CENTER ON FINANCE, LAW & POLICY
UNIVERSITY OF MICHIGAN

# Consumer Autonomy and Pathways to Portability in Banking and Financial Services

Working Paper No. 01

Released November 1, 2019
Revised November 3, 2019

Authors

**Michael S. Barr**
*Joan and Sanford Weill Dean*
*Gerald R. Ford School of Public Policy*
*University of Michigan*
msbarr@umich.edu

**Abigail DeHart**
*University of Michigan Law School '19*
deharta@umich.edu

**Andrew Kang**
*University of Michigan Law School '17*
adkang@umich.edu

Center on Finance, Law & Policy
University of Michigan
735 S. State St. – Suite 5211
Ann Arbor, MI 48109

*financelawpolicy.umich.edu*



The authors would like to thank Omidyar Network for its financial support of this research. They would also like to thank several people for their thoughtful comments on earlier drafts of this paper, including: Kaitlin Asrow, Melissa Koide, Kabir Kumar, and Lauren Saunders.

Finally, the authors thank the research assistants of the University of Michigan Center on Finance, Law & Policy, especially Jennifer Chasseur, Aviv Halpern, Nicholas John, Guanjun (Samon) Sun and Wenqi (Michael) Xu.

# CONSUMER AUTONOMY AND PATHWAYS TO PORTABILITY IN BANKING AND FINANCIAL SERVICES

## I. INTRODUCTION

One of the critical ways to promote economic security is by making financial services work better for more American families. Efforts to build a financial system that promotes consumer autonomy will involve innovation and reforms to our payment systems and more broadly, our policy and legal infrastructure. Such advances help empower consumers and harness technological innovation, but they also need to be grounded with strong consumer protections—especially in an era where people increasingly turn to technology to manage their financial lives. This white paper is designed to spark conversation among academics, private sector stakeholders, public interest organizations, legislators, policy-makers, and regulators about how to approach consumer financial data.

Consumer financial data is playing an increasingly important role in driving value creation in the financial services sector. [1] Banks can now leverage advanced processing technologies to obtain new insights about client behavior to develop smarter projects. [2] At the same time, data has fueled innovation by financial technology service providers ("FSPs") that source data from banks. These service providers harness the data to create products and services that perform key consumer financial activities once handled entirely by banks and offer new experiences that banks themselves are often not delivering. [3]

---

[1] *See* Popper, "Banks and Tech Firms Battle Over Something Akin to Gold" (providing a brief overview of the value of personal financial data to banks and tech companies).

[2] For example, Bank of America tracks customers across multiple channel interactions, using the combination of website clicks, transaction records, banker notes, and call-center records to design proactive offers to customers, including credit card and mortgage refinancing, as well as cash-back deals to holders of credit and debit cards based on spending patterns. Antle, "Banking Perspectives: The Looming Battle over Customer Data."

[3] Technology companies like Mint and Betterment aggregate financial data from a customer's different financial services accounts to present one coherent picture of that customer's finances; the data can also be used to offer loans and investment opportunities. *See* "Budget Tracker & Planner | Free Online Money Management | Mint," and "Betterment: The Smart Money Manager | Save. Invest. Retire."

But who owns a customer's financial data? FSPs assert that consumers should be empowered to own their own data, especially as this would introduce new competition into the financial service sector. Many banks, however, contend that opening up consumer information to third parties raises serious risks of fraud and abuse.[4] Both sides of the debate advocate for the consumer's interest: banks on the grounds of security and privacy, and the fintech sector on the grounds of access and innovation.

The issues surrounding consumer financial data ownership are not straightforward, and the questions involved are more complex than whether or not third parties ought to be allowed access to bank accounts using customers' credentials. For example, even if banks willingly shared financial data, a surge in the free flow of consumer data would create significant privacy, security, and liability issues. Moreover, the U.S. has no singular, overarching data protection law that imposes oversight over all entities that handle consumer data. The system of regulatory oversight of data-related issues is fragmented and inconsistent—preventing stakeholders from addressing issues in a systematic and consistent manner.

