Restoring Americans' Financial Privacy

By Robert E. Wright, Senior Faculty Fellow, American Institute for Economic Research

> *The transactions of the bank with their customers, are, in the ordinary course of their business, highly confidential; an examination into them by strangers, so far as it implicates the individuals with whom the bank has dealings, bears all the exceptionable and odious properties of general warrants and domiciliary visits (Adams 1832, p. 2).*

Introduction: Privacy and Protection from Harm

Americans today truly live in an age of not just "shriveled privacy"[1] but also declining privacy expectations. This trend is reflected in a recent survey in which almost a third of Americans under the age of 30 say that they would not object to the government surveilling them in their own homes (Nicastro 2023). That is a particularly stark statistic, especially when considering the fact that when talking about the surveillance of one's financial records, the reality is that the only real benefactors of such monitoring end up being either journalists (Rubin and Viswanatha 2023) or tax and law enforcement officials, not the common weal (Penney 2007; Strahilevitz 2013).

Mass government surveillance of individual communications and other forms of information (Friedman 2000, pp. 186-187, 188-191), including financial records, is too often dismissed by assertions that innocent parties have nothing to hide. Insistence on privacy, however, should not be taken as a sign of guilt (Solove 2007, 746-48). Because while most

[1] This is a reference to Freedman's dissent in *White v. California* (17 Cal. App. 3d., 1975): "Our age is one of shriveled privacy."

Americans in fact have nothing to hide, they do have much to fear from intrusive and extensive government surveillance (Alexander and Spurgeon 1978, p. 21). While privacy rules may sometimes shield wrongdoers from justice, that cost is far exceeded by the benefits associated with privacy's primary role, which is to protect and preserve the human rights triad (life, liberty, and property) of every citizen.

Government remains legitimate in Anglo-American governance theory only so long as it, at the very least, protects the human rights triad as espoused in the various foundational documents such as the Declaration of Independence and the U.S. Constitution among others. America's Founding Fathers and Framers understood that a legitimate government protects the human rights triad of its citizenry from foes foreign and domestic, including, most importantly, itself. To ensure that governments would not become the main threat to the human rights triad of Americans, as governments had in most other nations throughout history, policymakers enumerated important individual rights to expression, including the right to speak or *not* to speak (Oranburg 2022, p. 144) (First Amendment); to own and carry firearms (Second Amendment); to be protected from unreasonable government searches and seizures (Fourth Amendment); and to due process (Fifth Amendment), including protections against self-incrimination. Mindful that they could not enumerate every individual right, the Framers left most rights unenumerated but protected by the Ninth Amendment and similar "baby ninths" built into most state constitutions (Barnett 2004; Sanders 2023).

Privacy is one of those numerous unenumerated rights. Its primacy in Anglo-American common law traditions predating the American Revolution (Green 1989, p. 262; Rogovin 1986, p. 594; Engelhardt 2000, pp. 135-140) highlights how its lack of specific mention in the Bill of Rights is not indicative of its perceived unimportance to America's Founders and Framers

(Richardson 2017, pp. 1-3). Rather it indicated privacy's primeval nature. Privacy predates and undergirds the Bill of Rights because of its centrality to the human rights triad (Alexander and Spurgeon 1978, p. 25; Epstein 2000, pp. 6, 9). Explicit court cases regarding privacy became more numerous in the nineteenth century due to the proliferation of more invasive technologies like photographs (Richardson 2017, pp. 130-68), but also due to increased state surveillance (Richardson 2017, pp. 54-55; Scott 1999, pp. 22-23, 110).

A hoary of extensive case law, however, is not required to see how the right to privacy inheres in the human rights triad. To protect one's body from violence (life), one must be able to hide from potential brigands, be they outside or inside the government (Friedman 2000, pp. 199-200). To protect one's ability to choose between alternative courses of action (liberty), one must be able to maintain control of one's inner thoughts and volition (Debrabander 2020, pp. 28, 34). To protect one's assets (property), one must be able to conceal their characteristics and/or location from those who seek to seize them (Weber 2018, p. 102). Although privacy waned in jurisprudential importance beginning with the New Deal, human rights advocates like Skinner-Thompson have rediscovered privacy's key role in shielding minorities from public and private persecution (2021, pp. 1-2).

As Calo explains (2018, p. 198), "a person without privacy is vulnerable." As privacy decreases, vulnerability to myriad threats increases through the creation of new vulnerabilities or the exploitation of existing ones by bad actors, within government and without (Rubin and Viswanatha 2023). Once a certain threshold is breached, Calo warns, a spiral can ensue that can render individuals exposed to and defenseless against high levels of continuous exploitation (2018, pp. 200-202).

"Privacy," Cypherpunk Eric Hughes explained, "is the power to selectively reveal oneself to the world" (as quoted in Oranburg [2022], p. 114). That power is important because, as Bibas notes (1994, p. 591), anyone with access to our quotidian activities could "piece together a coherent picture of our actions" which would be sufficient to impinge upon our human rights triad, exposing all, but especially the least powerful among us, to myriad harms (Skinner-Thompson 2021, pp. 3, 171). Very little personal information is needed to threaten individual autonomy (Debrabander 2020, 157; Burton 2021). Bank records alone, Rogovin says (1986, p. 587), "provide a virtual current biography" of individual activities, from opinions and habits to associations sufficient, in the wrong hands, to disrupt or even end lives.

