] When written in this *expanded* form, it becomes clear that while Americans left the initial wake of the Bank Secrecy Act with *some* protections for their financial privacy, those protections didn't really apply in any of the places that truly mattered (Figure 1).

Figure 1

Notable agencies and conditions exempt from the privacy requirements of the Right to Financial Privacy Act of 1978

Agency or Condition	Does the Act Apply?
Internal Revenue Service (IRS)	No
Federal Reserve (the Fed)	No
Financial Crimes Enforcement Network (FinCen)	No
Consumer Financial Protection Bureau (CFPB)	No
Government Accountability Office (GAO)	No
Social Security Records	No
Tax Records	No
Bank Secrecy Act (BSA)	No
Criminal or Civil Court Cases	No
Legitimate Law Enforcement Requests	No
Administrative Subpeona	No
Grand Jury Subpeona	No

Source: 12 U.S. Code Section 3413.

A Lack of Financial Privacy Then and Now

The past 50 years has been marked by a continued erosion of Americans' financial privacy. Legislated expansions of financial surveillance, legal investigations and regulatory pressure

taking advantage of loopholes, and even unseen factors like inflation have intruded on Americans' financial activity.

Legislative Expansions

The lack of financial privacy in the United States caught the attention of most Americans when the U.S. government considered surveilling all bank accounts with at least $600 of annual activity. The saga began in the Spring of 2021 when the U.S. Treasury released its annual revenue proposals—known as the General Explanations of the Administration's Fiscal Year 2022 Revenue Proposals, or the Greenbook.[35] Nestled on page 88 was a proposal to "introduce comprehensive financial account reporting to improve tax compliance."[36] The plan was to require banks and other financial institutions to "report gross inflows and outflows with a breakdown for physical cash, transactions with a foreign account, and transfers to and from another bank account with the same owner" so long as the account in question had at least a gross flow threshold of $600.[37]

As the proposal gained favor in Congress and attention across the country, many Americans were left asking how such a proposal could be considered Constitutional and some members of Congress quickly responded with legislative proposals to stop what was a violation of the spirit of the Fourth Amendment.[38] For instance, Senator Tim Scott (R-NC) introduced the Prohibiting IRS Financial Surveillance Act alongside 49 cosponsors.[39] Likewise, Representative Ashley Hinson (R-IA) introduced the Protecting Financial Privacy Act of 2021 with 65 cosponsors.[40] To address these criticisms and defend their position, the U.S. Treasury Department issued a press release stating that,

> In reality, many financial accounts are already reported on to the IRS, including every bank account that earns at least $10 in interest. And for American workers, much more detailed information reporting exists on wage, salary, and investment income.[41]

While this statement is in fact a truthful defense,[42] it reveals the dismal state of financial privacy in the United States. For the Treasury Department is right: there is already a great deal of financial surveillance taking place and it has been steadily expanding for years.

In 1992, the Annunzio-Wylie Anti-Money Laundering Act was one of the first major expansions of the Bank Secrecy Act.[43] Much like the original passage of the Bank Secrecy Act that gave the Secretary of the Treasury the authority to require currency transaction reports, the Annunzio-Wylie Anti-Money Laundering Act gave the Secretary of the Treasury the authority to require financial institutions to further report on the activities of the public. This time, however, the financial institutions were required to "report any suspicious transaction relevant to a possible violation of law or regulation."[44] In doing so, the law also barred financial institutions from notifying the public of when a report was filed. To oversee this new reporting regime, the Money Laundering Suppression Act of 1994 authorized the Secretary of the Treasury to create a new agency—the Financial Crimes Enforcement Network (FinCEN).[45]

In 2001, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act was enacted to deter terrorism. While stopping terrorism is indeed a worthwhile endeavor, the law dramatically reduced financial privacy in the United States in its effort to identify and thwart terrorist financing.[46] For example, the law introduced "know your customer" (KYC) requirements to force financial institutions to

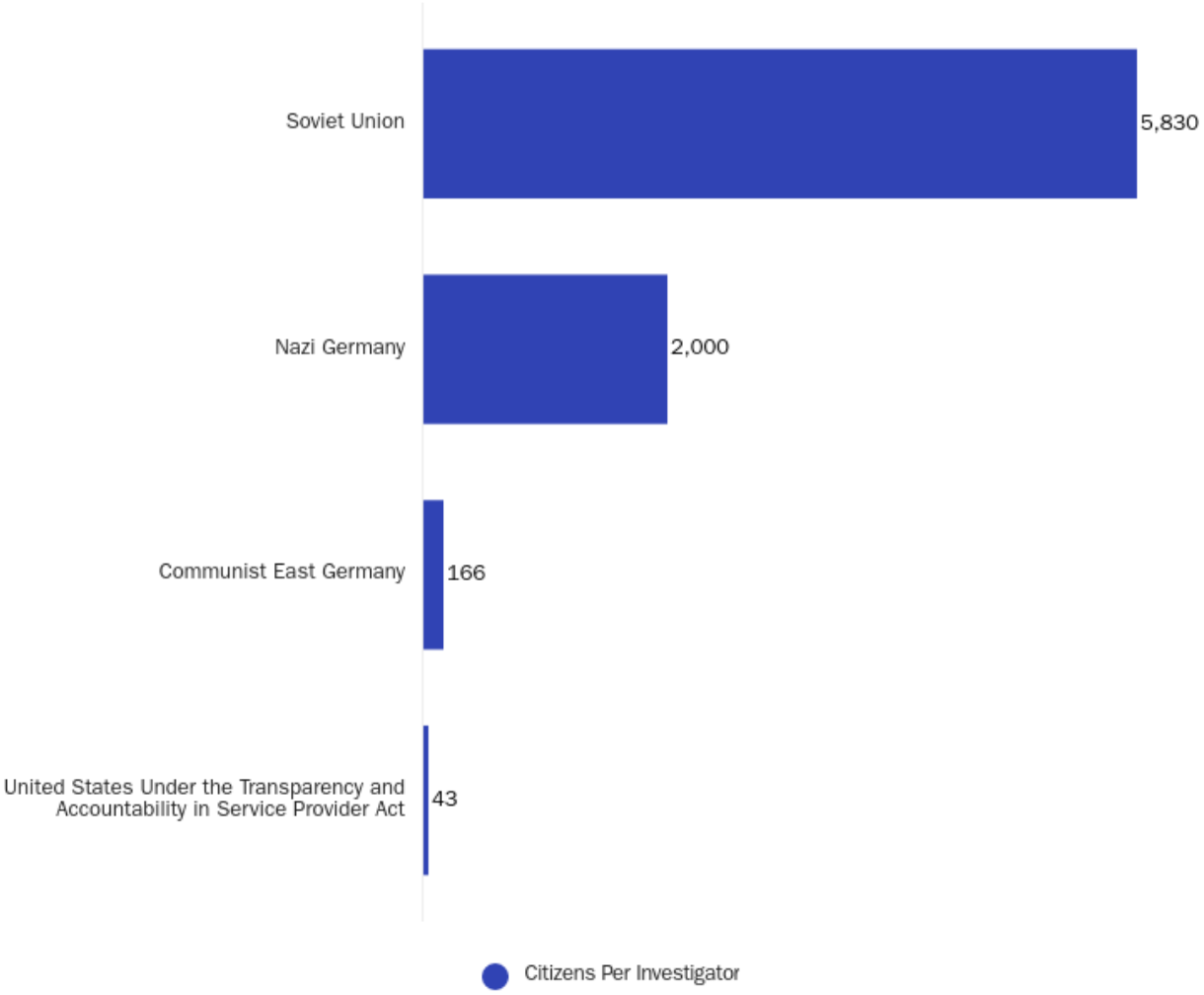
collect identifying information and run checks on potential customers. The law also expanded the requirements for financial institutions to file suspicious activity reports (SARs)—further conscripting financial institutions as deputy law enforcement investigators.[47] And as mentioned above, although one would be correct to wonder why such news is not more widely reported, both employees from financial institutions and the government are prohibited under the law from notifying customers when a SAR is filed.[48] In other words, there is an illusion of privacy because the violations of privacy taking place are done so in secrecy.[49]

In 2022, Representative Jim Himes (D-CT) tried to build off of the tools provided by the PATRIOT Act to expand the Treasury's powers and authority by removing the checks and balances designed to protect American citizens.[50] The House Committee on Financial Services initially described Himes's proposal as streamlining "the process by which special measures may be introduced and modernizes the authorities granted to the Financial Crimes Enforcement Network (FinCEN)."[51] In practice, said "streamlining" would have been achieved by removing the requirements to notify the public of when the Treasury uses special measures as part of its enforcement. For the Treasury to use its special measures authority, the current law requires a notice of proposed rulemaking as well as a 120-day limit on the enforcement. Representative Himes's bill, however, would eliminate both the requirement to notify the public and the 120-day limit on enforcement. As Jerry Brito and Peter Van Valkenburgh first described it in their analysis of the bill, "In other words, it is an attempt… to use the moral panic surrounding criminal usage of cryptocurrencies… to strip our surveillance laws of all public processes."[52] Despite still seeking to expand the Treasury's powers, the bill was later amended and reintroduced without the language that would have removed the checks on the Treasury's power.[53]

