Testimony before the

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON FINANCIAL SERVICES
Subcommittee on Consumer Protection and Financial Institutions

Regarding

"Banking Innovation or Regulatory Evasion?

Exploring Trends in Financial Institution Charters"

April 15, 2021

Raúl Carrillo, Esq.
Associate Research Scholar, Yale Law School
Deputy Director, Law and Political Economy Project

Summary

Chair Perlmutter, Ranking Member Leutkenmeyer, and Members of the Subcommittee, thank you for inviting me to this hearing. I offer my testimony as an attorney, an Associate Research Scholar at Yale Law School, and Deputy Director, Law and Political Economy Project.[1] I have previously served as Special Counsel to the Enforcement Director of the Consumer Financial Protection Bureau (CFPB) and worked as a Staff Attorney at New Economy Project in New York City, fighting on behalf of the low-income and ("no-income") people of New York City. I appeared before the Financial Technology Task Force last

[1] "The Law and Political Economy (LPE) Project brings together a network of scholars, practitioners, and students working to develop innovative intellectual, pedagogical, and political interventions to advance the study of political economy and law. Our work is rooted in the insight that politics and the economy cannot be separated and that both are constructed in essential respects by law. We believe that developments over the last several decades in legal scholarship and policy helped to facilitate rising inequality and precarity, political alienation, the entrenchment of racial hierarchies and intersectional exploitation, and ecological and social catastrophe. We aim to help reverse these trends by supporting scholarly work that maps where we have gone wrong, and that develops ideas and proposals to democratize our political economy and build a more just, equal, and sustainable future." https://lpeproject.org/.

September as Policy Counsel to the Demand Progress Education Fund (DPEF)[2] and a Fellow at the Americans for Financial Reform Education Fund (AFR Education Fund).[3]

My previous remarks humbly requested that policymakers consider the deeper impacts of nascent financial technologies on democracy and society. My remarks today echo these same themes. I respectfully urge Congress to acknowledge the true extent to which law and especially legislation are already governing the "fintech" space. We should not imagine that law and technology are separate or that the law needs to "catch up with technology." Rather, the law permits the technologies we are discussing today to exist. The pandemic response has cast into relief the fundamental ways in which Congress helps manage money and markets at the systems design level. New fintech does not appear as from nowhere; rather, it grows and flows from existing legal arrangements with all their idiosyncrasies and flaws. People who claim to separate law from technology, technology from politics, or politics from law are typically telling an inaccurate or incomplete story. As with the technology itself, humans build and use the legal tools at their disposal with certain ideas for their usage in mind.[4]

This morning, I have the luxury of presenting alongside Professor Kristin Johnson and other likeminded colleagues, and will thus merely refer to you my previous testimony for comments regarding algorithmic discrimination, capital markets, operational security and resiliency, and many themes of macroprudential regulation. Today I will focus on three core themes, which are intended to address the specific regulatory concerns highlighted by the Subcommittee in the Hearing Memo:

1) **Congress should pursue and support financial institutions' charter policies that protect the safety and soundness of U.S. monetary, banking, and financial systems as public "infrastructure" used not only by businesses, but everyday people around the world.** In general, I echo previous calls for policymakers to adopt a bright-line, precautionary approach to digital "bank-like" activities.[5] What industry calls "innovation" is often easily mapped to a longstanding financial service and therefore the substance of existing laws should govern.

---

[2] DPEF is a fiscally-sponsored project of New Venture Fund, a 501(c)3 organization. DPEF and our more than two million affiliated activists seek to protect the democratic character of the internet — and wield it to render government accountable and contest concentrated corporate power.
[3] AFR Education Fund is a coalition of more than 200 national, state, and local groups who have come together to advocate for reform of the financial industry. Members of AFR Education Fund include consumer, civil rights, investor, retiree, community, labor, faith based, and business groups.
[4] As Frank Pasquale details, we should not envision technology as a replacement of the human with the machine, but another another recalibration of a sociotechnical system of human decisionmakers and machine-aided decision analysis. *See* FRANK PASQUALE, THE NEW LAWS OF ROBOTICS (2020).
[5] *See, e.g.* Saule T. Omarova, *Dealing with Disruption: Emerging Approaches to Fintech Regulation*, 61 WASH. U. J.L. & POL'Y 27, 34-36 (2020) (discussing the problem with "smart" regulation: regulation that is "iterative, flexible, carefully tailored, risk-sensitive, and innovation-friendly."); JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 174, 182-187 (2019) (underscoring the importance of understanding platform digital activities in order to meet systemic threats).

At the same time, certain tools and certain forms of partnerships should have no place in our economy whatsoever -- whether they "evade" or arbitrage existing regulations or not. Money, payments, banking -- these are part of our very constitutional order and demand respect. Treating innovation as an unqualified good leads regulators to ignore both considerations of equity, privacy, safety, and the sort of long-term, sustainable, cooperative innovation that allows us all to truly prosper together. Given the interface between powerful corporations, complex products, and the broader public, precaution should be the norm, as it should be in food and drug regulation.[6]Although it is indispensably important to classify and assign regulatory responsibility for new products and the specific business relationships that enable them, Congress should not lose sight of its legislative purview over money, banking, and finance. That is to say, we should also discuss policy at the level of systems design via Congressional authority over matters involving the "public purse.

2) **Congress should reconsider the value "of vague but popular goals of "financial inclusion" & "access to credit", especially in light of the evolving surveillance-based business models used by fintech companies that violate our civil rights & liberties.** A bank account is not the answer to every problem; credit is not a cure for poverty. If we have learned anything from approximately 250 years of U.S. governance of money, banking, and finance, it is that we shouldn't trust business (or government agencies) just because they claim to have new technologies that obviate the need to comply with the law. We do not trust claims of privacy, security, or stability merely when they are asserted by people who stand to benefit lucratively from the blind acceptance of promises. At the product, firm, or systems level. That would be imprudent and poor stewardship over the machinery at the center of our broader economy.

   Even more importantly, we should not consign everyday people to accepting unnecessary and dangerous invasion of their privacy in order to participate in the payments system. We all deserve to participate in the broader economy and society without perpetual surveillance, to be "one in the crowd", as suggested by the Fourth Amendment, the First Amendment, and the law against general warrants that precedes them both. Currently, federal privacy law offers little meaningful protection to citizens against mass surveillance by their own government. This should be a subject of extreme concern regardless of political party affiliation.

3) **Congress should establish a framework for public sector financial services.** Innovation in this space is simply too important to leave to the private sector. This begins with properly respecting and stewarding our existing analog systems. The ongoing "War on Cash" assails our most democratic constitutional principles and aspirations with respect to monetary provisioning and privacy therein. The Court's legal tender doctrine, Fourth Amendment doctrine, and First Amendment doctrine could

[6] COHEN, *supra* note 5, at 91-92.

arguably be interpreted as providing constitutional protection to cash as a payment technology. Regardless, bans on paper cash should be prevented by federal legislation. Even more importantly, any provision of public services, including a public option for financial services, must preserve a place in our monetary design for a digital equivalent to *cash wallets* as well as *bank accounts.* While legal firewalls might prevent some level of abuse in a public ledger system, technological solutions are also required. In the context of privacy law, cash in "closed containers" affords substantially more obscurity (if not anonymity, nor necessarily secrecy) to users as we go about our everyday lives. We can circulate both analog and digital cash in a manner that respects some of the most democratic U.S. constitutional traditions.

Charter Policy: Money, Banking, & Finance as "Infrastructure"

Background

The Bill of Rights clearly recognized the right to privacy and protection from unreasonable searches and seizures are both fundamental liberty interests. The Fourth Amendment was created to protect American citizens from the type of government invasions rampant under King George that allowed British soldiers to invade the colonists' homes in search of anti-monarchists.[7] The law of search and seizure can be seen as the consequence of the strong tradition of using law as a shield for associational freedom and free speech.[8] The Third Amendment can also be read this way.[9]

There was less agreement among colonists as to how the monetary system should work. Many colonists came to the colonies to escape their debts. Throughout the 18th century, the question of who had the power to issue legal tender (the best method of debt cancellation) was a contentious one between the British Crown, Parliament, and American colonial governments. Nevertheless, the Constitution shifted the power to regulate money, debt, credit contracts, and tax forgiveness to the federal government.[10] Banking regulation flows from this constitutional authority over money itself. NIn various ways, scholars have argued the government has delegated some of its "money-creation" power to banks.[11] Indeed, 33 banking law scholars

[7] William Pitt, Earl of Chatham, Speech on the Excise Bill in the House of Commons (Mar. 1763).
[8] Deven R. Desai, *Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding*, 90 Notre Dame L. Rev. 579, 602 (2014).
[9] *The Intolerable Acts: American Revolution*, PORTLAND STATE UNIVERSITY COLLEGE OF URBAN & PUBLIC AFFAIRS, http://www.upa.pdx.edu/IMS/currentprojects/TAHv3/Content/PDFs/Intolerable_Acts.pdf (last visited Mar. 5, 2017) (The Third Amendment was a response to the Quartering Acts of 1765 and 1774, which were called the "Intolerable Acts" by American revolutionaries.).
[10] U.S. CONST. art. I, § 10.
[11] *See, e.g.,* Robert C. Hockett & Saule T. Omarova, *The Finance Franchise*, 102 CORNELL L. REV. 1143, 1147 (2017) ("At its core, the modern financial system is effectively a public-private partnership ...."); MORGAN RICKS, THE MONEY PROBLEM: RETHINKING FINANCIAL REGULATION (2016); CHRISTINE DESAN, MAKING MONEY: COIN, CURRENCY, AND THE COMING OF CAPITALISM (2014); Katharina Pistor, *A Legal Theory of Finance*, 41 J. COMP. ECON., 315, 315 (2013) ("[F]inancial markets are legally constructed and as such occupy an essentially hybrid place between state and market, public and private.").

submitted an amicus brief to the Second Circuit with respect to *Lacewell v. OCC*, arguing that "[c]reating deposit dollars is a delegated sovereign privilege" and that OCC lacks the authority to charter Silicon Valley firms.[12] In his "money as infrastructure" view, legal scholar Morgan Ricks frames *bank chartering* as procurement.[13] Following the Civil War, only state-chartered or nationally-chartered institutions have been allowed to incur bank deposit liabilities, creating a logical site for regulation. But myriad forces, including the Law and Economics movement, have driven a proverbial "race to the bottom" in terms of charter-based enforcement.[14]

National Bank Charters & Special Purpose National Bank Charters

Like authority over money itself, governments maintain authority over terms of credit. Since the American Revolution, states have set interest rate caps to protect their residents from predatory lending. Courts have long rejected efforts to evade usury laws, looking beyond the technical form of a transaction and toward its substance. However, beginning with a 1978 Supreme Court decision, a combination of federal and state law changes eliminated rate caps for most banks. Still the vast majority of states retain interest rate limits for longer-term loans by *nonbank companies.*[15] Around one in three states also maintain interest limits for shorter loans.[16]

The existing regulatory framework allows nonbank companies to "rent" a bank charter in order to evade state consumer protection laws. The recent "Madden-fix rules" adopted by the Office of the Comptroller of the Currency (OCC) and the Federal Deposit Insurance Corporation (FDIC), as well as the OCC's proposed "true lender rule" -- which I strongly support repealing via the Congressional Review Act -- is strongly exacerbated by this problem.