Solutions to these issues need not be mutually exclusive: banks, FSPs, and policy-makers can develop standards that improve customer choice, consumer protection, security, and privacy. A cooperative effort can promote new entrants, competition, and innovation that improves both efficiency and the economic well-being of consumers. Progress will involve both technological security improvements, as well as changes in how society and regulatory bodies interact with technology.

As it stands, however, consumer financial data lacks portability. In other words, the data lacks the freedom of movement that could drive competition among service providers by allowing consumers to choose the optimum mix of products and services that suit their particular financial needs. Portability would allow consumers to take greater ownership and control over their data, which could also be good for the economy as a whole: In 2013, the McKinsey Global Institute estimated that increasing access to data in consumer finance could add between $210 - $280 billion a year to global GDP, with up to 50 percent of this total flowing to consumers through enhanced price transparency and tailored product offerings.[5]

Globally, data portability is not a novel concept. In fact, the U.S. lags significantly behind some other countries such as the U.K., Australia, and India, which have taken strides toward attaining data portability; however, the challenge facing U.S. policymakers is to construct a sensible policy framework suited to the particular regulatory and technical attributes of the U.S. consumer financial services sector.

---

[4] See *infra* Part I.A.

[5]Manyika et al., "Open Data: Unlocking Innovation and Performance with Liquid Information."

## II. CHALLENGES TOWARD ACHIEVING PORTABILITY AND AUTONOMY

Achieving greater data portability will require addressing several key challenges: (A) the lack of impetus for data-sharing; (B) problematic data sharing methods; (C) privacy, security, and liability allocation issues; and (D) a fragmented system of regulatory oversight.

### A. LACK OF IMPETUS FOR DATA-SHARING

#### 1. Banks are reluctant to share data

Banks are concerned that FSPs deploy inadequate data protection procedures that would result in a significant increase in unauthorized transactions or transactions based on faulty information.[6] This may pose a security risk to consumers, and also means that financial institutions might bear responsibility and reputational risk beyond the scope of their control.[7] Banks are also concerned that involuntary outsourcing to FSPs will disrupt the status quo and put pressure on their business lines. Because consumer data has fueled much of this involuntary outsourcing, banks have been reluctant to share data unless it was on their terms.[8]

#### 2. Consumers have limited recourse under existing consumer protection laws

Under existing consumer protection laws, consumers have a right to access their data, but the provision has not yet been implemented. Section 1033 of the Dodd-Frank Act grants consumers the right to access their personal financial information[9]. But there is significant dispute about the scope of § 1033—some argue that it includes the right to give third parties permission to access a consumer's financial data, others

---

[6] This paper is predominantly focused on bank payment issues; however, there may be a different set of issues that arise in other contexts such as asset management and insurance.

[7] *See, e.g.*, Dimon, "Dear Fellow Shareholders," April 6, 2016; *see also* Spiotto, "Financial Account Aggregation: The Liability Perspective" (providing an overview of potential risks to consumers and financial institutions involved in data aggregation).

[8] During the formative years of the fin-tech sector, several banks filed lawsuits against providers of financial aggregation services to protect their data from unauthorized screen scraping. *See* Wierzel, "If You Can't Beat Them, Join Them: Data Aggregators and Financial Institutions." While some banks have begun to partner with FSPs, banks are reluctant to share data with FSPs with which they do not have outsourcing arrangements. *See e.g.*, Popper, "Banks and Tech Firms Battle Over Something Akin to Gold."

[9] Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, 12 USC §5533 (2010).

disagree.[10] Professor Barr notes, "As a drafter of the provision that became §1033, I can state that the scope of the provision was intended to be broad – providing a framework for customer access that would encourage competition and innovation, including through the use of third-party providers and aggregators. The Treasury Department has taken a similar view."[11]

On October 18, 2017, the Consumer Financial Protection Bureau ("CFPB") released guidance intended to provide the Bureau's "vision for realizing a robust, safe, and workable data aggregation market that gives consumers protection, usefulness, and value." [12] These "Consumer Protection Principles" followed the Request for Information that the CFPB issued regarding § 1033 of the Dodd-Frank Act. The CFPB addressed nine topics including access, scope of use, and consent, and it clarified that the principles were neither binding requirements nor statements of future intent.