In Germany, Austria, and occupied areas of Europe during World War II, invasions of financial privacy led to job loss, credit discrimination, and/or state expropriation of the liquid assets of members of scapegoated groups (Feldman 2015, pp. 22-23, 120-122, 450-452). If that threat seems foreign to those in the U.S., it's not. So much so that former President John Quincy Adams warned back in 1832 that members of Congress wanted access to the accounts of individuals with the Bank of the United States so that they could "ruin … a personal enemy, or a political adversary" (1832, p. 4). Little since has changed. In 2011 the U.S. government froze payments to Wikileaks (Weber 2018, p. 115). In 2022 Canada froze the bank accounts of hundreds of peaceful political protestors (Austen 2022). And on multiple occasions *legal* sex workers have lost access to various parts of the financial system (Dearing and Lane 2023).

Financial Confidentiality in the Anglo-American Tradition

To protect the human rights triad of Americans, its Founders and Framers considered bank accounts confidential, i.e., safe from third party disclosure without due process of law (Slobogin 2005, pps. 812-14; Green 1989-90, p. 262-63; Prabhu 2007, pps. 71-72). Commercial

banks arose along with the new nation, both a cause and an effect of the American Revolution (Wright 2001, 2023). They were soon joined by other depository institutions, including mutual savings banks, building and loan societies, and, later, credit unions (Wright 2019). In the mid-nineteenth century, investment banks also arose, to help governments and businesses sell securities (bonds, hybrids, and stocks) to investors (Carosso 1970, pp. 1-50). By credibly committing to maintaining customer confidentiality, banks could attract more customers, including borrowers, depositors, and securities traders (Harper and Chan 2003, pp. 33, 44). To enforce that commitment, banks enjoined their directors, managers, and clerks to declare an oath to maintain "the strictest secrecy" of account information (Patten 1891, pp. 315-316; Knox 1900, p. 557).

Under Anglo-American common law, banks were part of a class of "confidential servants," people and institutions tasked in large part with not divulging sensitive information to third parties. Any action undermining such a key confidence could constitute "one of the gravest breaches of faith and good propriety" (Bank of New Zealand 1876, p. 32). In the early days of the U.S., banks of all stripes had the right to keep information about *themselves* private while there was a culturally and socially implied (if not explicit) contractual duty to keep information about their clients (borrowers, depositors, securities issuers and buyers) confidential. The latter point was often mentioned in banking texts (e.g., Gilbart 1849, v. 2 p. 525) and by bankers in their professional literature, as in a *Bankers' Magazine* article that spoke of "the danger of tampering in any way with the confidential secrecy essential to the relations of bankers with their clients" (Leaf 1920, p. 581).

The primacy of privacy in banking remained uncontested until well into the twentieth century. It was apparently first litigated in the 1929 New Jersey case *Brex v. Smith* (104 N.J. Eq.

386 [N.J. 1929]), in which a judge barred a New Jersey prosecutor from obtaining the bank records of every member of the Newark police force, and some of their wives too (Rogovin 1986, pp. 594-595)! (It's a pernicious myth that women, single or married, did not have bank accounts until the 1960s [Wright 2019, pp. 213-33].)

Some banks agreed, as terms of their incorporation, to send basic balance sheet information to state officials and/or stockholders. Some also thought that it would aid business if they voluntarily published such general information in newspapers (Robertson 1968, pp. 23-27). They would not, however, divulge client information or general bank condition statements to third parties, including governments, simply upon request, "for it has been laid down that a banker has no right to reveal the state of his account with his customer" (Morse 1879, p. 57). The only financial transactions that were public were sales at public auction and bankruptcy or insolvency proceedings, the public nature of which not only shamed bankrupts but also helped to notify their creditors of the need to file claims (Ciment 1992). The worst anti-bank riot in U.S. history occurred when the leaders of a failed bank in Baltimore tried to keep their misconduct secret in part because their attempted cover up ran directly counter to prevailing bankruptcy norms (Shalhope 2009, pp. 34-39).

Just prior to the Civil War, some states like New York began to mandate call reports (periodic reports of balance sheet information) . During the Civil War, the federal government began to charter banks with alacrity and send examiners to physically inspect bank account books, including individual accounts (Robertson 1968, pp. 71-81). States like New York continued to charter banks and to implement examination regimes, as did various private clearinghouses, which swore themselves to secrecy (Bolles 1888, p. 252). By the twentieth

century, New York state bank examiners had power to subpoena witnesses and records but only to uphold banking regulations (Crowder 1942, pp. 236-243).

National bank regulators swore not to divulge customer information to other parties, within or without the government. That precedent was set by John Quincy Adams in his 1832 investigation of the Bank of the United States. After the words provided in the head quote to this article, Adams wrote that Congress gave him the power to examine and inspect the books and proceedings of a corporation, but it could not and did not give him the authority to examine the records of "any individual for purposes of crimination or of trial" (p. 2). Its wasn't until nearly a century and a half later that a check on government abuse was formally codified in the 1974 Privacy Act, which was passed due to fears of a "unified and government-run database" tracking the intimate details of each American, a la Orwell's Big Brother character in *1984* (Swire 2002, p. 1,275; Bibas 1994, p. 591).

Privately owned banks, which after the Civil War included thousands of depository banks, brokerage institutions (James 1978, pp. 40-44), and virtually all investment banks, similarly did not regularly provide even such basic information as balance sheets to the government on a regular basis. This changed however, during the 1933-34 Pecora Hearingsin which investment banker J.P. Morgan himself agreed while testifying before Congress after some hesitation, that his company would turn over five years of its balance sheets and its partnership agreement. Although this was due more to FDR's veiled threats than any law (Carosso 1970, pp. 336-39). This government overreach became the norm with states like New York thereafter regulating private banks the same way they did corporate ones by mandating call reports and examinations (Crowder 1942, pp. 198-202, 247).