Some bank and non-bank company partnerships may provide important benefits to individual customers. But others exist primarily as a means for the nonbank company to "rent" a bank charter in order to evade state and federal consumer protection laws.[17] Banks are also subject to the (now weakened) Community Reinvestment Act (CRA) and are able to export interest rates they charge that are allowable under their home state to borrowers in other states, even if those other jurisdictions have stricter usury laws.

---

[12] Brief of Thirty-Three Banking Law Scholars as Amici Curiae in Support of Appellee in *Lacewell v. OCC*, No. 19 Civ. 4271 (2d Cir. July 29, 2020), *available at* https://justmoney.org/lacewell-v-occ/.

[13] *See* generally, Morgan Ricks, *Money As Infrastructure*, 2018 COLUM. BUS. L. REV 757 (2018)

[14] *See* William K. Black, *Neo-Classical Economic Theories, Methodology, and Praxis Optimize Criminogenic Environments and Produce Recurrent, Intensifying Crises*, 44 CREIGHTON L. REV. 597, 628 (2011) (arguing these scholars wrongly assert that competition among the States to charter corporations acts like an 'invisible hand' to align the interests of investors and officers and produce governance rules that are 'optimal for society.)'

[15] For example, 43 states and the District of Columbia cap the rate on a $500, 6-month loan, at a median of about 36%. NAT'L CONSUMER LAW CTR. (NCLC), STATE RATE CAPS FOR $500 AND $2,000 LOANS, (2020), https://www.nclc.org/images/pdf/high_cost_small_loans/payday_loans/FactSheet-StateRateCap.pdf.
In addition, in recent years, votes in many states, including Arizona, Colorado, Montana, and South Dakota have approved rate cap initiatives that eliminate both short-term and longer-term high-cost loans.

[16] CRL, MAP OF U.S. PAYDAY INTEREST RATES (2019), https://www.responsiblelending.org/research-publication/map-us-payday-interest-rates.

[17] *See generally* Letter from Center for Responsible Lending (CRL) et al. to OCC (Sept. 3, 2020), https://www.nclc.org/images/pdf/high_cost_small_loans/payday_loans/OCC-True-Lender-Comments.pdf ("CRL et al. True Lender Comments").

For now, it appears the OCC lacks the authority to extend national bank charters to companies that do not hold deposits and are not banks in any traditional sense of the word.[18] But lending charters would simply be dangerous. Predatory lenders are eager to obtain national bank charters so that they can ignore state usury laws and charge rates that are illegal under most state laws. The OCC is already supporting predatory lenders that partner with national banks to evade state interest rate caps, and doing nothing to restrain the banks' role in predatory practices,[19] and I do not have confidence that a nonbank charter would not be available to predatory lenders. Moreover, the OCC does not intend for SPBNC recipients to be subject to the CRA, which only applies to depository institutions, creating a higher risk they would offer products that harm the communities where they do business rather than serve these communities with responsible products.

Industrial Loan Charters

Wall Street and Silicon Valley should not be permitted to intertwist any further.[20] Historically, commercially-owned banks have made unsound loans to business partners, denied services to competitors, and generally engaged in imprudent activities to spur commercial user purchases.[21] Commercial firms that also engage in financial services tend to use such enterprises to fund other risky business activities, heightening the moral hazard of bailout.[22] The risk of predatory behavior increases. Allowing Big Tech to take advantage of federal deposit insurance and other attendant protections (without concomitant responsibilities) threatens responsible practices within the tech sector overall. Just as distressingly, allowing Big Tech to engage in shadow banking activity jeopardizes financial stability.[23] These combinations should not be allowed. As a general matter, any companies acting as banks — regardless of the financial or nonfinancial nature of their parent companies — should be regulated as banks, under consolidated supervision. Companies acting as BHCs should be regulated as BHCs. It is time to permanently end the ILC exemption: I thus support the "Close the ILC Loophole" Act (C. Garcia), which would eliminate an exemption to the Bank Holding Company Act that permits ILCs and their corporate owners.

I am especially concerned by the encroachment of dominant platforms into the payments space. Big Tech companies use their "platform privilege" not only to analyze users, but to acquire and appropriate from competitors that rely on the infrastructure they supply. In late June

---

[18] Letter from NCLC to OCC 9 (Aug. 3, 2020), https://www.nclc.org/images/pdf/rulemaking/2020-OCC-fintech-NCLC-comments.pdf.
[19] *Id.* at 52-57.
[20] *See* Comment from Arthur E. Wilmarth, Jr., Prof. of Law, Geo. Wash. Univ. L. Sch., to FDIC (Apr. 10, 2020), https://www.fdic.gov/regulations/laws/federal/2020/2020-parent-companies-of-industrial-banks-3064-af31-c-002.pdf.
[21] Arthur E. Wilmarth, Jr., *Wal-Mart and the Separation of Banking and Commerce*, 39 CONN L. REV. 1539, 1598-1606 (2007).
[22] *Id.* at 1569.
[23] For relevant background, see, e.g., L. Randall Wray, *Global Financial Crisis: Causes, Bail-Out, Future Draft*, 80 UMKC L. REV. 1101, 1107 (2012) (describing how the shift of economic power to shadow banks triggered the operation of "Gresham's Law", whereby safer and stabler financial firms were driven out of business).

2020, the AFR Ed Fund and Demand Progress Ed Fund released the "Libra Black Paper", arguing policymakers should prevent Facebook and the Geneva-based Libra Association — a cartel of junior Silicon Valley partners — from moving forward with their global corporate currency project.[24] I encourage this subcommittee to read that report. Although the Facebook-driven Project has rebranded itself as "Diem", my fundamental concerns, especially with respect to surveillance remain. To put it bluntly, Facebook stands to leverage its platform power to expand its digital advertising monopoly, take over adjacent markets, self-deal, and establish a global surveillance system. The Diem Association would constantly, affirmatively monitor the Diem network for suspicious activity. There would be no real privacy.

Federal Payments Charters

Digital wallets systems that store cryptocurrency (like most mobile money platforms, including PayPal and Venmo) do not simply transfer funds, but store balances unprotected by federal deposit insurance, or any equivalent mechanism.[25] By avoiding custody agreements with FDIC-insured institutions, mobile payment companies avoid most banking regulation, constituting "shadow payment platforms."[26] In the event of disaster, the last line of defense is general corporate bankruptcy law.[27] Money Services Business (MSB) designation provides a shallow consumer protection arrangement, primarily in the form of mandated disclosure.[28] Fifty different state MSB regulators also apply a mix of minimum net worth requirements, surety bond, and other security and investment requirements.[29] These laws have proven ineffective in keeping MSBs afloat.[30] Some cryptocurrency advocates have framed the product as means of improving remittances, especially for low-income and excluded populations.[31] Critiques of cryptocurrency have largely responded in kind, by focusing on their implications for money laundering concerns. When one steps back and considers the state of money, currency, and the financial system in the U.S., however, cryptocurrency looks less like a significant departure from

[24] RAÚL CARRILLO, BANKING ON SURVEILLANCE: THE LIBRA BLACK PAPER, AFR EDUCATION FUND & DPEF (2020), https://ourfinancialsecurity.org/wp-content/uploads/2020/06/Libra-Black-Paper-FINAL-2.pdf.

[25] *See, e.g,* Sarah Jane Hughes & Stephen T. Middlebrook, *Advancing A Framework for Regulating Cryptocurrency Payments Intermediaries*, 32 YALE J. ON REG., 495, 527 (2015)

[26] *See* Dan Awrey & Kristin van Zwieten, *Mapping The Shadow Payment System* 41-44 (SWIFT Institute Working Paper No. 2019-00, 2019), *available at*: https://ssrn.com/abstract=3462351 (discussing comparative approaches in the U.S., UK, EU, and China).

[27] *See* Dan Awrey, *Bad Money,* 106 CORNELL L. REV. 1, 23 (forthcoming 2020), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3532681 (discussing how the corporate bankruptcy regime fails depositors). *See also* Ryan Surujnath, *Off the Chain! A Guide to Blockchain Derivatives Markets and the Implications on Systemic Risk*, 22 FORDHAM J. CORP. & FIN. L. 257, 301 (2017) (discussing how this dynamic can be especially dangerous when distributed ledger technology (DLT) is involved, as a lack of clear transaction finality may make it difficult to determine liability in the context of corporate insolvency).

[28] 12 C.F.R. § 1005.3. *See also* Dan Awrey, *Bad Money,* 106 CORNELL L. REV. 1, 34 (forthcoming 2020), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3532681.

