Testimony before the

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON FINANCIAL SERVICES
Task Force on Financial Technology

Regarding

"Preserving the Right of Consumers to Access Personal Financial Data"

September 21, 2021

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

Background & Summary

Chair Lynch, Ranking Member Davidson, distinguished Members of the Task Force, thank you for inviting me to testify. I offer my testimony as an Associate Research Scholar at Yale Law School. I am also the Deputy Director of the Law and Political Economy Project.[1] I have previously worked as an attorney for low-income consumers and served as Special Counsel to the Enforcement Director of the Consumer Financial Protection Bureau (CFPB).

My previous remarks before this task force have called for policymakers to consider the deeper impacts of nascent financial technologies on our society and principles of democracy. Today, I repeat the call for policymakers to adopt a bright-line, precautionary approach to technological developments involving financial products, sectors, and systems.[2] What industry calls "innovation" is often easily mapped to a longstanding financial service and therefore the substance of existing laws should govern.

However, in the cases when innovation is not easily mappable, it is often due to adoption of the tech company business model: mass data collection. Deeper changes in the information economy must inform regulatory responses. It is understandable to want regulations that endure the test of time. However, it is impossible to be truly "technology-neutral", as industry desires, because neither laws nor technologies are neutral. They are designed to serve some interests over others.

This morning, I have the luxury of presenting alongside Chi Chi Wu of the National Consumer Law Center (NCLC) and will defer to the NCLC on many urgent questions of consumer protection. Broadly, I agree that consumers deserve more control over their data relative to banks and other financial institutions. That said, consumer rights to access, review, manage, correct, and delete data about themselves can only be meaningful within a broader policy that minimizes data collection and inappropriate usage in the first place. Consumer control over financial data must operate within a broader paradigm of *data minimization:* collecting and processing only the minimum amount of data required to carry out an explicit, narrow purpose.[3]

Currently, every online interaction leaves "digital breadcrumbs" (purchasing histories, visited websites, and IP addresses, etc.) even if data collectors have not yet identified a purpose for the collection.[4] A mostly unregulated data broker industry adds payments and credit data to

---

[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." https://lpeproject.org/.

[2] *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).

[3] Data minimization means that only those data are processed (collected, stored, mined, inferenced, used for training algorithms) that are necessary. Mireille Hildebrandt, *Primitives of Legal Protection in the Era of Data-Driven Platforms*, 2 Geo. L. Tech. Rev. 252, 267 (2018).

[4] Evan I. Schwartz, *Finding Our Way with Digital Bread Crumbs*, MIT TECH. REV. (Aug. 18, 2010), https://www.technologyreview.com/s/420277/finding-our-way-with-digital-bread-crumbs/ [https://perma.cc/M4SY-VJ9Z].

data stocks regarding employment, marital status, homeownership status, medical conditions, and even our interests and hobbies, especially as articulated via social media. From the perspective of a human mind, there is too much data to process: the sets are too heterogeneous and the speed of analysis necessary to process them surpasses our abilities.[5] But predictive analytics take massive amounts of surface data and infer latent data from them: powerful institutions try to forecast the future with precision, in real-time, and at scale. Mass financial surveillance eventually creates a detailed picture of our most private social, familial, romantic, religious, and political activities, offering a "picture of the person behind the payment."[6]

Supporters of open banking are right that helpful data is underproduced and inequitably inaccessible to consumers given the centrality of reporting and scoring in our economy. Concern for consumer control also aligns with worries that big banks have monopolized data that could improve the profiles of consumers. Economists have argued for potential advantages to credit data sharing, including: increased competition in financial services markets; additional visibility, transparency, and completeness with respect to data dossiers; more efficient pricing of credit, debt management, and collection.[7] The U.S. government also uses financial data collection for purposes of the administrative state and security state.

However, under the current regime, harmful data is also overproduced. The business models of most fintech companies ultimately rely on *data maximization.* Data maximization leads to harms that may not be obvious or even immediate. They are not evenly distributed across society. Some of these harms sound more readily in the law than others.

Most obviously, screen-scraping enables data aggregators to get more data than needed, including sensitive PII that can be hacked, stolen, sold, or overly shared. However, as a structural matter, there are two key differences between the products of yesterday and today: the volume of data extracted by each participant, and the multiplication of participants in the service chain.[8] While a traditional credit card payment implicates a merchant, two banks and a payments processor, a payment made with a mobile wallet includes those parties and a mobile device maker, telecom or internet service provider, and often, but not always, a consumer-facing service provider that creates and manages the app that facilitates the payment. Each of the many entities involved in digital transactions may collect and share consumer data with other companies. While some data collection is necessary and appropriate, financial data collection tends to exceed this baseline. In many instances, financial service providers reserve broad rights to use consumer data for unrelated purposes. The roles of some of the parties involved are not always clear to consumers.[9]

---

[5] *See, e.g.,* Amy Kapczynski, *The Law of Informational Capitalism*, 129 YALE L.J. 1460, 1468 (2020).
[6] 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.
[7] Leon Yehuda Anidjar, Inbar Mizrahi-Borohovich, *Reinventing Credit Data Sharing Regulation*, 29 S. Cal. Interdisc. L.J. 177, 181–83 (2020).
[8] Consumer Reports, Comments to the CFPB in Response to the ANPR Regarding Consumer Access to Financial Records Under Section 1033 of the Dodd-Frank Act, Feb. 4, 2021. https://www.regulations.gov/comment/CFPB-2020-0034-0051
[9] NCLC Written Statement for CFPB's Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act, February 12, 2020, https://files.consumerfinance.gov/f/documents/cfpb_wu-statement_symposium-consumer access-financial-records.pdf

Financial data governance requires balancing the necessity of collecting highly personal and consequential information and the risk of harm that accompanies its processing. However, individual rights alone cannot account for the collective harms of datafication the flow within the financial system and beyond it. There are limits to the ways in which individual consumers can meaningfully make individual choices about how their personal data (or other people's data) can be used. The very point of data production in a digital economy is not to gain specific individual-level insights specific about specific data subjects. Rather, it is to put people into population-based relations with one another, and increasingly, to use a sample to make inferences about a class or population for the purpose of predicting behavior.[10] People may volunteer payments and credit data that, when aggregated by corporations and governments, confers sensitive information about disadvantaged groups in unpredictable ways. Consent to all data use is not possible in this context.

