Vanderbilt Law Review

Volume 74
Issue 2 *March 2021*

Article 6

3-2021

Data Autonomy

Cesare Fracassi

William Magnuson

Data Autonomy

*Cesare Fracassi**
*William Magnuson***

In recent years, "data privacy" has vaulted to the forefront of public attention. Scholars, policymakers, and the media have, nearly in unison, decried the lack of data privacy in the modern world. In response, they have put forth various proposals to remedy the situation, from the imposition of fiduciary obligations on technology platforms to the creation of rights to be forgotten for individuals. All these proposals, however, share one essential assumption: we must raise greater protective barriers around data. As a scholar of corporate finance and a scholar of corporate law, respectively, we find this assumption problematic. Data, after all, is simply information, and information can be used for beneficial purposes as well as harmful ones. Just as it can be used to discriminate and to embarrass, information can be used to empower and to improve. And while data privacy is often pitched at ending unauthorized data sharing, it all too often leads simply to the end of data sharing, period. This comes at a cost. Data silos can inhibit consumer choice, protect the positions of powerful incumbents, and reduce the efficiency of markets. The best example of these costs comes from the financial industry. For more than a century, banks and other financial institutions have built their information technology systems to keep financial records as private and nonshareable as possible. While security concerns can be a primary reason for such closed systems, banks also understand that financial data is an advantage that can protect them from market entry and competition. Banks can hold up consumers with unfavorable rates and inferior products as a result, and a set of market failures make it difficult for consumers to opt out. First, information asymmetries between consumers and financial institutions are large and difficult to resolve. Second, search and switch costs—the difficulty of finding out more information about the risks and benefits of financial products and of switching to a better financial service—are high in the financial industry. Finally, individuals struggle to take

* Associate Professor, University of Texas, McCombs School of Business; Ph.D. in Finance, UCLA; M.B.A., UCLA; B.A., Politecnico di Milano.

** Associate Professor, Texas A&M University School of Law; J.D., Harvard Law School; M.A., Università di Padova; A.B., Princeton University. The authors wish to thank Jane Barratt, Bose Chan, Rebecca Mulholland, John Pitts, Emmet Rennick, Sam Taussig, Nick Thomas, Rory Van Loo, and Glenn S. Lunney, Jr., for their suggestions and advice. The authors also wish to thank Tony Ho for helpful research assistance.

advantage of even simple financial strategies to save, borrow, and invest. Data sharing can help resolve these problems. The emergence of a new regulatory and technological framework called "open banking" raises the possibility of consumers being able to task trusted intermediaries with automatically analyzing their financial data, nudging them to achieve their goals, and switching them to better products, all in order to reduce the substantial inefficiencies in their financial lives. There is one problem, however. A combination of market failure and regulatory ambiguity has led to a situation in which data is limited, siloed, and inaccessible, thereby preventing individuals from using their data in efficient ways. Ultimately, this Article contends, resolving these problems will require us to replace the clarion call of "data privacy" with a new, more comprehensive concept, that of "data autonomy"—the ability of individuals to have control over their data. Data autonomy balances the need for data to be protected and secure with the need for it to be accessible and shareable. In this Article, we lay out a set of key principles that grant individuals a legal right to data autonomy, including a right of ownership over data, as well as obligations on institutions to safely share standardized and interoperable data with third parties that consumers so choose. Perhaps counterintuitively, the only way of expanding consumer welfare and protection today is by breaking down the barriers of data privacy.

INTRODUCTION

In recent years, "data privacy" has vaulted to the forefront of public attention. Major newspapers have written exposés about the myriad ways in which technology companies are exploiting and monetizing our data.[1] Congress has held hearings to question tech CEOs on the data practices of their businesses.[2] And regulators have begun to turn their attention to the topic as well, issuing fines and enacting rules to both punish and prevent shoddy data privacy protections.[3] All these efforts have been driven by the widespread perception that the pervasive use of technology in today's world has seriously harmed the legitimate privacy interests of citizens.

In response to these concerns, scholars have proposed a variety of reforms. Some have argued that we need to impose fiduciary duties on technology platforms, requiring them to act in the best interest of their users.[4] Others have argued that we need to create a new "right to be forgotten," allowing users to force internet companies to remove

---

1. *See* Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html [https://perma.cc/7DN4-BS8B]; Sam Schechner & Mark Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook.*, WALL ST. J. (Feb. 22, 2019, 11:07 AM ET), https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636 [https://perma.cc/V4A7-67H4]; Geoffrey A. Fowler, *I Found Your Data. It's for Sale.*, WASH. POST (July 18, 2019, 7:00 AM CDT), https://www.washingtonpost.com/technology/2019/07/18/i-found-your-data-its-sale/ [https://perma.cc/4BED-LUDA]; Carly Minsky, *Is Consumer Protection Legislation Fit for Purpose?*, FIN. TIMES (Nov. 19, 2019), https://www.ft.com/content/3901dd14-ca55-11e9-af46-b09e8bfe60c0 [https://perma.cc/5S7S-JTC5].

2. *See* Kevin Roose & Cecilia Kang, *Mark Zuckerberg Testifies on Facebook Before Skeptical Lawmakers*, N.Y. TIMES (Apr. 10, 2018), https://www.nytimes.com/2018/04/10/us/politics/zuckerberg-facebook-senate-hearing.html [https://perma.cc/P3UP-9ZR9]; Ryan Tracy, *Tech Giants Draw Fire in Congress*, WALL ST. J. (July 16, 2019, 7:05 PM ET), https://www.wsj.com/articles/congress-puts-big-tech-in-crosshairs-11563311754 [https://perma.cc/QHK5-WVWP].

3. *See* Emily Glazer, Ryan Tracy & Jeff Horwitz, *FTC Approves Roughly $5 Billion Facebook Settlement*, WALL ST. J. (July 12, 2019, 6:43 PM ET), https://www.wsj.com/articles/ftc-approves-roughly-5-billion-facebook-settlement-11562960538 [https://perma.cc/FJT8-RVKH]; Craig A. Newman, *The S.E.C. Dusts Off a Never-Used Cyber Enforcement Tool*, N.Y. TIMES (Oct. 8, 2018), https://www.nytimes.com/2018/10/08/business/dealbook/voya-sec-cyber.html [https://perma.cc/9NL8-ZEZH]; Tony Romm, *DOJ Issues New Warning to Big Tech: Data and Privacy Could Be Competition Concerns*, WASH. POST (Nov. 8, 2019, 2:22 PM CST), https://www.washingtonpost.com/technology/2019/11/08/doj-issues-latest-warning-big-tech-data-privacy-could-be-competition-concerns/ [https://perma.cc/3RUN-JHTP].

4. *See* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1205 (2016); Jonathan Zittrain, *How to Exercise the Power You Didn't Ask For*, HARV. BUS. REV. (Sept. 19, 2018), https://hbr.org/2018/09/how-to-exercise-the-power-you-didnt-ask-for [https://perma.cc/UW6W-FDYN]; Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, ATLANTIC (Oct. 3, 2016), https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/ [https://perma.cc/Y28R-QJF8].

personal information from their websites.[5] Still others assert that we need to grant individuals broader rights to sue technology companies for data privacy violations.[6] The assumption underlying these proposals is that we need to raise greater protective barriers around data.

As scholars of corporate finance and corporate law, we find this assumption troubling, or at least incomplete. Data, after all, is simply information. Information can be used for any number of purposes, some of which are problematic, of course, but many of which are in fact quite desirable. Just as information can be used to discriminate and embarrass, it can also be used to empower and improve.[7] Indeed, one of the core goals of financial regulation is to encourage, and in some cases require, the disclosure of useful information in order to make markets fairer and more efficient.[8] Data sharing, thus, is a tremendously powerful tool for social good.[9]

This is not to say that data privacy is not valuable as well. It certainly is, and any well-designed regulation needs to be deeply concerned with protecting it.[10] But the ability to share information is just as important as the ability to hide it. Too often, data privacy

---

5. *See, e.g.*, Jenny Roberts, *Expunging America's Rap Sheet in the Information Age*, 2015 WIS. L. REV. 321 (calling for mechanisms to remove criminal convictions from private background check databases after records are sealed or expunged); Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1, 43 (2013); Jason Mazzone, *Facebook's Afterlife*, 90 N.C. L. REV. 1643 (2012).

6. *See* Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 109 (2014); Jane Yakowitz Bambauer, *The New Intrusion*, 88 NOTRE DAME L. REV. 205, 235 (2012); Derek E. Bambauer, *Exposed*, 98 MINN. L. REV. 2025, 2052 (2014); *see also* Omri Ben-Shahar, *Data Pollution*, 11 J. LEGAL ANALYSIS 104, 109 (2019).

7. *See, e.g.*, Ronald J. Gilson & Reinier H. Kraakman, *The Mechanisms of Market Efficiency*, 70 VA. L. REV. 549 (1984); Frank H. Easterbrook & Daniel R. Fischel, *Mandatory Disclosure and the Protection of Investors*, 70 VA. L. REV. 669 (1984); Roberta Romano, *Empowering Investors: A Market Approach to Securities Regulation*, 107 YALE L.J. 2359 (1998); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).

8. *See* Victor Brudney, *Insiders, Outsiders, and Informational Advantages Under the Federal Securities Laws*, 93 HARV. L. REV. 322, 334 (1979); John C. Coffee, Jr., *Market Failure and the Economic Case for a Mandatory Disclosure System*, 70 VA. L. REV. 717, 722 (1984); Paul G. Mahoney, *Mandatory Disclosure as a Solution to Agency Problems*, 62 U. CHI. L. REV. 1047, 1047–48 (1995). *But see* Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647, 651 (2011).

9. On the importance of information sharing for empowering better decisionmaking and more efficient transactions, see George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q.J. ECON. 488, 488 (1970); Dwight M. Jaffee & Thomas Russell, *Imperfect Information, Uncertainty, and Credit Rationing*, 90 Q.J. ECON. 651, 664 (1976); Michael Spence, *Competition in Salaries, Credentials, and Signaling Prerequisites for Jobs*, 90 Q.J. ECON. 51, 52 (1976).

10. *See*, *e.g.*, Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998); A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461 (2000); James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1 (2003).

reforms have tended to favor the latter value over the former.[11] While they have been aimed at preventing *unauthorized* data sharing, they have often simply prevented data sharing at all.[12] This comes at a cost. Data silos—where data is stored by a company, but in a way that it is inconvenient to access or use—can inhibit consumer choice, protect the positions of powerful incumbents, and reduce the efficiency of markets.[13] We need to find a better balance.

This Article explores these problems by examining the world of financial data, an area that has seen an explosion of interest in recent years from Wall Street, Silicon Valley, and, just as importantly, Washington.[14] Despite the fact that the financial sector plays a very important role in the economy, efficiency within the sector has remained remarkably stagnant over the last century. The low level of productivity growth can be traced to weak competition in the financial sector, as incumbents enjoy oligopoly rents and underinvest in technological innovation.[15] Three main reasons can explain this lack of competition. First, the financial regulatory environment is complex and fragmented, causing high regulatory compliance costs and high barriers to entry. Second, banks hold up consumers with expensive and lower quality services, as information asymmetries between consumers and financial institutions are large and hard to resolve, and the search and switch costs involved in identifying and comparing financial products

11. *See* discussion *infra* Section II.E (examining how regulatory solutions to the issues identified have played out in other jurisdictions).

12. The Gramm-Leach-Bliley Act, for example, contains a broadly constructed privacy rule, prohibiting banks from "disclos[ing] to a nonaffiliated third party any nonpublic personal information [about a consumer]," but also includes an exception providing that the requirements for data privacy do not apply for data sharing "with the consent or at the direction of the consumer." *See* Gramm-Leach-Bliley Act of 1999, 15 U.S.C. § 6802(a), (e)(2).

13. *See* discussion *infra* Section I.A (exploring theories that explain why the financial sector has made little progress with respect to efficiency despite massive technological advances).

14. *See Masters of the Universe: The Rise of the Financial Machines*, ECONOMIST (Oct. 3, 2019), https://www.economist.com/leaders/2019/10/03/the-rise-of-the-financial-machines [https://perma.cc/VUZ6-RDAT]; Rochelle Toplensky, *Data and Deregulation Fuel the Global Fintech Boom*, WALL ST. J. (Nov. 22, 2019, 5:38 AM ET), https://www.wsj.com/articles/data-and-deregulation-fuel-the-global-fintech-boom-11574419137 [https://perma.cc/YA8N-8FUP]; Emily Birnbaum, *Lawmakers Call for FTC Probe into Top Financial Data Aggregator*, HILL (Jan. 17, 2020, 11:13 AM EST), https://thehill.com/policy/technology/478766-lawmakers-call-for-ftc-probe-into-top-financial-data-aggregator [https://perma.cc/Y528-879T].

15. *See* Lawrence M. Ausubel, *The Failure of Competition in the Credit Card Market*, 81 AM. ECON. REV. 50, 76 (1991); Victor Stango, *Pricing with Consumer Switching Costs: Evidence from the Credit Card Market*, 50 J. INDUS. ECON. 475, 489 (2002); Rory Van Loo, *Making Innovation More Competitive: The Case of Fintech*, 65 UCLA L. REV. 232, 242–48 (2018) [*hereinafter* Van Loo, *Making Innovation More Competitive*]; Rory Van Loo, *Broadening Consumer Law: Competition, Protection, and Distribution*, 95 NOTRE DAME L. REV. 211, 213 (2019) [*hereinafter* Van Loo, *Broadening Consumer Law*]; Carin van der Cruijsen & Maaike Diepstraten, *Banking Products: You Can Take Them with You, So Why Don't You?*, 52 J. FIN. SERVS. RSCH. 123, 124 (2017).

are high.[16] Finally, individuals often do not act as purely rational decisionmakers in their financial lives.[17] They fail to save, they fail to diversify, and they fail to take advantage of simple strategies that could substantially improve their financial positions.[18]

Data can help solve these problems. Over the last decade, a number of financial technology ("fintech") companies have sprung up, better serving consumers by automating and optimizing financial transactions.[19] Using a combination of big data, artificial intelligence, and mobile computing, these fintech companies have attempted to resolve the inefficiencies that bedevil consumers in the market.[20] They have both the expertise and the incentives to learn about consumer preferences, search for information about financial products, and take advantage of price differentials.[21] Their innovations have the potential to dramatically improve individuals' access to beneficial banking services.

But the promise of fintech has been held back by one essential feature of today's financial landscape: the lack of data. While financial institutions create and manage enormous amounts of data on a daily

16. *See* Liran Haim, *Rethinking Consumer Protection Policy in Financial Markets*, 32 J.L. & COM. 23, 36–44 (2013); Todd J. Zywicki, *The Economics and Regulation of Bank Overdraft Protection*, 69 WASH. & LEE L. REV. 1141, 1146–47 (2012).

17. *See* Raghuram G. Rajan, *Insiders and Outsiders: The Choice Between Informed and Arm's-Length Debt*, 47 J. FIN. 1367 (1992); Kathleen C. Engel & Patricia A. McCoy, *A Tale of Three Markets: The Law and Economics of Predatory Lending*, 80 TEX. L. REV. 1255, 1258 (2002); Edward B. Rock, *Foxes and Hen Houses?: Personal Trading by Mutual Fund Managers*, 73 WASH. U. L.Q. 1601, 1621–22 (1995); Jacob Hale Russell, *The Separation of Intelligence and Control: Retirement Savings and the Limits of Soft Paternalism*, 6 WM. & MARY BUS. L. REV. 35, 41 (2015); James J. Choi, David Laibson, Brigitte C. Madrian & Andrew Metrick, *For Better or for Worse: Default Effects and 401(k) Savings Behavior*, *in* PERSPECTIVES ON THE ECONOMICS OF AGING 81, 81–82 (David A. Wise ed., 2004); Brad M. Barber & Terrance Odean, *Trading Is Hazardous to Your Wealth: The Common Stock Investment Performance of Individual Investors*, 55 J. FIN. 773, 774 (2000); Deborah M. Weiss, *Paternalistic Pension Policy: Psychological Evidence and Economic Theory*, 58 U. CHI. L. REV. 1275, 1276–77 (1991).

18. *See* discussion *infra* Section I.B (explaining that although the arrival of fintech and big data have dramatically altered the amount of information available to investors, the U.S. financial sector has not yet seen efficiency gains).

19. *See* Rory Van Loo, *Digital Market Perfection*, 117 MICH. L. REV. 815, 863 (2019); Benjamin P. Edwards, *The Rise of Automated Investment Advice: Can Robo-Advisers Rescue the Retail Market?*, 93 CHI.-KENT L. REV. 97, 97–100 (2018).

20. *See* Christopher G. Bradley, *Fintech's Double Edges*, 93 CHI.-KENT L. REV. 61, 63 (2018); Chris Brummer & Yesha Yadav, *Fintech and the Innovation Trilemma*, 107 GEO. L.J. 235, 241–44 (2019); William Magnuson, *Regulating Fintech*, 71 VAND. L. REV. 1167, 1173–74 (2018) [hereinafter Magnuson, *Regulating Fintech*]; William Magnuson, *Financial Regulation in the Bitcoin Era*, 23 STAN. J.L. BUS. & FIN. 159, 163–64 (2018) [hereinafter Magnuson, *Financial Regulation*].

21. *See* Van Loo, *supra* note 19, at 833–36 (describing how AI can leverage dispersed data to make more effective decisions for consumers).

basis, individuals struggle to access and share that data with others.[22] A combination of market failure and regulatory ambiguity makes it difficult, and sometimes impossible, for consumers to grant fintech companies access to their financial data. This has led to a situation in which data is limited, siloed, and inaccessible, with large financial institutions possessing tremendously valuable data but failing to share it with others.[23] Again, there are perfectly valid reasons why financial institutions might be hesitant to do so. They worry about privacy violations, cybersecurity risks, and liability exposures, all of which are significant.[24] But without control of their own financial data, individuals struggle to overcome the many obstacles to efficient financial decisionmaking.

This Article argues that resolving these problems will require us to replace the clarion call of "data privacy" with a new, more comprehensive concept—"data autonomy." Data autonomy balances the need for data to be protected and secure with the need for it to be accessible and shareable. It grants individuals a set of rights over their data that wrests control over data back from the large institutions that, until now, have maintained a vice grip over it. And while data autonomy requires important changes in legal rights and responsibilities, it is not entirely without precedent. It is largely consistent with a wave of new regulations being put in place across the globe, often referred to as "open banking" rules, that seek to address the lack of data sharing in financial services. Perhaps counterintuitively, the only way of ensuring consumer protection today is by breaking down the barriers of

22. *See* Nathaniel Popper, *Banks and Tech Firms Battle Over Something Akin to Gold: Your Data*, N.Y. TIMES (Mar. 23, 2017), https://www.nytimes.com/2017/03/23/business/dealbook/banks-and-tech-firms-battle-over-something-akin-to-gold-your-data.html [https://perma.cc/7Y4C-SP7W] (suggesting that big banks limit data access to avoid ceding control over that data); AnnaMaria Andriotis & Emily Glazer, *Facebook and Financial Firms Tussled for Years Over Access to User Data*, WALL ST. J. (Sept. 18, 2018, 5:30 AM ET), https://www.wsj.com/articles/facebook-sought-access-to-financial-firms-customer-data-1537263000 [https://perma.cc/DY2J-DX6U] (describing banks' hesitancy to give Facebook access to consumers' financial information).