Similarly, another bill, the Transparency and Accountability in Service Providers Act, was introduced in 2022 to "expand the scope and authorities of anti-money laundering [procedures]."[54] In order to do so, the bill would require so-called "financial gatekeepers" to adopt anti-money laundering procedures to actively monitor for potential criminal activity. The bill calls for the Treasury to conscript any person involved in the exchange of foreign currency, digital currency, or digital assets; the managing, advising, or consulting with respect to money or other assets; the provision of cash vault services; the processing of payments; the wiring of money; the direct or indirect filing of any return on behalf of a foreign individual, trust, or fiduciary; the formation, registration, acquisition, or disposition of a corporation, limited liability company, trust, foundation, limited liability partnership, partnership, association, or arrangement; the sourcing, pooling, organization, or management of capital; and the process of acting as a trustee. The Project for Privacy and Surveillance Accountability (PPSA) estimates that the proposal would turn some 7.6 million financial service employees into government informants—meaning one informant for every 43 Americans.[55] To put that number in perspective, the PPSA noted that this bill, although limited to financial surveillance, would exceed the number of investigators per citizen in the surveillance states of Nazi Germany, the Soviet Union, and Communist East Germany (Figure 2).[56]

Figure 2

Comparing Surveillance Regimes



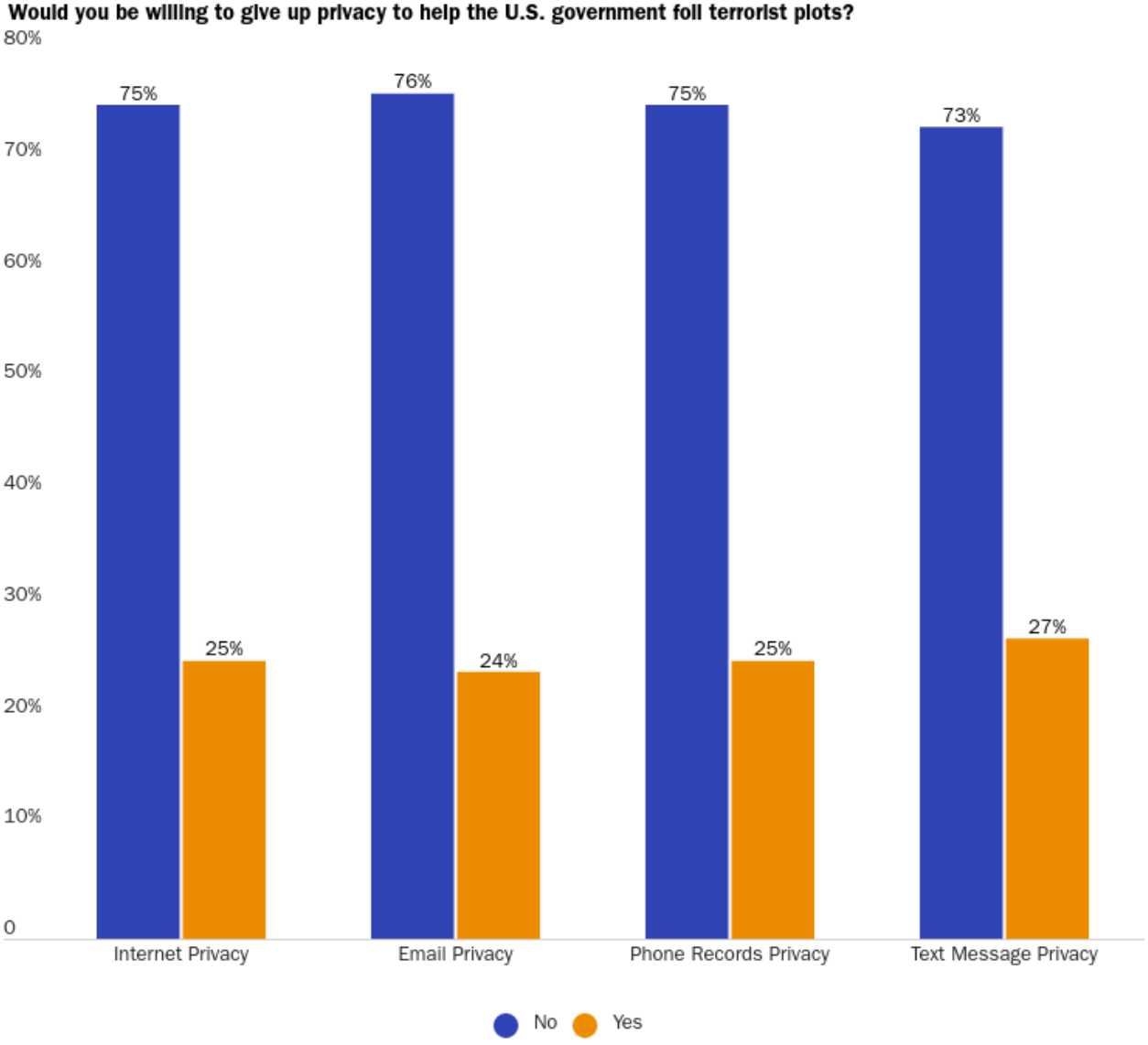
Source: Project for Privacy and Surveillance Accountability, "Proposal Would Turn 7.6 Million Financial Service Employees into Government Informants," News and Updates, May 26, 2022; John O. Koehler, "Stasi: The Untold Story of the East German Secret Policy," New York Times, 1999.

With Congress enacting such broad sweeping powers, and attempting to go even further on many occasions, it should be little surprise that Americans have steadily become more wary of the government's activities. In 2017, a Reuters and Ipsos poll found that 75 percent of adults—up from 67 percent in 2013—would not voluntarily let investigators monitor their internet activity to combat terrorism.[57] In fact, as the figure below shows, Americans are overwhelmingly unwilling to give up their privacy in the name of the war on terror. [58] Yet it isn't just the war on

terror that the U.S. government has used to justify further encroaching on Americans' financial privacy.

Figure 3

Would you be willing to give up privacy to help the U.S. government foil terrorist plots?



Source: Dustin Volz, "Most Americans Unwilling to Give Up Privacy to Thwart Attacks: Reuters/Ipsos Poll," Reuters, April 4, 2017, https://www.reuters.com/article/idUSKBN1762TQ.

Legal Investigations and Regulatory Pressure

The "wars" on drugs, crime, and poverty have been used for decades as a justification to peer into the lives of Americans. Most infamously, Operation Chokepoint was an initiative by the

Department of Justice to go after so-called controversial businesses (e.g., state-licensed cannabis dispensaries, payday lenders, pawn shops, or gun shops) with the intent of, as one official described it, "choking them off from the very air they need to survive."[59] In other words, as first reported in the Wall Street Journal, "Rather than just targeting individual firms, the government is now going after the infrastructure that enables companies to withdraw money from people's bank accounts."[60] After already having forced financial institutions to collect information on account holders, Operation Chokepoint was the next step forward in terms of the government taking action on all of that information en masse.[61]

But Operation Chokepoint was not an anomaly. Just a few years after the full scope of Operation Chokepoint was revealed,[62] Senator Ron Wyden (D-OR) helped to bring it to light that the U.S. Immigration and Customs Enforcement (ICE) had been collecting records on money transfers to or from Mexico greater than $500.[63] ICE had collected approximately six million transaction records between 2019 and 2022—all without a warrant. Instead, ICE issued eight administrative subpoenas asking Western Union and Maxitransfers Corporation to turn over records for six months at a time.[64] As Matthew Guariglia, a policy analyst at the Electronic Frontier Foundation, explained, "This is a blatantly illegal exploitation of the government subpoena power—and an all too familiar one that must stop."[65]

In August 2022, attention shifted to the U.S. Department of Treasury when it declared Tornado Cash—a decentralized software protocol—as a sanctioned entity and thus barred all Americans from using the service.[66] Much like when the government used Operation Chokepoint to target financial infrastructure instead of financial criminals, it seems that the Treasury opted to go after an entire software protocol dedicated to improving financial privacy rather than the bad actors that it was after on a paper.[67] The blurring of lines was made

abundantly clear when U.S. Secretary of State Antony Blinken tweeted (and then deleted) the claim that Tornado Cash was a North Korean state-sponsored hacking group.[68] It's certainly possible that Treasury officials similarly did not recognize that Tornado Cash was a decentralized software protocol (i.e., there's no one person in control of it), but there is little excuse to shut down an entire service in pursuit of criminals when there are ample tools to go after the criminals themselves.[69]