The Securities and Exchange Commission (SEC) was also careful about protecting personal information. In 1937, for example, it made explicit its existing implicit policy that no information about individuals would be shared with anyone except securities dealers screening potential brokers and other employees. The SEC was also clear that it would only supply information in the public record, such as "injunctions, indictments, convictions or revocations of license or registration formally entered against such person." It reiterated this sentiment in 1952 by stating that "the Commission's private investigation files, are generally not considered available to private litigants" (DuBois 1937; Adams and Rosebach 1952). That included some types of information even when under subpoena (Thorsen 1951; Katzin 1952).

Regulatory Reductions of Financial Privacy

As financial regulations ramped up during the New Deal, banks found it exceedingly more difficult to prevent law enforcement from uncovering individual account information, even without a subpoena or warrant. In the early 1940s, for example, FBI special agent S.K. McKee was allowed with no push back to review the bank and credit union records of Ben Botkin, a suspected socialist who had worked on WPA projects, including the famous slave narratives, during the New Deal (Davis 2010, 10-11).

In the postwar period, the U.S. government began to pressure banks (and other businesses) for client information with the expressed purpose of enforcing criminal and income tax laws. The former took shape in the form of an increasingly vehement crusade against sin, usually focusing on illicit drugs and sex-related crimes. The latter became particularly necessary after a 1935 law ended the use of so-called "pink slips" which had made summaries of personal income taxes public (Beito 2023, pp. 15-16).

Authorities often had two main tools at their disposal, subpoenas and warrants. After 1957 decision in favor of the Internal Revenue Service (IRS) in *United States v. Klein* (247 F.2d 908 [2d Cir. 1957]; Stessens 2000, p. 96) however, the effectiveness of those instruments and precedents was limited. Particularly so by the fact that the people most sensitive to the long arm of the law or the IRS began to bank in offshore accounts where U.S. writs were of limited or no force. In response to losing such customers, U.S. banks routinely began destroying checks and other documents as soon as they became no longer pertinent to their customers' current accounts (Green 1989, p. 263-64).

Subpoenas, a formal demand for information, come in two types: *duces tecum* and administrative. The former stems from the criminal system, i.e., grand juries and prosecutors. The latter is from the IRS and other federal regulatory and enforcement agencies. While probable cause is needed for a physical search warrant, the mere certification of a law enforcement official is sufficient to obtain a subpoena for financial (and medical and school!) records. Protection from subpoenas was once rooted in both the Fourth and Fifth Amendments, the latter due to the bar against self-incrimination. The courts, however, substantially weakened both over the course of the twentieth century, rendering subpoenas nearly impossible to quash whether they were directed at the target or at a third-party recordkeeper, like a bank (Slobogin 2005). And despite some claims to the contrary (Oranburg 2022, p. 144), the First Amendment provides no explicit privacy protection (Richards 2015).

By 1967, SCOTUS appeared poised in its decision in *Katz v. United States* (389 U.S. 347 [1967]) to use the Fourth Amendment to make it more difficult to obtain third-party subpoenas by concluding that the amendment protects people, not places, and hence that warrants become necessary whenever and wherever anyone has a reasonable expectation of privacy (Mangan

1981, p. 249; Alexander and Spurgeon 1978, p. 25). Over the next decade, however, the High Court backed off any notion that it might radically expand Fourth Amendment protections (Mangan 1981, p. 250). In *Couch v. United States* (409 U.S. 322 [1973]), it upheld the validity of a subpoena used to access a suspect's records with his tax accountant. In *Fisher v. United States* (425 U.S. 391 [1976]), SCOTUS repudiated most remaining Fifth Amendment defenses of private papers (Slobogin 2005, pp. 822-823).

The same day that it decided *Fisher*, SCOTUS held in *United States v. Miller* (425 U.S. 435 [1976]) that a bank depositor had no standing to contest the validity of a *duces tecum* subpoena. In other words, it found that depositors had no Constitutionally recognizable right to keep their bank account information private by reasoning that depositors volunteered information regarding deposits and withdrawals in the normal course of business (Rogovin 1986, p. 587). Substantial criticism of *Miller* (e.g., Mangan 1981) included the opinion of the two dissenting justices, who cited state case law showing that bank customers had long enjoyed an expectation of privacy. According to Alexander and Spurgeon (1978, pp. 13-14), the decision "opened the way for unrestrained access to personal banking records via an administrative summons," and was particularly "subject to abuse by I.R.S. agents."

Although some state courts accepted *Miller* and allowed police to access bank records without legal process (Rogovin 1986, p. 601), the Supreme Court of Pennsylvania called *Miller* "a dangerous precedent, with great potential for abuse" and the California Supreme Court argued that *Miller* opened "the door to a vast and unlimited range of very real abuses of police power" (Rogovin 1986, pp. 589, 598). Nevertheless, three years after *Miller*, in *Smith v. Maryland* (442 U.S. 735 [1979]), SCOTUS applied the same legal logic to phone records, including communications with financial institutions, and in 1980 extended its line of reasoning to bank

borrowers in *United States v. Payner* (447 U.S. 727 [1980]) (Jones 1988, p. 37; Solove 2007, pp. 764-65; Slobogin 2005, pp. 823-24).