[29] *See* Awrey, *supra* note 28, at 34-41 (surveying the various requirements).

[30] *Id.* at 39-41.

[31] *See*, *e.g.*, Testimony of Mark Zuckerberg Before the Committee on Financial Services, United States House of Representatives Oct. 23, 2019.

recent trends, and more like the culmination of a move away from strict state controls over money and currency, toward additional forms of "private money" that are dangerous for users.

Some analysts have argued that mobile payments platforms should be subject to full-scale banking regulation.[32] Yet regulators lack the authority to simply designate a nonbank company, as a bank. In fact, federal laws contain several different and potentially conflicting definitions of a "bank",[33] limiting regulators ability to constrain banking activities to institutions with banking charters.[34]

Despite widespread acknowledgement that definitional problems allow nonbanks to engage in arbitrage,[35] the issues remain unresolved. Banking regulators could attempt to promulgate rules clarifying the definitions of "bank" and "deposit", but courts have generally been unwilling to expand the scope of such statutory terms.[36]

Congress must prevent the rise of a surveillance-driven shadow banking sector.[37] Congress should designate the deposit-like obligations of dominant tech platforms as "deposits", prohibiting the platforms from issuing such obligations absent review and approval by banking regulators. We need a forward-looking bill that seeks to integrate emerging digital financial technologies into traditional banking services in a way that strengthens regulatory supervision, clarifies the legal status and classification of digital financial assets, but above all, promotes safety of consumer funds. We should recognize as a deposit any digital financial asset that promises a fixed nominal value, on demand, denominated in or pegged to the U.S. dollar, and regulates the relevant institutions as depository institutions. I believe the STABLE Act recently proposed by Rep. Rashida Tlaib (D-MI) achieves these goals.[38]

---

[32] *See, e.g.*, Paul Kupiec, *Why Libra Must Be Treated Like Traditional Banks and Currency*, THE HILL *(*Nov. 4, 2019), https://thehill.com/opinion/finance/468924-why-libra-must-be-treated-like-traditional-banks-and-currency.

[33] For discussions of these definitions, see Saule T. Omarova & Margaret E. Tahyar, *That Which We Call A Bank: Revisiting the History of Bank Holding Company Regulation in the United States*, 31 REV. BANKING & FIN. L 113, 115 (2011).

[34] For extensive discussion, see Ricks, *supra* note 13, at 811-821 (2018). (For instance, the Banking Act of 1933 classifies "banks" as institutions that take deposits and are examined and regulated by state or federal banking authorities. Section 21 makes it illegal for an entity to accept deposits without being regulated by a banking regulator. The provision has been interpreted as an "axiomatic" statement preventing firms other than banks from issuing deposit liabilities. Prof. Wilmarth has argued that it is a criminal offense for nonbanks to hold deposits. Unfortunately, the Banking Act of 1933 does not define "deposit", meaning regulators cannot easily invoke Section 21 to prevent nonbanks from engaging in general banking activities. Even if regulators or courts were to attempt to borrow the definition of "deposit" from another statute, there would be "no practical way forward." For instance, because the Federal Deposit Insurance Act defines a "deposit" as "money or its equivalent received or held by a *bank*..." (emphasis added), this creates a "perfect legal circle.")

[35] *See, e.g.*, U.S. TREAS., FINANCIAL REGULATORY REFORM: A NEW FOUNDATION (Oct. 8, 2009), https://www.treasury.gov/initiatives/Documents/FinalReport_web.pdf.

[36] For instance, the Supreme Court struck down a Board regulation intended to expand the BHCA definition of "bank" to cover "nonbank banks." *See* Board of Governors v. Dimension Financial Corp, 474 U.S. 361, 374 (1986).

[37] *See* Kristin N. Johnson et al., *(Im)perfect Regulation: Virtual Currency and Other Digital Assets As Collateral*, 21 SMU SCI. & TECH. L. REV. 115, 142 (2018) (arguing that expanding the existing definition of "deposit accounts" to include virtual wallets and platforms would presumably subject them to a host of intermediary regulations imposed on more traditional depository institutions).

[38] https://tlaib.house.gov/media/press-releases/tlaib-garcia-and-lynch-stableact

Policymakers may create a narrower space for firms that do not seek to engage in broader depository activities beyond accepting funds and making payments, but all companies must be subject to regulation that matches the risks posed to consumers and the broader public. We do not expect the OCC's Payments Charter to meet this goal.[39] As it stands the OCC lacks the authority to issue its Payments Charter.[40] But as a policy matter, the decision of whether and how to grant a national payments charter should be left to Congress. A payments charter raises important issues with respect to consumer and fair lending protections, the separation of banking and commerce, and supervision of holding companies.

Advocates and scholars across the political spectrum have argued our existing charter system is broken.[41] The public deserves comprehensive, federal regulation of firms that engage in fiscal agent services, money transmitter services, and/or "pass-through" services, but are clearly not engaged in providing depository or security-based services. That being said, it is not clear the OCC is the proper institution to take charge here and the regulation flowing from a charter deserves significant and substantial attention. In particular, federal payments charters must provide a basis for the more comprehensive regulation of minimum balances or maximum balances, quantitative and qualitative regulation of fees, and privacy, security, and data management policies. Like depository institutions, payments institutions should also be subject to regulations ensure that the services provided by such institutions are universal and comprehensively include historically excluded and marginalized groups. We must generally avoid the problems already identified within the existing dual banking system. Of special importance, we should not allow the regulations that flow from federal chartering to supersede or supplant any other stronger regulations or standards promulgated by other Federal or applicable State regulatory entities, including any such regulation issued by the FDIC or CFPB.

The most fundamentally important thing we can do to protect consumers in this space is strengthen direct credit regulation. Strengthen consumer protections, including by instituting a federal usury rate cap. Interest rate limits are the simplest and most effective protection against predatory lending.[42] In May 2019, Senator Bernie Sanders and Representative Alexandria Ocasio-Cortez unveiled the Loan Shark Prevention Act, a bill that would cap the cost of consumer credit nationwide.[43] Under the bill, the total cost of a loan, calculated as an annualized percentage rate (APR), could not exceed 15%. There is also an effort to extend the 36% APR interest rate cap on payday and car-title lenders in the Military Lending Act (MLA) to cover all Americans.[44]

---

[39] See ABA, "Podcast: OCC's Brooks Plans to Unveil 'Payments Charter 1.0' This Fall," June 25, 2020.
[40] Comment from NCLC to OCC 5 (Aug. 20, 2020), https://www.nclc.org/images/pdf/rulemaking/2020-OCC-fintech-NCLC-comments.pdf.
[41] *See* Dan Awrey, Unbundling Banking, Money, and Payments (January 31, 2021). European Corporate Governance Institute - Law Working Paper No. 565/2021, Available at SSRN: https://ssrn.com/abstract=3776739 or http://dx.doi.org/10.2139/ssrn.3776739.
[42] NCLC, MISALIGNED INCENTIVES: WHY HIGH-RATE INSTALLMENT LENDERS WANT BORROWERS WHO WILL DEFAULT, (2016), https://www.nclc.org/images/pdf/high_cost_small_loans/payday_loans/report-misaligned-incentives.pdf.
[43] https://www.govtrack.us/congress/bills/116/s1389/text/is
[44] *See, e.g,* Letter from CRL, Ams. for Fin. Reform, et al. to Leaders McConnell and Schumer, Speaker Pelosi and Leader McCarthy (July 1, 2020),

Civil Rights, Civil Liberties, & "Financial Inclusion"

Background: Data Governance

Many claims are made about the promise of Big Data to increase financial inclusion, but those claims fail to reckon with, much less solve, the systemic reasons people are left out or more accurately deliberately excluded. Too often, promises of technological empowerment yield "predatory inclusion" — a process whereby financial institutions offer needed services to specific classes of users, but on exploitative terms that limit or eliminate their long-term benefits.[45]

"Access to credit" talk pervades the current discourse of financial rights and equality for low-income communities. However, legal scholar Abbye Atkinson has argued, in concert with community advocates, the notion that credit is a valid form of social provision for low-income Americans, however, is deeply flawed.[46] At its best, credit is a mechanism of intertemporal and intrapersonal redistribution. The problem of entrenched and enduring poverty that leaves people consistently unable to afford basic necessities cannot be addressed by a device that requires future prosperity and economic growth. Indeed, the mechanism is fundamentally extractive. Too often, discussions about financial access disparities focus on the choices and behaviors of individuals, or on the need to design "alternative products," rather than on structural barriers that block poor people, immigrants, and people of color from mainstream financial institutions and systems. Atkinson highlights that this sort of rhetoric is popular in both political parties.[47]

Mass financial surveillance adds another dimension to financial inclusion, eventually creating a detailed picture of our most private social, familial, romantic, religious, and political activities. Data about a single transaction can be linked to purchase history, creating a "picture of the person behind the payment."[48] A massive data broker industry connects data regarding our finances to data about our employment, marital status, homeownership status, medical conditions, and even our interests and hobbies. Powerful institutions can make predictions with tremendous precision, in real-time, and at scale. The exponential growth in computer processing

---

https://ourfinancialsecurity.org/wp-content/uploads/2020/03/CRL-Group-Letter-on-Financial-Services-Stimulus-Recommendations.pdf (All new loans made during the crisis should comply with consumer safeguards in the Military Lending Act, including a cap of 36% APR.)

[45] Louise Seamster & Raphaël Charron-Chénier, *Predatory Inclusion and Education Debt: Rethinking the Racial Wealth Gap*, 4 SOC. CURRENTS 199, 199-200 (2017) (describing the targeting of mortgagors and students who borrow to purchase homes or education as "predatory inclusion."). Keeanga Yahmatta-Taylor uses "predatory inclusion" in the housing context - "[T]he turn to inclusion was only allowable by maintaining other forms of exclusion. Credit inclusion became possible by holding the line on neighbor exclusion. KEEANGA YAHMATTA-TAYLOR, RACE FOR PROFIT: HOW BANKS AND THE REAL ESTATE INDUSTRY UNDERMINED BLACK HOMEOWNERSHIP 254 (2019). *See also* Kristin Johnson et al., *Artificial Intelligence, Machine Learning, and Bias in Finance: Toward Responsible Innovation*, 88 FORDHAM L. REV. 499, 505, 517–21 (2019) (arguing fintech firms may "hardwire predatory inclusion" into financial markets for the "next several generations").