23. *See JPMorgan's Clampdown on Data Puts Silicon Valley Apps on Alert*, AM. BANKER (Mar. 26, 2019, 9:18 AM), https://www.americanbanker.com/articles/jpmorgans-clampdown-on-data-puts-silicon-valley-apps-on-alert [https://perma.cc/5WAF-73ZW]; Laura Noonan, *JPMorgan to Ban Fintech Apps from Using Customer Passwords*, FIN. TIMES (Jan. 1, 2020), https://www.ft.com/content/93dcfc52-210b-11ea-b8a1-584213ee7b2b [https://perma.cc/L9AM-LJ3R].

24. *See* BASEL COMM. ON BANKING SUPERVISION, BANK FOR INT'L SETTLEMENTS, REPORT ON OPEN BANKING AND APPLICATION PROGRAMMING INTERFACES 13–15 (2019), https://www.bis.org/bcbs/publ/d486.pdf [https://perma.cc/DGL3-MWBF]; *Open Banking, Open Liability: Accountability Issues for Open Banking APIs*, ASHURST (Feb. 28, 2018), https://www.ashurst.com/en/news-and-insights/legal-updates/open-banking-open-liability-accountability-issues-for-open-banking-apis [https://perma.cc/J3EH-FA9T].

data privacy.[25]

This Article proceeds in three parts. Part I analyzes the competition problems that beset the financial industry, with a particular focus on services for consumers. It then turns to the ways in which innovative, data-focused fintech could help improve competition within the industry and provide better results for consumers. Finally, it explores the current barriers, both market-based and law-based, that inhibit greater competition.

Part II sets forth a pathway to reform. It explores how a variety of legal changes aimed at creating true data autonomy for individuals would help resolve inefficiencies in the sector. It argues that these reforms would include rights of ownership and access to personal financial data, as well as obligations on financial institutions to maintain personal financial data in interoperable and secure formats. Finally, it explores how such "open banking" structures have been implemented in other countries and the lessons that can be drawn from their experiences.

Part III considers the broader implications of shifting from a privacy-focused conception of data to an autonomy-focused one. Giving individuals control over their data will raise new risks and concerns, and regulators will need to be wary of emerging practices that might exploit or defraud newly empowered consumers. Part III focuses on three areas that will require special vigilance. First, regulators will need to develop robust measures for ensuring that individuals consent in meaningful and thoughtful ways before their data is shared with others. Second, regulators will need to be wary of antitrust violations, as the diffusion of competitively sensitive data may lead to collusion between competitors. Finally, regulators will need to be mindful of the problem of cost, as the development and maintenance of comprehensive data platforms will be expensive and, thus, may spur further incentives to monetize data in problematic ways.

A final caveat: lest we be misunderstood, we do not believe that data autonomy as a concept is opposed to data privacy. A world in which individuals do not have the ability to keep their information, financial and otherwise, out of public view is a dangerous and unappealing one. We do not advocate for one. Instead, we view this Article as an effort to highlight the ways in which data privacy can be used as an excuse for resisting innovation and stifling competition. Data autonomy, rightly understood, restores to the individual the right both to hide and to

25. *See* Rory Van Loo, *The Missing Regulatory State: Monitoring Businesses in an Age of Surveillance*, 72 VAND. L. REV. 1563, 1583 (2019) (arguing that privacy undermines consumer protection and other regulatory goals).

reveal, to confide and to disclose. We believe it better protects individuals in an increasingly data-dependent world.

I. THE ROLE OF DATA IN FINANCE

Finance suffers from a competition problem. Despite the clear need for better products to facilitate consumer wealth and security, innovation within the sector has lagged, at least partially because there are few incentives for traditional actors to innovate. Fintech startups, on the other hand, have strong incentives to innovate but lack the means to do so, primarily because they struggle to access the data they need to provide better services. This Part explores the structural causes of the lack of competition within the financial sector, with a particular focus on consumer banking. It then discusses the ways in which data could be used to mitigate or solve these problems. Finally, it describes how market failure and legal uncertainty have raised obstacles to greater use of data to empower individuals and improve financial services. It concludes by discussing potential avenues for reform.

A. The Competition Problem in Finance

Finance plays a crucial role in the economy. Through their provision of credit, liquidity, and payment and investment services, financial institutions allocate resources to their best uses, thereby making markets more efficient.[26] In economic terms, banks and other financial institutions *intermediate* between borrowers and savers, providing the former with capital to invest and the latter with investment opportunities.[27] This is a crucial role that has led financial institutions to dominating positions in the U.S. economy. Finance is now one of the largest sectors in the United States, contributing 7.4 percent of GDP in 2018.[28] The financial sector's importance to the economy also appears to be growing. In 1880, the quantity of intermediated assets was approximately equal to GDP, whereas today,

26. *See* EUGENE F. FAMA & MERTON H. MILLER, THE THEORY OF FINANCE 3–15 (1972); Joseph E. Stiglitz, *The Allocation Role of the Stock Market: Pareto Optimality and Competition*, 36 J. FIN. 235, 235 (1981); Eugene F. Fama, *Efficient Capital Markets: A Review of Theory and Empirical Work*, 25 J. FIN. 383, 383 (1970).

27. *See* FAMA & MILLER, *supra* note 26, at 3–15.

28. This number includes both finance and insurance. *See* Int'l Trade Admin., Indus. & Analysis Unit, *Financial Services Spotlight: The Financial Services Industry in the United States*, SELECTUSA, https://www.selectusa.gov/financial-services-industry-united-states (last visited Oct. 4, 2020) [https://perma.cc/7BPC-GW3A].

it is four times GDP.[29] The income of financial institutions has grown proportionately. The revenues of financial intermediaries increased from 2 percent of GDP in 1880 to 7.4 percent of GDP in 2018.[30]

Despite the growing size and profits of financial institutions, efficiency within the sector has remained remarkably stagnant. One common measure of efficiency within the financial sector is the ratio of the income of financial intermediaries to the quantity of intermediated assets.[31] By representing the unit cost of intermediating one dollar of assets, the ratio is thought to be an accurate way of understanding the efficiency of financial institutions in performing their key function.[32] It turns out that the intermediation ratio within the financial sector has remained stable at around 1.5 to 2 percent for over a century.[33] This is a striking statistic. The world has undergone tremendous technological change during this time, from the invention of computers to the creation of the internet. And yet, despite all these technological advances—many of which fundamentally altered the way that financial services work—there has been no increase in efficiency, with the unit cost today roughly the same as it was around 1900. The stability of the ratio is particularly striking given that almost all other sectors in the economy today are much more efficient than they were a century ago.[34]

This raises an obvious question. Why has finance not grown more efficient over time? While many theories have been asserted, two theories (one market-based and one law-based) have gained widespread acceptance. The first theory holds that the lack of efficiency gains in the financial sector can be explained as a result of the excess rents that incumbent financial institutions extract from their customers (so-called "hold-up" costs).[35] Banks use two main channels to hold up their customers and charge them more than a competitive market would sustain: (i) informational advantages and (ii) switching costs.[36]

---

29. *See* Thomas Philippon, *Has the US Finance Industry Become Less Efficient? On the Theory and Measurement of Financial Intermediation*, 105 AM. ECON. REV. 1408, 1411 (2015).

30. *Id.*

31. *Id.* at 1409.

32. *Id.*

33. *Id.* at 1412.

34. *See id.* at 1434 (noting that although in the retail and wholesale sectors, "IT investment coincides with lower prices and lower (nominal) GDP shares," the inverse is true in finance).

35. *See* GERALD EPSTEIN & JUAN ANTONIO MONTECINO, ROOSEVELT INST., OVERCHARGED: THE HIGH COST OF HIGH FINANCE 2, 16–19 (2016), https://rooseveltinstitute.org/wp-content/uploads/2016/07/RI-Overcharged-201606.pdf [https://perma.cc/2NZB-J8S6] ("[E]conomic rents are the incomes that some individuals or institutions receive over and above what would be required to incentivize them to engage in a given economic activity.").

36. *See* Steven L. Schwarcz, *Systemic Risk*, 97 GEO. L.J. 193, 218 (2008) (informational advantages); Oren-Bar Gill & Kevin Davis, *Empty Promises*, 84 S. CAL. L. REV. 1, 10–11 (2010)

First, the process of lending to borrowers is fraught with asymmetric information, where the lender has significantly less information than the borrower about the credit quality of the borrower.[37] This is a classic example of adverse selection that can lead to market breakdowns.[38] Banks thus invest a significant amount of resources in assessing the creditworthiness of individuals in order to make more accurate loans. But once banks acquire this information, they can then charge borrowers rates that are higher than what the borrowers would pay if asymmetric information were not present. After all, even if consumers are overcharged by a bank, they will find it difficult to instead reapply for a loan at a different bank, because doing so is often interpreted by other banks as a negative signal of their creditworthiness. This is a typical information hold-up problem.[39] Another avenue for holding up customers is through bundling services.[40] Most financial institutions today offer a variety of services, from checking and savings accounts to brokerage services, from bill payment solutions to credit cards.[41] Many consumers choose to use their bank for several or even all of these services. While this may be convenient for customers, it also introduces a large transaction cost for moving to a new bank. The search and switch costs are high and, thus, serve as a strong preference for the status quo.[42]

The second explanation for the inefficiency of the financial sector focuses on the role of regulation.[43] In particular, it asserts that the complex and fragmented regulatory environment for finance creates

(switching costs); Daniel Hemel, Note, *Regulatory Consolidation and Cross-Border Coordination: Challenging the Conventional Wisdom*, 28 YALE J. ON REGUL. 213, 222 (2011) (switching costs).

37. *See* Susan Block-Lieb & Edward J. Janger, *The Myth of the Rational Borrower: Rationality, Behavioralism, and the Misguided "Reform" of Bankruptcy Law*, 84 TEX. L. REV. 1481, 1495–96 (2006).

38. *See* Akerlof, *supra* note 9, at 493 (describing adverse selection in the insurance industry as occurring when healthy policyholders discontinue coverage, causing the insurer to bear an increased proportion of risks and higher claim costs).

39. *See* Rajan, *supra* note 17, at 1367–68 (explaining that because bank financing requires firms to share information with the banks, "firms forsake informed and seemingly more efficient sources of debt finance [from banks] to borrow from less informed arm's-length sources").

40. *See* Aluma Zernik, *Overdrafts: When Markets, Consumers, and Regulators Collide*, 26 GEO. J. ON POVERTY L. & POL'Y 1, 26 (2018).

41. *See, e.g.,* Bank of Am. Corp., Annual Report (Form 10-K) 2 (Feb. 26, 2019).

42. *See* Chris M. Wilson, *Market Frictions: A Unified Model of Search Costs and Switching Costs*, 56 EUR. ECON. REV. 1070 (2012) (explaining how high costs constrain the ability of customers to change suppliers).

43. *See* Howell E. Jackson, *Variation in the Intensity of Financial Regulation: Preliminary Evidence and Potential Implications*, 24 YALE J. ON REGUL. 253, 270 (2007); Henry N. Butler & Jonathan R. Macey, *The Myth of Competition in the Dual Banking System*, 73 CORNELL L. REV. 677, 679 (1988); Lawrence A. Cunningham & David Zaring, *The Three or Four Approaches to Financial Regulation: A Cautionary Analysis Against Exuberance in Crisis Response*, 78 GEO. WASH. L. REV. 39, 75 (2009).

large barriers to entry in the sector, thereby impeding potential competitors from introducing change.[44] Currently, a multitude of federal and state regulatory agencies possess overlapping oversight of the U.S. financial system. Banks and credit unions are regulated by the Federal Reserve, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation ("FDIC"), and the National Credit Union Administration ("NCUA"), as well as by state agencies, while broker-dealers and market intermediaries are overseen by the Securities and Exchange Commission ("SEC"), the Commodity Futures Trading Commission, numerous self-regulatory organizations (e.g. FINRA, NFA, FASB), and state regulators.[45] Institutions wanting to become banks must first receive charters, a process that is lengthy, expensive, and uncertain.[46] The complexity of this arrangement, as well as the overlapping compliance requirements, discourages new and innovative companies from entering the financial sector.[47] As a result, incumbent financial institutions can enjoy an oligopolistic competitive environment with large market power, excess rents, and low pressure to innovate.[48]

A final and related point is that all of these factors have played a role in contributing to rising public distrust of financial institutions. In a recent survey by the Reputation Institute, the banking sector ranked fifteenth out of sixteen industries for general reputation, only barely edging out the telecommunications industry for the worst reputation.[49] A recent Gallup poll found that sixty-two percent of respondents had only some, very little, or no confidence in banks.[50] The tech industry, on the other hand, despite all its recent criticism, generally inspires greater levels of trust in consumers, even with respect to the provision of financial products.[51]

---

44. *See* Hilary J. Allen, *Regulatory Sandboxes*, 87 GEO. WASH. L. REV. 579, 587–92 (2019).

45. *See* Lee Hudson Teslik, *The U.S. Financial Regulatory System*, COUNCIL ON FOREIGN RELS. (Oct. 1, 2008), https://www.cfr.org/backgrounder/us-financial-regulatory-system [https://perma.cc/7QG6-MWAP].

46. *See* Van Loo, *Making Innovation More Competitive*, *supra* note 15, at 260.

47. *See* Allen, *supra* note 44, at 591.

48. *See* Lina Khan & Sandeep Vaheesan, *Market Power and Inequality: The Antitrust Counterrevolution and Its Discontents*, 11 HARV. L. & POL'Y REV. 235, 242–43 (2017) (describing an analogous phenomenon in the context of unionized labor).

49. Alan Kline, *2019 Reputation Rankings: The Biggest Movers*, AM. BANKER (June 30, 2019, 9:00 PM), https://www.americanbanker.com/list/2019-reputation-rankings-the-biggest-movers [https://perma.cc/L6QX-FEYA].

50. *Confidence in Institutions*, GALLUP, https://news.gallup.com/poll/1597/confidence-institutions.aspx (last visited Dec. 9, 2020) [https://perma.cc/6RQT-KVLU].

51. *See*, *e.g.*, Statista Rsch. Dep't, *United States: Is Your Overall Opinion of Google as a Provider of Financial Services Positive, Neutral or Negative?*, STATISTA (June 3, 2015), https://www.statista.com/statistics/433041/united-states-google-opinion/ [https://perma.cc/DBF5-

In summary, the financial sector is large, profitable, inefficient, and untrusted. It is thus an obvious target for technological disruption. As Jamie Dimon, Chairman and CEO of JPMorgan Chase, warned his shareholders in 2014: "Silicon Valley is coming."[52]

B. The Promise of Fintech

In recent years, a number of fintech companies have sprung up to attempt to disrupt the financial sector using new technologies and tapping into new markets.[53] These companies have tended to focus on addressing two of the most severe financial frictions: asymmetric information and switching costs. By using technology to automate and improve decisionmaking, they promise to lower frictions in the financial sector and bring more competition into the market for financial products.[54] Among other things, it is hoped that they will expand access to and usage of financial products and provide cheaper, more convenient, and better targeted financial service products.[55]

The explosion in fintech investment over the last decade has been spurred by several technological breakthroughs.[56] Nowadays, machines can replicate many intellectual tasks, including search and planning, reasoning and knowledge representation, perception, natural language processing, and social interactions.[57] These advancements have transformed traditional enterprises and created new business opportunities in the financial service industry.[58] They have also paved the way to entirely new financial services across the globe: marketplace lending, equity crowdfunding, robo-advising, cryptocurrencies, blockchains, algorithmic trading, mobile payments, and person-to-person cross-border remittances all emerged out of fintech innovations.[59]

One particularly promising sector of the fintech market focuses on the better usage of data. One way to reduce information asymmetry, of course, is to collect, analyze, and share more information. And there are tremendous amounts of relevant data to be analyzed. Indeed,

---

E7GN] (presenting survey results where ninety-five percent of respondents reported either a positive or neutral view of Google as a financial services provider).

52. *See* Jamie Dimon, *Letter to Shareholders*, JPMORGAN CHASE & CO. 29 (2015) [https://perma.cc/FV22-CC7G].

53. *See* Magnuson, *Regulating Fintech*, *supra* note 20, at 1173–87.

54. *Id.*

55. *Id.*

56. *See* Brummer & Yadav, *supra* note 20, at 264–78.

57. *Id.* at 269–75.

58. *Id.* at 272–78.

59. *Id.*

nowadays, most economic and social activities are digitalized in some form. Around 33 zettabytes (10^{21}) of data were created, captured, or replicated in 2018, and the number continues to grow, more than doubling every other year.[60] Furthermore, the ability to analyze and process that data is growing as well. Under the well-known Moore's law, computing and storage power doubles roughly every eighteen to twenty-four months.[61] Just as importantly, advancements in data analytics, such as machine learning and neural networks, allow companies to analyze greater amounts of data more accurately and in a shorter amount of time.[62]

The arrival of big data means that lenders and investors now have a much greater amount of information than in the past to decide on the creditworthiness of borrowers or the expected return of an investment.[63] For example, bank account transactions include a trove of data useful for lending decisions, from disposable income to cash flow stability.[64] Sharing such information with lenders could allow borrowers to get loans on better terms by providing the lenders with greater security about the borrowers' financial behavior.[65] A more comprehensive use of data might lead to even greater efficiency gains. By aggregating and merging disparate data, companies could more accurately understand, predict, and optimize consumer demand and use of financial products.[66] For example, fintech companies could manage the personal finance of an individual by analyzing their credit card transactions, bank direct deposits, spending patterns, investment returns, and risk profiles.[67]

---

60. *See* DAVID REINSEL, JOHN GANTZ & JOHN RYDNING, THE DIGITIZATION OF THE WORLD: FROM EDGE TO CORE 3, 6 (2018), https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf [https://perma.cc/P2HJ-6S5Z].

61. It should be noted that in the last few years, a growing number of commentators have called into question whether Moore's law still holds. *See* Shara Tibken, *CES 2019: Moore's Law Is Dead, Says Nvidia's CEO*, CNET (Jan. 9, 2019, 11:46 AM), https://www.cnet.com/news/moores-law-is-dead-nvidias-ceo-jensen-huang-says-at-ces-2019/ [https://perma.cc/9VY2-B5YN].

62. William Magnuson, *Artificial Financial Intelligence*, 10 HARV. BUS. L. REV. 337, 339–40 (2020).

63. Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 5 (2014); Christopher K. Odinet, *Consumer BitCredit and Fintech Lending*, 69 ALA. L. REV. 781, 820 (2018); Matthew A. Bruckner, *Regulating Fintech Lending*, BANKING & FIN. SERVS. POL'Y REP., June 2018, at 1, 1 [hereinafter Bruckner, *Regulating*]; Matthew Adam Bruckner, *The Promise and Perils of Algorithmic Lenders' Use of Big Data*, 93 CHI.-KENT L. REV. 3, 5 (2018) [hereinafter Bruckner, *The Promise and Perils*].