The Bank Secrecy Act of 1970 (PL 91-508) made decisions like *Miller* possible by breaking the traditional notion that bank customer records were protected from government scrutiny (Green 1989, pp. 261-62). America's first legislative attempt to make the laundering of illicit gains more costly, the act empowered the Treasury Secretary to mandate that banks (and other financial payments companies like credit card issuers) report cash transactions greater than $10,000 in a single day (Macey and Miller 1992, p. 200) and that they retain customer records of potential use in criminal, regulatory, or tax investigations for up to six years (Green 1989, p. 265-66; Stessens 2000, pp. 97-98). Many questioned the law's constitutionality on Fourth and Fifth Amendment grounds, but SCOTUS upheld it in *California Bankers Association v. Shultz* (416 U.S. 31 [1974]), arguing that the government could require banks to maintain certain records but could only access those records after legal due process (Jones 1988, p. 37; Mangan 1981, p. 243; Rogovin 1986, p. 588). The nature of that legal process, search warrant or mere subpoena, remained contested, with most individuals and state courts opting for more rigorous evidentiary levels. Others argued that SCOTUS in *Miller* had failed to appropriately apply the reasonable expectation of privacy standard established by *Katz* (Rogovin 1986, pp. 587-589).

Congress responded to the confusion over financial records privacy in 1978 by passing the Right to Financial Privacy Act (RFPA) (Mangan 1981, p. 291; Rogovin 1986, p. 589). Ostensibly, RFPA sought to protect bank clients from "unwarranted government intrusion into their financial records" (Jones 1988, p. 37) by joining with various state statutes, case law, and state constitutions (like that of Florida, which expressly protects privacy rights [Green 1989, pp. 282-283]) to create reasonable expectations of privacy and hence federal protection under *Katz*

(Mangan 1981, p. 292; Rogovin 1986, p. 594-606). Specifically, it prohibited bank disclosure of customer records to the federal government until the bank notifies the customer and a waiting period, during which time the customer can challenge, expires (Macey and Miller 1992, p. 201). An exception is made, however, if notice will jeopardize a federal investigation through flight risk, records destruction, and the like. Courts granted *all* 47 requests for waiving delayed notification filed prior to 1986, while granting only 1 of 74 customer challenges (Jones 1988, pp. 40-42).

Many considered the RFPA "flawed" due to such results, as well as the easy transferability of the records to other government agencies that have "not met the standards for judicial process" (Rogovin 1986, pp. 590-591). Most damningly of all, the courts found it difficult to apply the new law consistently. Some made the customer prove his or her innocence to quash the records request while others placed the burden on law enforcement officials in the middle of an investigation. Courts were also split on whether the RFPA's notice provisions covered grand jury subpoenas. In at least one instance, a court admitted evidence seized in violation of the RFPA (Rogovin 1986, pp. 592-593)!

Congress continued its eroding of customer rights in banking by passing in 1985 the Money Laundering and Related Crimes Act. It pre-empted some state laws by allowing banks to voluntarily provide information related to suspected criminal activity without liability or notice to the customer. It also made clear that customers need not be notified of grand jury *duces tecum* subpoenas (Jones 1988, pp. 39-40).

The following year, Congress amended both the Bank Secrecy Act and the RFPA in the Money Laundering Control Act, subtitle H of the Drug Enforcement Education and Control Act. The purpose was to make money laundering a crime and the laundered assets subject to

forfeiture (Stessens 2000, pp. 99-100). It also gave the Treasury Secretary summons authority for both bank records and bank officers (Jones 1988, p. 38; Green 1989, p. 273-274).

Congress also amended both acts in various other pieces of legislation to close loopholes by requiring that bank customers have proper identification, increasing penalties for financial institutions that violate anti-money laundering laws, and augmenting the enforcement authority of the U.S. Postal Service. Most importantly, the interagency transfer of personal bank records became explicitly allowed. In other words, bank regulators who thought they detected activities indicating violations of federal law could refer individual account information to the Department of Justice (Green 1989, pp. 276-77).

Congress included new privacy provisions in the Gramm-Leach-Bliley Act (GLBA), aka the financial modernization act. Passed in 1999, that law allowed depository institutions and investment banks to directly compete (or to merge) for the first time since the New Deal. It also allowed banks and insurers to merge or compete (Swire 2002, p. 1,264). To stymie fears that an integrated "financial supermarket" might grow too potent, GLBA promised to deliver the most comprehensive federal privacy legislation in the nation's history (Janger and Schwartz 2002, pp. 1,222-1,224).

Nevertheless, within a few years GLBA became the target of "scathing criticism" because it imposed significant costs on banks while providing "woefully weak" protection of their clients' privacy (Swire 2002, p. 1,263). Customer information could be shared within a "financial supermarket" without restriction and instead of preventing financial institutions from sharing individual information with outside companies until customers opt in, GLBA mandated that customers must opt out. To limit the number of customers opting out, financial institutions made their mandatory annual privacy disclosure practices opaque (Janger and Schwartz 2002,

pp. 1,224-1,225, 1,231-1232). According to Timothy Muris, chairman of the Federal Trade Commission, “acres of trees died to produce a blizzard of barely comprehensible privacy notices” designed to fatigue consumers into not opting out (as quoted in Janger and Schwartz 2002, p. 1,220). The tactic worked, as only about .5 percent opted out (Janger and Schwartz 2002, p. 1,230).