[46] Abbye Atkinson, *Rethinking Credit As Social Provision*, 71 Stan. L. Rev. 1093, 1093–94 (2019).

[47] *Id.* at 1093.

[48] Albert Fox Cahn & Melissa Giddings, *In the Age of COVID-19, the Credit Card Knows All*, SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT - URBAN JUSTICE CENTER (May 18, 2010), https://www.stopspying.org/latest-news/2020/5/18/in-the-age-of-covid-19-the-credit-card-knows-all.

power has rapidly changed how much information can be generated, and how much can be stored and analyzed at minimal cost to the surveiller. From the perspective of a human mind, there is too much data to process, the sets are too heterogeneous to make sense of, and the speed of analysis necessary to process them surpasses our abilities.[49] Predictive analytics takes surface data and infers latent data from it. A mostly unregulated data broker industry then connects to even more stocks of data regarding employment, marital status, homeownership status, medical conditions, and even our interests and hobbies, especially as articulated via social media.

For purposes of preventing payments data collection in the first place, FCRA remains the most relevant statute. FCRA was drafted before concentrated computerized data sharing became the standard industry business model.[50] FCRA restricted data procurement to "a legitimate business need." This was an easy provision to satisfy; the bureaus have easily argued that direct mail and targeted advertising programs constitute legitimate business needs. FCRA includes recursive definitions of "consumer reporting agency" and "consumer report" - consumer reports are communications of credit-related information by consumer reporting agencies. Today, the largest consumer reporting firms are not considered to be bound by FCRA at all. If FCRA is to make any sense by its own legislative logic, it should be expanded to encompass "alternative reporting systems."[51]

While the CFPB and FTC do have some additional tools at their disposal,[52] no overarching federal privacy law currently curbs the collection, use, and sale of personal data among corporations.[53] Experts argue the U.S. data protection and federal privacy framework is fundamentally broken, and will face imminent revision.[54] Ultimately, Congress should take action to minimize data collection to that which is narrowly tailored to permitted usages, so that many of the aforementioned anti-competitive practices become commercially unfruitful. Legislation should also shift the burden of privacy protection away from consumers, who have minimal resources to protect themselves, and toward the companies, which profit immensely from the aggregation of our data.

Millions of people are subject to data collection to which they may not have consented. This is especially true in the payments space, where counterparties between networked payment

[49] *See, e.g.,* Amy Kapczynski, *The Law of Informational Capitalism*, 129 YALE L.J. 1460, 1468 (2020).
[50] Dennis D. Hirsch, From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics, 79 Md. L. Rev. 439, 442–43 (2020)
[51] As stressed in a recent bill by Sen. Sherrod Brown. See DATA Act of 2020. https://www.washingtonpost.com/technology/2020/06/18/data-privacy-law-sherrod-brown/. There are strong arguments for total abolition of predictive analytics in finance and a return to localized, qualitative, or informal lending practices. But there is also a real concern as to what takes the place of credit scoring. Stratification economist Darrick Hamilton argues for building a bare-bones public system, as one level of legibility is necessary for vulnerable people to gain access to the formal economy. https://www.demos.org/policy-briefs/establish-public-credit-registry
[52] For extensive treatment of FTC power, see Sandeep Vaheesan, *Resurrecting "A Comprehensive Charter of Economic Liberty": The Latent Power of the Federal Trade Commission*, 19 U. PA. J. BUS. 645, 650-698 (2017)
[53] BERKELEY MEDIA STUDIES GROUP ET AL., THE TIME IS NOW: A FRAMEWORK FOR COMPREHENSIVE PRIVACY PROTECTION AND DIGITAL RIGHTS IN THE UNITED STATES, Citizen.org, (last visited Mar. 31, 2020), https://www.citizen.org/sites/default/files/privacy-and-digital-rights-for-all-framework.pdf.
[54] *See, e.g.*, Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1, 1687, 1687-88 (2020).

"stacks" are constantly exposed to each other. But the oppression that flows most directly from the collection disproportionately harms a certain sub-population. In general, more socially advantaged groups may engage in voluntary data collection that benefits them yet risks greater harm for socially disadvantaged groups.[55]

The *commercial* sharing and selling of predictions about human behaviors is only one dimension of payments technology and surveillance. We tend to obscure how the government itself is a financial data collector.[56] According to Virginia Eubanks, social welfare agencies turned to cost-cutting technologies in periods of austerity.[57] The "digital poorhouse" was erected to stand between recipients of public assistance and their rights. Payments technology is a significant part of this story, as account-based Electronic Benefits Transfer (EBT) cards have granted agencies unparalleled and unprecedented supervision over the finances of people receiving SNAP, Housing Assistance, Supplemental Security Income, Medicaid, and more. Increased surveillance compounds the violence inherent to more traditional forms of finance. As legal scholar Angela Harris argues, a spectrum of "slow violence"—the "sprawling system of surveillance, punitive discipline, and control that makes the lives of poor people profoundly unfree" dominates the "mundane world" of misdemeanor convictions, accompanies a similarly humdrum world of "payday loans, credit cards with ruinously high interest rates, for-profit colleges, and of course subprime mortgages."[58]

Reconstructing AML, CFT, and Sanctions Law

The first serious anti-money laundering statute enacted by the federal government was the Bank Secrecy Act in 1970. The BSA requires banks and other "financial institutions" to keep certain records and authorizes the Secretary of the Treasury to require such institutions and persons participating in transactions for such institutions to report financial transactions to the Secretary.[59] The Money Laundering Control Act of 1986[60] established money laundering as a crime, making the United States one of the first countries in the world to criminalize what was hitherto considered an omnipresent crime.

In 1988 Congress passed the Money Laundering Prosecution Improvements Act,[61] extending BSA regulations to every kind of financial institution. In 1992, Congress passed the

---

[55] *See generally,* Salome Viljoen, *Democratic Data: A Relational Theory For Data Governance* (November 11, 2020). Yale Law Journal, Forthcoming, Available at SSRN: https://ssrn.com/abstract=3727562 or http://dx.doi.org/10.2139/ssrn.3727562

[56] Marion Fourcade, Jeff Gordon (2020). Learning Like a State: Statecraft in the Digital Age. *Journal of Law and Political Economy*, 1(1). Retrieved from https://escholarship.org/uc/item/3k16c24g

[57] Virginia Eubanks, Automating Inequality 32-34 (2017).

[58] Angela Harris, *Criminal Justice and Slow Violence in Keilee Fant v. City of Ferguson, Missouri*, LAW & POL. ECON. (May 2, 2018), https://lpeproject.org/blog/criminal-justice-and-slow-violence-in-keilee-fant-v-city-of-ferguson-missouri/.

[59] 12 U.S.C. § 1829b(a)(1); 31 U.S.C. § 5311.

[60] Money Laundering Control Act of 1986, Pub. L. No. 99-570, 100 Stat. 3207-18 (1986) (codified as amended in scattered sections of 18 and 31 U.S.C.).

[61] Money Laundering Prosecution Improvements Act of 1988, Pub. L. No. 100-690, 102 Stat. 4354 (1988) (codified in various sections of 18 and 31 U.S.C.).

Annunzio-Wylie Anti-Money Laundering Act, which required the filing of "Suspicious Activity Reports" (SARs) that were relevant to *any possible violation of law or regulation.* The consequence of the increased reporting schemes was the generation of large numbers of extraneous reports. The flood of useless information. was hardly surprising given the incentives to over-report that are built into the law. The BSA imposes strict liability for failure to file appropriate reports, but the Annunzio-Wylie Act contains a provision holding reporting entities free from liability in connection with the filing of SARs, meaning it is better to file too many reports than not enough.[62]

All financial institutions must comply with Title III of the USA PATRIOT Act, which requires they implement robust customer identification programs, commonly labeled "know your customer" (KYC) provisions.[63] Financial institutions must generally assist police investigations requiring financial information and provide specific information to law enforcement agencies, including by filing SARs. SARs that are not deemed by the FBI to have a potential nexus to terrorism are distributed for follow-up investigation by other agencies at the state, local, and federal level, as well as fusion centers, which serve as data intermediators, or platforms, for other law enforcement agencies.[64] Mass surveillance and profiling through SARs and assessments, combined with enhanced inter-agency information-sharing through "fusion centers": data aggregators authorized by Congress to "co-locate" federal, state, and local officials together to work collaboratively, along with private contractors, on the collection and analysis of intelligence concerning a broad array of potential security threats.[65] Once a SAR is filed with FinCEN, Palantir -- a company founded by Peter Thiel, also a co-founder of PayPal -- aggregates the information which is then entered with the FBI's NSAC databases and may be forwarded to any other governmental agency that requests it.[66]

One might suppose that private banking records would be afforded some protection under the Fourth Amendment's prohibition against unreasonable searches and seizures by the state, at the very least, but the Court decided that not was not the case in *U.S. v. Miller*.[67] In *United States*

---

[62] Eric J. Gouvin, Bringing Out the Big Guns: The Usa Patriot Act, Money Laundering, and the War on Terrorism, 55 Baylor L. Rev. 955, 967–68 (2003)

[63] *See*, *e.g.,* Letter from Rep. Tlaib et al., to the Treas. Sec. Steve Mnuchin, et al., (July 17, 2019), https://tlaib.house.gov/sites/tlaib.house.gov/files/Final_BWM_Regulators.pdf (arguing many Muslim and Arab Americans have been automatically labeled "high-risk" and are therefore unable to maintain access to financial services). For a history of the relevant PATRIOT Act amendments, see, e.g., Maria A. de Dios, *The Sixth Pillar of Anti-Money Laundering Compliance: Balancing Effective Enforcement with Financial Privacy*, 10 BROOK J. CORP. FIN & COM. L. 495 (2016).