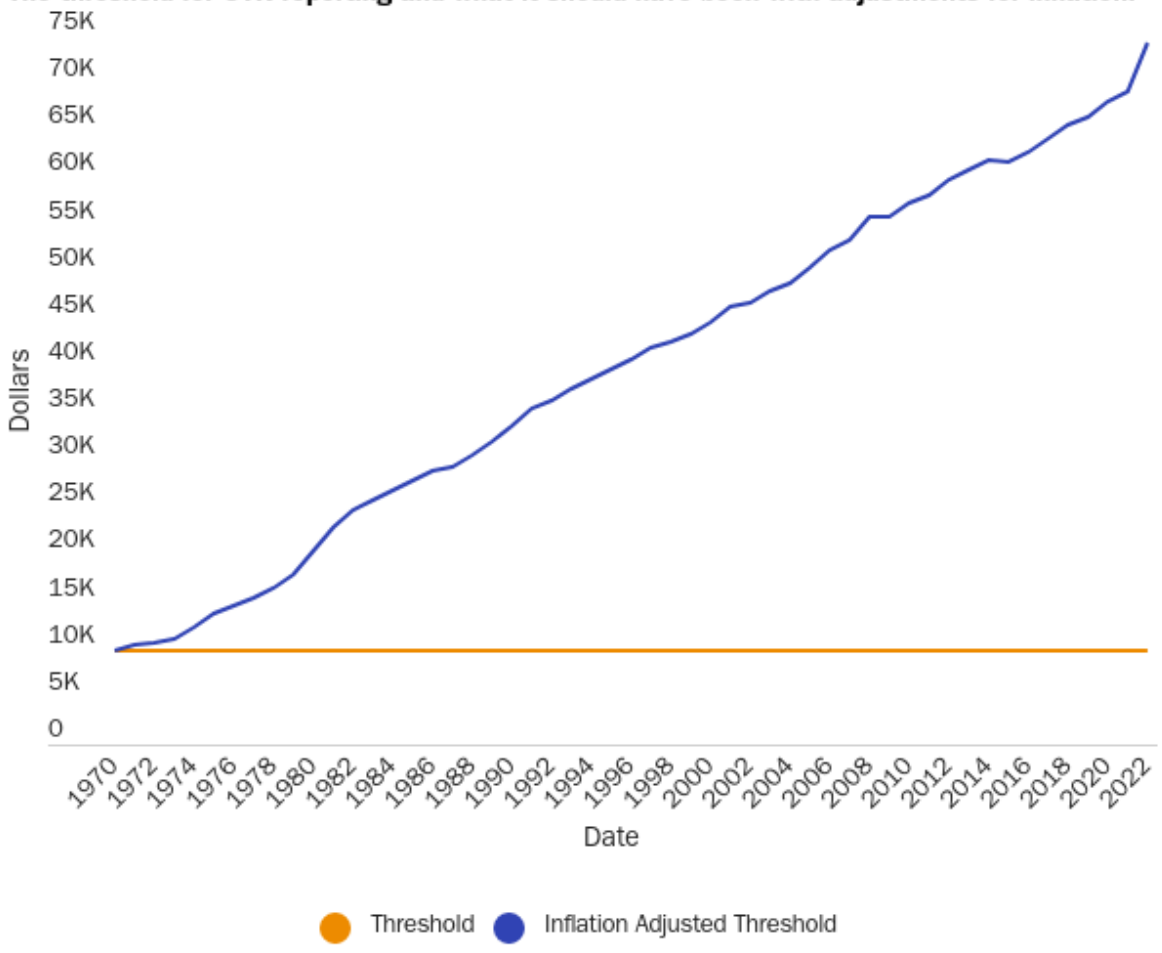
Looking just beyond America's borders, the public was also confronted with how much financial privacy has deteriorated and how real the risk of financial oppression can be in other free nations when Canadian Prime Minister Justin Trudeau invoked the Emergencies Act for the first time in Canadian history.[70] In doing so, Trudeau froze the bank accounts of protestors and expanded the reach of existing anti-money laundering laws in Canada to stop the protests over COVID-19 restrictions. While not in the United States, it's important to recognize that these tactics are usually reserved for authoritarian countries like Russia or China—not the sixth freest nation in the world, as rated by the Cato Institute's Human Freedom Index.[71] Mercatus scholar Brian Knight was correct to note that "the events in Canada should serve as a wake-up call [for the United States] and prompt us to change the laws, regulations, and institutions that govern who controls [your financial activity]."[72] In light of these actions by an otherwise non-autocratic country, and the demonstrable willingness of Congress to expand the weaponization of the financial infrastructure, there's little reason to think the United States will not do the same if presented with a similar emergency situation. Operation Chokepoint, the mass collection of records on money transfers, the sanctioning of Tornado Cash, and similar intrusions by the U.S. government are already proof of how real that risk is.

Unseen Expansions

Were legislated expansions and legal investigations not enough on their own, each year that passes with a positive inflation rate offers another unseen increase in the level of financial surveillance because the Bank Secrecy Act reporting thresholds were not crafted with an adjustment for inflation. The original reporting threshold for currency transaction reports (CTRs) was $10,000—a relatively large transaction in the 1970s. If, for instance, the threshold had been adjusted for inflation, then CTRs would now be required only for transactions of at least $75,000 (Figure 4).[73] The result is that thousands of reports are filed every day against Americans for merely using their own money.

Figure 4

The threshold for CTR reporting and what it should have been with adjustments for inflation.



Source: Bureau of Labor Statistics

The erosion of financial privacy in the wake of ever-expanding financial surveillance is especially important to consider given that Supreme Court Justices Lewis Powell and Harry Blackmun noted in their 1974 support of the Bank Secrecy Act that the $10,000 requirement was high enough to not create an undue burden.[74] It is unclear if Justices Powell and Blackmun would have felt that the 85 percent reduction since then would also have been considered "high enough" to avoid creating an undue burden, but their opinion suggests that they would view the current threshold as too low:

> The implementing regulations, however, require only that the financial institution "file a report on each deposit, withdrawal, exchange of currency or other payment or transfer, by, through, or to such financial institution, which involves *a transaction in currency of more than $10,000*." 31 CFR § 103.22 (italics added). … A significant extension of the regulations' reporting requirements, however, would pose substantial and difficult constitutional questions for me. In their full reach, the reports apparently authorized by the open-ended language of the Act touch upon intimate areas of an individual's personal affairs. Financial transactions can reveal much about a person's activities, associations, and beliefs. At some point, governmental intrusion upon these areas would implicate legitimate expectations of privacy.[75]

At a 2022 congressional hearing dedicated to the oversight of the Financial Crimes Enforcement Network (FinCEN), Representatives Barry Loudermilk (R-GA), Joyce Beatty

(D-OH), French Hill (R-AR), Bryan Steil (R-WI), and Roger Williams (R-TX) all expressed concern over inflation silently increasing the scope of financial surveillance.[76] In particular, Representative Steil pointed out at the hearing that by increasing the range of financial surveillance, the "haystack" investigators must search has been ever increasing in size—effectively hiding the "needle," or actual criminal activity, that investigators are looking for.[77]

Over the years, other members of Congress have tried to rectify the issue with legislative amendments to add inflation adjustments to the reporting required by the Bank Secrecy Act. For example, Representative Steven Pearce (R-NM) and Representative Blaine Luetkemeyer (R-MO) introduced the Counter Terrorism and Illicit Finance Act in 2018 to increase the reporting thresholds for CTRs, SARs, and money service businesses. In addition, the bill would have also required FinCEN to conduct a formal review of the effectiveness of those reporting thresholds.[78] Ultimately, only the requirement for a formal review was passed in the National Defense Authorization Act (NDAA) within Sections 6204 and 6205.[79] In short, those sections required FinCEN to provide several reports regarding the possibility of raising the reporting thresholds to account for inflation. FinCEN Acting Director Himamauli Das testified before Congress in April 2022 that the reports should be ready by the end of 2022.[80] The decision to increase the reporting thresholds per inflation should be a simple one considering that in 2016 FinCEN judged inflation as having been significant enough to warrant an increase for the monetary penalties that FinCEN charges to the public.[81]

The "invisibility" with which financial surveillance is being expanded should concern all Americans. Howard Anglin, former deputy chief of staff for Canadian prime minister Stephen Harper, pointed out this reality when the Canadian government began to freeze the bank

accounts of protestors in 2022, but his words are an eye-opening description of both the limited consideration of inflation and the broader consideration of financial surveillance as a whole:

> The government's action is troubling enough, but what should really disturb us is the ease and invisibility with which it is being done. When we can't see the consequences of government conduct, the risks of government misconduct increases. A government that sends in riot troops to dispel a crowd will rightly pay a price if the police commit abuses. But the diffuse and anonymous nature of financial enforcement mean that sweeping repression can easily go undetected. It is the political equivalent of using drone strikes instead of boots on the ground.[82]