64. *See* Citron & Pasquale, *supra* note 63, at 5.

65. *Cf. id.* at 8–18 (describing drawbacks of the "black box" created by the credit scoring system in which opacity undermines fairness and efficiency).

66. *See* Van Loo, *supra* note 19, at 817–18.

67. *Id.* at 826–30.

Despite the great promise of fintech and its data-focused approach to finance, however, there is little empirical evidence that, at least so far, it has led to greater efficiency within the United States. While technology is drastically changing the business models of most industries, from media and telecommunication to retail, the adoption of new technologies in the broader U.S. financial sector, and the financial inclusion and efficiency that comes with it, is still limited.[68] In a recent survey of fintech adoption rates, the U.S. market ranks twenty-fourth out of twenty-seven countries.[69]

The low level of fintech adoption in the U.S. financial sector can be explained partially as a result of the unique nature of the U.S. market. In particular, the U.S. financial sector has the odd feature of being both fragmented *and* concentrated. This strange structure has made it especially resistant to competition. Let us focus first on its fragmentation. As of 2018, there were more than 4,700 FDIC-insured commercial banks with over 81,000 bank branches.[70] This is an enormous number of firms and is perhaps best understood by examining it in comparison with other countries. The United Kingdom has only three hundred banks.[71] Canada has only eighty-eight.[72] Europe has around two-thirds the number of banks per capita that the United States does.[73] The fragmentation of the U.S. market might seem to suggest that the banking industry should be highly competitive, as oligopolistic behavior is usually associated with high industry concentration. But this is where the concentration of the market becomes relevant. Over the last twenty years, the banking industry has in fact been undergoing a significant consolidation, with a decline of over forty percent in the total number of banks, accompanied by a rise in the share of very large "supermarket" financial institutions: the five

68. *See* ERNST & YOUNG, GLOBAL FINTECH ADOPTION INDEX 2019, at 6–7 (2019), https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/financial-services/ey-global-fintech-adoption-index-2019.pdf [https://perma.cc/WSS2-NWKH].

69. *Id.*

70. *See* F. Norrestad, *Number of FDIC-Insured Commercial Banks in the United States From 2002 to 2018*, STATISTA (Nov. 30, 2020), https://www.statista.com/statistics/184536/number-of-fdic-insured-us-commercial-bank-institutions/ [https://perma.cc/44R7-WYE7]; F. Norrestad, *Number of FDIC-Insured Commercial Bank Offices in the U.S. 2000-2019*, STATISTA (Nov. 10, 2020), https://www.statista.com/statistics/193044/number-of-fdic-insured-us-commercial-bank-offices/ [https://perma.cc/H4U9-SBYE].

71. *Overview of Banks in the UK*, CORP. FIN. INST., https://corporatefinanceinstitute.com/resources/careers/companies/top-banks-in-the-uk/ (last visited Dec. 10, 2020) [https://perma.cc/33HF-EVSM].

72. *Focus: Fast Facts About the Canadian Banking System*, CANADIAN BANKERS ASS'N (Aug. 26, 2020), https://cba.ca/fast-facts-the-canadian-banking-system [https://perma.cc/7SZ6-YNQ4].

73. *See Commercial Bank Branches (Per 100,000 Adults)*, WORLD BANK, https://data.worldbank.org/indicator/FB.CBK.BRCH.P5 (last visited Dec. 10, 2020) [https://perma.cc/R2SP-AR3F].

largest banks in the United States accounted for around twenty-eight percent of total assets of large commercial banks in 2000 but now account for forty-seven percent.[74] The banking industry, thus, despite its fragmentation, is also quite concentrated. It has a large number of very small banks and a small number of very large ones. While the small ones struggle to find the resources needed to innovate, the large ones have limited incentives to do so due to their oligopoly rents and government guarantees as systemically important financial institutions (sometimes colloquially known as "too-big-to-fail" firms). This is a recipe for a competition-resistant market.

This problem, of course, creates an even greater opportunity for fintech companies. If small banks lack the ability to innovate, and large banks lack the incentives to do so, fintech companies have both. If they can gain access to the financial data of consumers, they should be able to provide better services at lower cost than other financial institutions and, in doing so, trigger greater competition within the sector. But the fintech industry relies on one key input: data. And as the next Section explores, data has become increasingly hard to access and share.

C. The Data Problem

For centuries, financial institutions have built their information systems to prevent loss, either in the form of theft or, more recently, cybersecurity breaches. Even today, the core banking systems of many U.S. banks rely on mainframe-based transaction systems, introduced in the 1970s, to allow centralized processing of large volumes of transactions with reduced downtime and high data security. But this core banking system is now antiquated and unable to keep up with the needs of the modern financial system. Over the last decade, fintech companies have introduced new technologies (such as screen-scraping) aimed at surmounting these problems and at accessing bank accounts to retrieve the data they need. In recent years, however, financial institutions have responded by introducing new barriers around consumer data, again making it difficult for consumers to access and share their data with others.[75] In some cases, banks have banned customers from sharing their passwords with third-party fintech

74. *See Large Commercial Banks Statistical Release*, FED. RSRV. BD., https://www.federalreserve.gov/releases/lbr/current/ (last updated June 30, 2020) [https://perma.cc/JYA4-TT5D] (identifying the five largest banks); Peter Eavis & Keith Collins, *The Banks Changed. Except for All the Ways They're the Same.*, N.Y. TIMES (Sept. 12, 2018), https://www.nytimes.com/interactive/2018/09/12/business/big-investment-banks-dodd-frank.html [https://perma.cc/FA7N-9MHT] (showing concentration of the banking industry over time).

75. *See* Van Loo, *supra* note 19, at 838–39.

companies.[76] In others, they have introduced platform changes that shut out fintech companies.[77] In still others, they have required fintech companies to enter into burdensome data sharing agreements before allowing consumers to share data with them.[78] More generally, banks have been slow to adapt their technological infrastructure to allow consumers to access and share financial data with other parties.[79]

If this were a more competitive sector, one might expect that the market would help resolve the problem. If consumers truly valued the ability to share their financial data with third parties, they might choose banks or other financial institutions that provided that service. After all, in functioning markets, when there is a demand for a specific service, it is generally expected that, where feasible, a market will arise to supply it.[80] But, as mentioned before, the financial sector is far from a perfect market. Several hurdles prevent a market for data sharing to arise naturally. First, because search and switch costs are large in the banking sector, consumers may well not shift to banks that spring up offering better services.[81] Consumers, after all, use the same financial institution for a multitude of financial transactions, from direct deposits to paying bills and mortgages, and moving all these services to a competing bank is time-consuming and expensive.[82] Second, until a sufficient number of institutions allow data sharing, the value of data sharing by a single institution is muted.[83] In other words, there are strong network effects to data sharing and, until a network develops, there will be few incentives for individual banks to suddenly offer it.[84] For example, personal financial management tools are valuable only if they aggregate all the financial information scattered among all financial institutions. Potential market entrants are thus waiting for

76. Noonan, *supra* note 23.

77. *See* Mary Wisniewski, *Fintechs' Vulnerability Apparent in Capital One Data-Access Flap*, AM. BANKER (June 29, 2018, 12:12 PM EDT), https://www.americanbanker.com/opinion/fintechs-vulnerability-apparent-in-capital-one-data-access-flap [https://perma.cc/XUS5-ENB4].

78. *See* Penny Crosman, *Wells Fargo Strikes Data-Sharing Agreement with Plaid*, AM. BANKER (Sept. 19, 2019, 7:00 AM EDT), https://www.americanbanker.com/news/wells-fargo-strikes-data-sharing-agreement-with-plaid [https://perma.cc/8TNZ-BBZW].

79. *See* Van Loo, *supra* note 19, at 838–39 (noting other examples of banks restricting fintech's access to customer data).

80. *See* Irena Asmundson, *Supply and Demand: Why Markets Tick*, INT'L MONETARY FUND, https://www.imf.org/external/pubs/ft/fandd/basics/suppdem.htm (last updated Feb. 24, 2020) [https://perma.cc/T7XJ-ZCRN].

81. *See* discussion *supra* Section I.A (noting that the cost of switching service providers creates a barrier for many consumers).

82. *See* discussion *supra* Section I.A.

83. *See* Peter Zhegin, *Data Network Effects for an Artificial Intelligence Startup*, MEDIUM (Dec. 8, 2018), https://towardsdatascience.com/data-network-effects-for-an-artificial-intelligence-startup-7f6fab10ba85 [https://perma.cc/Q5PK-HJLY].

84. *See id.*

more data to become available and for the regulatory environment to become clearer regarding data access and sharing. Consumers, in turn, are waiting for market entrants before they switch banks, a classic chicken-and-egg problem.

Furthermore, incumbent financial institutions have a strong interest in preventing data sharing in the first place.[85] Banks have little incentive to share their data with third parties if they are not being paid to do so, as customer data is valuable and gives banks a competitive advantage over others.[86] Relinquishing it to third parties erodes banks' competitive position. Just as importantly, the third-party fintech companies that gain access to the data may well use it in ways that harm the bank that gave it. They might, for example, recommend that the customer transfer his or her money to a different bank that pays a greater interest rate or refinance his or her mortgage with another lender offering better terms. So even if there is a strong customer demand for greater data sharing, banks will still have incentives to limit or prohibit it.

The current financial regulatory environment has not resolved this market failure. Financial regulators have, for the most part, taken a top-down approach to banking oversight, focusing more on stabilizing the financial system rather than spurring innovation and efficiency.[87] Proposals to break up big banks similarly fail to address the main causes of the market failure in the financial system: asymmetric information and switching costs.[88]

In order to resolve these problems, we need to develop a financial regulatory structure that focuses on data. But this structure must not simply increase rights to data privacy. Privacy is certainly an element of data rights, but it is not the only value. Just as important is the right of individuals to share, use, and access their data. Data autonomy, thus, embraces not just data privacy, but also data sharing, and includes a much more comprehensive array of rights and obligations.

While introducing a concept of data autonomy into financial regulation would require substantial changes to current law, it is not entirely without precedent. Around the globe, countries are

85. *See* Van Loo, *supra* note 19, at 838–39.

86. *See id.* ("[Banks] cite[ ] privacy concerns [as a reason to not share data] . . . , but those explanations must be viewed with some skepticism because the intermediaries pose a competitive threat.").

87. *See* Schwarcz, *supra* note 36, at 194.

88. *Cf.* Sheelah Kolhatkar, *How Elizabeth Warren Came Up with a Plan to Break Up Big Tech*, NEW YORKER (Aug. 20, 2019), https://www.newyorker.com/business/currency/how-elizabeth-warren-came-up-with-a-plan-to-break-up-big-tech [https://perma.cc/2M5K-ASY5] (outlining Senator Warren's antitrust plan to prohibit big tech companies from both owning and participating in an online marketplace).

experimenting with new financial regulatory structures to address the lack of data sharing in financial services.[89] These regulations, often referred to as "open banking" rules, enable consumers to give third-party providers access to their financial data and accounts in a secure, easy, transparent, and inexpensive way. Under these structures, fintech companies can use application programming interfaces ("APIs") to automatically access a consumer's bank account, analyze financial transactions, move money around, pay bills, and make investments. Consumers could, for example, completely outsource their personal financial management to certified third-party providers that analyze their spending and income flows, shop for the best credit card and loan rates for them, and even automatically switch them to better services. Open banking rules aim to open up data in the financial sector in order to lower asymmetric information and search and switch costs that inhibit competition. Thus, while data autonomy would mark a dramatic shift in the legal rules governing data, it is not implausible or even unprecedented. We now turn to the question of just precisely what it would require.

II. DATA AUTONOMY

We have argued that the financial system suffers from a lack of competition. This lack of competition is caused by a combination of market frictions and legal uncertainty. As a result, consumers have failed to benefit from many of the innovations that have been made possible in recent years by advancements in big data, artificial intelligence, and fintech more generally. Thus, we have argued, financial regulation must be recast in a comprehensive manner in order to facilitate the kinds of technological innovation that have largely been missing from the financial world.

Now we will turn to the question of reform. This Part lays out what data autonomy might look like in financial regulation and what new legal rules will be necessary in order to implement it. In particular, this Part argues that data-focused financial regulation must be guided by four key principles. First, it must establish that consumers own their financial data. Second, it must require financial institutions to grant access to that data to the persons and firms that consumers so choose. Third, it must set forth rules on the structure and terms of that access, with a focus on creating interoperable standards. And fourth, it must create strong incentives for firms throughout their financial ecosystem

89. *See* discussion *infra* Section II.E (taking "lessons from abroad" about implementing regulatory structures that account for data sharing in the financial sector).

to establish and maintain proper cybersecurity procedures. This Part also surveys how other jurisdictions have addressed these problems and draws lessons from their experiences.

A. Ownership

The first prong of data autonomy in financial regulation must focus on the ownership of financial data. In particular, it must establish, in clear and incontrovertible terms, that consumers own their financial data.[90] Property rights in data would bring with them all the separate benefits that property law entails: the right to use, destroy, exclude, and transfer.[91] Consumers would, as a result, have not just the *ability*, but the *right* to see, compile, aggregate, delete, and sell their financial data as they see fit, and without the permission of the financial institutions with which they transact.

Data ownership would seem to be a simple proposition, but it is not as incontrovertible as it might appear at first glance.[92] When asked

90. The importance of clarity here is hard to overstate. As will be discussed further below, property rights in the digital era have been deeply controversial and, to date, are still largely in flux. And without clear data ownership rules, participants have little certainty about the terms under which they are interacting with others. As property scholars have long recognized, this is problematic from many perspectives. *See* Abraham Bell & Gideon Parchomovsky, *Reconfiguring Property in Three Dimensions*, 75 U. CHI. L. REV. 1015, 1022 (2008) ("There cannot be ownership in land without some clear idea of who owns the land, what land is owned, and what rights accrue to the owner as a result of her status."); Steven J. Eagle, *Private Property, Development and Freedom: On Taking Our Own Advice*, 59 SMU L. REV. 345, 352 (2006) ("Individuals working to grow their assets must be supported by clear laws defining their property rights."); Henry E. Smith, *Property and Property Rules*, 79 N.Y.U. L. REV. 1719, 1797 (2004) ("Property rules have informational advantages."); Thomas W. Merrill & Henry E. Smith, *What Happened to Property in Law and Economics?*, 111 YALE L.J. 357, 359 (2001) (arguing that the fact that property "is required to come in standardized packages that the layperson can understand at low cost . . . constitutes a deep design principle of the law").

91. *See* Joseph William Singer, *The Rule of Reason in Property Law*, 46 U.C. DAVIS L. REV. 1369, 1390–1420 (2013) (exploring the features and functions of these core rights under property law).

92. *See, e.g.*, Jeffrey Ritter & Anna Mayer, *Regulating Data as Property: A New Construct for Moving Forward*, 16 DUKE L. & TECH. REV. 220 (2018) (surveying international approaches to data ownership); Mark A. Lemley & Philip J. Weiser, *Should Property or Liability Rules Govern Information?*, 85 TEX. L. REV. 783, 784 (2007) ("[T]he classic justification for legal entitlements protected by a property rule depends on the ability to define and enforce property rights effectively."); Vera Bergelson, *It's Personal but Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379, 392–93 (2003) (arguing that state and federal law "fail to provide coherent and systematic protection of personal information" on the internet); Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423, 432 n.36 (2018) (highlighting "the inadequacies of existing privacy frameworks in remedying consumer harms that may occur as a result of data disclosures"); Nancy S. Kim, *Contract's Adaptation and the Online Bargain*, 79 U. CIN. L. REV. 1327, 1356 (2011) ("It is unclear what legal right or interest, if any, consumers have in their personal information."); Andreas Boerding, Nicolai Culik, Christian Doepke, Thomas Hoeren, Tim Juelicher, Charlotte Roettgen & Max V. Schoenfeld, *Data Ownership: A Property Rights Approach from a European Perspective*, 11 J. CIV. L. STUD. 323, 325

whether a consumer owns the information in their bank account, one consumer rights advocate admitted, "You don't. You totally don't."[93] The Financial Data and Technology Association, an industry consortium, has similarly argued that "the right for the consumer to control their data . . . is murky."[94] Large financial institutions, while addressing the terms of data exchange, have avoided taking public stands on the issue.

This position of ambiguity is in stark contrast to many other technology sectors. For example, Mark Zuckerberg has stated in testimony before the Senate that "people own all of their own content" on Facebook.[95] Google's terms of service for its cloud storage accounts explicitly state that "[w]e do not claim ownership in any of your content."[96] Both of these companies have established rights for users to delete and transfer their data if they so choose.

The lack of clarity on the legal structure of financial data ownership has led to complaints about potentially harmful effects in the financial industry. In 2016, the director of the Consumer Financial Protection Bureau ("CFPB"), Richard Cordray, stated that "we are gravely concerned by reports that some financial institutions are looking for ways to limit, or even shut off, access to financial data."[97] In 2019, Senator John Kennedy introduced a bill, entitled the "Own Your Own Data Act of 2019," which, if enacted, would provide that "[e]ach individual owns and has an exclusive property right in the data that an individual generates on the internet."[98]

While the basic principle—that consumers own their financial data—is straightforward, how exactly that principle might apply to the financial sector, and in particular how it might be limited, raises difficult legal and policy issues. The initial problem, of course, is

---

(2018) (arguing that European property law provides "sufficient common principles to establish a comprehensive concept of data ownership").

93. *See* Colin Wilhelm, *Is Your Bank Data Yours?*, POLITICO (Oct. 11, 2017, 5:00 AM), https://www.politico.com/agenda/story/2017/10/11/who-owns-financial-data-000538 [https://perma.cc/7J5J-5XBR].

94. *See* Letter from Steven Boms, Exec. Dir., Fin. Data & Tech. Ass'n, to House Task Force on Fin. Tech. (June 20, 2019), https://fdata.global/north-america/wp-content/uploads/sites/3/2019/06/FDATA-FinTech-Task-Force-Letter-for-Record-6.25.19-Final.pdf [https://perma.cc/557X-X3CG].

95. *See Transcript of Zuckerberg's Appearance Before House Committee*, WASH. POST (Apr. 11, 2018, 8:53 PM CDT), https://www.washingtonpost.com/news/the-switch/wp/2018/04/11/transcript-of-zuckerbergs-appearance-before-house-committee/ [https://perma.cc/KF77-YRG8].

96. *See Google Drive Terms of Service*, GOOGLE DRIVE HELP, https://support.google.com/drive/answer/2450387?hl=en (last visited Sept. 26, 2020) [https://perma.cc/JB4R-BYFB].

97. *See* Richard Cordray, Dir., Consumer Fin. Prot. Bureau, Prepared Remarks at Money 20/20 (Oct. 23, 2016), https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-cfpb-director-richard-cordray-money-2020/ [https://perma.cc/E6CT-NGTD].

