Written Testimony of
Frank Pasquale
Professor of Law
University of Maryland

Before the United States Senate
Committee on the Banking, Housing, and Urban Affairs

"Exploring the Fintech Landscape"
Sept. 12, 2017
10:00 am
Dirksen Senate Office Building

Witness Background

Frank Pasquale is Professor of Law at the University of Maryland's Francis King Carey School of Law. His research addresses the challenges posed to law by rapidly changing technology. He has served as a member of the NSF-funded Council for Big Data, Ethics, and Society, and is an Affiliate Fellow of Yale Law School's Information Society Project. His recent publications focus on the legal implications of big data, artificial intelligence, and algorithms. His book *The Black Box Society: The Secret Algorithms that Control Money and Information* (Harvard University Press, 2015) has informed the global algorithmic accountability movement, and has been translated into Chinese, French, and Serbian. He is a co-founder of the Association for the Promotion of Political Economy and Law (APPEAL), with Jennifer Taub and Martha McCluskey.

Pasquale has been a Visiting Fellow at Princeton's Center for Information Technology Policy, and a Visiting Professor at Yale Law School and Cardozo Law School. He serves on the Advisory Boards of the Data Competition Institute, the New Economy Law Center, and the Electronic Privacy Information Center. He has co-authored a casebook on administrative law and co-authored or authored over 50 scholarly articles, including *Law's Acceleration of Finance: Redefining the Problem of High-Frequency Trading*, 36 Cardozo Law Review 2085 (2015); *Four Futures of Legal Automation*, 63 UCLA Law Review Discourse 26 (2015) (with Glyn Cashwell); *The Scored Society: Due Process for Automated Predictions*, 89 Washington Law Review 1 (2014) (with Danielle Citron); *The Troubling Consequences of Trade Secret Protection of Search Engine Rankings*, in *The Law and Theory of Trade Secrecy* (Rochelle Cooper Dreyfuss & Katherine Jo Strandburg eds., 2011); and *Democratizing Higher Education: Defending & Extending Income Based Repayment Programs*, 28 Loyola Consumer Law Review 1 (2015). He graduated with a B.A., *summa cum laude*, from Harvard University, an MPhil. from Oxford, and a JD from Yale Law School.

I. Introduction

The financial technology ("fintech") landscape is complex and diverse. Fintech ranges from automation of office procedures once performed by workers, to some genuinely new approaches to storing and transferring value, and granting credit.[1] New services—like insurance sold by the hour—are emerging. Established and start-up firms are using emerging data sources and algorithms to assess credit risk. And even as financial institutions are adopting some distributed ledger technologies, some proponents of cryptocurrency claim that it "changes everything" and will lead to a "blockchain revolution."

For purposes of this testimony, I will divide the fintech landscape into two spheres. One, incrementalist fintech, uses new data, algorithms, and software to perform classic work of existing financial institutions. This new technology does not change the underlying nature of underwriting, payment processing, lending, or other functions of the financial sector. Regulators should, accordingly, assure that long-standing principles of financial regulation persist here. I address these issues in Part II below.

Another sector, which I deem "futurist fintech," claims to disrupt financial markets in ways that supersede regulation, or render it obsolete. For example, if you truly believe a blockchain memorializing transactions is "immutable," you may not see the need for regulatory interventions to promote security to stop malicious hacking or modification of records. In my view, futurist fintech faces fundamental barriers to widespread realization and dissemination. I address these issues in Part III below.

II. Incrementalist Fintech

A. Big Data or Artificial Intelligence-based Underwriting

Many marketplace lenders are now using forms of data not traditionally used for credit underwriting, in order to offer consumer or small business loans. They may help correct some long-standing problems in US credit markets, including the problematic nature of contemporary credit scoring. However, as Mikella Hurley & Julius Adebayo have argued,

> Credit-scoring tools that integrate thousands of data points, most of which are collected without consumer knowledge, create serious problems of transparency.

[1] The Government Accountability Office has described fintech as follows: "The financial technology (fintech) industry is generally described in terms of subsectors that have or are likely to have the greatest impact on financial services, such as credit and payments. Commonly referenced subsectors associated with fintech include marketplace lending, mobile payments, digital wealth management, and distributed ledger technology." GAO, FINANCIAL TECHNOLOGY: INFORMATION ON SUBSECTORS AND REGULATORY OVERSIGHT (2017).

> Consumers have limited ability to identify and contest unfair credit decisions, and little chance to understand what steps they should take to improve their credit. Recent studies have also questioned the accuracy of the data used by these tools, in some cases identifying serious flaws that have a substantial bearing on lending decisions.
>
> Big-data tools may also risk creating a system of "creditworthiness by association" in which consumers' familial, religious, social, and other affiliations determine their eligibility for an affordable loan. These tools may furthermore obscure discriminatory and subjective lending policies behind a single "objective" score. Such discriminatory scoring may not be intentional; instead, sophisticated algorithms may combine facially neutral data points and treat them as proxies for immutable characteristics such as race or gender, thereby circumventing existing non-discrimination laws and systematically denying credit access to certain groups. Finally, big-data tools may allow online payday lenders to target the most vulnerable consumers and lure them into debt traps.[2]

The problem of "big data proxies" is a serious one recognized by leading privacy scholars.[3] Regulators should do much more to assure that next-generation technology does not simply reproduce old biases.[4] The alternative is a "scored society" where individuals lack basic information about how they have been treated in the credit granting context.[5]

These problems are troubling in the abstract. Their concrete implications are chilling, as a recent Privacy International Report revealed. Outside the United States, fintech firms have already scored creditworthiness based on the following factors:

- "If lenders see political activity on someone's Twitter account in India, they'll consider repayment more difficult and not lend to that individual."
- "The contents of a person's smartphone, including who and when you call and receive messages, what apps are on the device, location data, and more."
- "How you use a website and your location. [One firm] analyses the way you fill in a form (in addition to what you say in the form), and how you use a website, on what kind of device, and in what location."[6]

---

[2] Mikella Hurley & Julius Adebayo, *Credit Scoring the Era of Big Data*, 18 YALE J.L. & TECH. 148 (2017).
[3] See, e.g., Nicolas Terry, *Big Data Proxies and Health Privacy Exceptionalism*, HEALTH MATRIX (2015).
[4] For an up-to-the-minute overview of this and related problems, see Penny Crosman, *Is AI a threat to fair lending?*, at https://www.americanbanker.com/news/is-artificial-intelligence-a-threat-to-fair-lending.
[5] Danielle Keats Citron & Frank Pasquale, *The Scored Society*, 89 WASH. L. REV. 1 (2014).
[6] Privacy International, *Case Study: Fintech and the Financial Exploitation of Customer Data*, at

Moreover, machine learning systems are constantly developing even more invasive forms of assessing creditworthiness, or factors influencing it. A recently published paper claims to infer propensity to criminality merely from the features of persons' faces.[7] Sexuality and health are also now being predicted by machine learning researchers entirely on the basis of a picture of a person's face—something relatively easy to gather via a Google image search, or Facebook search.[8] Regulators need to be able to audit machine learning processes to understand, at a minimum, whether suspect sources of data like these are influencing fintech firms.[9]

1. Neither Machine Learning Nor Predictive Analytics are too Complex to Regulate

Some fintech firms which rely on artificial intelligence may counter that the computation involved in their decisionmaking now amounts to a form of cognition as hard to explain as that of a human decision-maker. Genetic algorithms may, for instance, themselves spawn, each second, dozens of ways of processing information, which are then evaluated on some metric, and Darwinianly given a chance to persist based on their performance. Iterative machine learning processes may be similarly complex and opaque. Their view is that, just as we can't map all the brain's neurons to connect a person's decision to eat a slice of cake to some set of synapses, we can't map or unravel the sequence of events that leads to a given algorithmic score or sorting.

I believe that we should be suspicious of the deregulatory impulse behind characterizations of machine learning as "infinitely complex," beyond the scope of human understanding. The artificial intelligence that commercial entities celebrate can just as easily evince artificial imbecility, or worse. Moreover, there are several practical steps we can take even if machine learning processes are extraordinarily complex.

---

https://privacyinternational.org/node/1499?PageSpeed=noscript (Aug. 30, 2017). *See also* Josh Chin & Gillian Wong, *China's New Tool for Social Control: A Credit Rating for Everything*, Wall St. J., Nov. 28, 2016, at https://www.wsj.com/articles/chinas-new-tool-for-social-control-a-credit-rating-for-everything-1480351590; Ian Bogost, *Cryptocurrency Might be a Path to Authoritarianism*, The Atlantic, May 30, 2017, at https://www.theatlantic.com/technology/archive/2017/05/blockchain-of-command/528543/.

[7] Blaise Agüera y Arcas, Margaret Mitchell and Alexander Todorov, *Physiognomy's New Clothes*, at https://medium.com/@blaisea/physiognomys-new-clothes-f2d4b59fdd6a (May 6, 2017).

[8] Sam Levin, LGBT groups denounce 'dangerous' AI that uses your face to guess sexuality, *The Guardian*, at https://www.theguardian.com/world/2017/sep/08/ai-gay-gaydar-algorithm-facial-recognition-criticism-stanford, Sept. 8, 2017; Barbara Marquand, *How Your Selfie Can Affect Health Insurance*, USA Today, at https://www.usatoday.com/story/money/personalfinance/2017/04/25/how-your-selfie-could-affect-your-life-insurance/100716704/.

[9] To be clear, I am not alleging any particular fintech firm in the United States is using such approaches in the United States at present. I am just pointing out that the possibility exists, and must be monitored.

For example, we may still want to know what data was fed into the computational process. Presume as complex a credit scoring system as possible. Regulators could still demand to know the data sets fed into it, and, for example, forbid health data from being included in that set. We already know that at least one credit card company has paid attention to certain mental health events, like going to marriage counseling.[10] When statistics imply that couples in counseling are more likely to divorce than couples who aren't, counseling becomes a "signal" that marital discord may be about to spill over into financial distress.[11] This is effectively a "marriage counseling penalty," and poses a dilemma for policy makers. Left unrevealed, it leaves cardholders in the dark about an important aspect of creditworthiness. Once disclosed, it could discourage a couple from seeking the counseling they need to save their relationship.

There doesn't have to be any established causal relationship between counseling and late payments; correlation is enough to drive action. That can be creepy in the case of objectively verifiable conditions, like pregnancy. And it can be devastating for those categorized as "lazy," "unreliable," "struggling," or worse. Runaway data can lead to *cascading disadvantages* as digital alchemy creates new analog realities.[12] Once one piece of software has inferred that a person is a bad credit risk, a shirking worker, or a marginal consumer, that attribute may appear with decision-making clout in other systems all over the economy. There is also little in current law to prevent companies from selling their profiles of consumers.[13]

2. The Problems of Extant Data Collectors are a Reason for More Scrutiny of Fintech, Not Less

Having eroded privacy for decades, shady, poorly regulated data miners, brokers and resellers have now taken creepy classification to a whole new level. They have created lists of victims of sexual assault, and lists of people with sexually transmitted diseases. Lists of people who have Alzheimer's, dementia and AIDS. Lists of the impotent and the depressed.