The CFPB also released a document of insights gained from reading stakeholders comments. It determined there were three broad camps staked out with respect to CFPB's authority under § 1033. (1) Some stakeholders, primarily account data holders, questioned § 1033's applicability to consumer-authorized data access (such as granting third parties access rather than direct access by the account holder) and encouraged the CFPB not to engage in § 1033 rulemaking.[13] (2) Other stakeholders argued that the CFPB had the necessary authority under § 1033 and that it ought to act to ensure that consumers are protected as the market develops. (3) Finally, some contended that although § 1033 grants authority, the CFPB should not engage in rulemaking but instead allow the industry to set its own mechanisms and standards.

Until regulations are issued, the matter is unresolved, despite the CFPB's public caution to banks that the right to data is self-executing. At present, some banks outright prohibit consumers from sharing their data with FSPs. Significant progress

---

[10] Wisniewski, "The Data Access Debate Is About to Get A Lot More Interesting" ("The new Consumer Financial Data Rights lobbying group, for instance, is citing Section 1033 of the Dodd-Frank Act as codifying consumers' right to access their financial data through third-party apps.").

[11] *See* "A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation" ["2018 Treasury Report"].

[12] "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation." *See* CFPB's "Request for Information Regarding Consumer Access to Financial Records," 2016.

[13] The American Banker Association, for example, contended that under §1033, the CFPB is not authorized to regulate third-party access to consumer financial information. They argue that because the statute does not mention third party access to information and that Congress would have been explicit given the greater risks associated with such access. *See* Morgan, "Request for Information Regarding Consumer Access to Financial Records," February 21, 2017. For stakeholders opposing section 1033 rulemaking, *see* "Consumer-Authorized Financial Data Sharing and Aggregation: Stakeholder Insights That Inform the Consumer Protection Principles."

has been made by other banks in developing and offering APIs for third-party data access.

## B. REFORMING DATA-SHARING METHODS

Currently, there are two primary methods for data-sharing: screen-scraping and direct data feeds under individually negotiated use agreements. But both methods are ill-equipped to support the free movement of data on a large scale, without a clear legal framework.

### 1. Screen-scraping

Since FSPs emerged to provide financial aggregation services in the 2000s, "screen scraping" has been the dominant method through which FSPs access data from accountholders such as banks. In screen-scraping, the FSP essentially impersonates the consumer, on whose behalf it is acting, without permission from the bank or even providing notice.[14] Despite its widespread use, there are some significant problems with screen-scraping.

#### a. Fraud and loss allocation issues

The FSP conducting the screen scraping is electronically indistinguishable from the consumer.[15] This is especially true in situations where the credentials given to the screen scraper enables it to not only view existing data but to initiate new transactions. In such cases, it may be difficult for banks to identify whether the account activity is actually the customer, a third-party acting with the customer's permission, or some other party who engages in a fraudulent transaction. Because customers often have to share their passwords with the FSP, this obstacle to accurate identification increases the risk of fraud.

Because screen-scraping does not require a separate risk-sharing agreement, unlike direct data feeds, financial institutions are concerned that they may bear the burden of losses in the event of fraudulent activity, faulty transactions, or downstream data breaches.[16] Even if not legally required, however, customers may expect the financial institution to make them whole in the event of a loss.[17] One concern expressed by

---

[14] *See* Alpert Gladstone, "Data Mines and Battlefields: Looking at Financial Aggregators to Understand the Legal Boundaries and Ownership Rights in the Use of Personal Data."

[15] *See* Hirschey, "Symbiotic Relationships: Pragmatic Acceptance of Data Scraping."

[16] *See* 2018 Treasury Report.