Like NCLC and other public interest organizations, I believe the laws on the books grant regulators authority that should be vigorously exercised. Existing rules and laws were meant to substantively protect consumers at the time of their drafting, but may not have not been sufficiently updated to account for the ways in which technology has changed the relationships between consumers and the companies with which they engage.[11] New rules and laws must establish the rights of consumers to review and correct this information, and to ask companies to delete information, but within demarcated boundaries for the collection, processing, holding, and "sharing" of consumer financial data.

Ultimately, Congress must shift the burden of data protection from consumer, courts, and litigators, to regulators and technology companies. The collision of Big Tech and Wall Street in this space demands especially careful scrutiny: the fintech field is now being swarmed not by quick and nimble entrepreneurs but the largest tech and finance companies.[12] Companies, whether fintech, techfins, or any other permutation, should not be collecting any data that is not strictly necessary for the provision of a good or service. For example, signing up for a credit card online should not lead to targeted advertising (or new accounts). We should not be able to forfeit our rights to data privacy and security, in particular, simply by clicking "I agree", or providing token consent to data usage policies consumers do not understand and firms cannot and do not uphold.

This is especially important as we consider practices of "financial inclusion." Most fintech business models rely on data maximization that renders marginalized communities more vulnerable. In perhaps its most dangerous instantiation, many tech and fintech

---

[10] For a general theory of data governance and democracy, informing this analysis, please see Salomé Viljoen, *Democratic Data: A Relational Theory for Data Governance* (Nov. 11, 2020). Yale L.J. forthcoming (unpublished manuscript) (manuscript at 3-9) (available at https://ssrn.com/abstract=3727562).

[11] *See,* e.g. Julie E. Cohen, *The Regulatory State in the Information Age*, 17 Theoretical Inquiries L. 369, 370 (2016) (arguing that the current regulatory institutions were designed in an era which industrialism was the principal mode of development and such institutions are not capable to deal with the challenges involved in the information age.)

[12] Zen Soo, *TechFin: Jack Ma Coins Term to Set Alipay's Goal to Give Emerging Markets Access to Capital*, South China Morning Post (Dec. 2, 2016, 9:38 PM), http://www.scmp.com/tech/article/2051249/techfin-jack-ma-coinstermset-alipays-goal-give-emerging-markets-access.

enterprises[13] are attempting to create a biometric "decentralized and portable digital identity" to substitute for government ID or functionally become the government ID in some places.[14] Many of these proposals involve biometric tools like facial recognition technology (FRT), iris-scanning, and palm prints, which are vehemently opposed by many privacy advocates.[15]

By law, this data is increasingly co-monitored by law enforcement via mass, pre-emptive, predictive, and perpetual surveillance. Poverty, family, criminal, immigration, and national security law have already made mass financial surveillance a channel for policing troubled by civil rights concerns. Moreover, the surveillance does not solve deeper issues of financial exclusion. The reasons people remain outside the financial mainstream in the United States are largely structural. Fintech applications are not solutions to structural problems.

As a general matter, the Bureau's regulatory, supervisory, and enforcement authorities were established at a different time, with a different technological terrain. The fintech industry's "endless capacity for self-referential growth"[16] suggests prudence on behalf of policymakers. This testimony makes six concrete policy recommendations:

1) **Section 1033 Rulemaking Should Promote Consumer Control in the Context of Data Minimization**

2) **FCRA Rulemaking Should Cement the Bureau's Authority over Data Aggregators**

3) **CFPB Rulemaking Should Grant the Bureau Authority to Supervise Data Aggregators**

4) **CFPB UDAAP Enforcement Should Center Unfair Data Collection**

5) **Congress Should Structurally Separate Commercial and Financial Power**

6) **Congress Should Constrain Data Usage to a Short List of Permissible Purposes**

---

[13] Leon Perlman & Nora Gurung, Focus Note: The Use of eKYC for Customer Identity and Verification and AML 8 (May 14, 2019), *available at* https://ssrn.com/abstract=3370665 (last visited June 22, 2020).

[14] S*ee* Ian Allison, *How Anti-Money-Laundering Rules Hinder Libra's Mission to Reach the Unbanked*, CoinDesk (Oct. 9, 2019), https://www.coindesk.com/how-anti-money-laundering-rules-hinder-libras-mission-to-reach-the-unbanked.; ET Bureau, *Aadhaar verdict: Telcos, banks & financial companies may feel the pinch*, The Econ. Times (Sept. 27, 2018), https://economictimes.indiatimes.com/news/politics-and-nation/aadhaar-verdict-telcos-banks-financial-companies-may-feel-the-pinch/articleshow/65973414.cms.

[15] Facial recognition software is likely to mislabel or misrecognize members of racial minority groups, especially Black Americans. *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. However, many civil rights advocates argue that the incompleteness of FRT databases is a good thing. Zoé Samudzi, "Bots Are Terrible at Recognizing Black Faces. Let's Keep It that Way," *Daily Beast*, February 8, 2019, https://www.thedailybeast.com/bots-are-terrible-at-recognizing-black-faces-lets-keep-it-that-way.

[16] *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.