It is important to note that GLBA did nothing to protect the customers of financial institutions from government prying, rather it concentrated on information theft and personal data sharing between companies, like credit reports (Swire 2002, pp. 1,274-1,275). In fact, it vested enforcement power not with customers but with the Federal Trade Commission, the Securities and Exchange Commission, the Comptroller of the Currency, and the Federal Reserve (Janger and Schwartz 2002, p. 1,225). Under the GLBA any law enforcement agency could gain access to a customer’s entire financial “supermarket” record with a single subpoena, prompting consumer advocacy groups to advise individuals to continue to maintain accounts with multiple institutions (Janger and Schwartz 2002, p. 1,226-1,227).

In 2002, in *Smith v. Chase Manhattan Bank* (741 N.Y.S. 2d 100), plaintiffs sued a bank for selling their information to third parties in violation of its own privacy policy. The court held there was no injury caused by “an unwanted telephone solicitation or a piece of junk mail” and hence no case (Savino 2003, pp. 12-14). America had evolved from a nation where banks voluntarily maintained customer confidentiality to one where laws seemed to mandate confidentiality but not enforce it (Savino 2003, p. 5).

The attacks of September 11, 2001, initiated a new wave of government intrusions of individual privacy. The 2001 Patriot Act is just another example of the government further reducing financial privacy by making it easier for law enforcement authorities to access

individual banks and other financial records. Specifically, it allowed federal authorities to access the records of individuals, without notice, through formal FISA (Foreign Intelligence Surveillance Act) subpoena-like requests or informal but essentially mandatory NSLs (national security letters). Requiring only a letter from an FBI supervisor, the latter are relatively easy to obtain and hence widely used even though unlike a subpoena they are not self-enforcing and would force the issue into court if an institution decided not to comply. The CIA and Department of Defense also issue NSLs, but they are not mandatory and hence remain unenforceable (Prabhu 2007, pp. 51, 57-62).

By 2002, various federal intelligence agencies and the Department of Defense had implemented a Total Information Awareness (TIA) data mining project. As its name implies, the TIA included financial data, including Swift (formerly the Society for Worldwide Interbank Financial Telecommunication) transactions (Solove 2007, p. 746). TIA faced criticism because the financial transactions of some Americans were surveilled without subpoenas or warrants on the thin justification that Swift was a messaging service and not a financial institution and hence exempt from the RFPA (Lichtblau and Risen 2006).

The reauthorized version of the Patriot Act passed in 2006 permitted banks to question FISA requests and NSLs in court but did not mandate that they do so. Given federal and state laws and the expectation of confidentiality, the reform arguably obligated financial institutions to review requests and file challenges and opened the door to creating confidentiality-related contractual obligations between financial institutions and their customers. By allowing court review, the reform also arguably created a process that would pass Fourth Amendment muster even though it did not enjoin banks to challenge information requests and even though NSL

appeals could be trumped by simply getting a higher-level officer to certify their importance to national security (Prabhu 2007, pp. 51, 60-62).

Over the last decade, Federal regulatory access to Americans' financial records has grown along with tax collection efforts, with small businesses especially targeted (Burton 2022). Pushback on Biden administration efforts to surveil virtually all transactions, however, only encouraged the government to look for high tech ways to monitor and tax more voluntary exchange. Today, a new technology, the blockchain or public ledger technology underlying Bitcoin and other cryptocurrencies, threatens to provide governments with complete and instantaneous access to every person's economic life, denuding them of all remaining financial privacy.

Central Bank Digital Currency and the End of Financial Privacy

From the nation's founding until recently, Americans could avoid government surveillance by avoiding instruments that leave an audit trail like checks or electronic transfers and instead opting for cash instruments like coins and paper notes. Cash forms of money allow for anonymous or pseudonymous purchases and sales and, unlike checks, are trustless because they constitute a final payment and not a promise to pay. Anti-money laundering and cash seizure laws raised the costs of transacting in cash, but it remains at least an option for smaller transactions.

Cryptocurrencies also remain legal for now, although they are subject to the Bank Secrecy Act and other regulations (Oranburg 2022, p. 138). Of the various cryptocurrencies, only Bitcoin held in a pseudonymous private "wallet" can be, and has been, traded without the possibility of defalcation and with minimal state intrusion or surveillance. A Central Bank Digital Currency (CBDC), a digital sovereign currency in other words, resembles Bitcoin but,

unlike that progenitor of all private cryptocurrencies, it is neither trustless nor inherently pseudonymous, much less anonymous. In other words, users of CBDCs could be expropriated and/or their transactions tracked (White 2022, pp. 154-155, 173-174, 199-200). CBDCs come in two major forms, wholesale (central bank to central bank or central bank to private bank) (Arslanian 2022, pp. 185-201) and retail (central bank to individual directly or central bank to individual indirectly via private bank). A direct retail CBDC that supplanted cash could end the last great bastion of financial privacy by effectively ending anonymous exchange (Arslanian 2022, p. 216).

CBDCs promise to leverage the blockchain technology undergirding Bitcoin and other cryptocurrencies to improve access to the financial system, including receipt of payments from the government during emergencies and to increase central bank control of the macroeconomy and parts of the financial system (Arslanian 2022, pp. 171-184, 203-204). In the process, however, CBDCs that entail a central bank monopoly on payment services threaten to eliminate the anonymity associated with traditional cash purchases and even the pseudonymity associated with Bitcoin (Weber 2018, pp. 106, 113, 116-17)and thus enable cheap and easy government surveillance of economic transactions (Weber 2018, p. 240n.10) which ultimately turn into tools of coercion by allowing governments to reduce or eliminate the liquid assets of individuals or other economic entities at will (Rennie and Steele 2021). It also risks invasion of personal privacy via data breaches by malign third party actors (Gross et al 2022, pp. 1-2; Arslanian 2022, p. 206). That especially applies to an account-based CBDC but could also potentially occur in a token-based one. (For more on the distinction between token and account-based CBDCs, see Arslanian 2022, pp. 206-11.)