---

[10] Charles Duhigg, "What Does Your Credit Card Company Know about You?" *New York Times*, May 17, 2009, http://www.nytimes.com/2009/05/17/magazine/17credit-t.html?pagewanted=all. For a compelling account for the crucial role that the FTC plays in regulating unfair consumer practices and establishing a common law of privacy, see Daniel J. Solove and Woodrow Hartzog, "The FTC and the New Common Law of Privacy," *Columbia Law Review* 114 (2014): 583–676.
[11] Charles Duhigg, "What Does Your Credit Card Company Know about You?", N.Y. Times, May 12, 2009.
[12] Cathy O'Neil, *Weapons of Math Destruction* (2016).
[13] Kashmir Hill, "Could Target Sell Its 'Pregnancy Prediction Score'?" *Forbes*, February 16, 2012, http://www.forbes.com/sites/kashmirhill/2012/02/16/could-target-sell-its-pregnancy-prediction-score/.

There are lists of "impulse buyers." Lists of suckers: gullible consumers who have shown that they are susceptible to "vulnerability-based marketing." And lists of those deemed commercially undesirable because they live in or near trailer parks or nursing homes. Not to mention lists of people who have been accused of wrongdoing, even if they were not charged or convicted. Typically sold at a few cents per name, the lists don't have to be particularly reliable to attract eager buyers. And there is increasing risk that your spouse, friends, boss, or acquaintances could buy such data.[14]

There are three problems with these lists. First, they are often inaccurate. For example, as The Washington Post reported, an Arkansas woman found her credit history and job prospects wrecked after she was mistakenly listed as a methamphetamine dealer. It took her years to clear her name and find a job.[15] Second, even when the information is accurate, many of the lists have no business being in the hands of fintechs. Having a medical condition, or having been a victim of a crime, should not be part of credit decisions, since such data use generates risk of compounding, self-reinforcing disadvantage via digital stigma.

Third, people aren't told they are on these lists, so they have no opportunity to correct bad information. The Arkansas woman found out about the inaccurate report only when she was denied a job. She was one of the rare ones. The market in personal information offers little incentive for accuracy; it matters little to list-buyers whether every entry is accurate — they need only a certain threshold percentage of "hits" to improve their targeting. But to individuals wrongly included on derogatory lists, the harm to their reputation is great.[16]

The World Privacy Forum, a research and advocacy organization, estimates that there are about 4,000 data brokers. They range from publicly traded companies to boutiques. Companies like these vacuum up data from just about any source imaginable: consumer health websites, payday lenders, online surveys, warranty registrations, Internet sweepstakes, loyalty-card data from retailers, charities' donor lists, magazine subscription lists, and information from public records.

It's unrealistic to expect individuals to inquire, broker by broker, about their files. Instead, we need to require brokers to make targeted disclosures to consumers. Uncovering

---

[14] Theodore Rostow, *What Happens When an Acquaintance Buys Your Data?: A New Privacy Harm in the Age of Data Brokers*, 34 YALE JOURNAL ON REGULATION (2016).

[15] Ylan Q. Mi, *Little-known firms tracking data used in credit scores*, WASH. POST, July 16, 2011, at https://www.washingtonpost.com/business/economy/little-known-firms-tracking-data-used-in-credit-scores/2011/05/24/gIQAXHcWII_story.html?utm_term=.db2a64c53efd.

[16] Note that information generated for or within a credit context may spread outside it—and vice versa. Amy Traub, *Discredited: How Employment Credit Checks Keep Qualified Workers Out of a Job* (2012), http://www.demos.org/discredited-how-employment-credit-checks-keep-qualified-workers-out-job. Such data and inferences are very important

problems in Big Data (or decision models based on that data) should not be a burden we expect individuals to solve on their own.

Privacy protections in other areas of the law can and should be extended to cover the consumer data now fueling fintech underwriting. The Health Insurance Portability and Accountability Act, or HIPAA, obliges doctors and hospitals to give patients access to their records. The Fair Credit Reporting Act gives loan and job applicants, among others, a right to access, correct and annotate files maintained by credit reporting agencies.

It is time to modernize these laws by applying them to all companies that peddle sensitive personal information. If the laws cover only a narrow range of entities, they may as well be dead letters. For example, protections in HIPAA don't govern the "health profiles" that are compiled and traded by data brokers or fintech firms, which can learn a great deal about our health even without access to medical records.

Congress should require data brokers to register with the Federal Trade Commission, and allow individuals to request immediate notification once they have been placed on lists that contain sensitive data. Reputable data brokers will want to respond to good-faith complaints, to make their lists more accurate. Plaintiffs' lawyers could use defamation law to hold recalcitrant firms accountable.

We need regulation to help consumers recognize the perils of the new information landscape without being overwhelmed with data. The right to be notified about the use of one's data and the right to challenge and correct errors is fundamental. Without these protections, we'll continue to be judged by a big-data Star Chamber of unaccountable decision makers using questionable sources.