Dodd-Frank & Data Governance

The main provision of Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank) in question today, Section 1033, has not yet been interpreted by the judicial system or any government agency.[17]

As we consider the scope of rulemaking under this provision, we should think of 1033 in the context of the CFPB's broader mission. No single agency is responsible for all matters regarding financial data governance, but the CFPB must deal with it under its own mandate. The CFPB is entrusted with enforcing federal consumer financial law to ensure that all consumers have "access to markets for consumer financial products and services and that markets for consumer financial products and services are fair, transparent, and competitive."[18] The Bureau is authorized to exercise its authority to ensure consumers are:

- (1) provided with timely and understandable information to make responsible decisions about financial transactions;
- (2) protected from unfair, deceptive, or abusive acts and practices and from discrimination;

Due its position at the "user interface" of the financial system, the CFPB is particularly well disposed to lead the way on financial data governance.[19] Financial datastreams often begin at the household level and are aggregated, disaggregated throughout the broader financial system, including capital markets.

The CFPB offers an example of an agency that avoids some of the major potential institutional challenges that other regulators might face: susceptibility to capture, a lack of technological sophistication, and insufficient authority. The CFPB embraced its identity as a 21st century, data-driven, technologically capable agency from the outset.[20] The CFPB hired a large number of computer engineers before becoming operational and has developed a suite of online digital tools for consumers.[21] Compared to the FTC, the CFPB has more authority to write rules, impose civil penalties, and supervise data collection.[22] More generally, it has the authority and power to meet the task of watching the watchers, ensuring consumer financial data is secure and bounded.[23]

---

[17] For timely legal analysis of data aggregators' relationships with banks, tech companies, and consumers in the context of Section 1033, see generally Nizan Geslevich Packin, *Show Me the (Data About the) Money!*, 2020 Utah L. Rev. 1277, 1288 (2020).
[18] 12 U.S.C. § 5511.
[19] *See* 12 U.S.C § 5495 (noting the Bureau shall coordinate with other regulators).
[20] K. Sabeel Rahman, *Envisioning the Regulatory State: Technocracy, Democracy, and Institutional Experimentation in the 2010 Financial Reform and Oil Spill Statutes*, 48 Harv. J. Legis. 555, 557 (2011).
[21] Rory Van Loo, *Technology Regulation by Default: Platforms, Privacy, and the CFPB*, 2 Geo. L. Tech. Rev. 531, 532 (2018).
[22] *Id.* at 531–32.
[23] *See* Rory Van Loo, *Rise of the Digital Regulator*, 66 Duke L.J. 1267 (2017) ("The unpleasant truth is that creating effective digital regulators would require investing heavily in a new oversight regime or sophisticated state machines.")

Consumer Financial Protection: From Market Power to Platform Power

Financial data collection has changed significantly since the passage of the Dodd-Frank Act. Technology companies entering the space are subject to far less regulation than traditional financial institutions.[24] It is now critical for policymakers to understand *platforms*: entities that generate and intermediate market activity by generating and intermediating data.[25] On its face, longstanding institutions in the financial system, including credit reporting agencies, fit this description. But analysis of payments and credit data increasingly represents a logical extension of the Silicon Valley platform business model.[26]

From the perspective of users, platforms make certain services more accessible or convenient. Platforms deploy additional services that expand the user base and yield more information, helping the platforms continually accumulate profits and power.[27] In a fashion familiar to financial regulators, dominant platforms produce "tranches" of data with corresponding predictive profiles, which they use to sell products to their users.[28] However, platforms also use these tranches for targeted advertising — essentially, to sell *access to their users* to third parties. Like mortgagors whose claims are bundled into mortgage-backed securities, surveilled users have no control over how our inputs are used for downstream products.[29] In one way or another, the platforms use our data to manufacture wealth for themselves.[30] Meanwhile, there is mounting evidence that commercial surveillance amplifies organized hate, junk science, and virulent nationalism, creates novel and potent pathways for discrimination, and generally facilitates unprecedented infringement of our rights to privacy, freedom of expression, and freedom of association.[31]

Among the network of platforms that increasingly define modern financial services are "data aggregators." When consumers use online banking and fintech apps (like Venmo) they are likely providing account information to data aggregators. In the U.S., roughly 50% of U.S. consumers are estimated to have signed up for financial apps or other products that frequently rely on data aggregators to collect information via authorized transfers.[32] The aggregation system is thought to reach about 95% of U.S. deposit accounts, and at least one aggregator estimates that it alone has connected to one in four financial accounts in the U.S.[33]

---

[24] *See* Kristin Johnson, Frank Pasquale & Jennifer Chapman, *Artificial Intelligence, Machine Learning, and Bias in Finance: Toward Responsible Innovation*, 88 Fordham L. Rev. 499, 505 (2019) (discussing the gaps in the supervision of FinTech companies and how that encourages them to engage in regulatory arbitrage).

[25] *See* Cohen, *supra* note 2, at 37-47 (2019) (outlining and discussing the historic transition from market-based to platform-based business activity).

[26] Platforms organized through the logic of networks provide "would-be counterparties with *access* to one another and techniques for rendering users *legible* to those seeking to market goods and services to them." *Id.* at 74, 182-187.

[27] *See*, *e.g.*, Bank for Int'l Settlements, BIS Annual Economic Report 2019 62-64 (2019), https://www.bis.org/publ/arpdf/ar2019e3.htm [hereinafter BIS Report]; Wilson C. Freeman & Jay B. Sykes, Cong. Research Serv., R49510, Antitrust and 'Big tech' 10 (2019), https://fas.org/sgp/crs/misc/R45910.pdf.

[28] *See* Cohen, *supra* note 2, at 69.

[29] *Id.* at 73.

[30] *Id.* at 70-73.

[31] *Id.* at 92, 239-250.

[32] Geslevich Packin, *supra* note 17, at 1286–87.

[33] Zack Meredith & Zeya Yang, Blog, The All-New Plaid Link, Plaid (Oct. 2, 2020); Michael Deleon, A Buyer's Guide to Data Aggregation, Tearsheet (Feb. 19, 2019).