In fact, survey respondents consider privacy the most important issue regarding CBDCs. Although it is technically possible to provide transaction privacy in a CBDC using electronic tokens akin to bearer cash instruments like notes or coins (Tinn and Dubach 2021, p. 1), most governments remain unwilling to provide any privacy protections that threaten their monitoring of money laundering or other illegal transactions (Grothoff and Moser 2021, pp. 1-3; Arslanian 2022, pp. 213-15). Under one proposal, the central bank would rely solely on the current regulatory regime to reduce money laundering and tax evasion but then it is unclear what benefits a CBDC brings as most money is already digital and cleared electronically. It appears that many central banks pursue CBDC development for fear of losing their seigniorage rents to Big Tech, cryptocurrencies, or foreign central banks (Gross et al 2022, p. 1).

Under another token-based proposal, buyers would remain anonymous, but sellers would not. Consumers could buy goods without worrying that their purchases are being tracked while also ensuring that sellers of goods pay their taxes (Tinn and Dubach 2021, p. 2).

A third proposal also tries to provide cash-like privacy in a CBDC while also addressing tax and regulatory issues, this one by using an account-based approach instead of tokens (Gross et al 2022). In the proposed system, small person-to-person and retail transactions would occur completely anonymously within a fully private pool, subject only to balance, transfer, and turnover limits designed to reduce money laundering and tax evasion. The pool then interacts with a payment service provider (PSP), like a bank, which only sees the amount of the transfer. The payments between PSPs and between PSPs and the central bank would be as fully transparent as current electronic payments are.

For the limits to function effectively, however, each user would have to use a government-issued digital ID. Moreover, users could share their payment history to prove that

they did, or did not, complete a particular transaction (Gross et al 2022, p. 33). So, the technology would allow a government entity with a subpoena or warrant to view at least one side of the transactions in the private pool and hence would be less private than a system that employs physical bearer cash instruments. The proposed system could be less invasive than an open ledger type CBDC (Arslanian 2022, p. 178), but it seems unlikely that a major government like that of the United States would, or could, commit to constraint itself from using its power to peek into the private pool. Its biggest incentive to make such a commitment would be to compete against anonymous, extra-legal payment systems without any built-in transaction limits.

Conclusion: Restoring Financial Privacy with Historical and Swiss Confidentiality Precedents

From 1934 until the Third Millennium, Swiss banking laws forbid bankers from disclosing any customer information to third parties (Stessens 2000, pp. 109-12). Contrary to myth, there are no strictly anonymous Swiss bank accounts but only so-called numbered accounts, the owner of which is known only to a few bank employees and must be verified by them before opening an account. Such accounts remain common, though less so than previously (Dreier 2023).

Swiss banks began to try to reduce money laundering starting in 1990 through a private code of conduct that bound them not to execute transactions that they knew to be unlawful (Stessens 2000, pp. 100-108). Later, the code and the law also mandated that Swiss bankers inform law enforcement officials if they spot any criminals or attempted criminal activity, although they must do so "without coming into conflict with the banking secrecy act" (Cocca and Csoport 2003, pp. 308-10). In that way, Swiss banks help law enforcement to understand

illicit fund transfer attempts without being essentially deputized to enforce criminal law, as U.S. banks currently are. That said, Swiss banks became much more complicit with the global anti-money laundering complex that began to emerge in the 1990s (Sharmin 2011).

It remains unclear why the U.S. could not move towards more stringent bank confidentiality laws and norms in line with its own history and even more preventative than the Swiss approach. U.S. authorities often suggest that the tradeoff is between "getting the bad guy" and individual privacy but they can find and punish wrongdoers without reducing everyone's financial privacy and certainly without creating the costly labyrinth of regulations and guidance that currently burdens existing enforcement efforts (Burton 2022). Restoring Americans' financial privacy and ensuring due process does not entail collecting fewer tax dollars or suffering more terrorism or illicit drugs. It simply means that authorities must work harder or smarter than they do presently (Coyne and Yatsyshina 2021). Protecting the human rights triad is more important than making it as easy as possible for government officials to stop terrorists and punish tax evaders.

References

Adams, Clarence H. and J. Howard Rosebach. (1952). "Meetings of the Securities and Exchange Commission, Wednesday, December 3." UD-WW 178, Box 255. Records of the Securities and Exchange Commission, RG 266, National Archives and Records Administration, College Park, Maryland.

Adams, John Quincy. (1832). "Report of Mr. Adams." House of Representatives Report No. 460, 22d Congress, 1st Session. (14 May): 1-42.

Alexander, Richard and Roberta K. Spurgeon. "Privacy, Banking Records and the Supreme Court: A Before and After Look at *Miller*," *Southwestern University Law Review* 10 (1978): 13-33.

Arslanian, Henri. *The Book of Crypto: The Complete Guide to Understanding Bitcoin, Cryptocurrencies and Digital Assets*. Cham: Palgrave, 2022

Austen, Ian. "Canada Ends Its Freeze on Hundreds of Accounts Tied to Protests." *New York Times*. (February 22, 2022)

Bank of New Zealand. "Reports of Joint-Stock Banks." *Bankers' Magazine* 36 (1876): 27-33.