98. *See* Own Your Own Data Act, S. 806, 116th Cong. § 2(a) (2019).

defining just what counts as consumer financial data.[99] Banks, credit card companies, lenders, and others possess tremendous amounts of information about their customers and users, and establishing the boundaries of which parts of that information belong to the financial institution and which parts belong to consumers is inevitably complicated.[100] Take, for example, a typical savings account at a bank. On one side of the spectrum, we have the consumer's personal information, such as name, social security number, driver's license number, etc. This would appear quite clearly to be the consumer's data and thus owned by the consumer, not the bank. On the other side of the spectrum is information that can be seen by the consumer but that is not directly related to them, such as the variety of accounts that the bank offers or their branch locations. This type of data would clearly be bank-owned data, not consumer-owned data.

But in between these clear cases lie a number of trickier scenarios. Is the interest rate offered by the bank the bank's data or the consumer's? If the bank provides budgeting tools or enhanced information about payments that would be unavailable to the consumer operating on their own, is the data produced by those tools the bank's or the consumer's? Much of this information is considered by financial institutions as confidential, meaning that its release to other parties might harm the institution itself. And yet, this information is vital to ensuring that consumers understand their financial lives. Credit events are an even starker example of the complexity of drawing ownership lines when it comes to financial data: when borrowers miss a payment, or outright default, does this information belong to the borrower or to the bank? If it belongs to the borrowers, they might have the right to ask the bank to erase the negative events and thus compromise the ability of banks to discern between good and bad borrowers.

Fortunately, the concept of data ownership has received significant attention from scholars and policymakers, and models for sorting through these problems exist. For example, under the administration of President Barack Obama, the Office of Management and Budget issued guidance on the protection of individual data within government offices.[101] This guidance sets forth the scope of what

99. *See* William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1148–52, 1164–68 (2019); Joseph V. DeMarco & Brian A. Fox, *Data Rights and Data Wrongs: Civil Litigation and the New Privacy Norms*, 128 YALE L.J. 1016, 1024–26 (2019).

100. *See* Stacy Cowley, *Banks and Retailers Are Tracking How You Type, Swipe and Tap*, N.Y. TIMES (Aug. 13, 2018), https://www.nytimes.com/2018/08/13/business/behavioral-biometrics-banks-security.html [https://perma.cc/X8LH-A7N7]; Andriotis & Glazer, *supra* note 22 (describing negotiations between Facebook and financial firms over access to customers' financial data).

101. *See* OFF. OF MGMT & BUDGET, EXEC. OFF. OF THE PRESIDENT, M-10-23, GUIDANCE FOR AGENCY USE OF THIRD-PARTY WEBSITES AND APPLICATIONS (2010).

personal data is, what the requirements are for accessing and using it, and the duties that government officials have with respect to it. In the health sector, the Health Insurance Portability and Accountability Act ("HIPAA") establishes ground rules on how healthcare companies handle personally identifiable information.[102] The European Union's much-debated General Data Protection Regulation ("GDPR") also includes extensive sections defining the boundaries of personal data and the rights of consumers over it.[103] All of these are potential models for defining consumer-owned financial data. Given the increasing value of data to consumer choice and market efficiency, we are inclined to adopt a more expansive definition of consumer data in order to ensure that consumers have control over their information. But regardless of the precise definition adopted, the very process of identifying the data that is owned by financial institutions and the data that is owned by consumers will itself produce important benefits. Greater clarity about the legal status of personal financial data is essential to improving competition within the sector.[104]

B. Access

But data ownership alone is not enough to ensure that consumers can use their financial data in the ways that they desire. Regulators must also focus on requiring banks and other financial institutions to grant access to this financial data, both to consumers and their desired delegates, in convenient and reasonably cost-effective ways. After all, if consumers own their financial data, but financial institutions limit the ways in which they may use it, then data ownership alone will be insufficient to ensure a competitive landscape. Data access rights, thus, are integral to establishing data autonomy in financial regulation.[105]

Again, it would appear largely unobjectionable that consumers should have rights to access their financial data and to show this

102. *See* Frank Pasquale & Tara Adams Ragone, *Protecting Health Privacy in an Era of Big Data Processing and Cloud Computing*, 17 STAN. TECH. L. REV. 595, 597 (2014); Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV. 331, 336 (2007).

103. *See* Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365, 375–80 (2019); W. Gregory Voss & Kimberly A. Houser, *Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies*, 56 AM. BUS. L.J. 287, 314–15, 328 (2019).

104. On the importance of clear property rules to efficiency, see *supra* note 90.

105. Here, for example, is how one consumer rights group describes the problem:

> Over the last several years, some U.S. financial institutions have sought to institute a range of technical and administrative hurdles that would interfere with consumers' ability to use third-party tools. These financial institutions have moved to limit the

financial data to whomsoever they choose. Indeed, of all the planks of data autonomy in financial regulation, access to data has the clearest legal grounding. Dodd-Frank section 1033, after all, requires financial institutions to make information available to consumers concerning their financial services, including "information relating to any transaction, series of transactions, or to the account including costs, charges and usage data."[106] The CFPB has bolstered this requirement by issuing a set of principles on data sharing practices, and these principles include specific sections devoted to access. They include, for example, provisions related to data scope, usability, and control, and they provide in-depth descriptions of the kinds of data that financial institutions should share with consumers and third-party fintech companies.[107] Thus, the right to access and share financial data stands on firm legal ground.

But despite the current regulatory framework, in recent years financial institutions have raised a number of technological and legal barriers to this access.[108] They have restricted access to account

---

> amount of data that consumers can share, or are seeking to define bilateral agreements with onerous contractual terms that would restrict consumers' ability to take full advantage of marketplace solutions that would empower them to improve their financial state. As a result, there are an escalating number of cases where consumers are excluded from engaging with fintech services best suited to improve their financial well-being.

Examining Opportunities and Challenges in the Financial Technology ("Fintech") Marketplace: Hearing Before the Subcomm. on Fin. Insts. and Consumer Credit of the H. Comm. on Fin. Servs., 115th Cong. 130–32 (2018) (Letter from the Consumer Financial Data Rights Group to the H. Fin. Servs. Comm.).

106. Section 1033 provides:

> Subject to rules prescribed by the Bureau, a covered person shall make available to a consumer, upon request, 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. The information shall be made available in an electronic form usable by consumers.

Dodd-Frank Wall Street Reform and Consumer Protection Act § 1033(a), 12 U.S.C. § 5533(a).

107. *See Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation*, CONSUMER FIN. PROT. BUREAU 3 (Oct. 18, 2017), https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf [https://perma.cc/G78Z-2H96]:

> Financial data subject to consumer and consumer-authorized access may include any transaction, series of transactions, or other aspect of consumer usage; the terms of any account, such as a fee schedule; realized consumer costs, such as fees or interest paid; and realized consumer benefits, such as interest earned or rewards.

108. *See* AM. BANKER, *supra* note 23 (describing how financial firms have resorted to using platforms that "restrict[ ] how much and how often apps can tap information, while also setting contractual limits on what they can do with it later").

information,[109] they have blocked traffic from some fintech servers,[110] and they have prevented customers from viewing their data through fintech portals.[111] Increasingly, financial institutions have refused to grant access to consumer-oriented fintech startups until those startups agree to burdensome data sharing agreements.[112] Financial institutions have listed a number of reasons for these obstacles, including ensuring the security of customer data released to third parties, clarifying where liability lies in the transaction, and protecting their own systems from cybertheft.[113] But regardless of the cause, these obstacles have made it difficult, and costly, for consumers to access and share their data in convenient ways. Adding to the dilemma, the CFPB has been significantly more active in ensuring data privacy than in ensuring data sharing.[114]

Thus, in order to ensure that financial markets are efficient and transparent, financial regulators must go further in creating, explaining, and enforcing data sharing rights. For one, they must set forth, in unambiguous language, the terms and conditions on which financial access occurs. Perhaps just as importantly, they must make clear that failures to grant access on such terms will be sanctioned. As the post-Dodd-Frank era has shown, financial institutions have many ways to restrict or limit otherwise clear statutory obligations.[115] Until there are strong incentives for them to grant consumers and fintech startups greater access to their data, it is likely that they will refrain

109. *See* Jennifer Surane, *Capital One Restricts Third-Party Data Access, Upsets Customers*, BLOOMBERG (June 27, 2018, 6:00 AM CDT), https://www.bloomberg.com/news/articles/2018-06-27/capital-one-restricts-third-party-data-access-upsets-customers [https://perma.cc/T7P5-SGYR].

110. *Cf.* Penny Crosman, *The Truth Behind the Hubbub over Screen Scraping*, AM. BANKER (Nov. 12, 2015, 2:15 PM EST), https://www.americanbanker.com/news/the-truth-behind-the-hubbub-over-screen-scraping [https://perma.cc/MF4U-62PM] (describing potential reasons why banks are justified in blocking fintech companies from accessing their servers).

111. *See* Robin Sidel, *Big Banks Lock Horns with Personal-Finance Web Portals*, WALL ST. J. (Nov. 4, 2015, 7:30 PM ET), https://www.wsj.com/articles/big-banks-lock-horns-with-personal-finance-web-portals-1446683450 [https://perma.cc/4CVW-AKR8] (describing how banks have become more protective of their customers' personal information).

112. *See* Penny Crosman, *U.S. Bank Embraces Open Banking with Data-Sharing Agreements*, AM. BANKER (Sept. 24, 2019, 10:24 AM EDT), https://www.americanbanker.com/news/us-bank-embraces-open-banking-with-data-sharing-agreements [https://perma.cc/W9PG-TMKS].

113. *See id.*; Crosman, *supra* note 110; AM. BANKER, *supra* note 23.

114. *See* Rory Van Loo, *Technology Regulation by Default: Platforms, Privacy, and the CFPB*, 2 GEO. L. TECH. REV. 531, 536–38 (2018).

115. *See* Eric C. Chaffee, *The Dodd-Frank Wall Street Reform and Consumer Protection Act: A Failed Vision for Increasing Consumer Protection and Heightening Corporate Responsibility in International Financial Transactions*, 60 AM. U. L. REV. 1431, 1434 (2011) ("Financial institutions and other businesses seeking lower levels of regulation can now move from nation to nation seeking weaker regulatory standards, producing a race-to-the-bottom in international financial regulation."); Arthur E. Wilmarth, Jr., *The Financial Services Industry's Misguided Quest to Undermine the Consumer Financial Protection Bureau*, 31 REV. BANKING & FIN. L. 881, 932 (2012).

from making the costly and time-consuming changes that will be necessary to facilitate efficient and competitive data sharing.[116]

One of the key problems in financial data sharing is that there are few compelling business reasons for banks to engage in it.[117] In the financial industry, banks tend to be net producers, not consumers, of data.[118] In other words, banks possess tremendous amounts of financial data, and they have limited need to gain access to the data of others. As a result, the concept of data sharing is often viewed within large banks as a cost-creating department, not a revenue-creating one.[119] To be sure, if banks fail to provide fintech firms with access to their platforms, while their competitors do, they may lose customers in the long-term.[120] But consumers are often held up by banks because of asymmetric information and search and switch costs, and the executive decisionmakers at banks, focused on immediate returns and with limited time horizons, may well discount the value of these long-term benefits.[121]

Furthermore, 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

---

116. *See* Melvin A. Eisenberg, *Corporate Law and Social Norms*, 99 COLUM. L. REV. 1253, 1253 (1999) ("Insofar as corporate law is regulatory, it provides incentives and disincentives to the major actors in the corporate enterprise—directors, officers, and significant shareholders—through the threat of liability.").

117. *See* discussion *supra* Section I.C (describing the financial sector's reluctance to hand over data to fintech firms).

118. *See* Maria Aspan, *Why Banks Still Struggle with Big Data*, AM. BANKER (May 21, 2014, 12:52 PM EDT), https://www.americanbanker.com/news/why-banks-still-struggle-with-big-data [https://perma.cc/H4CR-AEJ9] (describing why banks have been less successful with deploying the massive amounts of customer information they collect).

119. For a discussion of the perception of transaction costs and value creators in the corporate environment, and the extensive role that business lawyers can have in this paradigm, see Ronald J. Gilson, *Value Creation by Business Lawyers: Legal Skills and Asset Pricing*, 94 YALE L.J. 239 (1984).

120. *See, e.g.*, Lauren Brodsky & Liz Oakes, *Data Sharing and Open Banking*, MCKINSEY & CO. (Sept. 5, 2017), https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking [https://perma.cc/M9M2-VN3W] (discussing the competitive opportunities that open banking and data access provide to banks).

121. *See* Lucian A. Bebchuk & Holger Spamann, *Regulating Bankers' Pay*, 98 GEO. L.J. 247, 249 (2010):

> It is now well-recognized that by enabling executives to cash large amounts of equity-based and bonus compensation before the long-term consequences of decisions are realized, pay arrangements have provided executives with incentives to focus excessively on short-term results and give insufficient weight to the consequences that risk-taking would have for long-term shareholder value.

data.[122] Banks have responded by making it more difficult and cumbersome for customers to access their financial accounts.[123] But while this shift may have improved data security, it has also set up new obstacles for data sharing. If, for example, a bank only allows customers access through two-factor authentication models, some fintech startups may be excluded from access. The tension between data sharing and data privacy could not be starker.[124]

Given these dynamics, regulatory pressure to improve and increase data sharing within the financial industry is both desirable and necessary. Without it, it is likely that efforts to create open, transparent financial markets will be slow and halting. The right to access, and share, financial data must, at a minimum, include affirmative rights by consumers and fintech companies to see and use their financial data in convenient forms and on reasonable terms, backed up by monetary penalties if this access is obstructed or delayed.

C. Interoperability

Data-oriented financial regulation must also focus on creating interoperable standards for data sharing. Just as it is important to create clear ownership rights over data, and clear access rights, it is also important to ensure that this data is stored and managed in standardized ways. Interoperability is integral to the proper functioning of a market in data, and without it, transaction costs and market leverage may threaten to impede competition within the sector.

While ownership and access rights are justified primarily based on the reluctance of financial institutions to recognize or grant such rights on their own, interoperability rules are justified by simpler

122. *See* Eric Dash, *Citi Data Theft Points Up a Nagging Problem*, N.Y. TIMES (June 9, 2011), https://www.nytimes.com/2011/06/10/business/10citi.html [https://perma.cc/S6QU-XNE6] (discussing the federal response to a data hack against Citigroup); Telis Demos & Emily Glazer, *Banks Have a Solution for Their Identity-Fraud Woes: The DMV*, WALL ST. J., https://www.wsj.com/articles/banks-have-a-solution-for-their-identity-fraud-woes-the-dmv-1542018600 (last updated Nov. 12, 2018, 4:45 PM ET) [https://perma.cc/K5FJ-EE9V] (describing banks' efforts to work with government offices in order to properly screen and ensure that potential new customers "are who they say they are").

123. *See, e.g.*, Andy Bounds, *Lloyds Bank Swipes Callsign Deal to Bolster Cyber Security*, FIN. TIMES (July 10, 2019), https://www.ft.com/content/02037454-a312-11e9-a282-2df48f366f7d [https://perma.cc/SA52-32WS]; Brian Gaynor, *Are You Ready for PSD2 Strong Customer Authentication?*, GLOB. BANKING & FIN. REV. (Dec. 13, 2017), https://www.globalbankingandfinance.com/are-you-ready-for-psd2-and-strong-customer-authentication/ [https://perma.cc/2BA8-DFC6].

124. *See* INFO. SEC. MEDIA GRP., THE FUTURE OF ADAPTIVE AUTHENTICATION IN THE FINANCIAL INDUSTRY (2019), https://www.onespan.com/sites/default/files/2019-03/OneSpan-AnalystReport-ISMG-Future-of-Adaptive-Authentication-in-the-Financial-Industry.pdf [https://perma.cc/8VPR-NHPA] (arguing that banks do not need to choose between providing a secure service and providing a service that is convenient for customers).

coordination-based reasons. Despite the fact that scholars and policymakers focus much of their attention on large Wall Street banks of the "too big to fail" type, the banking landscape in the United States is in fact quite fragmented. There are over five thousand FDIC-insured banks in the United States.[125] There are another 5,733 NCUA-insured credit unions.[126] And this does not even count other financial firms, such as insurance companies, online lenders, and payment companies. Thus, despite the widespread perception that the financial industry is highly concentrated, in fact there exists a large number of relevant actors.

The fragmentation of financial markets increases the difficulty of accessing and analyzing data, and thus, increases the barriers to entry for fintech companies. The cost for a small fintech startup to gain access to this system—where there are thousands of different banks that must be taken into account, each with its own website, authentication procedures, and account design—is high.[127] One of the costs, of course, is simply software: it is hard to design a system for accessing many different types of websites and to maintain that system as myriad banks review, update, and change security procedures. This is more than just a theoretical problem. In 2015, J.P. Morgan and Wells Fargo changed technical features of their websites in a way that left Mint customers unable to see their account information through Mint's app for several days.[128] In 2018, Capital One changed its cybersecurity procedures for its website in a way that limited one of the biggest data aggregators, Plaid, from accessing account information.[129] As a result, customers of Venmo, Robinhood, and Acorns all lost the ability to use those companies' apps.[130] Fintech startups that seek to provide seamless service to customers must, as a result, spend tremendous resources and manpower just ensuring that their software continues working.

Another expense that stems from fragmentation in the market is negotiation cost.[131] Many banks now require fintech companies that

125. *See Statistics at a Glance*, FED. DEPOSIT INS. CO. (June 30, 2019), https://www.fdic.gov/bank/statistical/stats/2019jun/industry.pdf [https://perma.cc/STA2-HVPZ].

126. Baker Shogry, *How Many Financial Institutions Are in the U.S.?*, PLAID (July 19, 2017), https://blog.plaid.com/how-many-fis/ [https://perma.cc/V43U-28ZY].

127. *See* Van Loo, *Making Innovation More Competitive*, *supra* note 15, at 242–44 (discussing the significant barriers to entry that fintech firms face in the financial industry).

128. Sidel, *supra* note 111.

129. Surane, *supra* note 109.

130. *Id.*

131. *See* U.S. DEP'T OF THE TREASURY, A FINANCIAL SYSTEM THAT CREATES ECONOMIC OPPORTUNITIES: NONBANK FINANCIALS, FINTECH AND INNOVATION 29 (2018) ("Consumers' ability to realize the benefits of data aggregation is limited, in part due to the lack of agreement between data aggregators and financial services companies over access to consumer financial account and transaction data.").

seek to access their financial data to first sign burdensome data sharing agreements that set forth the terms on which that access occurs.[132] While these agreements have a clear rationale from the perspective of banks, which seek to limit their exposure to liability from data sharing as well as conduct due diligence on the identity of the fintech company accessing their website, they also impose outsized costs on fintech companies seeking to provide comprehensive services to customers.[133] After all, negotiating a single contract with a bank can be costly, but at least it has a limited time horizon and fixed costs. Negotiating thousands of such contracts, on the other hand, is beyond the reach of all but the largest fintech companies.[134] Without some sort of standardized set of terms and conditions of access, the cost of doing business for most fintech institutions will simply be prohibitive.