Frequently, the data aggregator stores the login credentials of consumers and uses them to continually log into the consumer's bank account to copy all personally identifiable data, ranging from transaction information to account numbers. Once it has accessed consumer data, the data aggregator can share or sell that data without the consumer's knowledge, much less consent.

Even though they are not new entities,[34] as Nizan Geslevich Packin argues in a timely law review article, companies like Plaid, Intuit, Finicity, Envestnet|Yodlee, Morningstar/ByAllAccounts, Fiserv/CashEdge, and MX are "barely subject to any regulation, have received little scholarly attention, and most consumers have never even heard of them or know what they do."[35]

Data Security

More than 4,000 known data breaches have shaken markets during the last decade.[36] Data aggregators and all other companies share blame for breaches and hacks that have plagued consumers in a generally insecure system. As consumer advocates have long noted, the credit bureaus' loose matching procedures contribute significantly to the problem of identity theft. However, the general lack of regulation over data aggregators, means that if fintech apps have exploitable vulnerabilities, then the login credentials of accounts, including traditional bank accounts, could be jeopardized. Banks have maintained that if consumers share their credentials with third-parties and fraud takes place, liability protections like Regulation E--establishing the rights, liabilities, and responsibilities of participants in electronic fund transfer systems--will not be available for consumers. [37]

There is no federal law creating uniform nationwide standards for alerting consumers about data breaches or for providing simple dispute solving mechanisms. Since 2002, the FTC has exercised its authority over security in this space, but because its power is restricted to enforcement action, the agency cannot supervise or examine nonfinancial companies on an ongoing basis. All businesses are subject to state laws, but these laws are few and ineffective.[38]

FinTech companies' data gathering is typically done by one of two ways: (i) screen-scraping of public data from a website and (ii) APIs, a technology that enable programmers to integrate data from one source into third-party apps, restrict how apps tap data, and contractually limit the data's usages. Industry participants believe that the most dangerous type of data sharing is done via screen-scraping because data aggregators extract transaction information to populate their services and store and maintain the credentials, sometimes even after the relationship with the consumer ends. At least some consumer

---

[34] *See generally* Kimberly L. Wierzel, *If You Can't Beat Them, Join Them: Data Aggregators and Financial Institutions*, 5 N.C. Banking Inst. 457 (2001) (explaining that data aggregators enable consumers to turn over their different accounts' login credentials at various banks to one operator, which in turn lets them view all of their data from one site).

[35] Geslevich Packin, *supra* note 17, at 1286-1286.

[36] *Examining the Use of Alternative Data in Underwriting and Credit Scoring to Expand Access to Credit: Hearing Before the Task Force on Fin. Tech. of the H. Comm. on Fin. Serv.*, 116th Cong. 14 (2019) (statement of Kristin N. Johnson, Professor, Tulane Univ. L. Sch.).

[37] Geslevich Packin, *supra* note 17, at 1302-03.

[38] *Id.* at 1326.

groups agree that data aggregators' screen-scraping practices must be legally prohibited.[39]

Data Privacy

No overarching federal privacy law currently curbs the collection, use, and sale of personal data among corporations.[40] Millions of people are subject to data collection to which they may not have meaningfully consented. This is especially true in the payments space, where counterparties between networked payment "stacks" are constantly exposed to each other.

For purposes of financial privacy, FCRA remains the most relevant statute. Yet FCRA was drafted before concentrated computerized data sharing became the standard industry business model.[41] FCRA restricted data procurement to "a legitimate business need." Companies have easily argued that direct mail and targeted advertising programs constitute legitimate business needs.

Of course, 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.[42] According to Virginia Eubanks, social welfare agencies turned to cost-cutting technologies in periods of austerity.[43] 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 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."[44] As I have discussed in previous testimony, the mass surveillance scheme attending AML, CFT, and sanctions law creates other racialized harms. Financial institutions must generally assist police investigations requiring financial information and provide specific information to law enforcement agencies, including by filing SARs. Payments data now have different lives in the law enforcement sphere.

It was once easier to imagine a notice-and-consent regime would allow individual

---

[39] *See Complaint, Cottle v. Plaid, No. 4:20-cv-03056-DMR (N.D. Cal. May 4, 2020).*

[40] 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.

[41] 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).

[42] 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.

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

[44] 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/.

internet users on how to manage trade offs between convenience and privacy.[45] Managing how one's data is collected and used is now virtually impossible to do comprehensively. The best people can do is manage their privacy haphazardly.

Fair Competition

Unregulated surveillance may also spoil competition. Dominant platforms grow by expanding their platforms' user base and information access, securing revenue by selling products directly to their users or by selling access to their users to third parties.[46] As U.S. legal scholars and European antitrust authorities have concluded, data begets market power, but market power also allows dominant platforms to continually extract data in unfair ways.[47] For instance, Amazon already provides the cloud-computing systems that serve as the "technological backbone" of many fintech firms, which grants Amazon access to data other companies are structurally unable to obtain.[48] The company could easily take advantage of this data to unfairly compete with its existing fintech business partners.

Increased attention is especially necessary as more traditional financial institutions, including banks, credit card companies, and credit reporting agencies jostle with data aggregators over control of consumer financial data and the law governing its use. There are many dynamics at play. For instance, as antitrust advocates argue for open banking, data sharing appears to cut against the trend in the industry towards data privacy. In recent years, regulators have increasingly pushed financial institutions to strengthen their authentication procedures and cybersecurity processes in order to ensure that hackers do not gain unauthorized access to customer data.[49]

The API approach may fundamentally leave traditional financial institutions in the drivers' seat. If not approached thoughtfully, regulators history demonstrates that open access and interoperability requirements can actually serve as instruments by which dominant firms obtain and entrench their monopoly power.[50] Allowing users to interact with banks as platforms by incorporating APIs would allow third-parties to plug straight into the relevant code and data feeds. However, with additional regulatory guidance, API access could be limited to specific types of information and sharing.