[64] U.S. GOV'T ACCOUNTABILITY OFF., ADDITIONAL ACTIONS COULD HELP ENSURE THAT EFFORTS TO SHARE TERRORISM-RELATED SUSPICIOUS ACTIVITY REPORTS ARE EFFECTIVE (2013), https://www.gao.gov/assets/660/652995.pdf [https://perma.cc/JPC5-4C5H]. (explaining how different state and local law enforcement agencies follow-up on non-terrorism SARs).

[65] Anil Kalhan, *Immigration Surveillance*, 74 Md. L. Rev. 1, 40 (2014).

[66] Cheryl R. Lee, *Constitutional Cash: Are Banks Guilty of Racial Profiling in Implementing the United States PATRIOT Act?*, 11 MICH. J. RACE & L. 557, 564 (2006) (arguing the Patriot Act 'puts banks in the business of practicing selective enforcement and racial profiling with every transaction, every hour of every business day").

[67] Appalled legislators would pass the Right to Financial Privacy Act of 1978, which bars government agencies from obtaining customer records maintained by financial institutions unless: 1) the customer authorizes the disclosure, 2) the government authority obtains an administrative subpoena, an administrative summons, a search warrant, or a judicial subpoena, or 3) the government authority makes a formal written request to the financial institution.# To this

v. Miller[68] and again in *Smith v. Maryland*,[69] the Court decided that government access to third-party business records is not a search for purposes of the Fourth Amendment. The Fourth Amendment protects only reasonable expectations of privacy, but the Supreme Court claimed one cannot have an expectation of privacy in anything shared with another person. Thus, the government could collect bank records (in *Miller*) or telephone metadata (in *Smith*) without a warrant, without probable cause, and without implicating the Fourth Amendment at all.[70]

The third-party doctrine is quite literally the product of another era -- before ubiquitous networked computing, digital data, electronic communications, mobile technologies, and the commodification of information. In the 1970s, Wall Street and Silicon Valley weren't merging to create totalistic and predictive dossiers for everyone in the world. The payments industry business model *only works through networks of third parties*. And then payments data now have different lives in the law enforcement sphere. As a general matter of course, "surveillance-as-a-service" companies sell data, including financial data, to local police departments.[71]

Given these obligations, and the racial injustices perpetrated by law enforcement, we are especially concerned by suggestions that banks — on their own initiative or in partnership with tech companies — should collect more geolocation or biometric data.[72] Geolocation data

---

day, the law ostensibly threatens banks with the possibility of high statutory damages if they illegally disclose customer information to the government, but all that is required for circumvention is a written request.# There is alo a general carveout for certain law enforcement, rendering the law more of a procedural rather than substantive barrier to violations of civil liberties. The full list of exemptions is as follows: These exceptions are (1) disclosures that do not identify a particular customer; (2) disclosures that benefit the financial institution, including its security interests, government loans, and other disclosures relevant to possible violations of the law; (3) disclosures in connection with supervisory investigations and proceedings; (4) disclosures under the tax privacy provisions; (5) disclosures pursuant to other federal statutes or rules, administrative or judicial proceedings, and legitimate functions of supervisory agencies; and (6) emergency disclosures and disclosure to federal agencies charged with foreign intelligence or counter intelligence or other national security protective functions.# Law enforcement officials can avoid giving the financial institution's customer notice and an opportunity to contest only by proving that: (1) "the records being sought are relevant to a legitimate law enforcement inquiry," and (2) notification will result in one of five specified harms. See Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3402, 3403(a), (b) (1994).

[68] 425 U.S. 435, 442-43 (1976) (holding persons have no expectation of privacy in information conveyed to a bank). (the police connected the defendant to a bootlegging conspiracy by subpoenaing his bank for checks written from his business account)

[69] 442 U.S. 735, 744 (1979).

[70] As Justice Brennan observed in his dissent in *Miller*, "[f]for all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional. It is impossible to participate in the economic life of contemporary society without maintaining a bank account." Justice Marshall voiced a similar objection in *Smith* , where he asserted that "privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."

[71] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 37 (2019).

[72] *See, e.g,* Letter from Demand Progress et al. to Leaders McConnell and Schumer, Speaker Pelosi and Leader McCarthy (July 1, 2020), https://s3.amazonaws.com/demandprogress/letters/2020-07-01_Facial_Recognition_Moratorium_and_Divestment_Letter_FINAL.pdf; Alfred Ng, *Facial recognition has always troubled people of color. Everyone should listen*, CNET (June 12, 2020), https://www.cnet.com/news/facial-recognition-has-always-troubled-people-of-color-everyone-should-listen/.

revealed by payment histories is uniquely difficult to anonymize.[73] Privacy and racial justice advocates vehemently oppose the use of biometric tools like facial recognition technology, iris-scanning, and palm prints.[74] Facial recognition software is likely to mislabel or misrecognize members of racial minority groups, especially Black Americans.[75] Overall, the general use of this kind of sensitive data not only increases the risk of predation by banks and civil liberties violations by governments, but security breaches by competitors and hackers.[76]

There is a further need to discuss whether AML, CFT, and sanctions law should continue to exist in their current form. SARs rarely lead to investigations of specific criminal activities, but rather feed the broader surveillance machinery.[77] Because many transactions are unnecessarily flagged, true money-laundering often continues without notice, perpetrated by multinational financial institutions, most notoriously HSBC.[78] Between 2010 and 2020, eighteen different financial institutions have received Deferred Prosecution Agreements, and at least four of them broke the same law again, and simply received another fine. This is not the sort of consequence experienced by real persons suspected of money laundering.

BuzzFeed News and the International Consortium of Investigative Journalists recently released thousands of leaked government documents known as the "FinCEN files."[79] These files contain over 2,100 SARs. Although the FinCEN files revealed only about 0.02% of the SARs that likely filed between 2011 and 2017, these records alone identify over $2 trillion in potential global money laundering. By its own logic, the SARS system is an utter failure. The secrecy of SARs, and the threat of imprisonment for revealing them through whistleblowing activity --

---

[73] *See, e.g.,* Cahn & Giddings, *supra* note 48.

[74] *See, e.g.*, *A Biometric Backlash Is Underway — And A Backlash To The Backlash*, PYMNTS (May 17, 2019), https://www.pymnts.com/authentication/2019/biometric-backlash-privacy-law/; *Mandatory National IDs and Biometric Databases*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/national-ids (last visited Apr. 25, 2020).

[75] *See, e.g.,* Victoria Burton-Harris & Philip Mayor, *Wrongfully Arrested Because Face Recognition Can't Tell Black People Apart*, ACLU (June 24, 2020), https://www.aclu.org/news/privacy-technology/wrongfully-arrestedbecause.

[76] *See, e.g.*, Jason Leopold & Jessica Garrison, *US Intelligence Unit Accused Of Illegally Spying On Americans' Financial Records*, BUZZFEED (Oct. 6, 2017), https://www.buzzfeednews.com/article/jasonleopold/Us-Intelligence-unit-accused-of-illegally-spying-on (reporting that FinCEN employees have accused colleagues at the Office of Intelligence and Analysis of illegally collecting and storing private financial records); Aaron Mackey & Andrew Corker, *Secret Court Rules That the FBI's "Backdoor Searches" of Americans Violated the Fourth Amendment*, ELECTRONIC FRONTIER FOUND. (Oct. 11, 2019), https://www.eff.org/deeplinks/2019/10/secret-court-rules-fbis-backdoor-searches-americans-violated-fourth-amendment; Chen Han & Rituja Dongre, *Q&A. What Motivates Cyber-Attackers?*, TECH. INNOV. MGMT. REV. 40, 40-41 (2014), https://timreview.ca/article/838 (describing economic motivations for hacking).

[77] *See, e.g.*, Mariano-Florentino Cuéllar, *The Tenuous Relationship Between the Fight Against Money Laundering and the Disruption of Criminal Finance*, 93 J. Crim. L. & Criminology 311, 364 n.211 (2003) ("Given the information available to banks, it is striking how few investigations are instigated ....")

[78] *See, e.g.*, Press Release, Dep't of Just., HSBC Holdings Plc. And HSBC Bank USA N.A. Admit to Anti-Money Laundering and Sanctions Violations, Forfeit $1.256 Billion in Deferred Prosecution Agreement (Dec. 11, 2012), https://www.justice.gov/opa/pr/hsbc-holdings-plc-and-hsbc-bank-usa-na-admit-anti-money-laundering-and-sanctions-violations.

[79] *See* Jason Leopold, Anthony Cormier, John Templon, Tom Warren, Jeremy Singer-Vine, Scott Pham, Richard Holmes, Azeen Ghorayshi, Michael Sallah, Tanya Kozyreva & Emma Loop, *The FinCEN Files*, BuzzFeed News (Sept. 20, 2020, 1:01 PM),
https://www.buzzfeednews.com/article/jasonleopold/fincen-files-financial-scandal-criminal-networks

undermines the public's ability to scrutinize the government's regulation of money laundering and undermines trust in the payments system as whole.

A recent rulemaking by FinCEN and the Board stands to make a bad situation worse. In a recent comment letter submitted on behalf of the Yale Privacy Lab and Fight for the Future, privacy lawyers Misha Guttentag and JP Schnapper-Casteras highlighted the proposed rule failed to even mention "privacy."[80]

Peace in the "War on Cash"

While we may use both cash and digital bank or tech company money to achieve the same thing – buying something in a shop – they come with different technical and social features. At the level of legal and technical design, cash requires no third party to stand between transactors. It does not affirmatively report back to a centralized system. Ledger activity, on the other hand, is increasingly accompanied by a scoring system: a closed box of algorithms which assesses our 'digital character' -- "a digital profile assessed to make inferences regarding character in terms of credibility, reliability, industriousness,responsibility, morality, and relationship choices."[81] Cash does not interact with this "sensing net" in the same way.