Just as importantly, there are strong reasons for financial institutions *not* to adopt interoperable standards.[135] As mentioned before, banks and other financial firms view data sharing as, at best, a compliance cost and, at worst, a competitive threat. Thus, to the extent that banks can achieve substantive compliance with the law, but at the same time erect barriers to growth in the market, they may view such scenarios as desirable business strategies. The current structure of varied and inconsistent access protocols and application program interfaces, which raises costs for fintech companies, thus serves their interests. As a result, they will have little interest in converging towards an industry-wide, interoperable standard, which would lower barriers to entry. Even in the best of cases, where market participants have a strong interest in consistent standards and interoperable software, coordination can be difficult. Where they have active interests in divergence, coordination becomes nearly impossible.

To be sure, some firms are seeking to overcome these difficulties. One major feature of the data economy today is the growth of data aggregators, who specialize in gathering business data from a wide variety of sources and then packaging and reselling it in more user-friendly formats.[136] Data aggregators have played an essential role in

---

132. *See, e.g.,* Crosman, *supra* note 110 (describing why banks and aggregators make these agreements that, for example, only allow the aggregators access to bank systems at certain times); Crosman, *supra* note 78 (describing Wells Fargo's data sharing agreement with Plaid).

133. *See* Crosman, *supra* note 110; Crosman, *supra* note 78.

134. *See* Magnuson, *Regulating Fintech*, *supra* note 20 ("The typical fintech firm is small, leanly staffed, and narrowly focused on one type of service.").

135. *See* C. Scott Hemphill & Tim Wu, *Parallel Exclusion*, 122 YALE L.J. 1182 (2013) (exploring the problem of parallel exclusion in which multiple firms engage in conduct that blocks or slows would-be market entrants).

136. *See* Brian Hurh, Adam D. Maarec & Chris Chamness, *Consumer Financial Data Aggregation and the Potential for Regulatory Intervention*, 71 CONSUMER FIN. L.Q. REP. 20, 21

enabling fintech startups to gain greater insight into consumer financial data.[137] Plaid and Finicity, for example, have negotiated agreements with many of the largest banks for access to their systems.[138] They have been able to take advantage of their larger size and position as more established market players to gain leverage with large financial institutions.[139] Other fintech companies, in turn, can work with the data aggregators to gain access to the financial data they need. Plaid counts among its customers Venmo, Betterment, Acorns, and Coinbase.[140]

But data aggregators cannot resolve the basic problem of fragmentation: until banks have interoperable standards for data sharing, fintech companies will either have to face the daunting challenge of finding ways to access thousands of banks' platforms or, alternatively, pay third-party middlemen to do it for them. Both of these options are expensive and burdensome. Neither of them facilitates the kind of open, transparent data sharing market that is necessary to increase competition and innovation in the sector.

Thus, in order for a transparent, data-focused financial market to develop, regulation will need to force convergence and interoperability on the industry. The basic principle here is simple. Regulation should encourage financial institutions to develop interoperable platforms that allow consumers and fintech companies

(2017) ("For roughly two decades, 'data aggregators' have sought to collect consumers' financial account information from various financial institutions, including transaction, balance, and fee information relating to credit cards, auto loans, mortgages, and securities.").

137. *See* Odinet, *supra* note 63, at 802 (discussing how online banking, accounting, and other software create information bundles that help fintech platforms operate efficiently).

138. *See* Telis Demos, *Fintech Firm Plaid Raises $44 Million*, WALL ST. J. (June 19, 2016, 7:10 PM), https://www.wsj.com/articles/fintech-firm-plaid-raises-44-million-1466377808 [https://perma.cc/QYU4-77WL] (discussing how Plaid's software "allows a variety of financial-technology startups to access their customers' bank account information"); John Detrixhe, *The Seeds of Visa's $5.3 Billion Acquisition of Plaid Were Planted More Than a Year Ago*, QUARTZ (Jan. 6, 2020), https://qz.com/1784765/the-seeds-of-visas-5-3-billion-acquisition-of-plaid-were-planted-more-than-a-year-ago/ [https://perma.cc/BLL2-82EP] (mentioning Plaid's agreements with JPMorgan, Wells Fargo, and PNC); *Working Together to Strengthen Data Sharing*, FINICITY (Aug. 7, 2020), https://www.finicity.com/td-bank-data-sharing-agreement/ [https://perma.cc/U5UU-LS5D] (mentioning Finicity's agreements with Chase, Wells Fargo, Capital One, USAA, Fidelity, and US Bank); Penny Crosman, *The Battle over Bank Customer Data May Finally Be Over*, AM. BANKER (Nov. 6, 2017, 12:17 PM EST), https://www.americanbanker.com/news/the-battle-over-bank-customer-data-may-finally-be-over [https://perma.cc/44KQ-UCFL] (discussing the increase in use of fintech platforms by large banks, such as Wells Fargo's use of Finicity).

139. *See Wells Fargo and Plaid Sign Data Exchange Agreement*, WELLS FARGO (Sept. 19, 2019), https://newsroom.wf.com/press-release/innovation-and-technology/wells-fargo-and-plaid-sign-data-exchange-agreement [https://perma.cc/6PZ9-CTHS] ("We want to be where our customers are . . . [a]nd if customers want to share their Wells Fargo account information with a Plaid-supported app to help them better manage their finances, we want to enable them to do so seamlessly . . . .").

140. PLAID, https://plaid.com (last visited Dec. 11, 2020) [https://perma.cc/9NTJ-B2Z9].

access to their financial data in standardized formats and processes.[141] If banks change or upgrade their security procedures, they should be obligated to ensure that these changes do not obstruct data access.[142] The terms of access (such as liability allocation, data security requirements, and consumer consent) should be reasonably uniform across the industry.[143]

The devil, of course, is in the details, and precisely *what* standards, *what* platforms, and *what* terms should be established will be matters of intense debate. Fintech firms tend to favor open-ended access that mirrors the data that consumers can see.[144] Large incumbent banks tend to favor more limited access that has clear liability and tracing requirements.[145] Industry groups are starting to work on some of these problems, attempting to reach consensus on the terms of data sharing and access. The Financial Data Exchange, for example, is a consortium of financial services and technology companies—including large institutions like Bank of America, Capital One, Citi, and Wells Fargo—that seeks to create and disseminate data sharing standards.[146] But progress within these groups has been slow—perhaps because of the lack of incentives for interoperability among the

141. For a general discussion of interoperability and market access, see Alan Devlin, Michael Jacobs & Bruno Peixoto, *Success, Dominance, and Interoperability*, 84 IND. L.J. 1157 (2009); Suzanne Van Arsdale & Cody Venzke, *Predatory Innovation in Software Markets*, 29 HARV. J.L. & TECH. 243 (2015); Aaron K. Perzanowski, *Rethinking Anticircumvention's Interoperability Policy*, 42 U.C. DAVIS L. REV. 1549 (2009); Stacy A. Baird, *Government Role and the Interoperability Ecosystem*, 5 I/S: J.L. & POL'Y FOR INFO. SOC'Y 219 (2009). *But see* Peter Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, 72 MD. L. REV. 335 (2013) (arguing that while "data portability is appealing," a new law requiring it as a right presents concerns for competition laws, privacy, and data protection).

142. *See* Crosman, *supra* note 138 (noting that consumers need a secure and transparent way to control access to their data as they please).

143. *See* Brad Carr, Pablo Urbiola & Adrien Delle-Case, *Liability and Consumer Protection in Open Banking*, INST. INT'L FIN. 6 (2018), https://www.iif.com/portals/0/Files/private/32370132_liability_and_consumer_protection_in_open_banking_091818.pdf [https://perma.cc/6DJQ-QMJ6] (recommending a formal consumer protection framework for open banking systems addressing security, customer problems, and liability).

144. *See* Daniel Döderlein, *Fintechs' Defense of Screen Scraping Is Shortsighted*, AM. BANKER (Sept. 7, 2017, 11:48 AM), https://www.americanbanker.com/opinion/fintechs-defense-of-screen-scraping-is-shortsighted [https://perma.cc/R2HH-YBAU] (noting that fintech firms prefer screen scraping because it provides access to the same information that consumers have, whereas banks' APIs provide only limited information).

145. *Id.*

146. *See* FIN. DATA EXCH., https://financialdataexchange.org/FDX/About/FDX/About/About.aspx (last visited Dec. 11, 2020) [https://perma.cc/9VJA-9PEF] ("The Financial Data Exchange (FDX) is a nonprofit organization that is dedicated to unifying the financial industry around a common, interoperable and royalty-free standard for the secure access of user permissioned financial data."); *Members*, FIN. DATA EXCH., https://financialdataexchange.org/FDX/The%20Consortium/FDX/The-Consortium/Members.aspx (last visited Dec. 11, 2020) [https://perma.cc/3CCL-N4KD] (listing Bank of America, Capital One, Citi, and Wells Fargo as members).

largest players.[147] Regulation could speed up the development and adoption of the kinds of standards that the industry needs.[148]

Ultimately, however, precisely *what* standard becomes the industry rule is less important than the fact that there *is* a standard in the first place.[149] As mentioned before, fragmentation in the market creates a high barrier to entry for fintech firms seeking to provide services to consumers. The lack of uniformity in data access and sharing standards has meant that fintech firms must spend extensive time and resources on ensuring their programs work across the wide variety of banks and financial institutions from which they draw data. The creation of a uniform interface or software standard could simultaneously reduce transaction costs and provide financial institutions with greater certainty about the liability risks and contract terms of data sharing.

D. Security

Finally, data-oriented financial regulation must also ensure that financial data sharing occurs in a secure and protected fashion. Just as it is important to ensure that consumers own their financial data and can access and share it in reasonably convenient formats, it is also important to establish legal frameworks governing the respective obligations of parties that possess or receive that data. As the financial industry becomes more open and transparent to third-party fintech companies that filter, aggregate, and analyze individual data, it is essential that these changes do not undermine the systems in place to protect financial data from hacking or unauthorized disclosure.

Of course, simply saying that financial institutions must protect data from cybertheft does not ensure that they will, or even that they can. Recent years have witnessed an explosion of large-scale and damaging data breaches that exposed the personal information of billions of people.[150] These hacks have affected some of the largest

147. *See* Ron Shevlin, *Why Open Banking Won't Work in the US*, FORBES (Apr. 15, 2019, 5:00 AM), https://www.forbes.com/sites/ronshevlin/2019/04/15/open-banking-wont-work-in-us/ [https://perma.cc/P8MK-US67] (noting that previous attempts by big banks to integrate fintech took many years and required outside assistance).

148. Similar regulations have been proposed in the healthcare industry. *See HHS Proposes New Rules to Improve the Interoperability of Electronic Health Information*, U.S. DEP'T HEALTH & HUM. SERVS. (Feb. 11, 2019), https://www.hhs.gov/about/news/2019/02/11/hhs-proposes-new-rules-improve-interoperability-electronic-health-information.html [https://perma.cc/MZC7-RTJ5].

149. *See* William Magnuson, *The Race to the Middle*, 95 NOTRE DAME L. REV. 1183, 1209 (2020) (discussing how a standard regulation produces interoperability effects, allowing systems to "interact seamlessly" due to lack of conflicting processes).

150. A study by the Identity Theft Resource Center identified 1,244 data breaches in 2018. These breaches led to the exposure of 446 million records. The financial sector alone accounted for

companies in the world.[151] Some researchers have found troubling flaws in the cybersecurity procedures of fintech companies.[152] And precisely how law can effect change in cybersecurity, if it can at all, is a matter of substantial uncertainty.[153] Two basic principles of cybersecurity law can, however, provide incentives for companies to adopt best practices in data protection, even if they cannot provide perfect compliance.

One important feature of data sharing is traceability. The idea behind traceability is to ensure that data is tracked as it moves from one party to another.[154] Traceability is essential in securing data and preventing data from being used for unauthorized purposes.[155] It also allows consumers to see where their data is going and how it is being used.[156] Existing technologies provide support for at least some measure

---

135 breaches and 1.7 million records exposed. IDENTITY THEFT RES. CTR., 2018 END-OF-YEAR DATA BREACH REPORT 9 (2019), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf [https://perma.cc/ACN6-PACD].

151. Among the companies that suffered data breaches were Google, Facebook, T-Mobile, and British Airways. *See* Saima Salim, *Revealed: The 21 Biggest Data Breaches of 2018*, DIGIT. INFO. WORLD (Dec. 19, 2018), https://www.digitalinformationworld.com/2018/12/biggest-data-breaches-of-2018.html [https://perma.cc/L2ZT-4ZGP].

152. *See* Steve O'Hear, *Monzo Says It Wasn't Storing 'Some' Customer PINs Correctly, but Has Now Fixed the Bug*, TECHCRUNCH (Aug. 5, 2019, 7:45 AM CDT), https://techcrunch.com/2019/08/05/monzo-says-it-wasnt-storing-some-customer-pins-correctly-but-has-now-fixed-the-bug/ [https://perma.cc/JLZ2-EN79]; Vincent Haupert, Dominik Maier & Tilo Müller, *Paying the Price for Disruption: How a FinTech Allowed Account Takeover*, ROOTS, Nov. 2017, at 1, 1 (arguing that fintech companies' focus on user experience and modern design has come at the expense of security).

153. The literature on the topic is vast and varied. *See generally, e.g.*, Brian B. Kelly, Note, *Investing in a Centralized Cybersecurity Infrastructure: Why "Hacktivism" Can and Should Influence Cybersecurity Reform*, 92 B.U. L. REV. 1663 (2012); Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel, *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817 (2012); Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913 (2007); Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373 (2014); Benjamin P. Edwards, *Cybersecurity Oversight Liability*, 35 GA. ST. U. L. REV. 663 (2019); Lawrence J. Trautman & Peter C. Ormerod, *Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach*, 66 AM. U. L. REV. 1231 (2017); Benjamin Dynkin & Barry Dynkin, *Derivative Liability in the Wake of a Cyber Attack*, 28 ALB. L.J. SCI. & TECH. 23 (2018); Jeff Kosseff, *Positive Cybersecurity Law: Creating a Consistent and Incentive-Based System*, 19 CHAP. L. REV. 401 (2016); Scott J. Shackelford & Austin E. Brady, *Is It Time for a National Cybersecurity Safety Board? Examining the Policy Implications and Political Pushback*, 28 ALB. L.J. SCI. & TECH. 56 (2018).

154. *See* OPEN DATA INST. & FINGLETON, OPEN BANKING IMPLEMENTATION ENTITY, OPEN BANKING, PREPARING FOR LIFT OFF 37 (2019), https://www.openbanking.org.uk/wp-content/uploads/open-banking-report-150719.pdf [https://perma.cc/P52D-CJTT] (discussing open banking mechanisms that rely on tracking information, such as data deletion practices upon revocation of consumer consent); *The Global Industry Standard for Consumer Access to Financial Data: Organizational Overview*, FIN. DATA EXCH. 7 (2019), https://financialdataexchange.org/common/Uploaded%20files/10.3_FDX_WhitePaper_Final.pdf [https://perma.cc/9E3C-TTYK] (discussing traceability as a core principle and stating that "data users should know each step the data takes").

155. *See* FIN. DATA EXCH., *supra* note 154, at 7 (noting that traceability may "result in faster detection and response to potential errors and suspicious traffic").

156. *Id.*

of traceability in financial data.[157] Companies can, for example, include user consent information in the metadata that is associated with transaction data.[158] This allows governments and market participants to observe an audit trail and confirm that regulatory requirements are being met.[159]

Another important prong of cybersecurity within the data sharing industry is liability. The stakes here are large. One study found that the average cost of a data breach in the financial industry was approximately $5.9 million.[160] The cost *per record lost* was $210.[161] Among participants in the study, the probability of a data breach in the next two years was estimated at 29.6 percent.[162] In other words, the likelihood of a data breach is high, and the damage from that breach is large. As a result, determining who is liable for data breaches and theft is essential. Currently, however, this determination is ambiguous—there is no overarching rule on when data sharing participants are liable for data breaches or how responsibility is partitioned.[163] Instead, market participants must reach agreement on how liability works through private negotiation. This in turn introduces new pathologies, as larger market players with greater leverage can impose burdensome rules on smaller players, with the threat of market exclusion backing

157. *See* OPEN DATA INST. & FINGLETON, *supra* note 154, at 37 (discussing "codifying consent," which involves "attaching [users'] codified intent to [each] transaction data as metadata" so the consent information goes wherever the data goes).

158. *Id.*

159. *Id.*

160. *See* IBM SECURITY, COST OF A DATA BREACH REPORT 2019, at 26 (2019), https://www.ibm.com/downloads/cas/ZBZLY7KL [https://perma.cc/PR3C-UEN5] (showing average total costs of data breaches by industry, with the financial industry's average cost at $5.86 million).

161. *Id.* at 27.

162. *Id.* at 10.

163. The Congressional Research Service describes the state of data protection law in the following stark terms:

> Despite the increased interest in data protection, the legal paradigms governing the security and privacy of personal data are complex and technical, and lack uniformity at the federal level. The Supreme Court has recognized that the Constitution provides various rights protecting individual privacy, but these rights generally guard only against government intrusions and do little to prevent private actors from abusing personal data online. At the federal statutory level, while there are a number of data protection statutes, they primarily regulate certain industries and subcategories of data. The Federal Trade Commission (FTC) fills in some of the statutory gaps by enforcing the federal prohibition against unfair and deceptive data protection practices. But no single federal law comprehensively regulates the collection and use of personal data.

STEPHEN P. MULLIGAN, WILSON C. FREEMAN & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., R45631, DATA PROTECTION LAW: AN OVERVIEW 2 (2019) (citations omitted).

their demands. And consumers seeking to be made whole for their losses face the prospect of expensive and time-consuming litigation.[164]

Instead, data-oriented financial regulation must provide clear rules about who is liable in the event of a data breach or theft. Several possible structures for determining liability exist, not all of them mutually exclusive.[165] First, one could establish a rule that the breached party is responsible for any losses that result from the breach. Such a rule would have the advantage of increasing incentives for financial institutions to maintain effective cybersecurity procedures, but perhaps the disadvantage of requiring difficult determinations of where breaches occurred. Alternatively, one could establish a rule that the primary financial institution (who will typically be the bank) must compensate the consumer for losses, with the provision that the financial institution can seek reimbursement from the breached party if the breached party has been negligent in protecting or storing data. This rule would have the advantage of providing a speedy remedy for consumers, but the disadvantage of placing a disproportionate burden on banks. Finally, one could establish an industry-wide insurance fund that would be used to compensate consumers for loss, with the fund being financed by all market participants. Again, this rule has advantages and disadvantages. On the one hand, it would provide prompt compensation to consumers and force market participants to bear the cost of data risks. On the other, it would involve substantial complexity in determining who would participate in funding the insurance fund and add yet another layer of government oversight.

To be sure, data sharing liability is not unregulated under current law. The Federal Trade Commission's ("FTC") Safeguards Rule requires financial institutions to take reasonable steps to keep consumer data secure.[166] The SEC's rules require investment

164. In 2018, a group of industry participants issued a proposed "Secure Open Data Access" framework addressing these problems. It proposed that financial institutions retain responsibility for financial losses stemming from data breaches for which they are responsible and that data aggregators ensure that third party customers have the capacity to make consumers whole for any losses that result from a breach at a third party. *See* Ron Barasch, *Statement of Joint Principles for Ensuring Consumer Access to Financial Data*, ENVESTNET YODLEE (May 11, 2018), https://www.yodlee.com/financial-data/envestnet-yodlee-quovo-and-morningstar-byallaccounts-statement-of-joint-principles-for-ensuring-consumer-access-to-financial-data [https://perma.cc/2XG2-UVDU].