Policymakers are also free to restrict the scope of computational reasoning too complex to be understood in a conventional narrative or equations intelligible to humans. They may decide: if a bank can't give customers a narrative account of how it made a decision on their loan application, including the data consulted and algorithms used, then the bank can't be eligible for (some of) the array of governmental perquisites or licenses so common in the financial field. They may even demand the use of public credit scoring models, or fund public options for credit. Finally, they should look to Europe's General Data Protection Regulation (GDPR), which provides several standards for algorithmic accountability.[17]

[17] See, e.g., Bryce W. Goodman, *A Step Towards Accountable Algorithms?: Algorithmic Discrimination and the European Union General Data Protection*, at http://www.mlandthelaw.org/papers/goodman1.pdf ("If implemented properly, the algorithm audits supported by the GDPR could play a critical role in making algorithms less discriminatory and more accountable.").

B. Emerging Issues in Preemption and Regulatory Arbitrage

Some fintech advocates advocate radical deregulation of their services, to enable their rapid entry into traditional banking markets. However, there is a risk of the fintech label merely masking "old wine in new bottles." The annals of financial innovation are long, but not entirely hallowed.[18] When deregulatory measures accelerated in the late 1990s and early 2000s, their advocates argued that new technology would expertly spread and diversify risk. However, new quantitative approaches often failed to perform as billed. Most fundamentally, a technology is only one part of a broader ecosystem of financial intermediation.[19]

I do believe that some fintech may promote competition and create new options for consumers. But we should ensure that it is fair competition, and that these options don't have hidden pitfalls. In my research on the finance and internet sectors, I have explored patterns of regulatory arbitrage and opaque business practices that sparked the mortgage crisis of 2008.[20] I see similar themes emerging today.

In the run-up to the crisis, federal authorities preempted state law meant to protect consumers.[21] The stated aim was to ensure financial inclusion and innovation, but the unintended consequences were disastrous. Federal authorities were not adequately staffed to monitor, let alone deter or punish, widespread fraudulent practices. Agencies like the Office of the Comptroller of Currency (OCC) also flattened diverse state policies into a one-size-fits-all, cookie-cutter approach. We all know the results.[22] It now appears that the OCC may be repeating its past mistakes.

---

[18] FINANCIAL CRISIS INQUIRY COMMISSION, FINAL REPORT OF THE NATIONAL COMMISSION ON THE CAUSES OF THE FINANCIAL AND ECONOMIC CRISIS IN THE UNITED STATES (2011)

[19] Tom C.W. Lin, *Infinite Financial Intermediation*, 50 WAKE FOREST L. REV. 643 (2015). This article's sections on "linked stability," "financial cybersecurity," and "intermediary independence" (pages 661 onwards) should be of particular interest to the committee. See also Tom C.W. Lin, *The New Financial Industry*, 65 ALA. L. REV. 567, 595 ff. (2014) (offering 10 "regulatory principles for the new financial industry).

[20] Frank Pasquale, *The Black Box Society* (2015). Chapter 4 (*Finance's Algorithms: The Emperor's New Codes*) describes these problems in detail. Chapter 5 offers regulatory proposals.

[21] FCIC Report, 112 and *passim* ("Once OCC and OTS preemption was in place, the two federal agencies were the only regulators with the power to prohibit abusive lending practices by national banks and thrifts and their direct subsidiaries."); id., at 350 ("The Office of Thrift Supervision has acknowledged failures in its oversight of AIG. . . a former OTS director[] told the FCIC that as late as September 2008, he had "no clue—no idea—what [AIG's] CDS liability was.").).

[22] Fortunately, the Supreme Court quickly signalled after the crisis that its pro-preemption approach here had gone too far. *See* Arthur E. Wilmarth, *Cuomo v. Clearing House: The Supreme Court Responds to the Subprime Financial Crisis and Delivers a Major Victory for the Dual Banking System and Consumer Protection*, in THE PANIC OF 2008: CAUSES, CONSEQUENCES AND IMPLICATIONS FOR REFORM, Lawrence E. Mitchell and Arthur E. Wilmarth Jr., eds., Edward Elgar Publishing, 2010, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1499216.

The OCC has released a White Paper, Exploring Special Purpose National Bank Charters for Fintech Companies, in 2016 ("White Paper").[23] The OCC believes that such charters "could advance important policy objectives, such as enhancing the ways in which financial services are provided in the 21st century, while ensuring that new fintech banks operate in a safe and sound manner, support their communities, promote financial inclusion, and protect customers."[24] The OCC is, to be sure, well-intentioned. Its Office of Innovation has energetically helped entrepreneurs to understand regulatory mandates by offering informal, candid discussions "with OCC staff regarding financial technology, new products or services, partnering with a bank or fintech, or any other matter related to financial innovation."[25] However, several negative consequences could arise out of OCC efforts to go beyond informal counseling about extant legal obligations, by substantively altering these obligations via special purpose national bank charters for fintech firms.

For example, such fintech charters could enable regulatory arbitrage around state restrictions on payday lending. As 270 entities--community, labor, civil rights, faith-based, and military and veterans groups--observed earlier this year, 90 million Americans "live in jurisdictions where payday lending is illegal." [26] These state consumer protection laws help consumers "save billions of dollars each year in predatory payday loan fees that trap people in long-term, devastating cycles of debt."[27] OCC should not take action to preempt them.[28]