Barnett, Randy E. *Restoring the Lost Constitution: The Presumption of Liberty*. Princeton: Princeton University Press, 2004.

Beito, David T. *The New Deal's War on the Bill of Rights: The Untold Story of FDR's Concentration Camps, Censorship, and Mass Surveillance.* Oakland: Independent Institute, 2023.

Bibas, Steven A. "A Contractual Approach to Data Privacy," *Harvard Journal of Law and Public Policy* 17 (1994): 591-611.

Bolles, Albert S. *Practical Banking*, 5th ed. New York: Homans Publishing Company, 1988.

Burton, David R.“The Heritage Foundation.” The Heritage Foundation. June 9, 2022. https://www.heritage.org/testimony/financial-privacy-free-society-balancing-the-needs-citizens-small-businesses-and.

Calo, Ryan. “Privacy, Vulnerability, and Affordance.” Chapter. In The Cambridge Handbook of Consumer Privacy, edited by Evan Selinger, Jules Polonetsky, and Omer Tene, 198–206. Cambridge Law Handbooks. Cambridge: Cambridge University Press, 2018.

Carosso, Vincent. *Investment Banking in America: A History.* Cambridge: Harvard University Press, 1970.

Ciment, James. “In Light of Failure: Bankruptcy, Insolvency and Financial Failure in New York City, 1790-1860.” Ph.D. Diss., City University of New York, 1992.

Cocca, Teodoro D., and Peter Csoport. "The Future of Swiss Banking." In The future of banking, pp. 271-316. Westport: Quorum Books, 2003.

Coyne, Christopher J. and Yuliya Yatsyshina. “Police State, USA.” *The Independent Review* 26, no. 2 (2021): 189-204.

Crowder, Edward T. “State Regulation of Commercial Banking in New York.” Ph.D. Diss., New York University, 1942.

Davis, Susan G. “Ben Botkin’s FBI File.” *Journal of American Folklore* 123, no. 487 (2010): 3-30.

Dearing, Tiziana and Rob Lane. “Legal Sex Workers in New England Find Themselves Shut Out from Banking, Payment Platforms.” WBUR Radio Boston, June 5, 2023. https://www.wbur.org/radioboston/2023/06/05/diti-kohli-sex-work-onlyfans-mintstars

Debrabander, Firmin. *Life After Privacy: Reclaiming Democracy in a Surveillance Society*. New York: Cambridge University Press, 2020.

Dreier, Daniel. "Swiss Numbered Bank Accounts: A Practical Guide." *Moneyland.ch*. January 16, 2023. https://www.moneyland.ch/en/numbered-bank-account-switzerland.

DuBois, Orval L. (1937). Memorandum to Mr. Saperstein et al Re: Bonner & Bonner. UD-WW 159, Box 321. Records of the Securities and Exchange Commission, RG 266, National Archives and Records Administration, College Park, Maryland.

Engelhardt, H. Tristram. "Privacy and Limited Democracy: The Moral Centrality of Persons." In Ellen F. Paul, Fred D. Miller, Jr., and Jeffrey Paul, eds. *The Right to Privacy*. New York: Cambridge University Press (2000), 120-40.

Epstein, Richard A. "Deconstructing Privacy and Putting It Back Together Again." In Ellen F. Paul, Fred D. Miller, Jr., and Jeffrey Paul, eds. *The Right to Privacy*. New York: Cambridge University Press (2000), 1-24.

Feldman, Gerald D. *Austrian Banks in the Period of National Socialism*. New York: Cambridge University Press. In Ellen F. Paul, Fred D. Miller, Jr., and Jeffrey Paul, eds. *The Right to Privacy*. New York: Cambridge University Press (2015), 186-212.

Friedman, David. "Privacy and Technology." *Social Philosophy and Policy* 17, no. 2 (2000): 186-212.

Gilbart, James W. *A Political Treatise on Banking*, 5th ed. London: Longman, Brown, Green and Longmans, 1849.

Green, Mary Catherine. "The Bank Secrecy Act and the Common Law: In Search of Financial Privacy," *Arizona Journal of International and Comparative Law* 7 (1989): 261-286.

Gross, Jonas, Johannes Sedlmeir, Matthis Babel, Alexander Bechtel, and Benjamin Schellinger. "Designing a Central Bank Digital Currency with Support for Cash-like Privacy." (July 22, 2021).

Grothoff, Christian and Thomas Moser. (2021). “How to Issue a Privacy-Preserving Central Bank Digital Currency.” SUERF: The European Money and Finance Forum Policy Briefs, No. 114, June.

Harper, Ian R. and Tom C. H. Chan. “The Future of Banking: A Global Perspective.” In Benton E. Gup, ed. *The Future of Banking*. Westport, Conn.: Quorum Books, 2003.

James, John A. *Money and Capital Markets in Postbellum America*. Princeton: Princeton University Press, 1978.

Janger, Edward J. and Paul M. Schwartz. “The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules,” *Minnesota Law Review* 86 (2002): 1,219-1,262.

Jones, Sarah Elizabeth. “Right to Financial Privacy: Emerging Standards of Bank Compliance,” *Banking Law Journal* 105 (1988): 37-51.

Katzin, Jerome S. (1952). Letter to Leonard E. Levenson. 13 Nov. UD-WW 178, Box 255. Records of the Securities and Exchange Commission, RG 266, National Archives and Records Administration, College Park, Maryland.

Knox, John Jay. *A History of Banking in the United States*. New York: Bradford Rhodes and Company, 1900.