165. For a summary of some of these structures and how they work in practice, see Carr et al., *supra* note 143, at 4–5.

166. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 647 (2014) (noting that the Safeguards Rule requires financial institutions to develop comprehensive information-security programs to protect consumer data); Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 258–59 (2007) (discussing the Comprehensive

intermediaries to protect customer records and information.[167] These rules impose liability on financial institutions if they fail to keep consumer data secure.

The problem, though, is that there is an inherent tension between data sharing and data liability. If a financial institution is responsible for any losses stemming from cyberthefts or breaches, it will be less likely to share data with others, who might lose it or fail to safeguard it. The more a financial institution opens its systems to third parties, the higher the chance that data breaches will occur. Thus, given the substantial compliance burdens on banks today, it is understandable that they would be hesitant to grant unfettered access to consumer data, even if the consumer consents to the sharing.

But there are ways to reduce these tensions. Clear rules about where liability lies within data sharing transactions are a start.[168] So are rules that exculpate financial institutions if they demonstrate that they have adopted reasonable cybersecurity procedures.[169] The availability of a ready reserve of insurance funds to pay consumer claims could also reduce risk to financial institutions from cyber-intrusions.[170] The problem of attribution is a difficult one, but it is not insurmountable.[171] Thus, financial regulation must aim to pair data sharing with enhanced data security.

E. Lessons from Abroad

This Part has argued that financial regulation must adjust in order to encourage the kinds of beneficial innovation in finance that technology has now made possible. It has proposed a number of

---

Identity Theft Protection Act, which provides standards parallel to the FTC's and requires financial institutions to design information-security programs to suit the data they store).

167. *See* Gregg Moran, Comment, *The SEC's Data Dilemma: Addressing a Modern Problem by Encouraging Innovation, Responsibility, and Fairness*, 96 NEB. L. REV. 446, 457 (2017) (explaining that the SEC's Safeguards Rule requires investment intermediaries to adopt written policies and procedures for protecting customer data).

168. *See* Edwards, *supra* note 153, at 676–77 (arguing that although courts typically hesitate before imposing liability for cybersecurity failure, they should impose liability where companies fail to protect against known risk).

169. *See* ASHURST, *supra* note 24 (discussing liability allocation between banks, fintech firms, and customers under Europe's regulation on exploiting and sharing data).

170. *See* DELOITTE, CREATING AN OPEN BANKING FRAMEWORK FOR CANADA: CONSIDERATIONS AND IMPLICATIONS OF KEY DESIGN CHOICES 45 (2019), https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/financial-services/ca-open-banking-aoda-en.pdf [https://perma.cc/9G5F-8LBC] (arguing that Canada should require a "mandatory insurance product . . . that pays out in case of disruptive losses that lead to complete failure of a data recipient" in operating their open banking system).

171. *See* Carr et al., *supra* note 143, at 4–5 (discussing options for dividing risk between banks and third parties and arguing that making all participants "directly and explicitly" responsible for failures is the best way to protect data).

important regulatory changes, including establishing a right of ownership in financial data, a right to share that data with others, and an obligation on financial institutions to create interoperable and secure data systems. Needless to say, these proposals would require substantial adjustments to the regulatory framework of the financial industry. Fortunately for policymakers in the United States, however, other jurisdictions around the world have already started acting on precisely these questions. From Europe to Asia, countries are taking steps to open up their financial systems to more fulsome and transparent data sharing. Indeed, much of the policy experimentation in banking today occurs outside of the United States.[172] Thus, the United States does not have to legislate in a vacuum. Instead, it can learn from the lessons of other countries that have enacted financial data sharing laws. This subpart will take a look at a few regulations, from the U.K., the E.U., and Australia, to show just how varied the landscape is.

1. European Union

Much like the United States, Europe has long had a fragmented financial industry.[173] The E.U. has twenty-eight member states, each with its own financial and banking rules and regulators, making it difficult and costly for financial firms to operate across borders.[174] Cognizant of this problem, the E.U. has passed several directives aimed at creating a "single market" for financial services across the continent.[175]

These efforts began in 2007 with a rule known as the Payment Service Directive.[176] The Payment Service Directive aimed to harmonize and simplify rules governing how financial payments were made in the E.U.[177] To do so, it created an authorization and

172. *See Tech's Raid on the Banks: Digital Disruption Is Coming to Banking at Last*, ECONOMIST (May 2, 2019), https://www.economist.com/leaders/2019/05/02/techs-raid-on-the-banks [https://perma.cc/JP98-X7XN] (noting that many new banking technologies originate outside the U.S.).

173. *See* Niamh Moloney, *'Bending to Uniformity': EU Financial Regulation with and Without the UK*, 40 FORDHAM INT'L L.J. 1335, 1339–59 (2017) (discussing the history of financial regulation in the E.U., particularly in light of the United Kingdom's influence on such regulation).

174. *See* Pablo Iglesias-Rodríguez, *Supervisory Cooperation in the Single Market for Financial Services: United in Diversity?*, 41 FORDHAM INT'L L.J. 589, 612 (2018) ("Nationally based supervisory models have lagged behind the integrated and interconnected reality of today's European financial markets, in which many financial firms operate across borders.").

175. *Id.* at 640–42.

176. For a history of the development of the Payment Services Directive, see Agnieszka Janczuk, Legislative Update, *The Single Payments Area in Europe*, 16 COLUM. J. EUR. L. 321 (2010).

177. *Id.* at 326–32.

supervisory regime for payment institutions, it set forth disclosure requirements for institutions offering services to consumers, and it established a uniform set of rights and obligations for payment providers and users.[178]

Although the Payment Service Directive provided consumers with more uniform rights with regard to their payment providers and established more expansive disclosures to consumers about the terms of their accounts, it was widely seen as not going far enough.[179] In particular, many observers noted that it failed to give fintech companies adequate access to the consumer data they needed.[180] In response to these criticisms, the E.U. Council passed a Revised Directive on Payment Services, widely known as "PSD2," in 2015.[181] PSD2 aimed to go further than the initial Payment Services Directive in opening up banks to data sharing arrangements and competition from fintech firms.

Three important features of PSD2 are relevant for our purposes. First, it requires payment providers to grant access to consumer accounts to third-party providers for account information aggregation services.[182] Second, it requires payment providers to use "strong customer authentication" to ensure that any time a consumer accesses his account or initiates transactions, payment processors confirm that he consented to the transaction.[183] And third, it sets forth rules aimed at speeding up the time in which customer complaints are resolved and clarifying how liability will be allocated.[184]

---

178. *Id.*

179. *See* Alan Brener, *Payment Service Directive II and Its Implications*, *in* DISRUPTING FINANCE: FINTECH AND STRATEGY IN THE 21ST CENTURY 103, 106–08 (Theo Lynn, John G. Mooney, Pierangelo Rosati & Mark Cummins eds., 2019) (arguing that the original Payment Service Directive aided efficiency in a number of ways but still had significant failures).

180. *See* DATASTAX, PREPARING FOR PSD2: THE ROLE FOR DATA AND THE FUTURE FOR BANKING 4 (2017), https://www.fintechfutures.com/files/2017/04/Whitepaper-Datastax-EMEA-PSD2.pdf [https://perma.cc/P7KR-VWN6] (arguing that old banking systems should be reengineered to provide more streamlined access to consumer data).

181. Council Directive, 2015/2366, 2015 O.J. (L 337/35). For a summary of PSD2's key requirements, see Douglas W. Arner, Dirk A. Zetzsche, Ross P. Buckley & Rolf H. Weber, *The Future of Data-Driven Finance and RegTech: Lessons from EU Big Bang II*, 25 STAN. J.L. BUS. & FIN. 245 (2020).

182. *See* Giuseppe Colangelo & Oscar Borgogno, *Data, Innovation and Transatlantic Competition in Finance: The Case of the Access to Account Rule*, 31 EUR. BUS. L. REV. 573 (2020) (describing the access-to-account rule, which requires banks and other payment providers to provide third-party aggregators access to consumer data on a non-discriminatory basis).

183. *See Delayed Implementation of Strong Customer Authentication*, BAKER MCKENZIE 1 (Sept. 18, 2019), https://www.bakermckenzie.com/-/media/files/insight/publications/2019/09/delayed-implementation-of-strong-customer-authentication.pdf [https://perma.cc/5HHM-CYED].

184. *See The Revised Payment Services Directive (PSD2): What You Need to Know*, ERNST & YOUNG (2018), https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/banking-and-

In some ways, these features of PSD2 represent an aggressive effort to force change in the market. They require payment providers to provide account access to a wide range of fintech companies for two main purposes: to analyze the consumer's financial data and to operate the account by initiating payments.[185] This requirement marks a significant change from the status quo before the passage of the regulation, when few third-party fintech companies could initiate payments through their apps.[186] PSD2 also forced banks to significantly bolster their customer authentication procedures. Article 97 requires banks to apply "strong customer authentication" any time a consumer accesses his payment account online, initiates a payment, or "carries out any action through a remote channel which may imply a risk of payment fraud or other abuses."[187] "Strong customer authentication," in turn, is defined generally as two-factor authentication—that is, a method that requires two different types of information, such as both a password and access to a phone.[188] Again, prior to the passage of the directive, many financial institutions did not use two-factor authentication for bank accounts. Thus, in some ways, the E.U. has forced significant changes on the way that financial institutions do business.

At the same time, the E.U. has adopted a surprisingly permissive and limited regulatory stance in many other aspects of PSD2. For one, and perhaps most importantly, PSD2 only applies to payment accounts.[189] This is perhaps an obvious point, given that the name of the directive is the Payment Services Directive, but it has

---

capital-markets/bcm-pdf/ey-regulatory-agenda-updates.pdf [https://perma.cc/UKB9-HP8T] (describing PSD2's rules governing the resolution of customer complaints).

185. *See* Council Directive, 2015/2366, *supra* note 181, arts. 66-67 (requiring payment initiation service providers to communicate with account servicing payment service providers immediately after transactions to share all available data).

186. Alessandro Longoni, *PSD2 - What Changes?*, FINEXTRA (May 30, 2016), https://www.finextra.com/blogposting/12668/psd2-what-changes [https://perma.cc/LLU8-E3F8].

187. Council Directive, 2015/2366, *supra* note 181, art. 97(1).

188. Article 4(30) defines "strong customer authentication" as

> an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data.

Id. art. 4(30).

189. *See, e.g.*, *id.* art. 36 ("Member States shall ensure that payment institutions have access to credit institutions' payment accounts services on an objective, non-discriminatory and proportionate basis."); *id.* art. 67(3) ("In relation to payment accounts, the account servicing payment service provider shall: (a) communicate securely with the account information service providers . . . and (b) treat data requests transmitted through the services of an account information service provider without any discrimination for other than objective reasons.").

surprisingly profound and, in some ways, perverse effects on the regulation's scope. All of PSD2's obligations (related to consumer rights, access to data, and strong customer authentication) only apply to a very specific and limited set of accounts.[190] They apply to checking accounts, but not savings accounts.[191] They apply to current accounts, but not retirement accounts.[192] They apply to some credit card accounts, but not others.[193] This narrow application for data sharing has been widely criticized as insufficient to enable the competition and innovation that proponents originally hoped for.[194]

PSD2 has also been criticized for failing to provide uniform standards for data sharing.[195] While the regulation requires financial institutions to share consumer data with fintech companies, it does not specify the form in which such sharing must occur.[196] As a result, financial institutions have devised their own proprietary platforms for

190. PSD2 applies to "payment accounts," which it defines broadly as "account[s] held in the name of one or more payment service users which [are] used for the execution of payment transactions." *Id.* art. 4(12). But courts have interpreted the term quite narrowly, such that it only includes accounts that can be used to pay third parties without the intervention of intermediate steps. *See* Michael McKee, James Barnard, Georgia Karamani & Marina Troullinou, *ECJ Ruling on Interpretation of Payment Account Under PSD2*, DLA PIPER (Oct. 8, 2018), https://www.dlapiperintelligence.com/investmentrules/blog/articles/2018/ecj-ruling-on-interpretation-of-payment-account-under-psd2.html [https://perma.cc/G59S-64KL] (discussing the ECJ's finding that a defining characteristic of "payment accounts" is the ability to directly execute payment transactions without an intermediary account).

191. McKee et al., *supra* note 190.

192. *See Frequently Asked Questions: Making Electronic Payments and Online Banking Safer and Easier for Consumers*, EUR. COMM'N (Sept. 13, 2019), https://ec.europa.eu/commission/presscorner/detail/en/QANDA_19_5555 [https://perma.cc/Y7Y6-GANZ] (clarifying that current accounts are covered by PSD2 because they are accounts "where the holder can place and withdraw funds" without any intervention by a payment service provider).

193. *See Response to EBA Consultation on RTS for SCA*, ASS'N OF CREDIT CARD ISSUERS EUR., http://www.accie.eu/pdf/ACCIE%20response%20to%20EBA%20consultation%20on%20RTS%20SCA_October%202016.pdf (last visited Dec. 19, 2020) [https://perma.cc/4SHT-7DYG] (calling for greater clarification of which credit card accounts are covered by PSD2).

194. *See* Carlos Torres Villa, *We Should Extend EU Bank Data Sharing to All Sectors*, FIN. TIMES (June 3, 2019), https://www.ft.com/content/0304b078-82c6-11e9-a7f0-77d3101896ec [https://perma.cc/5XD5-9HCH] (advocating for an expansion of these regulations into other sectors to push data-driven decisions into those sectors of the economy).

195. *See* Shahrokh Moinian, *Open Banking Can Benefit from Standardized APIs*, PAYTHINK: PAYMENTSSOURCE (Jan. 7, 2019, 12:01 AM EST), https://www.paymentssource.com/opinion/psd2-and-open-banking-need-standards-for-apis [https://perma.cc/X665-4H9G]; Saira Guthrie, *PSD2 Deadline 14 March: Questions You Should Be Asking Yourself*, PING IDENTITY (Feb. 28, 2019), https://www.pingidentity.com/en/company/blog/posts/2019/psd2-deadline-march-2019-api-interface.html [https://perma.cc/GGY2-C2GB] ("The most common critique of PSD2 is that it forces banks to provide open APIs, but it doesn't specify a standard format for APIs across the EU.").

196. Council Directive, 2015/2366, *supra* note 181, art. 67(1) ("Member States shall ensure that a payment service user has the right to make use of services enabling access to account information as referred to in point (8) of Annex I [which refers to 'account information services'].").

data sharing, without a focus on interoperability or harmonization.[197] Indeed, some software companies that develop these platforms for banks market their software as providing a "competitive advantage."[198] Fintech firms have thus struggled to gain access to consumer data in reasonable forms and on convenient terms.[199] Industry groups have emerged to push for more standardized data sharing platforms, but the groups themselves are so numerous that they have failed to develop a single widely recognized standard.[200]

Ironically, PSD2's combination of deep but narrow data sharing obligations may well lead to *less* access to data than existed before passage of the regulation. The balance that PSD2 struck, after all, was to open up banks' data to fintech companies but to pair that increased access with increased data security—what it referred to as strong customer authentication.[201] Both of these requirements legally only applied to payments accounts, a very narrow slice of the financial market.[202] But whereas it was easy to limit fintech companies' access to

---

197. Here, for example, is how one fintech company described its experience in attempting to gain access to the various bank APIs it required:

> Many access procedures add weeks if not months to an already tight timeline. Some have an online registration form, but nothing happens once you submit. Others take weeks to inform us they're still processing our request or need more information. And some require notarised copies of our licenses—a big surprise because we've been trying to access dummy data for testing, not real customer data for production (yet). The worst offenders have rejected us on the basis that we are a foreign third party that did not use a local provider (QTSP) for our eIDAS certificate. . . . Most of the documentation we've gotten access to is pretty awful, some lacking even the basic description of the available APIs and responses. A significant number of banks in southern Europe do not have English-language documentation, and even when a bank uses its native language, the documentation is often incomplete.

The Sobering September Preview: Banks' PSD2 APIs Far From Ready, TINK (June 14, 2019), https://tink.com/blog/2019/06/14/psd2-updated-sandbox [https://perma.cc/ECA5-3ZUW].

198. *See* Red Hat Verticals Team, *Open Banking — How to Leverage Open APIs for Competitive Advantage in Financial Services*, REDHAT (Sept. 26, 2017), https://www.redhat.com/en/blog/open-banking-%E2%80%94-how-leverage-open-apis-competitive-advantage-financial-services [https://perma.cc/VKC2-XZSL] (explaining how APIs can provide competitive advantages by fostering creativity, increasing brand awareness, and creating new revenue models).

199. *See* TINK, *supra* note 197 (providing negative feedback on the preparedness of banks' APIs after testing over one hundred of them).

200. Efforts include OpenID's Financial-Grade API specification, the U.K.'s Open Banking Implementation Entity standard, the Berlin Group's NextGenPSD2 Framework, Financial Data Exchange's Durable Data API standard, STET's PSD2 API, and the PolishAPI Standard. Guthrie, *supra* note 195.

201. *See Access vs. Security: Takeaways for U.S. Financial Institutions from the European PSD2 Open API Framework*, DYKEMA: THE FIREWALL (Aug. 1, 2018), https://www.thefirewall-blog.com/2018/08/access-vs-security-takeaways-u-s-financial-institutions-european-psd2-open-api-framework/ [https://perma.cc/NC4K-ETPE] (discussing tradeoffs of PSD2 for fintech companies and banks).

202. *See* Council Directive, 2015/2366, *supra* note 181, art. 36 (ensuring that payment institutions have access to credit institutions' payment accounts services).

just payment-related financial data—it simply required an application program interface related to that data, and not other data—it was not so easy to limit strong customer authentication in this way. Customers would naturally be confused if the log-in process for their savings account only worked for their savings account at a bank, but not for their checking account, and vice versa. Instead, banks tended to adopt increased data security procedures for *all* customer accounts.[203] These increased data procedures, in turn, made it more difficult for fintech companies to access financial data, at least if it was not payment related. Indeed, one common fintech technique, known as screen scraping, is widely believed to be prohibited under PSD2 regulations.[204] The result is a bifurcated system: better access to payment data, but worse access to everything else. This is surely a perverse result.

2. United Kingdom

In August 2016, after a longstanding investigation into the state of competition in the banking market, the U.K.'s Competition and Markets Authority ("CMA") published a scathing report about the consumer banking industry. Among the more striking findings was the fact that only three percent of personal customers switched to new banks in any year, a shockingly low turnover rate.[205] The report ultimately concluded that "older and larger banks . . . do not have to work hard enough to win and retain customers" and that "it is difficult for new and smaller providers to attract customers."[206] In order to remedy this problem, the CMA issued a comprehensive set of new rules aimed at improving competition and choice in the financial industry.