---

[45] *See* Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1 (2021). *Cf.* Cohen, *supra* note 11, at 386 ("[C]urrent consumer protection paradigms framed in terms of notice and choice are ill-suited to address these issues, which are fundamentally issues of economic and social inclusion.")

[46] *See, e.g.*, BANK FOR INTERNATIONAL SETTLEMENTS, *supra* note 27.

[47] Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 518 (2019).

[48] John Detrixhe, *Amazon is invading finance without really trying*, QUARTZ (Nov. 1, 2017), https://qz.com/1116277/amazons-aws-cloud-business-is-reshaping-how-the-financial-services-industry-works/

[49] Cesare Fracassi & William Magnuson, *Data Autonomy,* 74 Vand. L. Rev. 327, 349–53 (2021).

[50] "Our paper tells the untold story of how the SEC's attempt to promote competition in US securities clearing and depository markets through mandated interoperability ultimately paved the way for the DTCC's current monopoly over these systemically important markets." Awrey, Dan and Macey, Joshua, *Open Access, Interoperability, and the DTCC's Unexpected Path to Monopoly* (July 12, 2021). Available at SSRN: https://ssrn.com/abstract=3885194 or http://dx.doi.org/10.2139/ssrn.3885194.

CFPB Recommendations

CFPB Section 1033 Rulemaking Should Promote Consumer Control in the Context of Data Minimization

In October 2017, the CFPB released a set of non-binding principles on the use of financial data.[51] In particular, the principles permit consumers to "authorize trusted third parties to obtain" their data "from account providers to use on behalf of consumers, for consumer benefit, and in a safe manner. The principles also provide guidance for third-party providers of services, stressing issues such as protecting consumers' data from security breaches, obtaining clear and informed consent from consumers, and limiting access to data. Yet the principles provided little clarity on key issues, including whether Section 1033 preserves third-parties' right to pull data directly from bank customers' accounts.

On its face, 1033 is a disclosure rule. Subject to rules prescribed by the Bureau, financial institutions must make available to a consumer information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data.[52]

The Bureau's rule may require financial institutions to make available to a consumer information relating to any transaction, series of transactions, or to the account including costs, charges and usage data.[53] Herein the Bureau should clarify their rights under the Electronic Funds Transfer Act (EFTA) as implemented by Regulation E (Reg E). Two areas need particular attention. In addition to establishing rights and responsibilities of providers, the Bureau should clearly enumerate what data is included in 1033 access rights, and should strictly prohibit the collection of certain data for any purpose.[54]

Sometimes overlooked is the duty of the Bureau to prescribe or promote standardized formats for information to be made available to consumers under this section.[55] Arguably, this provides the Bureau with something like entry restriction power: if companies cannot comply with 1033 by providing an accurate record of data usage per the terms of the rule, they should be deemed to be out of compliance with 1033 and penalized thoroughly. The Bureau's rulemaking may also standardize how consumer financial information is disclosed and at what level of understandability. The current disclosures required by the GLBA, which are intended to give consumers the opportunity to opt-out of the sharing of nonpublic personal information with third parties and to outline the company's data use practices, are so confusing that consumers are unlikely to exercise their rights.[56]

---

[51] CFPB, Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation (2017) [hereinafter CFPB Consumer Protection], https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf [https://perma.cc/QE69-87KQ].

[52] 12 USC 5533.

[53] *Id.*

[54] Christina Tetreault. Comments to the CFPB re Consumer Access to Financial records, https://files.consumerfinance.gov/f/documents/cfpb_tetreault-statement_symposium-consumer-access-financial-records.pdf.

[55] 12 USC 5533(d).

[56] Statement of Travis Plunkett, Legislative Director, Consumer Federation of America on Behalf of the

FCRA Rulemaking Should Cement the Bureau's Authority over Data Aggregators

FCRA is also centered around disclosure. Any CFPB rulemaking in this space should impose such criteria and establish minimum procedures to ensure maximum possible accuracy. Just as importantly, the scope of FCRA must be redefined. We must apply FCRA rights to information data aggregators have for consumers who are permissioning data access for FCRA purposes. However, any Bureau rulemaking in this area should also remove any doubt that financial data aggregators are subject to FCRA. If FCRA is to make any sense by its own legislative logic, it should be expanded to encompass alternative reporting systems.

The text of FCRA includes recursive definitions of "consumer reporting agency" and "consumer report" -- consumer reports are communications of credit-related information by consumer reporting agencies. There are a number of open questions as to whether data aggregators and other new intermediaries qualify as consumer reporting agencies.[57] Despite the FCRA's very broad definitions of "consumer report" and "consumer reporting agency," circuit courts have recently shown a reluctance to respect the FCRA's plain language and its expansive coverage. These cases have undermined FCRA protections with respect to its scope of coverage. For example, the *Zabriskie* decision has provided support to certain types of specialty CRAs, such as criminal background check and tenant screening agencies, that claim they are not covered by the Act because they merely provide software to end users.[58]

Like most consumer advocates, I agree it is essential that if these recommendations result in separate systems for FCRA and non-FCRA rights, that rules do not undermine FCRA coverage. If there is a controversy as to whether certain data qualifies as a "consumer report," for instance in the context of 1033 rulemaking, regulation should explicitly provide nothing in it shall be construed to limit or restrict the applicability of the FCRA.

CFPB Rulemaking Should Grant the Bureau Authority to Supervise Data Aggregators

Consumer advocates have argued the CFPB should promulgate a rule authorizing it to supervise all "data aggregators" for compliance with consumer financial protection laws.[59]

Consumer Federation of America, Consumers Union, and the U.S. Public Interest Research Group, before the U.S. Senate Comm. on Banking, Housing, and Urban Affairs (July 13, 2004), available at https://www.govinfo.gov/content/pkg/CHRG-108shrg26700/html/CHRG-108shrg26700.htm.