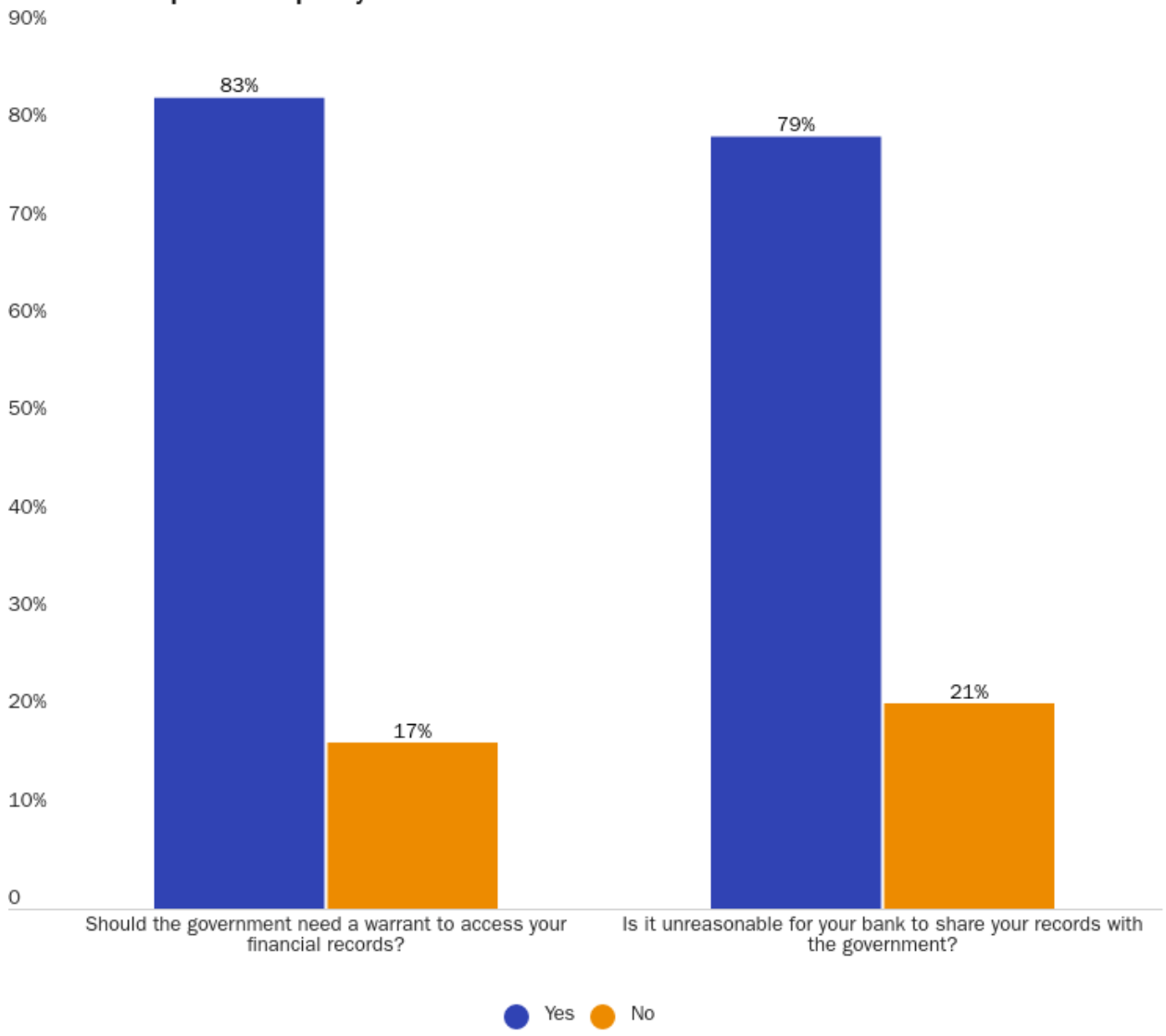
The invisibility of inflation is likely the reason why the American people have not objected en masse to the government's increased financial surveillance. This invisibility is also why the Bank Secrecy Act, with its suspicious activity reports and currency transaction reports hidden from the public eye, has been kept out of headlines and allowed to proceed unquestioned. These are all tools that easily go undetected. Such a strategy may be favorable for an authoritarian leader trying to seize control of the masses, but it should not be the strategy of a representative government—especially ones that are considered the freest nations in the world.[83]

A Reasonable Expectation of Privacy

At the core of much of the financial surveillance taking place in the United States is the third-party doctrine and a so-called reasonable expectation of privacy. Soon after Congress enacted the Bank Secrecy Act, the Supreme Court held in *United States v. Miller* that a person cannot reasonably expect privacy when providing information to a third party (e.g., a financial institution). But is it so unreasonable to expect privacy, or confidentiality, with your banker? The Cato Institute surveyed Americans in August 2022 and found that the answer is decidedly no. When asked if it is unreasonable for your bank to share your records and transactions with the federal government, 79 percent of respondents said yes.[84] More so, 83 percent of the respondents said that the government should need to obtain a warrant to access their financial records.

Figure 5

A reasonable expectation of privacy



Source: Cato Institute Survey, August 2022.

In recent years, the Supreme Court appears to have recognized the need for change.[85] In *Kyllo v. United States* (2001), the Supreme Court had to weigh the constitutionality of law enforcement using thermal imaging to surveil the inside of a home from afar.[86] Ultimately, the Court held that the right to be secure in one's home under the Fourth Amendment was not limited to physical intrusions. In *United States v. Jones* (2012), the Supreme Court held that attaching and monitoring a tracking device on an individual's vehicle "constitutes a search or

seizure within the meaning of the Fourth Amendment."[87] In *Carpenter v. United States* (2018), the Supreme Court likewise held that the government's acquisition of cell-phone tracking data was a search under the Fourth Amendment.[88] And across all of these cases, there were moments where the Supreme Court turned back to *Katz v. United States* (1967), in which the Supreme Court had held that the "Fourth Amendment protects people, not places."[89] In Katz v. United States, Justice John Marshall Harlan wrote that,

> a person has a constitutionally protected reasonable expectation of privacy; [that] electronic, as well as physical, intrusion into a place that is in this sense private may constitute a violation of the Fourth Amendment, and [that] the invasion of a constitutionally protected area by federal authorities is, as the Court has long held, presumptively unreasonable in the absence of a search warrant… My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person has exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable."[90]

Between rolling passwords, security questions, multi-factor authentication requirements, and closed-door meetings, one can make the case that most people exhibit an actual expectation of privacy with respect to their financial records. Moreover, as the Cato Institute's national survey demonstrates, a majority of Americans from across political ideologies do in fact find it reasonable to expect privacy with one's financial records. These facts suggest that Congress should better protect Americans' financial privacy.

The Elephant in the Room: Greater Financial Privacy Will Create a Greater Burden on Law Enforcement and Regulators

While financial privacy is in the interest of most Americans,[91] it is not in the interest of law enforcement, regulators, or other government agencies. Instead, these government agencies have been more interested in expanding their investigations than expanding citizens' privacy protections. As noted by the Electronic Privacy Information Center (EPIC), "Much of the opposition to the [Right to Financial Privacy Act] has been by federal law enforcement officials who are concerned that the proposed privacy protections would impede federal authorities in their investigation and prosecution of white-collar and organized crime."[92] In fact, the North American Securities Administration Association (NASAA) was quick to state their opposition in 1977 as the Right to Financial Privacy Act was gaining momentum,

> Agencies assigned the monumental task of ensuring that consumer/investor losses occur only as a result of normal business-market place risks shall be hard pressed by the policies and procedures set forth by this act. Persons will be tempted to commit such crimes so long as the chance of discovery and persecution are kept remote.[93]

NASAA went on to argue that getting warrants and subpoenas is sometimes too hard or takes too much time—an argument also made by U.S. attorney for the Southern District of New York Robert Morgethau in his supportive testimony for the Bank Secrecy Act nearly ten years earlier.[94] NASAA also took issue with the Right to Financial Privacy Act's requirement to seek permission from the account holder, stating that "to provide notice to a target that an agency is

investigating certain business activity permits the person to effectively cover up or pull out of the jurisdiction."[95]

When faced with a critique of this nature, there are two questions worth considering. First, what limit should there be to what the government may seize in pursuit of combatting crime? In one of the more extreme examples, the walls around one's home are sufficient to provide privacy for any number of possible crimes. Yet the Supreme Court has defended the home even from spying from afar.[96]

Second, with the fact that there is some limit to what the government can seize established, what amount of illegal activity must there be to justify crossing that limit? Although some policymakers may be quick to respond that they would completely eliminate all illegal activity, that policy is simply untenable.[97] The Bank Secrecy Act is already an example of this reality. With each expansion of the Bank Secrecy Act, it has become harder for financial institutions to stay in business and harder for consumers to have access to affordable services. It is estimated that complying with the Bank Secrecy Act in 2019 cost the U.S. financial industry $26.4 billion.[98] Yet as it stands, despite the millions of Bank Secrecy Act reports filed each year, there is little to show for its ability to eliminate illegal activity.[99] Instead, it is only the American public that is bearing the cost of this financial surveillance policy.

In short, the government should not be able to force financial institutions, whether by direct order or implied pressure, to disclose Americans' financial information without a court order. Yes, stronger financial privacy protections will make it harder for law enforcement and other government agencies. However, the Constitution exists for a reason: it was designed to protect American citizens from unchecked powers of the state.

Recommendations for A Better Framework for Financial Privacy

To better establish a stronger Right to Financial Privacy Act, Congress should remove the exceptions to its protections. Doing so would merely require that law enforcement and other government agencies seek a warrant for Americans' financial records. Otherwise, offering protections everywhere except where there really matter is to offer no protections at all. To do so, Congress should strike 12 U.S.C. Section 3413 (a)-(r).

At the very least, Congress should repeal the sections of the Bank Secrecy Act that require financial institutions to report on their customers—if not repeal the Bank Secrecy Act in its entirety.[100] To do so, Congress should amend 12 U.S.C. Sections 3402, 3413, and 3414 as well as 31 U.S.C Sections 5313-16, 5318(a)(2), 5318A, 5321, 5325, 5326, 5331-32, 5341-5342, and 5351-55.

To the extent that reporting requirements may still exist after amending the Right to Financial Privacy Act and Bank Secrecy Act, Congress should require annual inflation adjustments for all Bank Secrecy Act reporting thresholds. To do so, Congress could use the following language:[101]

> (1) Not later than the end of the 180-day period beginning on the date of the enactment of this Act, and annually thereafter, the Secretary of the Treasury shall revise regulations issued with respect to section 5313 of title 31, United States Code, to update each $10,000 threshold in such regulations to [insert inflation adjusted amount as of the current day].
>
> (2) Section 5331 of title 31, United States Code, is amended by striking "10,000" each place such term appears in heading or

text and inserting "[insert inflation adjusted amount as of the current day]".

(3) Not later than the end of the 180-day period beginning on the date of the enactment of this Act, and annually thereafter, each Federal department or agency that issues regulations with respect to reports on suspicious transactions described under section 5318(g) of title 31, United States Code, shall update each $5,000 threshold amount in such regulations to [insert inflation adjusted amount as of the current day] and each $2,000 threshold amount in such regulation to [insert inflation adjusted amount as of the current day].