---

203. *See* Edward Corcoran, *PSD2 and Strong Customer Authentication: New Rules Set to Change How Bank Customers' Identity Is Checked*, BBVA (Aug. 19, 2019), https://www.bbva.com/en/opinion/psd2-and-strong-customer-authentication-new-rules-set-to-change-how-bank-customers-identity-is-checked/ [https://perma.cc/8NDH-W4CY] (discussing how the authentication requirements will likely make user experiences with banking more complex).

204. There is some debate about the proper interpretation of PSD2's implementing guidelines. Some believe that screen scraping is banned entirely. *See PSD2: 'Screen Scraping' Ban Confirmed in Finalised Standards*, PINSENT MASONS: OUT-LAW (Nov. 28, 2017), https://www.pinsentmasons.com/out-law/news/psd2-screen-scraping-ban-confirmed-in-finalised-standards [https://perma.cc/6E97-LNSU]. Others believe it is simply prohibited without proper identification by the fintech firm using it. *See* Arturo González Mac Dowell, *Screen Scraping Is Dead, Long Live Screen Scraping*, FINEXTRA (Nov. 30, 2017), https://www.finextra.com/blogposting/14793/screen-scraping-is-dead-long-live-screen-scraping [https://perma.cc/Q5W8-Q5MC] (providing resources and explanations for determining when screen scraping is allowed).

205. *Making Banks Work Harder for You*, COMPETITION & MKTS. AUTH. 1 (Aug. 9, 2016), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/544942/overview-of-the-banking-retail-market.pdf [https://perma.cc/3RNR-ZDVB].

206. *Id.*

Among these was a set of "Open Banking" rules focused specifically on financial data.[207]

The Open Banking rules created broad obligations on the U.K.'s nine largest banks to share consumer data in a secure and standardized format and share it with third parties as requested by consumers.[208] The financial data that is covered by the rules ranged from such basic information as branch and ATM locations to more detailed information such as transaction data and product prices.[209] The CMA did not itself set the specific standards under which data sharing would occur, however. Instead, it set up a special purpose entity, the Open Banking Implementation Entity, for this task.[210] The implementation entity is itself a private organization, but it is funded by the nine largest U.K. banks and overseen by the CMA, the Financial Conduct Authority, and the Treasury.[211] The implementation entity has since issued detailed technical standards on how banks must handle financial data sharing.[212] It has also been remarkably responsive to consumer feedback. After complaints that the initial standards issued by the entity were overly cumbersome, the entity revised the standards to simplify the consumer experience.[213] The implementation entity is also tasked with managing the process for handling disputes and complaints related to open banking.[214] Importantly, however, not every fintech company can gain access to the newly open and transparent financial data ecosystem. Instead, in order to access the open banking system,

---

207. *Id.* at 7–11.

208. Other banks could opt into the arrangement, but were not obligated to do so. *See The Retail Banking Market Investigation Order 2017*, COMPETITION & MKTS. AUTH., at art. 12 (2017), https://assets.publishing.service.gov.uk/media/5893063bed915d06e1000000/retail-banking-market-investigation-order-2017.pdf [https://perma.cc/AUR9-HB5M] (listing information and data that "provider" banks, as defined in the order, must make available); Sebastian Anthony, *Which Banks Support Open Banking Today?*, BANKRATE, https://www.bankrate.com/uk/open-banking/which-banks-support-open-banking-today (last visited Oct. 2, 2020) [https://perma.cc/LWP3-HJRT] (listing "challenger banks" that have *voluntarily* taken on open banking requirements).

209. COMPETITION & MKTS. AUTH., *supra* note 208, art. 12–14.

210. *Id.* art. 10.

211. The funding banks are HSBC, Barclays, RBS, Santander, Bank of Ireland, Allied Irish Bank, Danske, Lloyds, and Nationwide. Rowland Manthorpe, *What Is Open Banking and PSD2?*, WIRED (Apr. 17, 2018), https://www.wired.co.uk/article/open-banking-cma-psd2-explained [https://perma.cc/97QP-P77K].

212. *See Open Banking: Guidelines for Open Data Participants*, OPEN BANKING IMPLEMENTATION ENTITY (2018), https://www.openbanking.org.uk/wp-content/uploads/Guidelines-for-Open-Data-Participants.pdf [https://perma.cc/7XAJ-9DW6].

213. *See* Ana Badour, Domenic Presta & Arie van Wijngaarden, *UK Open Banking Implementation Entity Report Released*, MCCARTHY TETRAULT (July 26, 2019), https://www.mccarthy.ca/en/insights/blogs/snipits/uk-open-banking-implementation-entity-report-released [https://perma.cc/TX2R-XVPT].

214. OPEN BANKING IMPLEMENTATION ENTITY, *supra* note 212, § 7.

startups must first be approved by the Financial Conduct Authority.[215] The Financial Conduct Authority, thus, plays a gatekeeping role in accrediting and regulating third-party providers in the open banking industry.[216]

It is surely too early to tell how open banking rules in the U.K. will ultimately change the consumer banking market. Rules continue to be issued and revised, and banks are still working on updating their platforms.[217] There are signs, however, that the rules have introduced more competition into the financial market. As of November 2019, more than 150 companies had enrolled in the open banking framework and been approved by the Financial Conduct Authority.[218] The companies range from large institutions, such as American Express and Barclays, to innovative startups, such as Revolut and Starling.[219] The accounting firm PwC issued a report that estimated that more than thirty-three million people would sign up for open banking services by 2022.[220]

At the same time, there are reasons for caution. Some observers have noted that banks' open banking platforms are remarkably unreliable.[221] In April 2019, the CMA reprimanded several banks for failing to meet their mobile app functionality requirements.[222] And consumers have little awareness of the new efforts to facilitate data sharing: one survey found that only one in four people had heard of open banking and that, of those who had heard of it, only one in five knew what it meant.[223]

---

215. *See* Manthorpe, *supra* note 211 ("Only startups that have been approved by the Financial Services Authority [now known as the Financial Conduct Authority] will be allowed to use the system.").

216. *See id.*

217. *See CMA Issues Directions to 5 Banks*, OPEN BANKING IMPLEMENTATION ENTITY (Apr. 1, 2019), https://www.openbanking.org.uk/about-us/latest-news/cma-issues-directions-to-5-banks/ [https://perma.cc/QNX6-K86R] (reporting that the CMA issued new directions to five banks not meeting Open Banking deadlines).

218. *See Meet the Regulated Providers*, OPEN BANKING IMPLEMENTATION ENTITY, https://www.openbanking.org.uk/customers/regulated-providers/ (last visited Oct. 2, 2020) [https://perma.cc/5PWF-ENDJ] (listing each currently regulated provider).

219. *Id.*

220. Lucy Warwick-Ching, *Open Banking: The Quiet Digital Revolution One Year On*, FIN. TIMES (Jan. 10, 2019), https://www.ft.com/content/a5f0af78-133e-11e9-a581-4ff78404524e [https://perma.cc/9QQG-G3X7].

221. *See Is Open Banking Being Hobbled by Outages?*, FINEXTRA (May 23, 2019), https://www.finextra.com/newsarticle/33870/is-open-banking-being-hobbled-by-outages [https://perma.cc/MJ3W-7AQU].

222. Peter Walker, *CMA Reprimands Banks over Open Banking Delays*, FSTECH (Apr. 9, 2019), https://www.fstech.co.uk/fst/CMA_Reprimands_Banks_Over_Open_Banking_App_Delays.php [https://perma.cc/KNV9-TM89].

223. *See* Warwick-Ching, *supra* note 220.

3. Australia

In 2017, the Australian government began a multiyear effort to reform its laws on data governance, with a particular focus on the treatment of consumer data. In connection with this effort, Prime Minister Turnbull announced that the government would be introducing "Consumer Data Right" legislation across sectors to ensure the "very simple idea that the customer should own their own data."[224] As part of this effort, the government commissioned a report on the state of the banking sector and how a consumer data right might be implemented.[225] The resulting report concluded that aggressive new regulation would be required in the sector in order to stimulate innovation and competition, noting that "given the competitive advantages afforded to large incumbent firms by limiting the ability of customers to share their data with third parties, [private sector] initiatives alone seem unlikely to lead to a widespread increase in data sharing across the banking sector."[226] After a period of consultation, the Australian government eventually enacted the Consumer Data Right Bill into law in 2019.[227]

Australia's open banking rules are both broad and deep. They apply to a wide array of consumer data, including product data, customer data, account data, and transaction data.[228] They also apply to a broad array of accounts, including credit and debit cards, deposit accounts, transaction accounts, and loans.[229] And finally, they apply to a broad array of financial institutions—all deposit-taking institutions are obliged to comply with the open banking rules.[230] In connection with these efforts, the Australian government has created a new "Data

224. Media Release, Assistant Minister for Cities and Digital Transformation, The Hon. Angus Taylor MP, Australians to Own Their Own Banking, Energy, Phone and Internet Data (Nov. 26, 2017), https://parlinfo.aph.gov.au/parlInfo/download/media/pressrel/5656429/upload_binary/5656429.pdf;fileType=application%2Fpdf#search=%22media/pressrel/5656429%22 [https://perma.cc/JA9P-3BRB].

225. *Open Banking: Customers, Choice, Convenience, Confidence*, AUSTL. GOV'T, at vii (2017), https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-_For-web-1.pdf [https://perma.cc/CSE5-FZTG].

226. *Id.* at 4.

227. Robyn Chatwood & Ben Allen, *Australian Government Passes Consumer Data Right Legislation on 1 August 2019*, DENTONS (Aug. 8, 2019), https://www.dentons.com/en/insights/alerts/2019/august/8/australian-government-passes-consumer-data-right-legislation-on-1-august-2019 [https://perma.cc/2YXJ-YJPJ].

228. *Id.*

229. *Id.*

230. *Id.*

Standards Body," with authority to establish the technical standards for data sharing within the industry.[231]

At the same time, in order to prevent a chaotic transition in the industry, Australia has created a series of stages in which progressively more burdensome requirements come into force. In the first stage, which began in January 2020, Australia's four largest banks—Commonwealth Bank of Australia, the National Australia Bank, the Australia and New Zealand Banking Group, and Westpac (the "Big Four")—were required to publicly share product data about credit cards, debit cards, deposit accounts, and transaction accounts.[232] In the second stage, which came into force in February 2020, the Big Four are required to share consumer data about these accounts, as well as data for mortgage accounts.[233] In later stages, data sharing requirements would expand to personal loan and other financial accounts and also apply to financial institutions beyond the Big Four.[234]

Finally, Australia's efforts to govern the handling and sharing of data go beyond just the financial industry. The Consumer Data Right Bill specified that the financial industry would be the first industry to be regulated, but that other industries would also come under its rules.[235] In future years, it is expected that industry-specific rules will be developed for the energy, phone, and internet sectors.[236]

While Australia's open banking rules are still in development, with many of the most significant obligations yet to come into force, they give a sense of the range of approaches that are available to

---

231. *See Banking Advisory Committee*, CONSUMER DATA STANDARDS, https://consumerdatastandards.org.au/about/advisory-committee/ (last visited Oct. 3, 2020) [https://perma.cc/TY5P-JLS2] (describing the Banking Advisory Committee's role in developing banking-specific technical standards and supporting the Data Standards Body).

232. *See Consumer Data Right Rules – Data Sharing Obligations, Phasing Summary Table*, AUSTL. COMPETITION & CONSUMER COMM'N (Sept. 2, 2019), https://www.accc.gov.au/system/files/Proposed%20CDR%20rules%20-%20Phasing%20table.pdf [https://perma.cc/W7K7-QUMM] [hereinafter *Phasing Summary Table*] (scheduling phases for banks' data sharing obligations by product type); *Competition and Consumer (Consumer Data Right) Rules 2019*, AUSTL. COMPETITION & CONSUMER COMM'N 120 (Sept. 2, 2019), https://www.accc.gov.au/system/files/Proposed%20CDR%20rules%20-%20August%202019.pdf [https://perma.cc/5UNH-GVUH] [hereinafter *Competition and Consumer Rules*] (detailing which products are categorized as phase one products).

233. *See Phasing Summary Table*, *supra* note 232 (scheduling banks' data sharing obligations for phase two products for February 2020); *Competition and Consumer Rules*, *supra* note 232, at 120 (detailing that mortgage offset accounts are phase two products).

234. *See Phasing Summary Table*, *supra* note 232 (scheduling banks' data sharing obligations for phase two and phase three products); *Competition and Consumer Rules*, *supra* note 232, at 120–21 (detailing that personal loan accounts are phase two products and other financial accounts are phase three products).

235. *See Treasury Laws Amendment (Consumer Data Right) Bill 2019* (Cth) 89–90 (Austl.) (establishing procedures for the banking and energy sectors' transition to data regulation).

236. *See id.* (establishing procedures for data regulation in the energy sector).

governments crafting data autonomy in financial regulation. Unlike the E.U.'s PSD2 framework, Australia's rules apply broadly to a wide range of financial products. Unlike the U.K.'s Open Banking framework, they extend not just to the largest banks, but also to smaller financial institutions. And finally, unlike either the E.U.'s or the U.K.'s regulatory frameworks, Australia's data rules will eventually apply outside of just financial institutions, touching the vast majority of consumer data across sectors. It remains to be seen how effective the various approaches will prove to be.

III. THE LIMITS OF DATA SHARING

This Part highlights three types of risk that increased financial data sharing presents and sketches out some initial thoughts on how to limit these risks. First, data sharing raises a difficult question of *consent*, involving how to determine whether a consumer has truly agreed in an informed way to data sharing arrangements. Second, data sharing presents a problem of *cartelization*, regarding how to prevent financial institutions from colluding with each other. Finally, data sharing presents a problem of *cost*, regarding how to pay for the necessary technological upgrades. None of these problems are insurmountable, but they do involve tricky questions of law and economics that must not be ignored by policymakers.

A. Consent

Consent is at the foundation of data sharing.[237] If consumers own their data, then they have the right to share it. Where they agree to allow others to use their data—whether for better map directions, more interactive social media accounts, or simply cheaper services—then data sharing should take place. Where they do not, then data sharing should be prohibited. Nearly all legislative efforts to improve the treatment of data have focused on the idea of consumer consent as the threshold requirement. For example, Europe's GDPR makes it unlawful for companies to process data related to an individual *unless the individual has given consent to such processing*.[238] The U.S.'s Cable

237. *See* Cohen, *supra* note 7, at 1423–24 (explaining that individual autonomy is a fundamental value of informational privacy).

238. *See* Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 6(1)(a), 2016 O.J. (L 119) (EU) [hereinafter GDPR] ("Processing shall be lawful only if and to the extent that at least one of the following applies: . . . the data subject has given consent to the processing of his or her personal data for one or more specific purposes . . . .").

Communications Policy Act of 1984 prohibits cable companies from collecting personally identifiable information about individuals *without their prior consent*.[239] Canada's Personal Information Protection and Electronic Documents Act requires companies to obtain *consent* from users before collecting, using, or disclosing personal information.[240] The underlying assumption behind these requirements is that if companies are required to receive a consumer's consent before using their data, then data will be used in ways that are more beneficial for the consumer.

But if data autonomy begins with the concept of consent, then a lot hinges on precisely how consent is defined. If a fintech company offers a retirement savings tracker, and it includes in its terms and conditions a provision that it may use your data to "improve its services," does this mean that it can sell your data to others in order to hire better engineers? If an AI startup that analyzes your payments history to improve your budget states that it may use your payments history to "develop new features," does that mean that all of its employees can examine what you are buying from the grocery store, or on Amazon, or from the pharmacy, as long as they are working on a project related to it? And if you delete an account aggregator app like Mint from your phone, but fail to explicitly tell the company to stop accessing your data, can the company keep doing so in perpetuity?

The problem here, of course, is that it is remarkably easy to get consumers to consent to anything on the internet. Numerous studies show that the vast majority of users fail to read the terms and conditions of apps and software.[241] Consumers use so many different services now that it would be an overwhelming task to read and process the sometimes hundred-page agreements that companies impose on them—one study found that it would take the average user seventy-six work days just to read the terms of service of the websites they visit

239. 47 U.S.C. § 551(b)(1).

240. *See* Personal Information Protection and Electronic Documents Act, S.C. 2000, c 5, art 6.1 (Can.) ("[T]he consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.").

241. *See* Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1884 (2013) (noting that most people do not regularly read privacy notices and even fewer people read end-user license agreements or boilerplate contract terms); George R. Milne & Mary J. Culnan, *Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices*, 18 J. INTERACTIVE MKTG. 15, 20–21 (2004) (explaining that 17.3 percent of study participants never read privacy notices and 65.1 percent of "readers" rarely or sometimes read privacy notices); Solon Barocas & Helen Nissenbaum, *On Notice: The Trouble with Notice and Consent*, PROCS. ENGAGING DATA F., Oct. 2009, at 1 (arguing that privacy regulations' notice and consent provisions are insufficient to attain moral legitimacy).

over the course of a year.[242] Another found that ninety-eight percent of users failed to notice that the terms of service for a fictitious social networking service included a clause assigning their first born child to the network.[243] And while the problem of consent in browsewrap and clickwrap agreements[244] is well known among contract scholars, there are no quick fixes.[245] This is more than just a theoretical problem, too. In 2019, it was discovered that Amazon workers were using Amazon's Alexa devices to listen in on conversations in people's homes—Amazon defended the practice as "help[ing] us train our speech recognition and natural language understanding systems, so Alexa can better understand your requests, and ensure the service works well for everyone."[246] In 2018, Google admitted that employees of third-party app developers could read people's Gmail emails—the practice was defended as being consistent with the terms contained in user agreements.[247] In 2018, the New York Times reported that Facebook was allowing Netflix and Spotify to read Facebook users' private messages—Facebook defended the practice by arguing that the companies were simply service providers that allowed users to interact with one another better.[248]

While there are no easy solutions here, a few important principles could help reduce the problem of consent.[249] First, consent

242. *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. POL'Y INFO. SOC'Y 543, 565 (2008) ("[R]eading privacy policies carries costs in time of approximately 201 hours a year, worth about $3,534 annually per American Internet user. Nationally, if Americans were to read online privacy policies word-for-word, we estimate the value of time lost as about $781 billion annually.").

243. *See* Jonathan A. Obar & Anne Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*, 23 INFO. COMMC'N & SOC'Y 128, 128 (2018).

244. *Clickwraps and Browsewraps: What's the Difference?*, OSTERBERG LLC (May 4, 2015), https://www.osterbergllc.com/clickwraps-and-browsewraps-whats-the-difference/ [https://perma.cc/63FW-WSTM] (explaining that clickwrap consent requires an overt act by the user, like clicking an "agree" button, but browsewrap consent is effective if the website's terms provide that only users who consent to the terms should access the site).

245. *See* Solove, *supra* note 241, at 1882–93 (explaining the cognitive and structural problems with relying solely on user consent to regulate data privacy).

246. Matt Day, Giles Turner & Natalia Drozdiak, *Amazon Workers Are Listening to What You Tell Alexa*, BLOOMBERG (Apr. 10, 2019, 5:34 PM CDT), https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio [https://perma.cc/F3BC-6FT6].