[57] Under the FCRA, information that nominally suits as a "consumer report" will not trigger the Act's requirements unless it is provided by an entity meeting the definition of a "consumer reporting agency" ("CRA"). *See* 15 USC § 1681a(f).

[58] In *Zabriskie v. Federal National Mortgage Association*, 912 F.3d 1192 (9th Cir. 2019), a divided panel of the Ninth Circuit held that Fannie Mae, which licenses its proprietary software program known as Desktop Underwriter to lenders, is not a CRA because its role is purportedly limited to providing this software that in turn allows lenders to assemble or evaluate information.
https://library.nclc.org/data-gatherers-evading-fcra-may-find-themselves-still-hot-water

[59] *See, e.g.*, EDITH RAMIREZ ET AL., FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY i-ix (2014), *available at* http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf?utm_source=govdelivery (suggesting the CFPB could define "large data brokers" as subject to its examination authority under 12 U.S.C. § 5514(a)(1)(B)); *Banking on Your Data: The Role of Big Data in Financial Services: Hearing Before the H. Comm. on Fin. Services*, 116th Cong. 20-21 (2019) (Statement of Lauren Saunders, Assoc. Dir., Nat'l Consumer Law Center), *available at*

Under existing privacy and data protection laws, such supervision only entails compliance with the aforementioned disclosure, notice-and-consent, and minimal information security rules, but 1033, FCRA, or UDAAP rulemakings could all augment the power of supervision.

As a condition of secure data management, the Bureau should insist that credit reports should be frozen by default to prevent identity theft and give consumers more control over their credit reports. The switch for access to our credit reports should automatically be set to "off."

Through its supervision power, the Bureau can also take the lead on algorithmic accountability. Rory Van Loo argues the CFPB has the clear statutory authority to examine financial institutions' non-public data, even without suspecting any wrongdoing, through its supervision group.[60] Most importantly for present purposes, their examination manual specifies that examiners can review computer program and system details. A review of these highlight reports indicates that examinations sometimes unearth problems in regulated entities' source code.

It is possible that the Bureau's authority could reach major tech companies that have developed payment systems. Once a platform has taken in consumer financial data, the company's overall data security practices would arguably be relevant to any determination of whether Apple, Amazon, or Facebook sufficiently safeguard the financial data they collect.[61]

Additionally, if fintechs share or sell customer information with third parties (including data brokers), the CFPB could impose requirements on how those third parties use that information indirectly, by holding the entity that the CFPB regulates--the fintech or bank--accountable for what the third party does with the information.

In the platform era, the CFPB should monitor platforms to ensure those companies are respecting users' privacy.[62] The information collected under these auspices can be limited to business data. Unlike crime agencies--which need users' identities to assess their personal targets--regulators are looking for wrongdoing by the business. They can analyze companies' internal policies and procedures, or even examine the code behind various algorithms, without obtaining any user data. Furthermore, for some harms requiring access to user accounts, it may be possible to provide the data to the regulator in de-identified form.

CFPB UDAAP Enforcement Should Center Unfair Data Collection

Should it find a violation of UDAAP or federal consumer financial law, the CFPB has broad enforcement powers.[63] It can not only use any remedies authorized by the individual enumerated consumer laws, but may also order "any appropriate legal or equitable relief" including, among other remedies, rescission of contracts, restitution, disgorgement, and civil money penalties. Against covered persons and service providers, it can issue cease-and-desist

---

https://www.nclc.org/images/pdf/cons-protection/testimony-lauren-saunders-data-aggregator-nov2019.pdf (arguing the same point).

[60] Van Loo, *supra* note 21, at 542–43.

[61] *Id.*

[62] *Id.*

[63] *See* Katherine M. Porter, Modern Consumer Law 171 (2016) (lauding the "flexibility" of UDAAP statutes because otherwise you leave legislatures to play "whack-a-mole").

orders or obtain consent orders in settlement of those proceedings. And for both covered and non-covered persons, the Bureau has the discretion to proceed in federal district court or through its own administrative procedure process. Finally, the Bureau may prescribe rules identifying specific practices as unfair, deceptive, or abusive acts or practices.[64]

The Biden Administration's inclusion of CFPB UDAAP authority in its recent Executive Order is welcome.[65] Section 1033 rulemaking and other changes should be considered alongside a tougher enforcement strategy. The CFPB could pursue its mission by bringing enforcement actions directly against financial institutions, tech companies providing financial services, and third-party service providers including data aggregators. In particular, the unfairness authority deserves increased attention.

A practice is "unfair" if it causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Bureau may consider established public policies as evidence to be considered with all other evidence.

Proving injury has become substantially more difficult in privacy and security cases in recent years. Rulemaking can clear this up. "Substantial injury" can include small harms inflicted on a large number of people.[66] More easily identifiable harms from flowing from financial data collection and sharing include cyber fraud, unauthorized transactions, and identity theft. If customers' credentials are jeopardized, they would be exposed to data and financial losses with very limited, if any, legal recourse. Similarly, focusing on the issue of credential sharing, banks have maintained that if consumers share their credentials with third-parties and fraud takes place, liability protections like Regulation E--establishing the rights, liabilities, and responsibilities of participants in electronic fund transfer systems--will not be available for consumers.[67]

"Reasonably avoidable" focuses on whether consumers have reason to anticipate the impending harm and the means to avoid it. As discussed, consumers typically have no idea data aggregators are even collecting their data. Yet aggregators are often given access to consumer accounts per contractual agreements with a financial services provider, although they are not regulated like financial services providers.