Cash is the most common form of payment for purchases and bill-paying, and its use is not limited to underbanked or unbanked consumers.[82] In fact, studies show high cash users also employ many other forms of payment, including credit cards, debit cards, mobile wallets, and online checkout services. It also showed that consumers make the choice to use cash for a variety of reasons: privacy, security, reliability, availability, and even its universal and egalitarian nature. Cash users are not Luddites who shun fintech; they're all kinds of people who pay with cash for a variety of legitimate and understandable reasons.

Cities, states, and storefronts that have moved toward cashlessness and coinlessness have necessarily segregated the payment system, even if that is not the intention. Unbanked consumers have little access to noncash forms of payment.[83] Without a bank account, they are unable to obtain credit or debit cards or to use other non-cash payment methods, with the possible exception of prepaid cards. Moreover, they fundamentally ask consumers to share data with third-party corporations and the government in order to gain financial inclusion. By contrast, some cities and states have enacted laws or ordinances that bar brick-and-mortar retail

---

[80] Comment from Yale Privacy Lab and Fight to the Future to FinCEN 5 (Dec. 22, 2020), https://www.federalreserve.gov/SECRS/2020/December/20201222/R-1726/R-1726_112720_137391_507288521968_1.pdf.

[81] *See* Tamara K. Nopper, *Digital Character in the "Scored Society": FICO, Social Networks, and the Competing Measurements of Creditworthiness, in* CAPTIVATING TECHNOLOGY: RACE, CARCERAL TECHNOSCIENCE, AND LIBERATORY IMAGINATION IN EVERYDAY LIFE 170, 170-188 (Ruha Benjamin ed., 2019), (coining and analyzing the concept of "digital character"). *See also* Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 13 (2014).

[82] Cardtronics and Javelin Strategy & Research, 2020 Health of Cash Study (Feb, 2020), *available at* https://landing.cardtronics.com/hubfs/Cardtronics/Docs/Health_Of_Cash_Study_2019.pdf.

[83] Letter from Consumer Action, the Consumer Fed. of America, Ams. for Fin. Reform, Demand Progress, et al. to U.S. Sens. Kevin Cramer, Sen. Bob Menendez, and Rep. Donald M. Payne, Jr., https://www.consumer-action.org/press/articles/consumers-should-have-the-right-to-pay-retailers-with-cash.

stores from refusing to accept cash. Rep. Ritchie Torres (D-NY) has been at the forefront of this effort in New York City. Led by Rep. Donald Payne, a coalition in New Jersey advanced the first state-level bill in nearly fifty years to ban cashless retailers, which was signed into law by the governor in March 2019. Conglomerates such as Amazon are pushing back, worried that the bill circumvents their heavy investment in their cashless brick-and-mortar bookstores and future grocery stores. Aware of both states' and cities' responses towards the anti-cash movement, Congress joined the effort and introduced two cash discrimination bills in 2019, including one authored by Payne.[84]

Building a Public Option for Financial Services

Background

The fintech industry's "endless capacity for self-referential growth"[85] suggests prudence. In fact, it can only be disciplined by policymakers' own forward thinking about services people actually need in an informational economy.[86] Policymakers must avoid being swayed by general promises of innovation and create systems specifically designed for real accountability on behalf of the public. Congress is the proper body for this discussion.

One response to some of the privacy issues discussed throughout this testimony is cryptocurrency. The idea of an anonymous (or pseudonymous) and cryptographic currency developed over the course of the 1990s.[87] Since this initial phase, distributed ledger technology (DLT) including "blockchain", has helped create over 700 cryptocurrencies, most famously Bitcoin.[88] Cryptocurrencies are ostensibly token-based monies, but operate using ledgers wherein transactions are validated via encryption. DLT allows all users to record transactions and third parties to verify them. The ledger thus replaces bank ledger systems, ostensibly ensuring everyone really has the financial wherewithal that they claim and are not seeking to complete transactions with resources that they do not actually possess.

Proponents of cryptocurrencies at once stress their transparency and privacy, as distributed ledgers are essentially held in common rather than "owned" by an intermediary. Advocates of blockchain are inclined to suggest that blockchain is *necessarily* decentralized or

---

[84] *See also* Meera Jagannathan, "World Health Organization: We did NOT say that cash was transmitting the coronavirus," MarketWatch (March 9, 2020), *available at* https://www.marketatch.com/story/who-we-did-not-say-that-cash-was-transmitting-coronavirus-2020-03-06. (neither the World Health Organization (WHO) nor the Centers for Disease Control and Prevention (CDC) have concluded that cash presents any more danger than credit cards or other forms of payment).

[85] *Fintech: Examining Digitization, Data, and Technology: Hearing Before the U.S. S. Comm. on Banking, Hous., and Urban Affairs*, 115th Cong. 17 (2018) (Statement of Saule T. Omarova, Prof. of Law, Cornell L. Sch.), *available at* https://www.banking.senate.gov/download/omarova-testimony-and-appendix-91818.

[86] Kapczynski, *supra* note 49, at 1467 ("we need...a more serious engagement with the political economy of data, grounded in the recognition that data is a social relation--an artifact not only of human cognition but also of legal structures.")

[87] Sarah Jeong, The Bitcoin Protocol as Law, and the Politics of a Stateless Currency 9 (Harvard Law Sch., Working Paper, May 8, 2013), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2294124.

[88] Terri Friedline, Banking on a Revolution: Why Financial Technology Won't Save a Broken System 3 (2020).

"peer-to-peer. But blockchains are not "decentralized" from a constitutional or corporate governance perspective. Even in the bitcoin systems, network participants, known as "miners," gather together blocks of transactions and compete to verify transactions.[89] In return, miners that successfully verify a block of transactions receive newly created cryptocurrency as well any transaction fees that the parties have put on offer.[90] That is to say, there is labor involved, and power dynamics exist between the laborers and others. Moreover, as Pasquale notes, blockchain enthusiasts misleadingly insist on calling that technology "immutable" and "unstoppable"[91] But the parties that validate the "nodes" of blockchain can and have colluded to determine the true identities of transacting parties — or modulate or "fork" the contents of the blockchain. Even the most ostensibly powerless systems still operate based on standards set by private institutions (see, e.g. Ethereum Foundation). Like most distributed ledger technology, the Blockchain is not decentralized in the sense that certain actors cannot exercise concentrated power over others.[92] Moreover, as a general matter, *node validators* in a distributed ledger system can still collaborate to change it.[93] Some blockchains can also take advantage of contextual "off-chain" data, or otherwise collude with third parties to determine the true identities of transacting parties and better monitor their behavior.[94] Network and platform power still permeates the infrastructure, especially in the form of the comparative computing power of participants.

Just as many analysts predicted, the ledger technology that Bitcoin birthed, the blockchain, has now fallen into the same perverse status as cyberspace, which was initially considered as a source of individual freedom.[95] Just as open-source software is fully integrated into Google's Android phones,[96] blockchain is integrated into J.P. Morgan Chase's ledger system.

---

[89] *Id.*

[90] *Id.*

[91] Frank Pasquale, Arthur J. Cockfield, *Beyond Instrumentalism: A Substantivist Perspective on Law, Technology, and the Digital Persona*, 2018 Mich. St. L. Rev. 821, 840 (2018). See also Angela Walch, *The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk*, 18 N.Y.U. J. LEGIS. & PUB. POL'Y 837, 861 (2015).

[92] *See* Angela Walch, *Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems*, *in* CRYPTOASSETS: LEGAL, REGULATORY, AND MONETARY PERSPECTIVES 39, 39-69 (Chris Brummer ed., 2019) (arguing misleading claims of "decentralization" function as a liability shield for developers operating the systems, creating a "Veil of Decentralization").

[93] *See, e.g.*, Angela Walch, *The Path of the Blockchain Lexicon (and the Law)*, 36 REV. BANKING & FIN. L. 713, 735–45 (2017) (discussing various ways in which prominent blockchains have been mutated, most notably the 51% attach).

[94] *See, e.g.*, Rainey Raitman, *In Foreshadowing Cryptocurrency Regulations, U.S. Treasury Secretary Prioritizes Law Enforcement Concerns*, ELECTRONIC FRONTIER FOUND. (Feb. 13, 2020), https://www.eff.org/deeplinks /2020/02/foreshadowing-cryptocurrency-regulations-us-treasury-secretary-prioritizes-law (noting that even pseudonymous wallet systems can still reveal a "huge number" of identities and financial transactions); Gregory Barber, *Everyone Wants Facebook's Libra to Be Regulated. But How?*, WIRED (July 18, 2019), https://www.wired.com/story/Everyone-wants-facebooks-libra-regulated-but-how/ (arguing companies that offer Libra services could use the same tools as law enforcement to re-identify users); Julie E. Cohen, *The Regulatory State in the Information Age*, 17 THEORETICAL INQUIRIES L. 369, 394 (2016) (describing how reidentification creates large unsecured data reservoirs).

[95] Georgios I. Zekos, Economics and Legal Understanding of Virtual Currencies, Banking & Fin. Services Pol'y Rep., August 2019, at 1, 13.

[96] Ron Amadeo, *Google's Iron Grip on Android: Controlling Open Source by Any Means Necessary*, ARS TECHNICA (July 21, 2018, 9:56 AM),

Because it is still ledger technology, blockchain is still used to regulate people's conduct, to make certain that they comply with the law or with the contractual obligations that they have entered into. To that extent, the blockchain can be employed to control identity, making it easier to check or merely keep track of numerous online actions.