---

[23] Office of the Comptroller of the Currency, Exploring Special Purpose National Bank Charters for Fintech Companies (2016), https://www.occ.treas.gov/topics/bank-operations/innovation/special-purposenational-bank-charters-for-fintech.pdf ("White Paper").
[24] Id., at 2.
[25] OCC Office of Innovation Office Hours, at, e.g., https://www.occ.gov/topics/responsible-innovation/innovation-office-hours.pdf; see also CFPB's Project Catalyst.
[26] Center for Responsible Lending, States without Payday and Car-title Lending Save Over $5 Billion in Fees Annually, at http://www.responsiblelending.org/sites/default/files/nodes/files/research-publication/crl_payday_fee_savings_jun2016.pdf (2016); Comment Letter of Over 200 Community, Labor, and Nonprofit Groups, at http://www.neweconomynyc.org/wp-content/uploads/2017/01/comment_occ_fintech_01132017.pdf (2017) ("While the fintech industry has the potential to encourage innovation, we have also seen costly payday lenders hide behind the costume of "fintech.").
[27] Id.
[28] Americans for Financial Reform, Exploring Special Purpose National Bank Charters for Fintech Companies, Comment Letter, Jan. 15, 2017, at https://www.occ.gov/topics/responsible-innovation/comments/comment-americans-for-financial-reform.pdf (explaining broad array of legal and policy concerns that would arise if such charters were granted); Center for Digital Democracy and U.S. PIRG, Exploring Special Purpose National Bank Charters for Fintech Companies, Comment Letter, at https://www.occ.gov/topics/responsible-innovation/comments/comment-cdd-uspirg.pdf ("lack of transparency around the processing of data and automated algorithms may lead to increasing information asymmetries between the financial institution and the individual and thus consumers are left with less awareness and a lack of understanding and control over important financial decisions.").

These are not mere hypothetical concerns; as the New Economy Project has documented, online lenders "have been subject to a long list of state and federal enforcement actions, settlement agreements, and investigations."[29] Moreover, they may lure unsuspecting borrowers away from much more sustainable alternatives, including publicly vetted options.[30]

Nor should the Senate rush to consider a proposed bill to legislatively overturn the 2nd Circuit's decision in *Madden v. Midland Funding, LLC*, which applied New York state usury law to loans purchased by a debt collector who believed that those laws would be preempted, since the loans were originated by a national bank.[31] As Adam Levitin has explained, there are not sound legal or policy arguments to ground present challenges to *Madden.*[32] As Levitin explains, "Preemption is part of a package with regulation, but once the loan passes beyond the hands of a National Bank, it loses its preemption protection and becomes subject to state usury laws."[33] There is little reason to undermine the dual banking system by applying a talismanic shield against usury laws to loans even once they have been sold by the intended beneficiary of preemption.[34]

One more aspect of regulatory arbitrage is now in fintech news: recent applications by Square and SoFi for Industrial Loan Company (ILC) charters. Walmart's 2006

---

[29] New Economy Project, Testimony Of New Economy Project Before The New York Senate Committees On Banks And Consumer Protection and the Assembly Committees On Banks, Small Business, and Consumer Affairs & Protection, Public Hearing on Online Lending Practices, at http://www.neweconomynyc.org/resource/testimony-nys-senate-assembly-hearing-regarding-online-lending/. For more on New York concerns, see Daniel Alter, The "Business of Banking" in New York – An Historical Impediment To the OCC's Proposed National "Fintech Charter," Notice & Comment, Blog of the Yale J. Reg., June 29, 2017, at http://yalejreg.com/nc/the-business-of-banking-in-new-york-an-historical-impediment-to-the-occs-proposed-national-fintech-charter-by-daniel-s-alter/.

[30] David Lazarus, Pricey 'fintech' lenders put the squeeze on cash-strapped small businesses, LA Times, June 16, 2017, at http://www.latimes.com/business/lazarus/la-fi-lazarus-small-business-loans-20170616-story.html (reporting that an "associate administrator for the federal Small Business Administration's Office of Capital Access, advised starting the hunt for capital not with a fintech firm but with the agency's LINC search tool (that's LINC as in Leveraging Information and Networks to access Capital)," in response to Lazarus's story of a small business owner charged amounts that "translated to an annual percentage rate of 55%" by a fintech firm).

[31] Madden v. Marine Midland Funding, No. 14-2131 (2d Cir. 2015).

[32] Adam Levitin, Madden v. Marine Midland Funding, http://www.creditslips.org/creditslips/2015/07/madden-v-marine-midland-funding.html.

[33] Id.; see also Adam Levitin, *Hydraulic Regulation: Regulating Credit Markets Upstream*, 26 Yale Journal on Regulation (2009).

[34] Adam Levitin, *Guess Who's Supporting Predatory Lending*, Credit Slips, http://www.creditslips.org/creditslips/2017/08/guess-whos-supporting-predatory-lending.html (2017) ("[T]here's no problem with the world post-Madden, so why mess with things. But if a "fix" is needed, it ought to be (1) narrowly tailored, and (2) ensure maximum consumer protection. . . .[A]ny fix that goes beyond protecting securitizations by banks in which servicing is retained is facilitating predatory lending.").

application for an ILC charter was eventually withdrawn, but it led to a compelling policy argument about the optimal separation between banking and commerce.[35] Arthur E. Wilmarth, Jr., warned that allowing commercial firms to acquire ILCs would conflict with the general American financial policy of separating banking and commerce, generate systemic risk, and enable the resulting ILCs and their parent firms to avoid necessary regulatory scrutiny, since "FDIC does not have authority to exercise consolidated supervision over commercial owners of ILCs."[36] Professor Mehrsa Baradaran countered that, in some instances, allowing firms to merge banking and commerce functions could enhance the safety and soundness of the banking system.[37]