[17] *See* Spiotto, "Financial Account Aggregation: The Liability Perspective." There are a number of remaining questions associated with the liability issue. For example, who is the party responsible to

some about imposing data sharing requirements through § 1033 is that it would substantially burden small banks and credit unions that lack the resources to negotiate with data aggregators and fintech companies to develop necessary data security measures.[18]

b. Unilateral prevention measures by banks

Some banks have taken protective measures to make screen-scraping less attractive to consumers. For instance, some banks have included language in their terms and conditions that forbids the customer from passing security credentials to a screen scraper. Other banks have implemented alternative data access measures to prevent screen-scraping from working at all, such as token-based access.[19] The uncertainty caused by these measures may limit choice by pushing consumers away from services that rely on screen-scraping to access data.

c. Reliability of data

The data gathered through screen-scraping can be unreliable because it is not updated in real time. Problems can arise when a financial institution changes the design of its web site or screen. The design changes often make it difficult for the screen-scraping software to locate data, creating potential problems with inaccurate or incomplete data.[20] Consumers may rely on inaccurate data to make faulty financial decisions, and if this happens, as mentioned above, it is not clear who would be liable for any damages.

d. Summary

Screen-scraping is sub-optimal. Ideally, the system should move towards an open banking system with a right to access, date securely, and resolve liability allocation. At the same time, in the absence of a sound policy environment, screen-scraping allows for more competition by lowering costs to market entry and providing a method for FSPs to access data from smaller banks, who may lack the resources to build APIs.

---

notify consumers of a breach? *See* Maarec, Chamness, and Hurh, "Consumer Financial Data Aggregation & the Potential for Regulatory Intervention."

[18] *See e.g.*, Asrow and Brockland, "CFSI's Consumer Data Sharing Principles: A Framework for Industry-Wide Collaboration."

[19] Crosman, "Wells Fargo's Bid to Vanquish Screen Scraping," (explaining various measures taken by banks to reduce financial data aggregation by means like token-based authentication technology).

[20] Wierzel, "If You Can't Beat Them, Join Them: Data Aggregators and Financial Institutions."

2. Direct data feeds

Where banks choose to partner with FSPs through outsourcing arrangements, they usually share data through a method called a direct data feed. A direct data feed involves an agreement between the bank and the FSP where the bank communicates the account information to the FSP, which can then use it for its intended purpose. The mechanism through which this exchange is conducted can vary; one increasingly popular mechanism is the Application Programming Interface, or API, which allows different software applications to communicate with each other and exchange data directly. Direct data feeds have been gaining traction as banks and FSPs alike have begun to realize the limits and issues with screen-scraping.[21]

The use of direct data feeds, however, can also create problems. First, direct data feed access by the FSPs can place demands on smaller banks' computer systems, which could have a harmful effect on the system's speed and resilience. More importantly, reliance on privately negotiated direct data feeds results in a highly fragmented data-sharing infrastructure. It leads to a network of privately negotiated bilateral data-sharing agreements between banks and FSPs. These agreements are inconsistent among different partnerships, which limits interoperability and creates fragmentation of the data-sharing infrastructure.[22] And fragmentation makes it difficult to attain common, industry-wide standards for data privacy and security.[23] Moreover, the significant technical and legal costs required to build and maintain APIs and negotiate bilateral data-sharing agreements can effectively exclude smaller financial institutions, fintech startups, and other providers (as well as the millions of consumers they may serve) from full participation in the data-sharing ecosystem.[24]

## C. Addressing Privacy, Security and Liability allocation issues

Even if banks were more willing to share data and data-sharing methods were improved, significant privacy, security, and liability issues would remain.

---

[21] J.P. Morgan Chase's entry into a partnership with Intuit in January 2017 provides a recent example of a direct data feed. *See* Wisniewski, "JPMorgan Chase and Intuit Partner to Share Data via API." Other, less common methods include mirror sites and read-only credentials and other techniques to lessen loads on financial institutions.

[22] *See* Asrow and Brockland, "CFSI's Consumer Data Sharing Principles: A Framework for Industry-Wide Collaboration," at 2.

[23] *See* 2018 Treasury Report.