Likewise, if such reporting requirements are permitted to continue, Congress should require FinCEN to publicly report the number of SARs and CTRs that effectively curb financial crime. The report should detail how many reports are received, reviewed, and requested by other governmental agencies. In addition, FinCEN should report how many reports resulted in conviction, settlement, or additional charges in investigations unrelated to money laundering. The reports should make a clear distinction between criminal investigations that originated with SARs or CTRs and criminal investigations that merely used existing SARs or CTRs to strengthen existing cases. To do so, Congress could use the following language:[102]

(1) Annual Report.—Not later than 1 year after the date of enactment of this Act, and annually thereafter, the Attorney General, in consultation with the Secretary of the Treasury,

Federal law enforcement agencies, the Director of National Intelligence, Federal functional regulators, and the heads of other appropriate Federal agencies, shall publish a publicly available report that contains statistics, metrics, and other information on the use of data derived from financial institutions reporting under the Bank Secrecy Act, including the number of reports that—

(A) have been received by the Financial Crimes Enforcement Network;

(B) have been reviewed by the Financial Crimes Enforcement Network;

(C) have been requested by other governmental agencies;

(D) have led to a secondary investigation by the Financial Crimes Enforcement Network;

(E) have led to further procedures by law enforcement agencies including the use of a subpoena, warrant, or other legal process;

(F) have resulted in a conviction or settlement;

(G) have resulted in additional charges in investigations unrelated to money laundering;

While there are still many other improvements that may be made to past legislation, Congress should also eliminate 26 U.S.C. Section 6050I. No American should be forced by law to report on the activity of another American—especially when that activity is between only two parties. Yet, 26 U.S.C. Section 6050I requires exactly that when Americans choose to use cash or cryptocurrencies.[103] This section should be repealed in its entirety.

Finally, Congress should turn its focus toward the future by enacting protections for two-party, or peer-to-peer, transactions. Holding cryptocurrency in a "self-hosted" wallet is merely the digital equivalent of holding physical cash in a traditional wallet. It gives the owner complete control over what's held inside it and, to the extent that they want to do so, the ability to maintain their privacy. Congress should not let financial surveillance further encroach on American's privacy by being expanded to cover self-hosted wallets and peer-to-peer exchanges. To do so, Congress could use the following language:[104]

> (1) In General.—No agency head may prohibit or otherwise restrict the ability of a covered user to—
>
> (A) use cryptocurrency or its equivalent for such user's own purposes, such as to purchase goods and services for the user's own use; or
>
> (B) conduct transactions through a self-hosted wallet.

Conclusion

In a concurrent opinion in *United States v. Jones*, Justice Sonia Sotomayor wrote,

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.[105]

Considering how much has changed since the Bank Secrecy Act, *United States v. Miller*, and the Right to Financial Privacy Act took effect in the 1970s, Justice Sotomayor is right: it is time to reconsider the third-party doctrine, the reasonable expectation of privacy, and financial privacy. "Having technology" in the 1970s meant having a television and a typewriter. Today, technology is now an integral part of modern life: Americans use credit or debit cards for nearly all purchases, acquire loans directly on their phones, and leave a digital trail nearly everywhere they go. So while such financial records may have only offered limited insights into one's life in the 1970s, these financial records now offer a full, detailed representation of one's life that likely exceeds that offered on social media.[106]

Such unrivaled access to the lives of all Americans makes it evident that now, more than ever, it is time to rethink how financial privacy is treated in the United States. There will still be much to do in the long run, but the recommendations proposed here could help to significantly restore the financial privacy protections that have been eroded away over the last 50 years.

Appendix A

To better understand the exceptions provided in the Right to Financial Privacy Act,[107] this appendix breaks down and explains each of the 18 exceptions.

Disclosure of financial records not identified with particular customers.

The Right to Financial Privacy Act does not apply to financial records if the records do not identify particular customers. Examples could include benefit packages for employees, budgeting outlays, and similar high-level records that might be maintained by a financial institution.

Disclosure to, or examination by, supervisory agency pursuant to exercise of supervisory, regulatory, or monetary functions with respect to financial institutions, holding companies, subsidiaries, institution-affiliated parties, or other persons.

The Right to Financial Privacy Act does not apply to financial records shared with any regulatory agency that has oversight over the institution in question. Examples could include records requested by the Federal Deposit Insurance Corporation (FDIC) or Federal Reserve during an audit.

Disclosure pursuant to title 26[, or the Internal Revenue Code].

The Right to Financial Privacy Act does not apply to financial records shared in accordance with the Internal Revenue Code, or tax system. Examples could include credit card statements, check records, invoices, and receipts.

Disclosure pursuant to federal statute [(e.g., the Bank Secrecy Act)] or rule promulgated thereunder.

The Right to Financial Privacy Act does not apply to financial records sought in connection with federal statutes. For example, this exception means there are no protections regarding suspicious activity reports (SARs) or currency transaction reports (CTRs).

Disclosure pursuant to federal rules of criminal procedure or comparable rules of other courts.

The Right to Financial Privacy Act does not apply to financial records sought under the rules and procedures that govern civil and criminal cases in the U.S. court system. Examples could include records sought during an ongoing court case.

Disclosure pursuant to administrative subpoena issued by administrative law judge.

The Right to Financial Privacy Act does not apply to financial records if an administrative law judge issues a subpoena. Examples could include relevant papers, books, electronically stored information, or documents.

Disclosure pursuant to legitimate law enforcement inquiry respecting name, address, account number, and type of account of particular customers.

The Right to Financial Privacy Act does not apply when law enforcement officials have a "legitimate inquiry" for only the name, address, account number, and account type of a particular customer.

Disclosure pursuant to lawful proceeding, investigation, etc., directed at financial institution or legal entity, or consideration or administration respecting government loans, loan guarantees, etc.

The Right to Financial Privacy Act does not apply to financial records in connection to a government loan program on the condition that they are only used for their initial purpose with the government loan program. However, if a civil, criminal, or regulatory violation is suspected, the official overseeing the government loan program can instruct the relevant agency to independently seek out the records.

Disclosure pursuant to issuance of subpoena or court order respecting grand jury proceeding.

The Right to Financial Privacy Act does not apply to financial records sought by a grand jury subpoena. Examples could include relevant papers, books, electronically stored information, or documents.

Disclosure pursuant to proceeding investigation, etc., instituted by government accountability office and directed at a government authority.

The Right to Financial Privacy Act does not apply to financial records requested by the Government Accountability Office as part of an ongoing proceeding, investigation, examination, or audit of another government authority.

Disclosure necessary for proper administration of programs of certain government authorities.

The Right to Financial Privacy Act does not apply to financial records required to carry out the Social Security or Railroad Retirement Acts. Examples could include credit card statements, check records, invoices, and receipts.

Crimes against financial institutions by insiders.

The Right to Financial Privacy Act does not apply to financial records concerning the possible commission of a crime by an executive, employee, or customer of a financial institution, furnished to either the Attorney General, Secretary of Treasury or other enforcement agency. Examples could include credit card statements, check records, invoices, and receipts.

Disclosure to, or examination by, employees or agents of board of governors of federal reserve system or federal reserve banks.

The Right to Financial Privacy Act does not apply to financial records sought by employees of the Federal Reserve system. Examples could include bank reserves, capital-ratios, and balance sheets.

Disclosure to, or examination by, resolution trust corporation or its employees or agents.

The Right to Financial Privacy Act does not apply to financial records sought by the Resolution Trust Corporation. Examples could include bank reserves, capital-ratios, and balance sheets.

Disclosure to, or examination by, federal housing finance agency or federal home loan banks.

The Right to Financial Privacy Act does not apply to financial records sought by the Federal Housing Finance Agency or federal home loan banks. Examples could include bank reserves, capital-ratios, and balance sheets.

Access to information necessary for administration of certain veteran benefits laws.

The Right to Financial Privacy Act does not apply to financial records disclosed to the Department of Veterans Affairs solely for the purpose of properly carrying out benefits programs. Examples could include credit card statements, check records, invoices, and receipts.

Disclosure pursuant to federal contractor-issued travel charge card.

The Right to Financial Privacy Act does not apply to financial records disclosed regarding a contractor-issued travel card issued for official government travel. Examples could include receipts, invoices, and statements.

Disclosure to the bureau of consumer financial protection.

The Right to Financial Privacy Act does not apply to financial records disclosed to the Bureau of Consumer Financial Protection. Examples could include bank reserves, capital-ratios, and balance sheets.

Appendix B

To understand the erosion of financial privacy over time at a glance, this appendix provides a brief timeline of significant events between 1970 and 2022.

- 1970 Bank Secrecy Act
- 1972 The Currency Transaction Report
- 1972 The American Civil Liberties Union (ACLU), California Bankers Association, and Security National Bank applied for a temporary restraining order in the United States District Court for the Northern District of California

- 1973 Representative Fortney Stark (D-CA) sought to better protect financial privacy arguing that the Bank Secrecy Act undermined the long-held tradition of confidentiality between bankers and customers
- 1974 California Bankers Association v. Shultz
- 1974 Privacy Act
- 1976 United States v. Miller and the creation of the third-party doctrine
- 1977 Privacy Protection Study Commission released a report titled, "Personal Privacy in an Information Society," criticizing the 1974 Privacy Act for failing to deliver the protections one would expect.
- 1978 Right to Financial Privacy Act
- 1980 Adjusting CTR threshold for inflation puts it at approximately $20,000
- 1992 Annunzio-Wylie Anti-Money Laundering Act
- 1994 Money Laundering Suppression Act
- 1996 Financial Crimes Enforcement Network
- 1996 The Suspicious Activity Report
- 2000 Adjusting CTR threshold for inflation puts it at approximately $40,000
- 2001 Kyllo v. United States
- 2001 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act
- 2010 Adjusting CTR threshold for inflation puts it at approximately $60,000
- 2012 United States v. Jones
- 2013-2017 Operation Chokepoint
- 2018 Carpenter v. United States

- 2021 U.S. Treasury Seeks to Monitor Bank Accounts with $600 of Annual Activity
- 2022 Adjusting CTR threshold for inflation puts it at approximately $75,000
- 2022 Canadian Prime Minister Justin Trudeau froze over 200 bank accounts in attempt to stop protestors
- 2022 Rep. Jim Himes Introduces Bill to Expand Treasury's ability to censor financial transactions
- 2022 ICE revealed to have been collecting approximately 6 million records from 2019-2022 on money transfers to and from Mexico greater than $500
- 2022 Treasury Sanctions Tornado Cash

Endnotes

[1] The author thanks Norbert Michel and Nicholas Thielamn for their suggestions. The author also thanks Emily Ekins for surveying the American public on questions regarding financial privacy. Any errors belong to the author alone.