However, in this case, neither SoFi nor Square appear to be the type of commercial firms which would fit Baradaran's account, since they would not inject the source of strength that was praised by Baradaran in the Walmart scenario (a large and viable non-financial business) into the banking system. I agree with Professor Wilmarth that "Banking-industrial combinations would . . . create unfair competitive advantages for large commercial and industrial firms that can afford the costs of acquiring and operating banks."[38] Far more study of fintech as a sector is needed before the FDIC grants such applications. As Rep. Maxine Waters has observed, in a detailed letter to the FDIC calling for a public hearing on the issue, premature granting of applications for ILCs "would set a precedent that a wide variety of other fintech companies may choose to follow even though concerns related to financial inclusion, consumer benefits, supervision, and regulation of such entities are still unresolved."[39]

The Fed was right to call for the closure of the ILC loophole last year. Though there was an interesting scholarly debate after WalMart applied to obtain an ILC charter in 2006, some more recent, post-moratorium applicants do not appear to have the redeeming characteristics of a large commercial firm. They could also be acquired by other firms, further eroding the division between banking and commerce that lies at the heart of U.S. financial regulatory goals. As Professor Wilmarth has argued, given high concentration levels in the economy in general, and the technology sector in particular, "If we permit the formation of new banking-industrial conglomerates, we will be putting more of our eggs

[35] WalMart and several other commercial firms applied to acquire ILCs from 2005-2006.
[36] Arthur E. Wilmarth, Jr., *Wal-Mart and the Separation of Banking and Commerce*, 39 Conn. L. Rev. 1539 (2007).
[37] Mehrsa Baradaran, *Reconsidering the Separation of Banking and Commerce*, 80 George Washington Law Review 385 (2012).
[38] Arthur E. Wilmarth, Jr., *Beware the Return of the ILC,* American Banker, Aug. 2, 2017, at https://www.americanbanker.com/opinion/beware-the-return-of-the-ilc.
[39] Press Release, Waters Calls on FDIC to Hold Public Hearing on SoFi's Application for Bank Charter, at https://democrats-financialservices.house.gov/news/documentsingle.aspx?DocumentID=400739.

into very few baskets, and federal regulators will be under great pressure to protect those baskets during future financial and economic disruptions."[40]

III. Futurist Fintech

Though sober reports from the World Economic Forum, Deloitte, and governmental entities give a good sense of the incrementalist side of fintech, it is important to realize that much of the excitement about the topic of financial technology arises out of a more futuristic perspective. On Twitter, hashtags like #legaltech, #regtech, #insurtech, and #fintech often convene enthusiasts who aspire to revolutionize the financial landscape—or at least to make a good deal of money disrupting existing "trust institutions" (e.g., the intermediaries which help store and transfer financial assets).

Futurist fintech envisions "smart contracts," which would be executed via some degree of automatic, code-based enforcement.[41] As one article puts it, "Where a smart contract's conditions depend upon real-world data (e.g., the price of a commodity future at a given time), agreed-upon outside systems, called oracles, can be developed to monitor and verify prices, performance, or other real-world events."[42] However, until robotic assessments of physical reality are far less delayed, corroded by a lack of data, and contestable (thanks to the messy complexity of discordant human meanings), the prevalence of totally automated, smart contracts is likely to be limited.

There are many contractual relationships that are too complex and variable, and require too much human judgment, to be reliably coded into software. Code may reflect and in large part implement what the parties intended, but should not *itself* serve as the contract or business agreement among them.

Still, some technologists and lawyers aspire to that subsumption, echoing older movements for financial deregulation.[43] The rise of Bitcoin as an alternative currency has

---

[40] Arthur E. Wilmarth, Jr., *Beware the Return of the ILC,* American Banker, Aug. 2, 2017, at https://www.americanbanker.com/opinion/beware-the-return-of-the-ilc

[41] Joshua Fairfield, *Smart Contracts, Bitcoin Bots, and Consumer Protection*, 71 WASH. & LEE L. REV. ONLINE 35, 38—39 (2014) ("Smart contracts--automated programs that transfer digital assets within the block-chain upon certain triggering conditions--represent a new and interesting form of organizing contractual activity.").

[42] Nicolette De Sevres, Bart Chilton & Bradley Cohen, *The Blockchain Revolution, Smart Contracts and Financial Transactions*, 21 NO. 5 CYBERSPACE LAWYER 3, 3 (June 2016).A smart contract is created by encoding the terms of a traditional contract and uploading the smart contract to the blockchain. "Contractual clauses are automatically executed when pre-programmed conditions are satisfied," and because the transactions are monitored, validated, and enforced by the blockchain, there is no need for a trusted third party, such as an escrow agent. *Id.*

[43] DAVID GOLUMBIA, THE POLITICS OF BITCOIN (2016) (describing parallels between crytocurrency movement, crypto-anarchist beliefs, and older movements to discredit or dismantle financial regulation and central banking).

sparked an interest in automation of transactions and recordation.[44] Software can allow distributed computers to transfer information en masse and monitor one another.[45] Bitcoin is a particular case of using blockchain technology to ensure a durable record of ownership, which is intended to be regulated by code.[46] Blockchain enthusiasts envision it scaling en masse to serve as a distributed ledger of all manner of transactions.

Given enthusiasm expressed for blockchain at the highest levels of international finance,[47] governments may soon explore more extensive use of blockchain-based, public ledgers of ownership transactions, such as land records.[48] Such a digital transition would cut out a fair number of time-consuming steps in current financial processing. Using technology to modernize transactions would seem to be a huge opportunity for saving personnel costs and reducing inconvenience.

Yet there are also reasons for caution. As James Grimmelmann observed in 2005, "software is vulnerable to sudden failure, software is hackable, and software is not

---

[44] Joshua Fairfield, *Bitproperty*, 88 S. CAL. L. REV. 805, 805 (May 2015) ("Increased interest in cryptocurrencies has driven the development of a series of technologies for creating public, cryptographically secure ledgers of property interests that do not rely on trust in a specific entity to curate the list.").