Lauren Willis has argued that the exploitation of false consumer beliefs about facts material to a transaction is an unfair trade practice.[68] Exploiting these beliefs fits comfortably within the existing definition of unfairness. Given the extremely widespread use of deceptive dark patterns by major retailers and app sellers, the only way for consumers to avoid such materials today would be to refrain from online commerce, which would be an unreasonable

---

[64] 12 U.S.C. § 5531(b).

[65] https://www.consumerfinancemonitor.com/2021/07/12/president-biden-issues-executive-order-encouraging-ftc-rule making-on-consumer-data-collection-cfpb-rulemaking-on-data-portability-and-cfpb-udaap-enforcement/

[66] *See, e.g.*, FTC v. Commerce Planet, 878 F. Supp. 2d 1048, 1078 (C.D. Cal. 2012) (holding that a small monthly charge, when assessed on many misled consumers, can constitute "substantial injury" (citation omitted)).

[67] Geslevich Packin*, supra* note 17, at 1302-03.

[68] *See* Lauren E. Willis, *Deception by Design*, 34 Harv. J.L. & Tech. 115 (2020).

demand to place on consumers and would harm both consumers and competition. Unfairness doctrine would thus act as a prophylactic against deceptive trade practices.

Under Director Corday, the Bureau virtually always asserted its "abusive" authority alongside claims of an unfair or deceptive act or practice. To the extent that algorithmic lenders use their credit-scoring models to engage in predatory lending practices, especially via unsubstantiated claims about the use of artificial intelligence and machine learning in financial services, the CFPB should use its "abusiveness" authority to curtail those practices.[69]

Congressional Recommendations

Congress Should Structurally Separate Commercial and Financial Power

Smart enforcement of Section 1033 could give consumers control over their financial data, which should make it easier for them to switch between banks and other financial institutions, which could make them less reliant on the nation's largest and most politically powerful banks, the big three credit reporting bureaus, and Mastercard and Visa's duopoly over payment processing.[70] Just as the CFPB opens the space for competition, though, legislators should reestablish a bright line between the ownership of large tech companies and the ownership of financial institutions. We need structural partitions between commerce and banking, profit-driven enterprise and "money creation", and platforms and payment systems.[71] Even smaller tech and fintech companies are now acquiring regulated banks.[72]

Congress Should Constrain Data Usage to a Short List of Permissible Purposes

No overarching federal privacy law currently curbs the collection, use, and sale of personal data among corporations.[73] Congress should take action to minimize *all* data collection to that which is narrowly tailored to permitted usages.[74] However, in doing so, Congress must go beyond the notion of the notice-consent standard, where consumers are expected to decide to permit — or forbid — use of their data. This standard supports data collection, but fails

---

[69] Matthew Adam Bruckner, *The Promise and Perils of Algorithmic Lenders' Use of Big Data*, 93 Chi.-Kent L. Rev. 3, 47–49 (2018).

[70] https://www.huffpost.com/entry/the-obscure-biden-administration-rule-that-could-help-americans-flee-big-banks_n_606e0dd0c5b6034a708417e9

[71] *See* Letter from Ams. for Fin. Reform Ed. Fund and Demand Progress Ed. Fund to H. Comm. on the Judiciary (Apr. 17, 2020), https://ourfinancialsecurity.org/2020/04/joint-letter-promote-tradition-of-separating-banking-and-commerce-regarding-dominant-platforms/ (arguing for the structural separation of large tech platforms and payments).

[72] *See, e.g.*, Hugh Son, *LendingClub buys Radius Bank for $185 million in first fintech takeover of a regulated US bank,* CNBC (Feb. 18, 2020), https://www.cnbc.com/2020/02/18/lendingclub-buys-radius-bank-in-first-fintech-takeover-of-a-bank.html.

[73] 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

[74] In the FCRA, the term "permissible purposes" is also far broader than credit. Three of these purposes are for credit, insurance, or employment. But a permissible purpose also includes use for government benefits, licenses, and the FCRA "catch-all" purpose of a "legitimate business need for the information – (i) in connection with a business transaction that is initiated by the consumer,…" 15 U.S.C. § 1681b(a)(3)(F)(i). For more on these "permissible purposes," see National Consumer Law Center, Fair Credit Reporting (9th ed. 2017), updated at www.nclc.org/library.

consumers, as they are frequently determined to have "consented" to mass data collection and unknown down-stream uses. The FCRA established essential accuracy requirements for the data used in credit assessment tools, but consumers and their advocates carry the full burden of identifying and disputing inaccuracies.[75] While consumers should certainly have a right to notice (and to appeal of inaccuracies), it is not reasonable to believe that if consumers are provided with better information to assist them in making the right decisions as consumers, we will have met the greater challenges of financial data governance.

Nearly 7 in 10 Americans think companies use personal data in ways they're comfortable with — about the same number who admit they never or only sometimes read privacy policies.[76] The very notion of digital consent has been complicated by "dark patterns" and other technology platforms used to exploit limits in user cognition and understanding.[77] Consumers typically have no knowledge of what they are consenting to on the internet.[78] Many experts argue the existing notice-and-consent regime does nothing to curb commercial surveillance.[79] Definitionally, the notice-and-consent paradigm cannot empower people to protect their privacy because, when people agree to share data, they do not know what they are really revealing or to what end.[80] Critically, corporate and government actors frequently do not even know the purpose until *after* they analyze an aggregated data set and identify the proxies.

The appropriate approach is to create bright-lines with respect to data collection in the first place. Sen. Sherrod Brown's Data Accountability and Transparency Act, released in discussion draft form in 2020, would prohibit most collection and sharing of personal data as its starting point.[81] Data could only be used in ways stipulated in the law, wherein collection is limited to that which is "strictly necessary" for a permissible purpose, such as providing a service a consumer asked for — and no more. Not permitted: using data for alternate purposes, holding onto it longer than necessary to carry out the original purpose, or sharing it unless that's needed for the original purpose. One goal of his bill is thus to disrupt the business models of targeted advertising firms. Yet it still leaves a place for ads based on the contents of an ongoing search, for instance.