Moreover, we should question the general impulse here. Is the freedom crypto seeks simple opposition to control? Powerful actors are already appropriating liberatory language for their own aims. Democracy demands we be able to participate in society without constant fear and apprehension of being watched (or found out). The limited conception of what is "private", as expressed by the third-party doctrine is a form of social control that devastates marginalized communities.[97] We do not want to live in subordinated or subaltern spaces; we want to be ourselves for the world to see. Cryptocurrency may allow us to transact in public without revealing who we are. But we do so under the cover of fear: to "stay inside" -- is not freedom.[98]

Postal Cash & Coin Circulation

The Federal Reserve Act (FRA) expressly sought a more elastic currency, based on the new technology afforded to the banking system, to meet the needs of a rapidly industrializing economy.[99] The Act completed a process begun with "Greenbacks", issuing Federal Reserve notes, rendering paper currency in the United States plentiful, "safe", and circulated at par.[100] The FRA established the Fed that we all know today, and transferred de facto *and* de jure administration of the national money supply from the Comptroller to this new entity.

Although it is the popular belief that merchants are constitutionally required to accept cash,[101] private businesses are not, in fact, mandated by federal statute to accept any type of currency for their goods or services.[102] Because Federal Reserve Notes (and the coins minted by the U.S. Treasury) must only be accepted as legal tender for "debts incurred", per the Constitution, a customer must first establish that they "owed" the relevant merchant, for example, by possessing the purchased item. This custom is heavily rooted in implied-in-fact contract theory and is easily avoided by a merchant simply waiting to provide a good until payment is received.

---

https://arstechnica.com/gadgets/2018/07/googles-iron-grip-on-android-controlling-open-source-by-any-means-necessary [https://perma.cc/9H3D-6F6N].

[97] *See generally* Scott Skinner-Thompson, Privacy at the Margins (2020).

[98] *See* Khiara M. Bridges, The Poverty of Privacy Rights 96 (2017).

[99] Steven A. Ramirez, *The Emergence of Law and Macroeconomics: From Stability to Growth to Human Development*, Law & Contemp. Probs., 2020, at 219, 223.

[100] John Crawford, *Making Money Safe*, 95 Notre Dame L. Rev. Reflection 1, 3 (2019)

[101] Legal Tender Status, U.S. Dep't of the Treasury, https://www.treasury.gov/resource-center/faqs/Currency/Pages/legal-tender.aspx [https://perma.cc/2R4J-FZML] (last updated Jan. 4, 2011, 4:47 PM).

[102] Is It Legal for a Business in the United States to Refuse Cash as a Form of Payment?, Board of Governors of the Fed. Res. Sys. [hereinafter Is It Legal to Refuse Cash?], https://www.federalreserve.gov/faqs/currency_12772.htm [https://perma.cc/4Z8G-YHFT] (last updated June 17, 2011) ("There is ... no Federal statute mandating that a private business, a person, or an organization must accept currency or coins as payment for goods or services.").

Among a list of ten security systems design principles offered by the Berkman Klein Center for Internet and Society, the very first is minimizing data collection, period. Yale University security expert Bruce Schneier stresses that we also need to start disconnecting systems, quickly, to prevent an insecure free-for-all throughout the IoT.[103] If we cannot build secure systems, we should think twice about engineering the interconnected surveillance that renders insecurity.[104] Preserving a place for cash also helps with operational security as digital systems can be compromised by failure or hacking.[105]

Online data should be encrypted wherever possible. As the crypto community has demonstrated, it is the single best security feature for the Internet Age.[106] But re-embracing the analog is a more basic solution for payment systems. We must increase the general circulation of cash and coins products, as the COVID-19 payments crises showed. Banks, partially by statute and partially by convention, are currently in charge of most cash and coin circulation and prohibit non-customers from making change at their branch locations. During the pandemic, this has meant unbanked people have not been able to for instance, wash clothes or purchase food from a vending machine on the job. Coin circulation problems inevitably link to cash circulation problems. Some retailers are adjusting by offering consumers loyalty points,[107] donations to charity, or other alternatives. But more importantly a number retailers have simply shied away from accepting cash payments.

In order to streamline cash and coin circulation and redemption, we should look to Treasury and its broader attachments. There is no constitutional requirement that all forms of cash or coins must enter broader commerce through the Federal Reserve System, much less the commercial banking system.[108] Indeed, even though the Federal Reserve "issues cash", new currency designed and printed by the Treasury's Bureau of Engraving and Printing, new coins are minted by the Mint, and most all circulation is achieved via the commercial banking system.

A strong defense of cash would be to partner with the U.S. Postal Service for cash and coin circulation. Long before the telegraph, broadcast radio and television, and the internet, the post office was an essential system for mass communication among American citizens.[109]

---

[103] *See generally* BRUCE SCHNEIER, "CLICK HERE TO KILL EVERYBODY" (2018) (hereinafter CLICK HERE).
[104] *Id.* at 167-170
[105] Hilary J. Allen, *Payments Failure*, 62 B.C. L. Rev. 453, 454, 513 (2021)
[106] Encrypting computer devices and communications, including payments, is not a panacea. Encrypted data can still be decrypted and backdoors obviate many of the advantages of encryption, generally. Breaches and invasions of privacy can still occur if the spy has log-in credentials. Metadata cannot be encrypted.
[107] https://www.latimes.com/business/story/2020-07-30/coin-shortage-quarters-change
[108] See Philip N. Diehl, Why Don't the Banks Pass the Buck?, Wash. Post, Sept. 2, 2000, at A25 (noting that banks do not have exclusive rights to new coins). *See Policies: The Federal Reserve in the Payments System*, Bd. of Governors Fed. Rsrv. Sys., https://www.federalreserve.gov/paymentsystems/pfs_frpaysys.htm [https://perma.cc/XWM6-VQ7H].
[109] *See* Winifred Gallagher, How the Post Office Created America: A History 1, 5 (2016); Richard R. John, Spreading the News: The American Postal System from Franklin to Morse vii (1995); Anuj C. Desai, *The Transformation of Statutes into Constitutional Law: How Early Post Office Policy Shaped Modern First Amendment Doctrine*, 58 Hastings L.J. 671-73, 676 (2007). From 1911 to 1967, the US Postal Service ran a Postal Savings Bank. Importantly, however, this was not integrated into the broader payment systems. See generally Act of June 25, 1910, 36 Stat 814, repealed by Act of Mar 28, 1966, Pub L No 89-377, 80 Stat 92. Democratic presidential candidate Bernie Sanders has called for the revival of postal banking. See *Text of Bernie Sanders' Wall Street and*

Baradaran, the APWU, and many policymakers argued for "postal banking" for some time.[110] Postal banks would offer a free savings and checking account that would enable the unbanked and underbanked to engage in simple financial transactions instead of high cost non-bank options like check-cashing or prepaid debit cards.[111] This should be complemented with a demand for "postal payments" more broadly, including the ability to store paper cash and coins at the post office and for USPS to aid in cash & coin circulation. It should comfort those worried about security that USPS is also subject to the BSA-AML regime, even if cash will lessen the intensity of its application.[112]

Public Banking, Postal Banking, Central Bank Digital Currency, Fed Accounts, E-Cash Wallets, & Postal Payments

Congress should explore the creation of a full-fledged digital public payments & banking system, bolstering the existing authority of USPS and other federal agencies. An increasingly large group of legal scholars advocating that we offer a ledger-based system to everyone via public option.[113] The Federal Reserve Board should be commended on its decision to establish and implement FedNow, a new interbank 24x7x365 real-time gross settlement (RTGS) system to facilitate real-time payments (RTP) between financial institutions of all sizes.[114]

Economy Speech (MarketWatch, Jan 5, 2016), archived at http://perma.cc/PMM6-NWMW. Adam J. Levitin, *Safe Banking: Finance and Democracy*, 83 U. Chi. L. Rev. 357, 380 (2016)

[110] *See, e.g.,* Mehrsa Baradaran, *It's Time for Postal Banking*, 127 HARV. L. REV. F. 165 (2014). "The Post Office or any public banking option must learn to adapt existing modern technology to offer fair, useful, and self-sustaining products to those neglected by mainstream banks." Mehrsa Baradaran, *Credit, Morality, and the Small-Dollar Loan*, 55 Harv. C.R.-C.L. L. Rev. 63, 126–27 (2020)

[111] *See* Campaign for Postal Banking, Postal Banking: Know the Facts, http://www.campaignforpostalbanking.org/wp-content/uploads/2015/05/KnowtheFacts.pdf [https://perma.cc/TBA8-YUXG].

[112] 31 C.F.R. §1010.100(ff).

[113] See, e.g. Morgan Ricks, John Crawford, and Lev Menand, *FedAccounts: Digital Dollars*, 89 George Wash. L. Rev. 113 (2020); Robert Hockett, *Digital Greenbacks: A Sequenced 'TreasuryDirect' and 'FedWallet' Plan for the Democratic Digital Dollar*, 25 J. of Tech. L. & Pol. (2020). Professor Hockett's plan for an "Inclusive Value Ledger" bears some technical, but little substantive similarity to the plan discussed in this Part. Ledger systems are not "peer-to-peer" by their very definition. Hockett's idea for a "digital dollar", influenced by Comm. Giancarlo and others, actually manifests via reinforcement of the already existing ledger of Treasury Direct Accounts (TDAs), used for securities transactions. Adding horizontal connectivity between the accounts Hockett misleadingly refers to as "wallets" does not mean vertical connectivity with the state disappears or is even mitigated. The Treasury obviously still intermediates all transactions and it is not clear what payments data the IRS or FinCen can collect. Indeed for Hockett, the IVL's ability to enhance tax collection, AML, CFT, and sanctions law is somehow characterized as a privacy **feature** of the system. Hockett also states that transactions on the ledger will be subject to Fourth Amendment protections, but provides no Fourth Amendment analysis.

[114] *See* Letter from AFR Education Fund & DPEF to Board (2019) https://www.federalreserve.gov/SECRS/2019/December/20191230/OP-1670/OP-1670_110719_136983_394241172069_1.pdf. *See also* Comment from FTC Comm'r Rohit Chopra to FTC (Nov. 7, 2019), https://www.ftc.gov/public-statements/2019/11/comment-commissioner-rohit-chopra-federal-reserve-proposal-develop-round (urging the Board to proceed promptly, arguing that slow development has created space for the Libra project and "attempts to bypass our banking system altogether.")