Leaf, Walter. “Education of the Modern Banker: An Interesting Address.” *Bankers’ Magazine* Jan.-Jun. (1920) : 579-586.

Lichtblau, Eric and James Risen. “Bank Data Is Sifted by U.S. in Secret to Block Terror.” *New York Times* 23 (2006): 66-205.

Macey, Jonathan R. and Geoffrey P. Miller. *Banking Law and Regulation*. Boston: Little, Brown and Company, 1992.

Mangan, Joseph R. “Reasonable Expectations of Privacy in Bank Records: A Reappraisal of United States v. Miller and Bank Depositor Privacy Rights,” *Journal of Criminal Law and Criminology*, 72 (1981): 243-292.

Morse, John T. *A Treatise on the Law Relating to Banks and Banking*, 2nd ed, rev. Boston: Little, Brown, and Company, 1879.

Nicastro, Jonathan *Nearly a Third of Adults under 30 Support Government Surveillance in Their Homes*. National Review. June 7, 2023 https://www.nationalreview.com/corner/nearly-a-third-of-adults-under-30-support-government-surveillance-in-their-homes/

Oranburg, Seth C. *A History of Financial Technology and Regulation: From American Incorporation to Cryptocurrency and Crowdfunding*. New York: Cambridge University Press, 2022.

Patten, Claudius B. *The Methods and Machinery of Practical Banking*. 2nd ed. New York: Bradford Rhodes & Company, 1891.

Penney, Steven. “Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach,” *Journal of Criminal Law and Criminology* 97 (2007): 477-530.

Prabhu, Aditi A. “Contracting for Financial Privacy: The Rights of Banks and Customers Under the Reauthorized Patriot Act,” *Loyola University of Chicago Law Journal* 39 (2007): 51-121.

Rennie, Ellie and Stacey Steele. . “Privacy and Emergency Payments in a Pandemic: How to Think About Privacy and a Central Bank Digital Currency,” *Law, Technology and Humans* 3 (2021): 6-17.

Richards, Neil M. (2015). "Why Data Privacy Law Is (Mostly) Constitutional," *William & Mary Law Review* 56 (2015): 1,501-1,533.

Richardson, Megan. *The Right to Privacy: Origins and Influence of a Nineteenth-Century Idea*. New York: Cambridge University Press, 2017.

Robertson, Ross M. *The Comptroller and Bank Supervision: A Historical Appraisal*. Washington, D.C.: Office of the Comptroller of the Currency, (1968).

Rogovin, Michael. "Privacy of Financial Records," *Annual Survey of American Law* (1986): 587-607.

Rubin, Richard and Aruna Viswanatha. "IRS Contractor Is Charged in Leak of Trump Tax Returns, Thousands of Wealthy Americans' Records," *Wall Street Journal.* September 29 2023. https://www.wsj.com/us-news/law/u-s-charges-irs-contractor-with-tax-return-leak-90756f09

Sanders, Anthony B. *Baby Ninth Amendments: How Americans Embraced Unenumerated Rights and Why It Matters* Ann Arbor: University of Michigan Press, 2023.

Savino, William M. "Bank Privacy Disputes Reach the Courts," *Banking Law Journal*, 120 (2003): 5-17.

Scott, James C. *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed.* New Haven: Yale University Press, 1999.

Shalhope, Robert E. The Baltimore bank riot: political upheaval in antebellum Maryland. Urbana: University of Illinois Press, 2009.

Sharmin, J.C. *The Money Laundry: Regulating Criminal Finance in the Global Economy*. Ithaca: Cornell University Press, 2011.

Skinner-Thompson, Scott. . *Privacy at the Margins*. New York: Cambridge University Press, 2021.

Slobogin, Christopher. . "Subpoenas and Privacy," *DePaul Law Review* 54 (2005): 805-846.

Solove, Daniel J. "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy," *San Diego Law Review* 44 (2007): 745-772.

Stessens, Guy. *Money Laundering: A New International Law Enforcement Model*. New York: Cambridge University Press, 2000.

Strahilevitz, Lior J. "Toward a Positive Theory of Privacy Law." *Harvard Law Review* 126 (2013): 2,010-2,042.

Swire, Peter P. "The Surprising Virtues of the New Financial Privacy Law," *Minnesota Law Review* 86 (2002): 1,263-1,323.

Thorsen, Nellye A. (1951). Kaiser-Frazer Corporation vs. Otis & Co. Memorandum, 4 Jan. UD-WW 178, Box 248. Records of the Securities and Exchange Commission, RG 266, National Archives and Records Administration, College Park, Maryland.

Tinn, Katrin and Christophe Dubach.. "Central Bank Digital Currency with Asymmetric Privacy," SSRN Working Paper, March 2021.https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3787088.

Weber, Beat.. *Democratizing Money?: Debating Legitimacy in Monetary Reform Proposals*. New York: Cambridge University Press, 2018.

White, Larry. *Better Money: Gold, Fiat, or Bitcoin?* New York: Cambridge University Press, 2022.

Wright, Robert E. *Origins of Commercial Banking in America, 1750-1800*. Lanham, Md.: Rowman and Littlefield, 2001.

Wright, Robert E. *Financial Exclusion: How Competition Can Fix a Broken System*. Great Barrington, Mass.: American Institute for Economic Research, 2019.

Wright, Robert E. "Consequences Unintended: The Bubble Act and American Independence," in Helen Paul and D'Maris Coffman, eds. *The Bubble Act: New Perspectives from Passage to Repeal and Beyond*. New York: Palgrave, 2023.