[45] Michael J. Madison, *Social Software, Groups, and Governance*, 2006 MICH. ST. L. REV. 153, 156 (2006).

[46] Nicolette De Sevres & Bart Chilton & Bradley Cohen, *The Blockchain Revolution, Smart Contracts and Financial Transactions*, 21 NO. 5 CYBERSPACE LAWYER NL 3, 3 (June 2016). A blockchain is a peer-to-peer network where each computer in the network verifies and records every transaction on the network, where transactions are only recorded on the ledger once the network confirms the validity of the transaction, thus preventing third party manipulation and streamlining the record.

[47] World Economic Forum, *The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services*, (Aug. 2016) http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf; South African Reserve Bank, *Position Paper on Virtual Currencies*, (Dec. 3, 2014), https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf; *see also* David Mills, et. al., *Distributed ledger technology in payments, clearing and settlement*, Federal Reserve Board (2016) *available at* https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf.

[48] It is at this point unclear whether decentralization via distributed ledger technology would address or exacerbate key problems identified in the Mortgage Electronic Registration Systems, Inc. (MERS) in the wake of the financial crisis. Its implementation of "cloud computing" technology was meant to enable instantaneous transfers of ownership rights within the confines of a centralized database. MERS aspired to remove recording responsibilities from the state to a private entity owned by parties (mortgage lenders) with an interest in ownership disputes. Christopher L. Peterson, *Two Faces: Demystifying the Mortgage Electronic Registration System's Land Title Theory*, 53 WILLIAM AND MARY LAW REVIEW 111 (2011).

robust."[49] No technology has developed that would make the blockchain environment impervious to these problems. Waves of hacking and illicit intrusions have rocked health care institutions,[50] banks,[51] and even campaigns[52] and governments.[53] While blockchain enthusiasts claim that distributed ledgers help avoid the "honeypot" problem of database centralization (which is an inviting target for hackers), concentration of "mining power" could lead to a 51% attack on even a distributed ledger system. Excessive forking is also a threat to the integrity of such networks.

Moreover, some early adopters of this ideal of self-executing or coded law have experienced troubling and telling failures.[54] Investors in a "decentralized autonomous organization" (DAO) run on code have already experienced the turbulent and troubling aspects of software-governed legal orders. In early 2016, a hacker managed to take millions of dollars in a fashion unanticipated by the drafters of the code governing the organization. The main organizer of the DAO, Vitalik Buterin had to code a "hard fork" for the organization, which essentially shifted funds from the hacker's account to an account where the original investors in the project could withdraw their funds.[55]

According to Buterin and other organizers of the DAO, this intervention was a success story: it proved the recoverability of their system. But for advocates of futurist fintech, this was a Pyrrhic victory. The *post hoc* intervention violated the principle of autonomy supposedly at the core of the DAO.[56] Persons managed the smart contract—not mere code.[57] In other words, the only way the supposedly smart, incorruptible, automated,

---

[49] James Grimmelmann, *Regulation by Software*, 114 YALE L.J. 1719, 1742-44 (2005); see also James Grimmelmann, *Anarchy, Status Updates, and Utopia*, 35 PACE L. REV. 135 (2015) (demonstrating the persistence of governance problems in social software).

[50] *See* Jessica Jardine Wilkes, *The Creation of HIPAA Culture: Prioritizing Privacy Paranoia over Patient Care*, 2014 B.Y.U. L. REV. 1213 (2014) ("In 2009, the Office of Civil Rights started recording incidents of PHI breaches and created the "Wall of Shame," which publicly exposes breaches affecting 500 people or more").

[51] Paul Merrion, *NY Fed's role in SWIFT cyber heist prompts House panel data request*, WL 3085306, CQ ROLL CALL 2016. **(**describing hack of Bangladesh's central bank).

[52] Anthony J. Gaughan, *Ramshackle Federalism: America's Archaic and Dysfunctional Presidential Election System*, 85 FORDHAM L. REV. 1021 (2016). (discussing Russian hackers); Melissa Eddy, *After a Cyberattack, Germany Fears Election Disruption*, N.Y.TIMES, Dec. 8, 2016.

[53] Tim McCormack, *The Sony and OPM Double Whammy: International Law and Cyber "Attacks"*, 18 SMU SCI. & TECH. L. REV. 379 (2015).

[54] Nathaniel Popper, *A Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency*, N.Y. TIMES (June 17, 2016).

[55] Michael del Castillo, *The Hard Fork: What's About to Happen to Ethereum and the DAO*, COINDESK July 18, 2016, http://www.coindesk.com/hard-fork-ethereum-dao/; Vitalik Buterin, *Hard Fork Completed*, ETHEREUM BLOG (July 20, 2016), https://blog.ethereum.org/2016/07/20/hard-fork-completed/.

[56] Matt Levine, *Blockchain Company's Smart Contracts Were Dumb*, BLOOMBERG NEWS (June 17, 2016), https://www.bloomberg.com/view/articles/2016-06-17/blockchain-company-s-smart-contracts-were-dumb.

[57] *Id.*

and immutable contract actually protected investors was by *allowing human intervention to change its terms and consequences.* Rather than demonstrating the dispensability of human interventions, the DAO has proved the opposite—the vital necessity of human governance over even extensively coded and computerized forms of human cooperation.