247. *See* Douglas MacMillan, *Tech's 'Dirty Secret': The App Developers Sifting Through Your Gmail*, WALL ST. J. (July 2, 2018, 11:14 AM ET), https://www.wsj.com/articles/techs-dirty-secret-the-app-developers-sifting-through-your-gmail-1530544442 [https://perma.cc/8H9W-A44R].

248. *See* Gabriel J.X. Dance, Michael LaForgia & Nicholas Confessore, *As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants*, N.Y. TIMES (Dec. 18, 2018), https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html [https://perma.cc/V7AG-9FWA].

249. This problem is more than just theoretical, as senators have called for investigations of consent practices in the industry. *See* Ryan Tracy, *Lawmakers Call for Investigation of Fintech*

should be defined as narrowly as possible in order to eliminate the sort of broad catchall provisions that are too common in user agreements today. One model here is the GDPR's definition of consent, which requires a user's agreement to be "freely given, specific, informed and unambiguous."[250] It also considers the context of the consent: in clarifying comments, the GDPR states, "[w]hen assessing whether consent is freely given, utmost account shall be taken of whether . . . the performance of a contract . . . is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."[251]

Second, consent should be easily revoked, either by creating a presumption that the deletion of an app amounts to a revocation of consent or through a prescribed period of time after which renewed consent must be given. This would help prevent fintech companies from continuing to gather data after a user stops using the service.[252]

Finally, given the integral importance of the financial sector to people's lives, policymakers should impose more mandatory, rather than default, rules on the sector. No matter how narrow or limited our concept of consent, consumers cannot be expected to have the resources or sophistication necessary to forecast and understand all the potential risks from data sharing. Therefore, data autonomy in financial regulation requires a robust set of mandatory rules governing data sharing, from which parties may not depart *even if* the consumer agrees to them. This Article has already highlighted a few of these—from cybersecurity to access to interoperability—but more will be needed, particularly where there is a significant risk of consumer harm. Some examples might include prohibiting broad indemnification clauses from consumers, or waivers of the right to sue in court, or unnecessarily expansive data-use provisions. The CFPB's guidance on consumer protection principles in data sharing provides a useful summary of the key areas of concern.[253]

Firm Yodlee's Data Selling, WALL ST. J. (Jan. 17, 2020, 1:45 P.M.), https://www.wsj.com/articles/lawmakers-call-for-investigation-of-fintech-firm-yodlees-data-selling-11579269600 [https://perma.cc/NQ3K-C27P] (noting that three senators asked the Federal Trade Commission to investigate Yodlee for potentially selling consumers' personal financial data without consent).

250. GDPR, *supra* note 238, art. 4(11).

251. *Id.* art. 7(4).

252. *See* Penny Crosman, *Is Finra's Dire Warning About Data Aggregators on Target?*, AM. BANKER (Apr. 9, 2018, 4:54 PM EDT), https://www.americanbanker.com/news/is-finras-dire-warning-about-data-aggregators-on-target [https://perma.cc/RB5Z-43HU] (explaining privacy and security risks of allowing financial data aggregators to gather and store consumer account information).

253. *See* CONSUMER FIN. PROT. BUREAU, *supra* note 107 (highlighting significant consumer protection challenges as the fintech industry continues to innovate).

B. Antitrust

Increased data sharing in the financial industry also raises several antitrust-related concerns.[254] The purpose of antitrust law is to ensure that companies do not engage in anticompetitive conduct.[255] While the classic case of such conduct would be the creation of a monopoly, there are many other ways in which ostensible competitors can restrict competition among themselves. These include such practices as price fixing (where competitors agree to sell their goods or services at a set price or on set terms), bid rigging (where competitors manipulate prices in a competitive bidding process), and market allocation (where competitors divide particular sectors of a market among themselves).[256] All of these problematic behaviors are facilitated, and indeed premised, on information sharing between competing companies.[257] And as the opportunities for such information sharing increase, so too do the risks.

In some ways, of course, increased data sharing should reduce concerns about competition in the financial industry. The very purpose of open banking is to incentivize competition and innovation in the sector.[258] When scholars discuss the antitrust concerns raised by big data, they typically focus on the problems that are generated when large players monopolize information and thus make it difficult for smaller players to compete with them.[259] By forcing large players to share this data with others, data autonomy can mitigate this problem. Even if large banks possess more data than fintech companies, fintech companies can gain access to the data through data sharing platforms

254. *See* ORG. FOR ECON. COOP. & DEV., INFORMATION EXCHANGES BETWEEN COMPETITORS UNDER COMPETITION LAW 2010, at 28–30 (2010) (discussing possible anticompetitive effects of information exchanges).

255. *See* Frank H. Easterbrook, *The Limits of Antitrust*, 63 TEX. L. REV. 1, 1 (1984) ("The goal of antitrust is to perfect the operation of competitive markets."); Robert H. Lande, *Wealth Transfers as the Original and Primary Concern of Antitrust: The Efficiency Interpretation Challenged*, 34 HASTINGS L.J. 65, 67 (1982) ("[I]t is unanimously agreed that Congress enacted [antitrust] laws to encourage competition . . . .").

256. *See* John M. Connor & Robert H. Lande, *How High Do Cartels Raise Prices? Implications for Optimal Cartel Fines*, 80 TUL. L. REV. 513, 533 n.111 (2005) (defining cartel behavior to include naked price fixing, customer allocation, territorial allocation, and bid-rigging conspiracies).

257. *See* ORG. FOR ECON. COOP. & DEV., *supra* note 254, at 294 ("The antitrust concern is that information exchanges may facilitate anticompetitive harm by advancing competing sellers' ability either to collude or to tacitly coordinate in a manner that lessens competition.").

258. *See Open Banking 2019 Review*, OPEN BANKING IMPLEMENTATION ENTITY (2020), https://www.openbanking.org.uk/about-us/latest-news/open-banking-2019-highlights [https://perma.cc/Z68X-AQSR] ("Open Banking was created to enable innovation, transparency and competition in UK financial services.").

259. *See* Nathan Newman, *Search, Antitrust, and the Economics of the Control of User Data*, 31 YALE J. ON REGUL. 401 (2014) (using Google as a case study to argue "for reorienting many antitrust investigations in the technology sphere").

and thus should have lower costs of entry. As a result, data sharing provides a helpful way to prevent companies from gaining or abusing dominant positions in the market.

But while data autonomy might help reduce the concerns over data monopolization, it simultaneously raises concerns about data collusion. Data collusion might occur in any number of ways. If financial institutions can see precisely what their competitors are doing, in terms of interest rates, loan terms, fees, customer base, and other sensitive areas, they may be able to reach agreements, either tacit or explicit, about accepted behaviors in the industry. They might agree to increase mortgage rates, or decrease the interest paid on checking accounts, or maintain set transaction fees. The very data that is so valuable to consumers, and that is essential to opening up financial innovation, is also quite useful for the purpose of cartelization. And, if used in ways that are difficult to detect, data sharing between competitors could provide an impetus for financial institutions to chill competition. Indeed, the FTC provides the following guidance to companies about the circumstances in which information exchanges between competitors become problematic:

> The reasonableness of an information exchange depends mainly on the nature of the information that is shared. The sharing of information relating to price, cost, output, customers, or strategic planning is more likely to be of competitive concern than the sharing of less competitively sensitive information. . . . And the sharing of company-specific data is more likely to raise concerns than the sharing of aggregated data of multiple firms that does not permit identification of information by company.[260]

One of the key considerations that the FTC takes into account when determining whether an information exchange is likely to harm competition is whether the exchange "reduc[es] uncertainty about a rival's product offerings, prices, and strategic plans."[261]

Again, this is more than just a hypothetical risk. In recent years, financial institutions have been charged with major price fixing violations in a range of areas, from the LIBOR interest rate,[262] to the prices of Fannie Mae and Freddie Mac bonds,[263] to the interest rate on

---

260. Michael Bloom, *Information Exchange: Be Reasonable*, FED. TRADE COMM'N: COMPETITION MATTERS BLOG (Dec. 11, 2014, 11:48 AM), https://www.ftc.gov/news-events/blogs/competition-matters/2014/12/information-exchange-be-reasonable [https://perma.cc/FF45-JZW6].

261. *Id.*

262. *See* Sharon E. Foster, *LIBOR Manipulation and Antitrust Allegations*, 11 DEPAUL BUS. & COM. L.J. 291, 292 (2013).

263. *See* Mike Leonard, *Citi, Other Banks Must Face Fannie-Freddie Bond Price-Fix Suit*, BLOOMBERG L. (Oct. 16, 2019, 12:18 PM), https://news.bloomberglaw.com/banking-law/citi-other-banks-must-face-fannie-freddie-bond-price-fix-suit [https://perma.cc/7DZL-A586] (reporting that ten banks allegedly colluded to drive down the price at which they bought unsecured bonds and pump up the bid prices at which they sold them).

Treasury bonds,[264] to the fees at ATMs.[265] The ready availability of data on competitors' prices, terms, and conditions will make such problematic behaviors both easier to engage in and harder to detect.[266] Even if there are no formal agreements to engage in price fixing or similar behavior, competitors might use pricing algorithms that lead to similar results.[267] Regulators will need to be attuned to these risks.

Two features of data sharing regulation could help reduce these risks. First, under any plausible version of a data sharing rule for finance, financial institutions can only share consumer financial data with the third parties that the consumer consents to.[268] Only authorized parties can gain access to consumer financial data, and thus broad information sharing between competitors would continue to be prohibited even under a data sharing framework. This rule is not perfect, of course, because it may well be that a consumer voluntarily shares financial data from one financial institution with another competing financial institution. Indeed, large banks have been some of the biggest investors in the fintech sector in recent years.[269] Even if only a small portion of consumers overlap in financial institutions, companies could gain significant insight into competitors' practices.

Second, data sharing regulations must make clear that financial institutions may only use data for the purposes that the consumer explicitly authorizes. If a consumer shares loan information from one financial institution with another firm for the purpose of optimizing the timing of loan payments, the receiving firm should not be permitted to use that information to, say, determine the prices of its own loans. This may well mean that, for large financial institutions with many different business divisions, companies will need to set up Chinese walls that prevent teams in one division from seeing the data that other divisions

---

264. *See* Kevin Dugan, *Justice Department Probes Banks for Rigging Treasuries Market*, N.Y. POST (June 8, 2015, 7:00 AM), https://nypost.com/2015/06/08/department-of-justice-probes-treasuries-market/ [https://perma.cc/77HL-WZ3N].

265. *See ATM Group Sues Visa, Mastercard over Price Fixing*, REUTERS (Oct. 12, 2011, 5:55 PM), https://www.reuters.com/article/visa-mastercard-suit-idUSN1E79B22I20111012 [https://perma.cc/F28A-BQ76] (explaining that ATM operators sued Visa and Mastercard for allegedly fixing the prices of ATM fees).

266. *See* Magnuson, *supra* note 62, at 358–59 (noting possible antitrust risks raised by the use of artificial intelligence algorithms in finance).

267. In the 1990s, for example, the Department of Justice concluded that airlines had created a computerized booking system that led them to collude on prices. *See* Ariel Ezrachi & Maurice E. Stucke, *Artificial Intelligence & Collusion: When Computers Inhibit Competition*, 2017 U. ILL. L. REV. 1775, 1786 (2017).

268. *See* discussion *supra* Section II.E (discussing lessons from international data privacy rules).

269. *See* Kate Rooney, *Wall Street Banks Are Upping Bets on Their Potential Fintech Competitors*, CNBC (Sept. 15, 2019, 9:30 AM CDT), https://www.cnbc.com/2019/09/15/wall-street-banks-are-upping-bets-on-potential-fintech-competitors.html [https://perma.cc/69EG-VMDX].

receive. Siloing information is not perfectly effective, of course, but there is evidence that it can reduce opportunistic use of information.[270]

Needless to say, these proposals will not resolve the antitrust concerns raised by data sharing in the financial world. Regulators will need to devise ways to identify and sanction firms that attempt to use consumer data for anticompetitive purposes. Similarly, they will need to clarify the kinds of information exchanges that are permitted and the range of behaviors that are not. Data sharing regulation must not be used as an excuse for financial collusion.

C. Cost

Another major issue created by an open banking framework is the problem of cost. Forcing financial institutions to adopt new data sharing technologies will impose substantial costs on them. It is hoped that these costs are more than compensated for by the benefits of increased consumer options and the incentives to create innovative new financial services. But those benefits are amorphous and long-term, while the costs are direct and immediate. And while the costs may be easily borne by large actors, smaller actors will be more burdened. Finding ways to pay for these expenses will be important to ensuring compliance.

As an initial matter, it may be helpful to examine just how expensive data sharing is for financial institutions. It is important to recognize that the transition to a data-sharing-enabled financial sector will involve expense. In the U.K., the funding needs of the Open Banking Implementation Entity were £28 million in 2017 and rose to £39 million in 2018.[271] Some estimate that the total cost of the transition could exceed £100 million.[272] The Australian bank Westpac estimated that implementing Australia's open banking platform would

---

270. On the effectiveness of information barriers, see Andrew F. Tuch, *Financial Conglomerates and Information Barriers*, 39 J. CORP. L. 563, 583–85 (2014); Martin Lipton & Robert B. Mazur, *The Chinese Wall Solution to the Conflict Problems of Securities Firms*, 50 N.Y.U. L. REV. 459, 462 (1975) ("[T]he Chinese Wall is generally the best solution to the inside information problems created by a single multiservice firm's performing potentially conflicting roles . . . ."); Massimo Massa & Zahid Rehman, *Information Flows Within Financial Conglomerates: Evidence from the Banks-Mutual Funds Relation*, 89 J. FIN. ECON. 288, 305 (2008) (noting that Chinese walls were designed to wall in information obtained from one department and prevent it from being disseminated throughout the firm); H. Nejat Seyhun, *Insider Trading and the Effectiveness of Chinese Walls in Securities Firms*, 4 J.L. ECON. & POL'Y 369, 387 (2008) (finding that Chinese walls in securities firms are porous).

271. *See* Ryan Weeks, *The Cost of Open Banking: £81m and Counting*, FIN. NEWS (May 30, 2019, 8:48 AM), https://www.fnlondon.com/articles/the-cost-of-open-banking-81m-and-counting-20190530 [https://perma.cc/ZG34-8DSN].

272. *Id.*

cost the bank between $150 and $200 million Australian dollars (or approximately $100 to $140 million U.S. dollars).[273] These are not outsized sums for the largest U.S. banks—J.P. Morgan had revenues of $30 billion just in the second quarter of 2019—but they would be substantial for many smaller regional and community banks.[274]

Much of these costs, however, stem from the process of developing the appropriate technological and regulatory standards through which financial data sharing will take place.[275] Once these standards are in place, the actual implementation of them for any given bank becomes much simpler. An estimate from the U.K.'s Open Data Institute concluded that the cost of implementing API access for a typical bank would be less than £1 million and probably in the "low-to-mid hundreds of thousands."[276] While compliance costs might increase in a data sharing environment, these estimates suggest the overall cost from a technical standpoint would be reasonable.

Moreover, the transition costs could be lowered by phasing in the regulatory obligations of data sharing over time. Just as Australia has structured its data sharing rules to initially only apply to the largest banks, and only to a portion of their data, the United States might phase in data sharing obligations to first apply to large banks (such as the "Big Four" of JP Morgan Chase, Bank of America, Wells Fargo, and Citibank), and later to smaller ones. This approach would have the dual advantage of requiring the initial costs of transition to be borne by the financial institutions that have the greatest capacity to bear them, and also opening up the benefits of data sharing to a large share of consumers.

The larger costs, of course, are not so much the initial setup costs of implementing data sharing platforms, but rather the long-term strategic costs of increased competition from a variety of fintech

273. *See* Asha Barbaschow, *Westpac Predicts Open Banking to Cost AU$200m to Implement*, ZDNET (Oct. 12, 2018, 3:52 PM GMT), https://www.zdnet.com/article/westpac-predicts-open-banking-to-cost-au200m-to-implement/ [https://perma.cc/88SG-87XK].

274. *See* Hugh Son, *JP Morgan Posts an Earnings Beat, but Forecast on Interest Income Disappoints*, CNBC (July 16, 2019, 6:23 AM EDT), https://www.cnbc.com/2019/07/16/jp-morgan-earnings-q2-2019.html [https://perma.cc/MB3B-XRML].

275. *See* Weeks, *supra* note 271 and accompanying text (discussing the cost of implementing open banking in the U.K.).

276. OPEN DATA INST. & FINGLETON ASSOCS., DATA SHARING AND OPEN DATA FOR BANKS: A REPORT FOR HM TREASURY AND CABINET OFFICE 87 (2014), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/382273/141202_API_Report_FINAL.PDF[https://perma.cc/X3Q8-LVXB].

startups.[277] Forcing banks to share data with companies that are potentially competitors creates a threat to the business models of financial institutions. Fintech companies could erode profit margins by alerting customers to better investments elsewhere or taking control over more financial transactions. Financial institutions might need to find new ways to generate revenue or they might become less profitable. Forcing banks to bear the cost of creating accessible technological platforms (such as APIs) would allow them to spread the cost over all of its business lines and customers, rather than offload it onto the consumers that need the access in the first place, but it would still be costly.

Yet the mere fact that data sharing could change the business model of financial institutions is not sufficient to conclude that doing so is undesirable. There are many behaviors in the financial markets that might be profitable for financial institutions to do in the absence of regulation, but that are prohibited, either for reasons of fairness, or efficiency or stability. The important question to ask is whether the regulation encourages free and fair competition in a way that will benefit consumers. This Article argues that it does.

CONCLUSION

This Article has argued that the clarion call of data privacy has led policymakers and scholars to ignore the broader importance of data. The emphasis on protecting consumer data from exposure has created a situation in which consumers are prevented from being able to access, use, and share their data in convenient and transparent ways. As a result, innovation and competition suffers. The financial sector provides a particularly striking example of this problem. Large asymmetric information and search and switch costs make it hard for consumers to identify and use better financial products. Banks can thus hold up customers with higher prices, worse services, and fewer options without facing strong competition. While fintech companies could potentially resolve these problems, they face one nearly insurmountable barrier: they lack access to the financial data they need. And given the inefficiencies in the market, it is unlikely that purely private sector efforts can overcome this problem. Therefore, this Article argues, we must recast financial regulation in a way that focuses on data

277. *See* Laura Brodsky, Chris Ip & Tobias Lundberg, *Open Banking's Next Wave: Perspectives from Three Fintech CEOs*, MCKINSEY & CO. (Aug. 20, 2018), https://www.mckinsey.com/industries/financial-services/our-insights/open-bankings-next-wave-perspectives-from-three-fintech-ceos [https://perma.cc/R5FD-FUF8] (discussing the ways in which fintech innovation is forcing banks to produce new products at low cost).

autonomy. Data autonomy will require clear rules on data ownership, data access, and data liability, and it will require renewed attention to the way that data is protected. While these changes will not be easy or cheap, they hold tremendous potential to drive innovation and competition for the benefit of consumers.