[24] *Id.*

1. Privacy

With data portability, an increase in the number and type of available FSPs may make it more difficult for consumers who use them to stay informed of the different privacy implications of their service providers. So, consumers may consent to data access without fully understanding what precise data is accessed, for how long, how their data will actually be used, and whether the data will be shared with or sold to third parties; some uses, which may be incidental to the actual service being provided, can even harm consumer privacy interests. For example, data can be used by "bad actors," such as predatory lenders, abusive debt collectors, and data brokers that do not obtain meaningful consent. Moreover, financially underserved communities who are already vulnerable to these misuses may be more prone to accept discounts and deals offered by FSPs in exchange for access to their data.[25]

One such use of data that especially raises concern is the practice of selling data to third parties who may use it for marketing or other purposes. While data protection laws limit how companies can reuse or re-disclose non-public consumer data they receive from a financial institution,[26] they do not prohibit FSPs from scrubbing and repackaging such data to make it purportedly anonymous before selling it.[27] Yet, when seemingly innocuous data is combined with other datasets and processed with advanced technologies, it can reveal insights that can harm consumer privacy interests.[28] On the one hand, these insights may benefit consumers by allowing companies to create or market better, more nuanced products. Aggregated data can create a public good that makes the market as a whole work better, as, at least in principle, is the case with credit reporting, even with all of its quite evident flaws. On the other hand, such a system may run counter to consumers' privacy interests and raises questions about fairness and data ownership. When aggregated data benefits private interests rather than the public as a whole, shouldn't consumers reap

[25] *See* "Big Data: A Tool for Inclusion or Exclusion?" (detailing concerns about financial inclusion and discrimination). *See also* Schmitz, "Secret Consumer Scores and Segmentations: Separating 'Haves' from 'Have-Nots,'" (arguing that sharing aggregation of consumer data can widen the income gap).
[26] *See* "How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act."

[27] See, *e.g.*, Hope, "Provider of Personal Finance Tools Tracks Bank Cards, Sells Data to Investors," (explaining that Yodlee, an FSP that provides personal financial management tools by aggregating and processing consumer data from a number of different accounts, sells scrubbed and anonymized transactional data).

[28] Such insights can be used to "re-identify" individuals; researchers from the Massachusetts Institute of Technology have said that they could unmask roughly 90% of people in a database of anonymous credit-card transactions with four pieces of information that included date and transaction location from a private database provided to them by an unidentified company. De Montjoye et al., "Unique in the Shopping Mall."

some of the benefit or have control over its use? And if the data are not sufficiently de-identified, FSPs face liability under GLB, Section 5 of the FTC Act and a variety of state laws.

Even with foolproof de-identification techniques, there is a concern that purportedly anonymized data can fuel algorithmic techniques that lead to the profiling of individuals. When anonymous data from an FSP can reveal individualized, day-by-day information about water bills for 25,000 citizens of San Francisco or the daily spending habits at McDonald's throughout the country,[29] firms can more easily practice price discrimination, targeted advertising, and other techniques that can have a disparate impact on minority communities or other protected groups. These techniques can harm consumer privacy interests in several ways. Algorithms can fuel faulty insights, which harm people by lumping them into the wrong group. Such techniques might also run the risk of excluding marginalized groups who are not as involved in the formal economy.[30] But even when these algorithms operate correctly, they run the risk of unfairly harming historically disadvantaged groups, whether intentionally or not. At the same time, individualized credit decisions based on big data could have a positive effect, helping members of historically disadvantaged groups get access to credit despite generalized stereotypes. Ongoing analysis to flesh out disparate impacts is important.

2. Security

Online sites are daily subject to data breaches and hacking attacks.[31] Data breaches have targeted government databases, technology companies, and prominent corporations. Successful breaches are troubling from a number of perspectives, but it has particular significance in finance—especially as more consumers make financial transactions through online platforms.

Data portability may breed new security risks because it expands the security perimeter beyond that which had traditionally been protected and controlled by banks.[32] With data portability, bad actors have a number of attack points. They can

---

[29] Hope, *supra* note 27.

[30] *See* Barocas and Selbst, "Big Data's Disparate Impact." ("Errors…may befall historically disadvantaged groups at higher rates because they are less involved in the formal economy and its data-generating activities, have unequal access to and relatively less fluency in the technology necessary to engage online, or are less profitable customers or important constituents and therefore less interesting as targets of observation.")