[2] Nancy M. Kirschner, "The Right to Financial Privacy Act of 1978-The Congressional Response to United States v. Miller: A Procedural Right to Challenge Government Access to Financial Records," University of Michigan Journal of Law Reform, Volume 13, Page 13, 1979, https://repository.law.umich.edu/cgi/viewcontent.cgi?article=2122&context=mjlr.

[3] Chris Van Hollen, "Van Hollen, Whitehouse Ask GAO to Dig Deeper Into Issue of Money Laundering and Real Estate," Press Release, October 3, 2018,

https://www.vanhollen.senate.gov/news/press-releases/van-hollen-whitehouse-ask-gao-to-dig-deeper-into-issue-of-money-laundering-and-real-estate.

[4] California Bankers Association, 416 U.S. at 93–95. Justice Thurgood Marshall argued, "By compelling an otherwise unwilling bank to photocopy the checks of its customers the Government has as much of a hand in seizing those checks as if it had forced a private person to break into the customer's home or office and photocopy the checks there. Our Fourth Amendment jurisprudence should not be so wooden as to ignore the fact that through microfilming and other techniques of this electronic age, illegal searches and seizures can take place without the brute force of the general warrants which raised the ire of the Founding Fathers." See also Cato Institute, "Financial Privacy in a Digital Era," Live Online Policy Forum, April 21, 2022, https://www.cato.org/events/financial-privacy-digital-era.

[5] Recent examples of governments violating financial freedom will be discussed at length later in this paper. However, those examples include the proposals to expand financial surveillance in the United States to all bank accounts with at least $600 in yearly activity, the decision by the Canadian government to freeze the bank accounts of protestors, the U.S. Department of Treasury's decision to sanction a privacy service, and other similar events.

[6] For a full discussion of the Bank Secrecy Act, see Norbert J. Michel and Jennifer J. Schulp, "Revising the Bank Secrecy Act to Protect Privacy and Deter Criminals," Policy Analysis No. 932, Cato Institute, July 26, 2022, https://www.cato.org/policy-analysis/revising-bank-secrecy-act-protect-privacy-deter-criminals.

[7] Privacy Protection Study Commission, "Personal Privacy in an Information Society," Page, 103, July 1977, https://archive.epic.org/privacy/ppsc1977report/.

[8] Public Law 91-508 Section 101; Norbert J. Michel and Jennifer J. Schulp, "Revising the Bank Secrecy Act to Protect Privacy and Deter Criminals," Policy Analysis No. 932, Cato Institute, July 26, 2022, https://www.cato.org/policy-analysis/revising-bank-secrecy-act-protect-privacy-deter-criminals.

[9] California Bankers Association v. George P. Shultz 1974, https://law.resource.org/pub/us/case/reporter/US/416/416.US.21.72-1196.72-1073.72-985.html

[10] California Bankers Association v. George P. Shultz 1974, https://law.resource.org/pub/us/case/reporter/US/416/416.US.21.72-1196.72-1073.72-985.html

[11] Nancy M. Kirschner, "The Right to Financial Privacy Act of 1978-The Congressional Response to United States v. Miller: A Procedural Right to Challenge Government Access to Financial Records," University of Michigan Journal of Law Reform, Volume 13, 1979, https://repository.law.umich.edu/cgi/viewcontent.cgi?article=2122&context=mjlr.

[12] Subcommittee on Financial Institutions Supervision, Regulation and Insurance of the House, "The Safe Banking Act," Committee on Banking Finance and Urban Affairs, October 3, 1977, https://books.google.com/books/about/The_Safe_Banking_Act_of_1977.html?id=rm5FAQAAMAAJ; Nancy M. Kirschner, "The Right to Financial Privacy Act of 1978-The Congressional Response to United States v. Miller: A Procedural Right to Challenge Government Access to Financial Records," University of Michigan Journal of Law Reform, Volume 13, 1979, https://repository.law.umich.edu/cgi/viewcontent.cgi?article=2122&context=mjlr.

[13] Representative Fortney Stark, "Right to Financial Privacy Act," H.R. 10181, September 11, 1973, https://www.congress.gov/bill/93rd-congress/house-bill/10181?r=106&s=1.

[14] 5 U.S. Code Section 552a. https://www.law.cornell.edu/uscode/text/5/552a. For a backgrounder on the Privacy Act of 1974, see Electronic Privacy Information Center, "The Privacy Act of 1974," https://epic.org/the-privacy-act-of-1974/.

[15] 5 U.S. Code Section 552a(b)(1)-(12), https://www.law.cornell.edu/uscode/text/5/552a.

[16] California Bankers Assn. v. Shultz

[17] "1970 C3 Chevrolet Corvette Model Guide," Corv Sport, https://www.corvsport.com/1970-c3-corvette/.

[18] California Bankers Assn. v. Schultz, https://scholar.google.com/scholar_case?case=17636318791181551809&q=money+laundering&hl=en&as_sdt=4,60&as_ylo=1970&as_yhi=1980

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

[20] Nicholas Anthony, "Why Don't Americans Have Stronger Financial Privacy Rights?," Cato at Liberty, October 28, 2021, https://www.cato.org/blog/why-dont-americans-have-stronger-financial-privacy-rights; Marta Belcher, Jennifer J. Schulp, and Caleb O. Brown, "Marta Belcher and Jennifer Schulp on Financial Privacy in a Digital Era," Cato Audio, Cato Institute, June 1, 2022, https://www.cato.org/multimedia/cato-audio/marta-belcher-jennifer-schulp-financial-privacy-digital-era.

[21] Electronic Privacy Information Center, "Right to Financial Privacy Act," https://epic.org/the-right-to-financial-privacy-act/.

[22] Privacy Protection Study Commission, "Personal Privacy in an Information Society," July 1977, https://archive.epic.org/privacy/ppsc1977report/.

[23] Privacy Protection Study Commission, "Personal Privacy in an Information Society," Page, 13, July 1977, https://archive.epic.org/privacy/ppsc1977report/.

[24] Privacy Protection Study Commission, "Personal Privacy in an Information Society," Page, 103, July 1977, https://archive.epic.org/privacy/ppsc1977report/.

[25] Privacy Protection Study Commission, "Personal Privacy in an Information Society," Page, 502, July 1977, https://archive.epic.org/privacy/ppsc1977report/.

[26] Nicholas Anthony, "Why Don't Americans Have Stronger Financial Privacy Rights?," Cato at Liberty, October 28, 2021, https://www.cato.org/blog/why-dont-americans-have-stronger-financial-privacy-rights.

[27] Electronic Privacy Information Center, "Right to Financial Privacy Act," https://epic.org/the-right-to-financial-privacy-act/. The Right to Financial Privacy Act is Title XI of the Financial Institutions Regulatory and Interest Rate Control Act. https://www.congress.gov/bill/95th-congress/house-bill/14279

[28] Electronic Privacy Information Center, "Right to Financial Privacy Act," https://epic.org/the-right-to-financial-privacy-act/.

[29] Electronic Privacy Information Center, "Right to Financial Privacy Act," https://epic.org/the-right-to-financial-privacy-act/.

[30] 12 U.S. Code Section 3413, https://www.law.cornell.edu/uscode/text/12/3413.

[31] Notably, the exceptions included in the final version of the law were not part of the original 1973 proposal. Representative Fortney Stark, "Right to Financial Privacy Act," H.R. 10181, September 11, 1973, https://www.congress.gov/bill/93rd-congress/house-bill/10181?r=106&s=1.

[32] 12 U.S. Code Section 3413.

[33] Financial Crimes Enforcement Network, "Suspicious Activity Report Supporting Documentation," FIN-2007-G003, June 13, 2007, https://www.sec.gov/about/offices/ocie/aml2007/fin-2007-g003.pdf; 12 U.S.C. Section 3413(b), https://www.law.cornell.edu/uscode/text/12/3413.

[34] Financial Crimes Enforcement Network, "SAR Activity Review: Trends, Tips, & Trends," Bank Secrecy Act Advisory Group, October 2005, https://www.fincen.gov/sites/default/files/shared/sar_tti_09.pdf; Federal Financial Institutions Examination Council, "Suspicious Activity Reporting—Overview," BSA/AML Manual, https://bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/04.

[35] Department of the Treasury, "General Explanations of the Administration's Fiscal Year 2022 Revenue Proposals," May 2021, https://home.treasury.gov/system/files/131/General-Explanations-FY2022.pdf.

[36] Department of the Treasury, "General Explanations of the Administration's Fiscal Year 2022 Revenue Proposals," May 2021, https://home.treasury.gov/system/files/131/General-Explanations-FY2022.pdf.