When Primavera De Filippi and Samer Hassan speak of the "incorporation of legal rules into code" and "regulation by code," culminating in a reliance on code "not only to enforce legal rules, but also to draft and elaborate these rules," they do not present these phenomena as unalloyed goods.[58] Rather, they are cautious about the "the prospect of automated legal governance" because it may "reduce the freedoms and autonomy of individuals."[59] The answer to these concerns is not to double down on the translation of legal rules into code. Rather, the preservation of human control over financial systems will require an alternative paradigm—a vision of software as a tool to assist persons, rather than a machine replacing them. Nor should policymakers abandon long-standing principles of financial regulation to make way for forms of financial automation that have yet to be proven. There is little evidence that regulation means their "revolutionary promise" would be lost, as it was probably never there in the first place.[60]

IV. Conclusion

This testimony has presented reasons to be cautious about legislative or regulatory efforts to federally preempt state laws now applying to both incrementalist and futuristic fintech. I know that advocates for deregulation will likely argue that imposing a level playing field on fintech and non-fintech firms will harm innovation in the fintech sector. But innovation is not good in itself. The toxic assets at the core of the financial crisis were innovative in many ways, but ultimately posed unacceptable risks.[61] So, too, may the superficially attractive services of many fintech firms.

To be sure, promoters of fintech deregulation may claim that such worries are anecdotal. But many tech firms have only themselves to blame for obscuring what we know about the sector. As I explain in my book *The Black Box Society*, aggressive assertion of trade secrecy claims—both about data collection and use, and the algorithms used to make judgments about us—keep regulators and legislators in the dark about the full range of

---

[58] Primavera De Filippi & Samer Hassan, *Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Cod*e, FIRST MONDAY, 21 (12-5) (2016); http://firstmonday.org/ojs/index.php/fm/article/view/7113/5657#author.

[59] *Id.*

[60] ADAM GREENFIELD, RADICAL TECHNOLOGIES 303 (2017) ("the inventors of the blockchain overtly intended to erode statism and central administration. Virtually everywhere, decision algorithms are touted to us on the promise that they will permanently displace human subjectivity and bias. And yet in every instance we find that these ambitions are flouted, as the technologies that were supposed to enact them are captured…by existing concentrations of power.).

[61] JENNIFER TAUB, OTHER PEOPLE'S HOUSES (2015).

risks in fintech.[62] If there is any message I can deliver to the committee today, it is to empower agencies like CFPB and the OFR, and to expand their funding, as they try to come to grips with a rapidly financial landscape.

Data gathering is important, because nearly every story of technologized "financial inclusion" can be countered with other stories of exclusion, via digital redlining. As Cathy O'Neil's book *Weapons of Math Destruction* shows, consumers often are in the dark about what new algorithms are judging them, and how they can respond if they think they've been treated unfairly.[63] Regulators need to understand more fully what these firms are doing, and how they are performing. Moreover, as the recent Equifax hack shows, concentration of information in almost any firm creates great risks to consumers. Improving financial cybersecurity should be an essential goal in fintech policy.[64] I applaud the GAO for highlighting security issues in its report, and Senator Jack Reed for proposing forward-thinking legislation on this front.

We should not have faith that accelerated deregulation will free the financial sector to solve important social problems. The value proposition of some fintechs merely points out larger problems in existing credit provision that could be solved by more direct action. For example, if fintechs can make a hefty profit by refinancing student debts owed to the U.S. government, perhaps that is less an indication of fintechs' business prowess, than it is evidence that the government is overcharging students for loans.[65] If consumers are desperate for marketplace lending to cover next month's utility bills, maybe we need to ensure work pays more fairly, rather than plying them with digital loans. I am confident

---

[62] FRANK PASQUALE, THE BLACK BOX SOCIETY (2015).

[63] CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION (2016).

[64] Kristin Johnson, *Managing Cyber Risks*, 50 Ga. L. Rev. 547 (2016), at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2847234 (discussing SEC cyber-risk management disclosure obligations); Kristin Johnson and Steven Ramirez, *Sustainability: A New Guiding Principle for Financial Market Regulation*, 11 U. ST. THOMAS L. J. 386 (2015).

[65] Michael Simkovic, *The Knowledge Tax*, U. Chi. L. Rev. (2015), at http://chicagounbound.uchicago.edu/uclrev/vol82/iss4/4/; Marc Nerlove, *Some Problems in the Use of Income-contingent Loans for the Finance of Higher Education*, 83 J. POL. ECON. 157, 160, 180 (1975). When private sector refinancers can "cherry pick" or "cream skim" the most creditworthy borrowers from a federal credit program, that risk selection eventually leaves the government dependent on repayment by the worst credit risks. That erodes the sustainability of the federal loan program—and its borrower protections, like income based repayment. *See* Frank Pasquale, *Democratizing Higher Education: Defending & Extending Income Based Repayment Programs*, 28 LOY. CONSUMER L. REV. 1 (2015), at http://lawecommons.luc.edu/lclr/vol28/iss1/2, for more on the politics of public finance accounting and the role of private lenders in undermining the perceived and actual sustainability of federal credit programs.

that a system of postal banking would do far more than the fintech sector to deliver financial inclusion to the millions of Americans without adequate access to deposit accounts.[66]

In conclusion: Fintech should not be an excuse for more regulatory arbitrage. We need far more information about how fintech firms are gathering and processing data. And we should be wary about the ability of technology alone to solve much larger social problems of financial inclusion, opportunity, and fair, non-discriminatory credit provision.

[66] MEHRSA BARADARAN, HOW THE OTHER HALF BANKS (2015). Over 25% of US households are unbanked or underbanked. FDIC, *FDIC National Survey of Unbanked and Underbanked Households* (2016).