[31] *See, e.g.*, "Data Protection," (explaining how hackers utilized vulnerabilities in Equifax's online dispute portal to expose the names, addresses, birth dates, and Social Security numbers of over 140 million Americans); *see also* Andriotis, Rapoport, and McMillan, "'We've Been Breached."

[32] Bolotin, "The Open Banking Standard.

attack naïve consumers at the consent stage and obtain credentials by posing as FSPs through phishing or social engineering attacks, or they can target devices such as laptops, tablets and phones that store consumers' credentials.[33] They can also attack FSPs that aggregate consumer data, a strategy that can expose a significant amount of data across a number of different accounts.[34] Because FSPs can vary widely in their ability and commitment to protect consumer data, clever attackers can target the weakest link in the chain and obtain sensitive information that can then be used to compromise stronger security protections. While such attacks would be illegal under Section 5 of the FTC Act, and the Dodd-Frank Act, in practice it may be difficult to enforce these provisions. This raises more concerns for low-income, financially vulnerable households in the U.S. because empirical studies have found that low-income internet users are more likely to report problems with internet security than those with higher incomes.[35]

3. Liability allocation

Data portability creates challenges for allocating liability among various parties—the bank, the FSP that accessed data, and the consumer—when an unauthorized or fraudulent transaction occurs. Not only is it factually difficult to assess fault, but current loss allocation rules do not provide a clear system of guidelines for apportioning liability. At a high level of generality, the consumer must be protected and be made whole, and initially, this responsibility will be borne by the bank.[36] But some losses may be shifted to other parties through a number of complex private contractual arrangements.[37] Loss allocation becomes significantly more complicated and confusing when a fraudulent or unauthorized transaction happens to a consumer who uses the services of a FSP that is authorized to access and use her data. In these cases, the account holding bank's liability will largely depend on whether the cause of the fraudulent or unauthorized transaction was the consumer's involvement with the FSP. For the FSP's activities to be relevant in determining liability for an unauthorized transaction, the bank must first realize that the consumer arranged for

[33] *Id.*

[34] *Id.*

[35] Rainie et al., "Part 5: Online Identity Theft, Security Issues, and Reputational Damage."

[36] Spiotto, "Financial Account Aggregation: The Liability Perspective," at 574-75. But, even this generality is more complicated because some banks claim that consumers waive their Regulation E rights when they share their credentials with third parties. These E rights are not, however waivable. *See* 12 C.F.R. Part 205. Regulation E implements the Electronic Fund Transfer Act, which governs the rights, responsibilities, and liabilities of participants in electronic fund and remittance transfer systems. *Id.* Moreover, regardless of liability rules, consumers may still expect their bank to make them whole. *See* 2018 Treasury Report, *supra* note 14, at 35.

[37] 2018 Treasury Report.

the services and then prove that the FSP's data access had some relevant connection to the fraud. This requires resolving a host of factual issues and leads to case-specific conclusions. For instances of internal misuse of data, the liability question becomes even more compounded, requiring banks to audit data aggregators and data aggregators to audit their consumers—a practice not occurring presently. It is critical that consumers be left out of these disputes, leaving the businesses to resolve these complicated issues between themselves, while ensuring consumers are made whole. Since FSPs lack both regulatory supervision and capital requirements, bonding or insurance would need to cover potential losses, and the banks will undoubtedly be on the hook if such coverage were to prove insufficient.