[37] Department of the Treasury, "General Explanations of the Administration's Fiscal Year 2022 Revenue Proposals," May 2021, https://home.treasury.gov/system/files/131/General-Explanations-FY2022.pdf.

[38] Nicholas Anthony, "Why Don't Americans Have Stronger Financial Privacy Rights?," Cato at Liberty, October 28, 2021, https://www.cato.org/blog/why-dont-americans-have-stronger-financial-privacy-rights.

[39] Tim Scott, "Scott, Colleagues Introduce Bill to Block Democrats' IRS Snooping Proposal," Press Release, October 21, 2021, https://www.scott.senate.gov/media-center/press-releases/scott-colleagues-introduce-bill-to-block-democrats-irs-snooping-proposal; Senator Tim Scott, "Prohibiting IRS Financial Surveillance Act," S.2056, October 21, 2021, https://www.congress.gov/bill/117th-congress/senate-bill/3056/.

[40] Representative Ashley Hinson, "Protecting Financial Privacy Act of 2021," H.R. 5451, September 30, 2021, https://www.congress.gov/bill/117th-congress/house-bill/5451

[41] Department of the Treasury, "Fact Sheet: Tax Compliance Proposals Will Improve Tax Fairness While Protecting Taxpayer Privacy," Featured Stories, October 19, 2021, https://home.treasury.gov/news/press-releases/jy0415.

[42] This defense brings Maya Angelou's famous quote to mind: "When people show you who they are, believe them." The defense may have been true, but that does not mean it was a defensible position.

[43] Representative Henry Gonzalez, "Housing and Community Development Act of 1992," H.R. 5334, October 28, 1992, https://www.congress.gov/bill/102nd-congress/house-bill/5334.

[44] Representative Henry Gonzalez, "Housing and Community Development Act of 1992," H.R. 5334, October 28, 1992, Page 2389, https://www.congress.gov/bill/102nd-congress/house-bill/5334.

[45] For a larger discussion of the Bank Secrecy Act, see Norbert J. Michel and Jennifer J. Schulp, "Revising the Bank Secrecy Act to Protect Privacy and Deter Criminals," Policy Analysis No. 932, Cato Institute, July 26, 2022, https://www.cato.org/policy-analysis/revising-bank-secrecy-act-protect-privacy-deter-criminals.

[46] For the relevant portions of the USA Patriot Act, see sections 311, 314, 326, 352, 356, and 359. Representative James Sensenbrenner Jr., "Uniting and. Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001," H.R. 3162, October 26, 2001, https://www.congress.gov/bill/107th-congress/house-bill/3162.

[47] 31 U.S.C. Section 5318(g), https://www.law.cornell.edu/uscode/text/31/5318.

[48] 31 U.S.C. Section 5318(g)(2)(A)(i)-(ii), https://www.law.cornell.edu/uscode/text/31/5318.

[49] The law also established a formalized anti-money laundering (AML) program requirement where financial institutions are required to develop internal policies, employ a compliance officer, train employees, and conduct audits to guard against money laundering and terrorist financing. See 31 U.S.C. Section 5318(h), https://www.law.cornell.edu/uscode/text/31/5318.

[50] Nicholas Anthony, "America COMPETES Act Gives Treasury Unchecked Power," Cato at Liberty, January 27, 2022, https://www.cato.org/blog/america-competes-act-gives-treasury-unchecked-power.

[51] U.S. House Committee on Financial Services, "America COMPETES Act Contains Key Provisions Authored by Committee Democrats," Press Releases, January 25, 2022. https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=409024.

[52] Jerry Brito and Peter Van Valkenburgh, "New Bill Would Hand Treasury Blank Check to Ban Crypto at Exchanges," Coin Center, January 26, 2022, https://www.coincenter.org/new-bill-would-hand-treasury-blank-check-to-ban-crypto-at-exchanges/.

[53] Nicholas Anthony, "The Treasury's Special Enforcement Measures, Again," Cato at Liberty, May 4, 2022, https://www.cato.org/blog/treasurys-special-enforcement-measures-again.

[54] At the time of this writing, no member of Congress has claimed ownership of the Transparency and Accountability in Service Providers Act. Instead, in a moment of irony, the bill, one that seeks to further remove financial privacy, was published anonymously. "Transparency and Accountability in Service Providers Act," https://financialservices.house.gov/uploadedfiles/bills-117pih-transparencyandaccountabilit-u2.pdf.

[55] Project for Privacy and Surveillance Accountability, "Proposal Would Turn 7.6 Million Financial Service Employees into Government Informants," News and Updates, May 26, 2022, https://www.protectprivacynow.org/news/proposal-would-turn-76-million-financial-service-employees-into-government-informants.

[56] John O. Koehler, "Stasi: The Untold Story of the East German Secret Policy," New York Times, 1999, https://archive.nytimes.com/www.nytimes.com/books/first/k/koehler-stasi.html.

[57] Dustin Volz, "Most Americans Unwilling to Give Up Privacy to Thwart Attacks: Reuters/Ipsos Poll," Reuters, April 4, 2017, https://www.reuters.com/article/idUSKBN1762TQ.

[58] Dustin Volz, "Most Americans Unwilling to Give Up Privacy to Thwart Attacks: Reuters/Ipsos Poll," Reuters, April 4, 2017, https://www.reuters.com/article/idUSKBN1762TQ.

[59] Alan Zibel and Brent Kendall, "Probe Turns Up Heat on Banks," Wall Street Journal, August 7, 2013, https://www.wsj.com/articles/SB10001424127887323838204578654411043000772.

[60] Alan Zibel and Brent Kendall, "Probe Turns Up Heat on Banks," Wall Street Journal, August 7, 2013, https://www.wsj.com/articles/SB10001424127887323838204578654411043000772.

[61] Brian Knight, "How Financial Regulatory Tools Are Used Against Law-Abiding Americans—And How to Fix It," The Hill, March 3, 2022, https://thehill.com/opinion/finance/596697-how-financial-regulatory-tools-are-used-against-law-abiding-americans-and-how?rl=1.

[62] Dennis Shaul, "There's No Downplaying the Impact of Operation Choke Point," American Banker, November 28, 2018, https://www.americanbanker.com/opinion/theres-no-downplaying-the-impact-of-operation-choke-point.

[63] Michelle Hackman and Dustin Volz, "Secret Surveillance Program Collects Americans' Money-Transfer Data, Senator Says," Wall Street Journal, March 8, 2022, https://www.wsj.com/articles/secret-surveillance-program-collects-americans-money-transfer-data-senator-says-11646737201?st=egkffjxa3sszg5c&reflink=desktopwebshare_permalink

[64] Matthew Guriglia, "Here's How ICE Illegally Obtained Bulk Financial Records from Western Union," Electric Frontier Foundation, March 10, 2022, https://www.eff.org/deeplinks/2022/03/heres-how-ice-illegally-obtained-bulk-financial-records-western-union.

[65] Matthew Guriglia, "Here's How ICE Illegally Obtained Bulk Financial Records from Western Union," Electric Frontier Foundation, March 10, 2022, https://www.eff.org/deeplinks/2022/03/heres-how-ice-illegally-obtained-bulk-financial-records-western-union.

[66] Department of the Treasury, "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash," Press Releases, August 8, 2022, https://home.treasury.gov/news/press-releases/jy0916.

[67] Alan Zibel and Brent Kendall, "Probe Turns Up Heat on Banks," Wall Street Journal, August 7, 2013, https://www.wsj.com/articles/SB10001424127887323838204578654411043000772.

[68] Nikhilesh De, "U.S. Secretary of State Tweets, Deletes Claim That Crypto Mixer Tornado Cash Is North Korea-Sponsored," Coin Desk, August 8, 2022, https://www.coindesk.com/policy/2022/08/08/us-secretary-of-state-tweets-deletes-claim-that-crypto-mixer-tornado-cash-is-north-korea-sponsored/.

[69] Nicholas Anthony and Ivane Nachkebia, "How the Market, Not Government, Regulates Cryptocurrency Crimes," Cato at Liberty, August 23, 2022, https://www.cato.org/blog/how-market-not-government-regulates-cryptocurrency-crimes; Nicholas Anthony, "Treasury's Tornado Warning," Cato at Liberty, August 9, 2022, https://www.cato.org/blog/treasurys-tornado-warning; Jerry Brito and Peter Van Valkenburgh, "Analysis: What Is and What Is Not a Sanctionable Entity in the Tornado Cash Cast," Coin Center, August 15, 2022, https://www.coincenter.org/analysis-what-is-and-what-is-not-a-sanctionable-entity-in-the-tornado-cash-case/.

[70] Norbert Michel and Nicholas Anthony, "Keep Your Coins, Canada," Cato at Liberty, February 15, 2022, https://www.cato.org/blog/keep-coins-canada; Cato Institute Human Freedom Index

[71] Sumeet Chatterjee and Clare Jim, "Hong Kong Bank Account Freezes Rekindle Asset Safety Fears," Reuters, December 8, 2020, https://www.reuters.com/article/hongkong-security-banks/hong-kong-bank-account-freezes-rekindle-asset-safety-fears-idUSKBN28I1ZK; Andrew Osborn, "Russia Freezes Bank Accounts Linked to Opposition Politician Navalny," Reuters, August 8, 2019, https://www.reuters.com/article/us-russia-politics-navalny/russia-freezes-bank-accounts-linked-to-opposition-politician-navalny-idUSKCN1UY1ER.