We should also have public banking accounts. Currently, we are forced to rely on the banks as middlemen to deliver government assistance. Some of them have even seized emergency COVID-19 payments to collect debts.[115] Some experts have called for Silicon Valley firms to partner with the government on this endeavor.[116] But Big Tech's involvement in public money development would doom any future financial privacy in public.[117] A new "digital dollar" should respect the privacy of its users.[118] Such respect would entail, among other features, taking a queue from the crypto community and offering digital *wallets* as well as *bank accounts*.[119]

Herein the legal and technical expertise of Professor Rohan Grey at Willamette School of Law, who also serves as Privacy Lead at the International Telecommunications Union -- wherein they have been discussing the relationship between privacy and evolving communications infrastructure for decades -- is especially indispensable. Professor Grey was the first legal scholar to emphasize the imperative of preserving "bearer instruments" in a digital transformation. As Grey argues, the terms "central bank digital currency", "digital dollar", and "e-cash" are often conflated. This is unhelpful: a 'digital dollar' may be issued by any agency of the U.S. government, while a CBDC, by definition, must be issued by the Central Bank. While some blockchains may blur the lines between these categories, none provide true peer-to-peer, offline

---

115 *See* Press Release, U.S. S. Comm. on Banking, Hous., and Urban Affairs, *Brown, Warren Call On Banks To End The Seizure Of Stimulus Checks* (Apr. 15, 2020), *available at* https://www.banking.senate.gov/newsroom/minority/brown-warren-call-on-banks-to-end-the-seizure-of-stimulus-checks.

116 *See, e.g., The Digitization of Money and Payments: Hearing Before the S. Comm. on Banking, Hous., and Urban Affairs,* 116th Cong. 7-10 (2020) (Statement of Hon. J. Christopher Giancarlo, Chair Emeritus, CFTC), *available at* https://www.banking.senate.gov/download/giancarlo-testimony-6-30-20&download=1.

117 As would Wall Street's involvement. *See, e.g.,* Raúl Carrillo, *Postal Banking: Brought to you by JP Morgan Chase?*, TAKE ON WALL ST. BLOG (Aug. 27, 2020), https://takeonwallst.com/2020/08/postal-banking-jp-morgan-chase/.

118 *See, e.g.*, Jason Brett, *Congress Considers Federal Crypto Regulators In New Cryptocurrency Act Of 2020*, FORBES (Dec. 19, 2019), https://www.forbes.com/sites/jasonbrett/2019/12/19/congress-considers-federal-crypto-regulators-in-new-cryptocurrency-act-of-2020/#716eff165fcd (describing the popularization of the idea of the digital dollar in response to Libra's development).

119 David Beckworth & Rohan Grey, *The Future of Digital Currency*, MERCATUS CENTER BLOG (Feb. 11, 2019), https://www.mercatus.org/bridge/podcasts/02112019/future-digital-fiat-currency,
Rohan Grey (2019), Banking in a Digital Fiat Currency Regime, in Philipp Hacker et al (eds.), *Regulating Blockchain: Techno-Social and Legal Challenges.*; JONATHAN DHARMAPALAN & ROHAN GREY, THE CASE FOR DIGITAL LEGAL TENDER: THE MACROECONOMIC POLICY IMPLICATIONS OF DIGITAL FIAT CURRENCY, ECURRENCY MINT LTD. (2018), https://www.ecurrency.net/static/resources/201802/TheMacroeconomicImplicationsOfDigitalFiatCurrencyEVersion.pdf.

transactions like e-Cash in the ABC Act sponsored by Rep. Tlaib (D-MI) [120] or the model currently being considered by the Bank of Canada.[121]

While legal firewalls might prevent some level of abuse in an account-based system, technological solutions are necessary. If the owner of a public centralized ledger system, (for instance, the Federal Reserve Bank of New York) were able to access digital dollar transaction activity at any given time, that data could be inappropriately accessed by other governmental entities, including law enforcement.[122] By contrast, within our existing monetary system, the Federal Reserve System does not make any records of where individual Federal Reserve Notes are at any given time; circulation is merely recorded as a single aggregate liability on the Fed's balance sheet titled 'Federal Reserve Notes Outstanding.'[123]

A new public system for payments should proceed from the principle that data that is not harvested in the first place cannot be abused. In some sense, maintaining a place for cash can even be characterized as "conservative" of our best traditions. In order to mitigate illicit flows, policymakers could choose to only offer anonymity under a certain threshold of holdings, as federal law does now with paper cash.[124] Cash has security techniques, most notably the barcode. A number of public features enable people to visually inspect and verify the authenticity of each bill. For example, the U.S. The Bureau of Printing and Engraving publishes details about some of the features of new U.S. dollars, such as color-shifting ink, a new watermark, a metallic security thread, and the use of micro print.[1] Privacy and public sector innovation need not conflict.

Herein, we can learn something from the crypto community's deployment of cryptographically-verifiable electronic tokens. Assuming the security of the cryptographic mechanisms and the secrecy of the associated cryptographic information are preserved, digital

---

[120] Critically, Rep. Tlaib's ABC Act asks the Treasury to offer recipients the option to receive payments via FedAccounts *or prepaid debit cards*, which in the future would be loaded with funds via an eCash wallet instead of connected to a regular commercial bank account via TreasuryExpress. This vision – of disseminating relief payments via a pre-loaded 'cash card,' while avoiding any need for individuals to register for an account that could be monitored or tracked, was a critical design feature of the bill and one of the major differentiating features between it and other FedAccount proposals, which risk discriminating against undocumented people who may not be able to open an account. The digital dollar 'eCash' wallets would be capable of being self-hosted by any person in possession of a cheap, handheld device, regardless of residency status, just like cash today. https://tlaib.house.gov/media/press-releases/tlaib-jayapal-introduce-groundbreaking-bill-deliver-universal-recurring-0

[121] https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-10/.

[122] *See, e.g.*, Matla Garcia Chavolla, *Cashless Societies and the Rise of the Independent Cryptocurrencies: How Governments Can Use Privacy Laws to Compete with Independent Cryptocurrencies*, 31 PACE INT'L L. REV. 263, 273 (2018).

[123] *See* Rohan Grey, *Administering Money: Coinage, Debt Crises, and the Future of Fiscal Policy*, KY. L.J. 1, 16-18 (forthcoming 2020), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3536440.

[124] *See* Marco Dell'Erba, *Stablecoins in Cryptoeconomics: From Initial Coin Offerings to Central Bank Digital Currencies,* 22 N.Y.U. J. LEGIS. & PUB. POL'Y 1, 43 (2020). However, *see also*, Jason Leopold et al., *The FinCEN Files*, BUZZFEED (Sept. 20, 2020), https://www.buzzfeednews.com/article/jasonleopold/fincen-files-financial-scandal-criminal-networks (arguing the post-9/11 AML, CFT, and sanctions regime, in addition to violating civil rights, does not work as purported. Surveillance has not necessarily led to increased law enforcement).

cash cannot be counterfeited.[125] More decentralized verification attempts to achieve security by enabling individuals (or their digital wallet) to perform real-time validation of bills they receive. QR codes can also help prevent counterfeiting.[126]

Wallets are also especially important to privacy and security for doctrinal reasons: creating a password-protected account to store information is comparable to storing papers in a lock box where only the owner has the key.[127] Historically, wallets, as well as paper receipts, checkbooks, and wallets have been deemed "closed containers" and sometimes provided with Fourth Amendment protections.

Surveillance must be centered within any discussion of a public option for financial services. FDIC surveys consistently note that many "unbanked" households refuse to open bank accounts due to privacy concerns.[128] While providing increased access to digital financial services is important, a rapid shift to digitization stands to harm low-income people of color in particular.[129] Many current proposals for a public system center round a certain technological infrastructure (like universal *quality* broadband),[130] not to mention a certain level of household financial stability.

There are limits to what a reconstruction of the payments architecture can accomplish; many poor people have no privacy regardless.[131] What the proliferation of cash and e-cash accomplishes is at once more subtle and more impactful. It removes the possibility of certain data being collected *in the first place.* Where bearer-instruments replace ledger-instruments, they decrease surveillance. Cash -- and financial privacy in general -- deserve priority in our evolving digital systems.

---

[125] Nicolas Christin et. al., *Monetary Forgery in the Digital Age: Will Physical-Digital Cash Be A Solution?*, 7 I/S: J.L. & Pol'y for Info. Soc'y 171, 173–75 (2012)

[126] Beckworth & Grey. https://www.mercatus.org/bridge/podcasts/02112019/future-digital-fiat-currency

[127] *See* David D. Thomas, *Dangerously Sidestepping the Fourth Amendment: How Courts Are Allowing Third-Party Consent to Bypass Warrants for Searching PasswordProtected Computer*, 57 CLEV. ST. L. REV. 279 (2009).

[128] FDIC, NATIONAL SURVEY OF UNBANKED AND UNDERBANKED HOUSEHOLDS, 2017 4, 23-24, https://www.fdic.gov/householdsurvey/. *See also, id.* at 3 (noting Black households are nearly six times more likely to be unbanked than white households, while Hispanic households are nearly five times more likely to be unbanked than white households).

[129] Jay Stanley, *Say No to the "Cashless Future" — and to Cashless Stores*, ACLU (Aug. 12, 2019), https://www.aclu.org/blog/privacy-technology/consumer-privacy/say-no-cashless-future-and-cashless-stores.

[130] *See*, *e.g.*, Terri Friedline, *An Open Internet is Essential for Financial Inclusion, FinTech Revolution*, HUFF. POST (Dec. 14, 2017), https://www.huffpost.com/entry/an-open-internet-is-essential-for-financial-inclusion_b_5a3345dce4b0e1b4472ae520.

[131] Bridges, *supra* note 98, at 67.