This sort of bright-line approach appropriately shifts the burden of privacy protection

---

[75] Anidjar & Inbar Mizrahi-Borohovich, *supra* note 7, at 197.

[76] https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/

[77] *See, e.g.*, Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1461-1478 (2019) (borrowing a definition of dark patterns as"'tricks used in websites and apps that make you buy or sign up for things that you didn't mean to.'"). For instance, consent could be gained by inserting a clause in extensive terms and conditions. *See, e.g.,* Thibault Schrepel, *Libra: A Concentrate of 'Blockchain Antitrust',* 118 MICH. L. REV. ONLINE 160, 166 (2020).

[78] Comment from Freedom from Facebook to FTC (Aug. 20, 2018), https://www.ftc.igov/system/files/documents/public_comments/2018/08/ftc-2018-0051-d-0008-147767.pdf.

[79] *See, e.g.*, Nizan Geslevich Packin & Yafit Lev-Aretz, *Big Data and Social Netbanks: Are You Ready to Replace Your Bank?*, 53 HOUS. L. REV. 1211, 1279–81 (2016); Nathan Newman, *How Big Data Enables Economic Harm to Consumers, Especially to Low-Income and Other Vulnerable Sectors of the Population*, 18 J. INTERNET L. 11, 19 (2014).

[80] 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, 453–61 (2020).

[81] *See* Press Release, Brown Releases Proposal to Protect Consumers Privacy, Jun. 18, 2020, *available at* https://www.brown.senate.gov/newsroom/press/release/brown-proposal-protect-consumers-privacy/.

away from consumers, who have minimal resources to protect themselves, and toward corporations, which profit immensely from the aggregation of our data. In a boon to security concerns, personal data would not be retainable beyond a period of time *strictly necessary* to carry out a permissible purpose. The bill's ban on discriminatory uses of personal data, and the safeguards it would put in place against unfair algorithmic decision-making, address serious and growing dangers to equity.

Passage of legislation of this type would mean that certain kinds of data would be prohibited at the point of generation. In addition to banning the collection, use or sharing of personal data unless specifically allowed by law, DATA 2020 bans the use of facial recognition technology and prohibits the use of personal data to discriminate in housing, employment, credit, insurance, and public accommodations (subject to minimal exceptions).

The bill aligns with the general idea that non-credit uses of credit reports and scores should be greatly limited. Policymakers, advocates, fintech companies, and the credit industry incumbents have all promoted alternative sources of data as the solution to credit invisibility.[82] While there is promise in some forms of alternative data, there are also significant risks. A bad credit history is more harmful than no credit history, and alternative data will not mitigate racial wealth disparities. There is no good evidence for the use of credit reports in employment, and its use in rental housing and insurance is also highly problematic. Some data shows promise, other data is a mixed bag, and some data is harmful enough that it should not be used. According to NCLC, the collection of gas and electric utility data for credit scoring is likely net harmful. Rental and telecommunications data could be promising, but carry significant risks, including the replication of racial inequity. Finally, many consumer advocates have argued that medical data should not be collected for credit scoring purposes.[83]

Given the racial injustices perpetrated by law enforcement, it is concerning that fintechs might collect more geolocation or biometric data.[84] Geolocation data revealed by payment histories is uniquely difficult to anonymize.[85] Privacy and racial justice advocates vehemently oppose the use of biometric tools like facial recognition technology, iris-scanning, and palm prints.[86] Facial recognition software is likely to mislabel or misrecognize members of racial

---

[82] Consumer Financial Protection Bureau, Data Point: Credit Invisibles, May 2015, http://files.consumerfinance.gov/f/201505_cfpb_data-point-credit-invisibles.pdf. *See also* 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) (illuminating how scoring by fintech lenders construct 'digital character' in a manner that can be opaque and discriminatory).

[83] Consumer Fin. Prot. Bureau, Market Snapshot: Third-Party Debt Collections Tradeline Reporting, July 2019 ("More than half (58 percent) of total third-party debt collections tradelines were for medical debt alone"), https://files.consumerfinance.gov/f/documents/201907_cfpb_third-party-debt-collections_report.pdf#page=13.

[84] *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/.

[85] *See, e.g.,* Cahn & Giddings, *supra* note 6.

[86] *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).

minority groups, especially Black Americans.[87] 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.[88]

Financial Inclusion in the Informational Economy

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.[89]

"Access to credit" talk pervades the current discourse of financial rights and equality for low-income communities. However, as 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.[90] 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.[91]

The intensity of data collection in consumer finance demands reflection about the role of banking and credit in the economy. 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

---

[87] *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.

[88] *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).

[89] 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").

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

[91] *Id.* at 1093.

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 invasions of their privacy in order to participate in the financial system.

Financial technology can provide great benefits to society, but only if shaped by policymakers' own forward thinking about services people need in an informational economy.[92] Policymakers must avoid being swayed by general promises of 'innovation' and create systems for real accountability on behalf of the public.

[92] In previous testimony, I have urged Congress to establish privacy-respecting public options for real-time payments, safe deposits, international money transfer, and other basic digital financial services, as well as ensuring affordable, reliable internet access for these services to work. Public sector innovation is necessary to truly regulate the space, and privacy and public sector innovation need not conflict. *See, e.g., License to Bank: Examining the Legal Framework Governing Who Can Lend and Process Payments in the Fintech Age, Hearing Before the Task Force on Financial Technology of the Committee on Financial Services*, 116th Cong. (Statement of Raúl Carrillo, Policy Counsel, Demand Progress Education Fund & Fellow, Americans for Financial Reform Education Fund), https://www.congress.gov/116/meeting/house/111057/witnesses/HHRG-116-BA00-Wstate-CarrilloR-20200929.pdf.