[72] Brian Knight, "If You Use a Bank Account, Don't Get on the Wrong Side of the Government," Discourse, April, 1, 2022, https://www.discoursemagazine.com/economics/2022/04/01/if-you-use-a-bank-account-dont-get-on-the-wrong-side-of-the-government/.

[73] Nicholas Anthony, "How Inflation Erodes Financial Privacy," Cato at Liberty, June 10, 2022, https://www.cato.org/blog/how-inflation-erodes-financial-privacy; Norbert Michel and Nicholas Anthony, "Review of Bank Secrecy Act Regulations and Guidance," Cato Institute, February 7, 2022, https://www.cato.org/public-comments/review-bank-secrecy-act-regulations-guidance.

[74] California Bankers Association v. Schultz (1974)

[75] The concern shared by Justices Powell and Blackmun was also shared in the decision in Burrows v. Superior Court. California Bankers Assn. v. Schutz (1974), https://scholar.google.com/scholar_case?case=17636318791181551809&q=money+laundering&hl=en&as_sdt=4,60&as_ylo=1970&as_yhi=1980; Burrows v. Superior Court.

[76] U.S. House Committee on Financial Services, "Oversight of the Financial Crimes Enforcement Network," Full Committee Hearing, April 28, 2022, https://financialservices.house.gov/events/eventsingle.aspx?EventID=409259.

[77] "Finding a needle in the haystack is dependent on a number of things," said Representative Steil at the hearing, "One of them being how big the haystack is. So if we can find a way to get the haystack down, I think it may actually put us in the position to more easily find the needle." U.S. House Committee on Financial Services, "Oversight of the Financial Crimes Enforcement Network," Full Committee Hearing, April 28, 2022, https://financialservices.house.gov/events/eventsingle.aspx?EventID=409259

[78] Representative Stevan Pearce, "Counter Terrorism and Illicit Finance Act," H.R. 6068, June 12, 2018, https://www.congress.gov/bill/115th-congress/house-bill/6068/cosponsors. Notably, Representative Dina Titus (D-NY) also had a bill to increase the threshold for reporting winnings from slot machines so that it would adjust according to inflation. Representative Dina Titus, "H.R. 6937," March 3, 2022, https://www.congress.gov/bill/117th-congress/house-bill/6937.

[79] Representative Adam Smith, "William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021," H.R. 6395, January 1, 2021, https://www.congress.gov/bill/116th-congress/house-bill/6395.

[80] U.S. House Committee on Financial Services, "Oversight of the Financial Crimes Enforcement Network," Full Committee Hearing, April 28, 2022, https://financialservices.house.gov/events/eventsingle.aspx?EventID=409259.

[81] Financial Crimes Enforcement Network, "Civil Monetary Penalty Adjustment and Table," Federal Register, June 30, 2016, https://www.federalregister.gov/documents/2016/06/30/2016-15653/civil-monetary-penalty-adjustment-and-table.

[82] Howard Anglin, "In Our Cashless Society, We Need to Take Digital Jail Seriously," The Hub, February 22, 2022, https://thehub.ca/2022-02-22/howard-anglin-in-our-cashless-society-we-need-to-take-digital-jail-seriously/.

[83] Ian Vásquez, Fred McMahon, Ryan Murphy, and Guillermina Sutter Schneider, "The Human Freedom Index 2021," Cato Institute, 2021, https://www.cato.org/human-freedom-index/2021.

[84] Katz v United States: Justice Harlan described a two-step test in which a person must exhibit an expectation of privacy and it must be one "that society is prepared to recognize as reasonable." Katz v. United States (1967), https://supreme.justia.com/cases/federal/us/389/347/.

[85] Marta Belcher, Jennifer J. Schulp, and Caleb O. Brown, "Marta Belcher and Jennifer Schulp on Financial Privacy in a Digital Era," Cato Audio, Cato Institute, June 1, 2022, https://www.cato.org/multimedia/cato-audio/marta-belcher-jennifer-schulp-financial-privacy-digital-era.

[86] Kyllo v. United States (2001), https://www.law.cornell.edu/supct/html/99-8508.ZO.html.

[87] United States v. Jones (2012), https://www.law.cornell.edu/supremecourt/text/10-1259

[88] Carpenter v. United States (2018), https://www.law.cornell.edu/supremecourt/text/16-402.

[89] Katz v. United States (1967), https://www.oyez.org/cases/1967/35

[90] Katz v. United States (1967), https://supreme.justia.com/cases/federal/us/389/347/#tab-opinion-1946919

[91] Nicholas Anthony, "Update: Two Thirds of Commenters Concerned about CBDC," Cato at Liberty, July 27, 2022, https://www.cato.org/blog/update-two-thirds-commenters-concerned-about-cbdc.

[92] Electronic Privacy Information Center, "Right to Financial Privacy Act," https://epic.org/the-right-to-financial-privacy-act/.

[93] United States House of Representatives, "The Safe Banking Act of 1977," Hearings Before the Subcommittee on Financial Institutions, Supervision, Regulation, and Insurance of the Committee on Banking, Finance, and Urban Affairs, 1977. Pages 19-20.

[94] United States House of Representatives, "The Safe Banking Act of 1977," Hearings Before the Subcommittee on Financial Institutions, Supervision, Regulation, and Insurance of the Committee on Banking, Finance, and Urban Affairs, 1977. Pages 20-25.

[95] United States House of Representatives, "The Safe Banking Act of 1977," Hearings Before the Subcommittee on Financial Institutions, Supervision, Regulation, and Insurance of the Committee on Banking, Finance, and Urban Affairs, 1977. Pages 20. Norbert J. Michel and Jennifer J. Schulp, "Revising the Bank Secrecy Act to Protect Privacy and Deter Criminals," Policy Analysis No. 932, Cato Institute, July 26, 2022, https://www.cato.org/policy-analysis/revising-bank-secrecy-act-protect-privacy-deter-criminals.

[96] Carpenter v. United States (2018), https://www.law.cornell.edu/supremecourt/text/16-402.

[97] John Paul Koning, Twitter, September 5, 2022, https://twitter.com/jp_koning/status/1566771124792352775?s=20&t=bGQ8rpBJoNBwTVxBM1JUFA.

[98] LexisNexis Risk Solutions, "True Cost of AML Compliance Study," 2019, https://risk.lexisnexis.com/insightsresources/research/2019-true-cost-of-aml-compliance-study-for-united-states-and-canada

[99] Nicholas Anthony, "Reporting FinCEN's Suspicious Activity," Cato at Liberty, Cato Institute, April 13, 2022, https://www.cato.org/blog/reporting-fincens-suspicious-activity. When considering FinCEN's performance, Representative John Rose (R-TN) was right to express his concern about how "the federal government deputizes financial institutions" considering the financial industry suffers costs in the billions for its role in the process and its largely unknown what benefit has come out of it all. Nicholas Anthony, "Stop Deputizing Banks as Law Enforcement Agents," Cato at Liberty, Cato Institute, May 3, 2022, https://www.cato.org/blog/stop-deputizing-banks-law-enforcement-agents; Nicholas Anthony, "Oversight of the Financial Crimes Enforcement Network," Statement for the Record, Cato

Institute, April 28, 2022, https://www.cato.org/testimony/statement-record-hearing-oversight-financial-crimes-enforcement-network.

[100] Norbert J. Michel and Jennifer J. Schulp, "Revising the Bank Secrecy Act to Protect Privacy and Deter Criminals," Policy Analysis No. 932, Cato Institute, July 26, 2022, https://www.cato.org/policy-analysis/revising-bank-secrecy-act-protect-privacy-deter-criminals.

[101] This language is slightly modified from the Counter Terrorism and Illicit Finance Act. Representative Stevan Pearce, "Counter Terrorism and Illicit Finance Act," H.R. 6068, June 12, 2018, https://www.congress.gov/bill/115th-congress/house-bill/6068/text.

[102] This language is slight modified from the Financial Crimes Enforcement Network Improvement Act and National Defense Authorization Act for Fiscal Year 2021. Representative Warren Davidson, "Financial Crimes Enforcement Network Improvement Act," Congress.gov, April 28, 2022, https://www.congress.gov/bill/117th-congress/house-bill/7623?s=1&r=14; Representative Adam Smith, "William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021," H.R. 6395, January 1, 2021, https://www.congress.gov/bill/116th-congress/house-bill/6395.

[103] Nicholas Anthony, "The Infrastructure Investment and Jobs Act's Attack on Crypto: Questioning the Rationale for the Cryptocurrency Provisions," Cato Institute, November 15, 2021, https://www.cato.org/briefingpaper/infrastructure-investment-jobs-acts-undue-attack-crypto; Abraham Sutherland, "Research Report," Proof of Stake Alliance, September 17, 2021, https://www.proofofstakealliance.org/wp-content/uploads/2021/09/Research-Report-on-Tax-Code-6050I-andDigital-Assets.pdf.

[104] This language is slight modified from the Keep Your Coins Act. Representative Warren Davidson, "Keep Your Coins Act," H.R. 6727, February 15, 2022, https://www.congress.gov/bill/117th-congress/house-bill/6727.

[105] United States v. Jones (2012), https://www.law.cornell.edu/supremecourt/text/10-1259.

[106] Although social media users "document" their lives for the public to see, there's important difference to note in comparing this documentation to that in one's financial records: the difference between stated and revealed preferences. Social media users are inclined to filter, exaggerate, and select who reaches the public. However, one does not have that luxury with financial records. In fact, attempting to do so would likely be a violation of structuring and other anti-money laundering laws.

[107] 12 U.S. Code Section 3413, https://www.law.cornell.edu/uscode/text/12/3413/.