## D. Clarifying a Fragmented System of Regulatory Oversight

Unlike countries such as the U.K.,[38] the U.S. has no singular, overarching data protection law that imposes oversight over all entities who handle consumer data. Rather, the regulatory framework for data-related issues is built around a patchwork of sectoral regulation that applies only to statutorily defined groups. For the consumer financial services sector, the Gramm-Leach-Bliley Act ("GLBA") imposes privacy and security requirements on all entities deemed to be "financial institutions." Because banks were typically the firms that collected and handled consumer financial data, they were clearly made subject to the privacy and security requirements of GLBA, which are complemented by the general enforcement activities of the Federal Trade Commission ("FTC") under the FTC Act. The increase in the number and type of FSPs that collect and handle consumer financial data has created problems in the application of the current framework. Even though FSPs handle the same types of data and face the same nature of privacy and security risks in their data handling as banks, many FSPs argue, quite wrongly in Professor Barr's view, that they fall outside the scope of GLBA.[39] Even if covered by GLBA, oversight of FSPs is noticeably inconsistent. Some of them are effectively unsupervised, while others that enter into outsourcing agreements with banks are subject to oversight from their partner banks which are mandated by prudential regulatory agencies to oversee their technology service providers.[40]

The inconsistencies and gaps created by this fragmented system of oversight can hinder data-handling firms from addressing issues in a unified, coherent manner. This is true even though these firms handle similar types of data and face the same

---

[38] *See* Data Protection Act 1998.

[39] *But see*, Morgan, "Request for Information Regarding Consumer Access to Financial Records," February 21, 2017 (arguing that data aggregators are "financial institutions" subject to the requirements of the Gramm-Leach-Bliley Act).

[40] "Ensuring Consistent Consumer Protection for Data Security: Major Banks vs. Alternative Payment Providers."

nature (albeit a different magnitude) of privacy and security risk. A consumer whose credentials are stolen by a bad actor from a small FSP faces the same consequences as a consumer whose credentials were stolen from a security breach of a bank. A fragmented approach to regulatory oversight also creates division and mistrust among the different firms with respect to the issues.

## III. GLOBAL APPROACHES TOWARD DATA PORTABILITY

### A. THE UNITED KINGDOM / EUROPEAN UNION

The United Kingdom and European Union have been among the first movers with respect to data portability. Generally speaking, the approach involves two complementary initiatives that largely seek to address the problems described in the previous section. First, the two-pronged regulatory reform at the E.U. level is driving the impetus for data-sharing by both mandating data-sharing by banks under the new Payment Services Directive (PSD2)[41] and establishing consumers' right to portability under the General Data Protection Regulation (GDPR).[42] Second, the U.K. Government enacted "Open Banking," an initiative to work with the financial services industry to build an open banking platform built on industry-wide API standards.[43] Specifically, "Open Banking" requires large U.K. banks to give third parties access to transaction data and has been progressing slowly but steadily since its roll out in January 2017.[44] It is worth noting that there are many similarities between the CFPB's "Consumer Protection Principles" and the E.U.'s GDPR, especially with regard to the right to data access and control.

---

[41] The European Commission issued a proposal for a revised Payment Services Directive (PSD2) in July 2013. Central to its recommendations are requirements for "payment account providers", which include banks, to allow third parties – with appropriate consent – to share account information and to initiate payments. *See* Bolotin, "The Open Banking Standard." Moreover, PSD2 makes it mandatory for these providers to provide information on the terms and conditions for the service (execution time, actual or reference exchange rate and all charges payable with breakdown) to the payer, before execution and after execution of the payment and to provide the actual exchange rate and charges (with breakdown) applied. Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, art. 52 (L337/35).

[42] The E.U. is progressing the General Data Protection Regulation (GDPR) initiative in order to provide more clarity on the basis on which their financial data is assessed and ultimately shared. Among others, one of the basic principles of the regulation is to enshrine the individual's rights to data portability – the individual may share their data freely with whomever they choose. The GDPR was finalized in 2015. Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, art. 52 (L337/35).

[43] "Data Sharing and Open Data in Banking," March 18, 2015.

[44] *See* Cocheo, "Open Banking, Present and Future - Banking Exchange." The U.K.'s Competition and Markets Authority formally implemented these reforms and had set the timeline for introducing open banking standards. *See* "Open Banking Revolution Moves Closer," February 2, 2017.

Even though GDPR is an E.U. law, privacy experts predict it may affect U.S. consumers because some international companies may find it cheaper and easier to adopt a single set of global privacy standards. Already some U.S. banks are positioning themselves to begin complying with standards set by the GDPR for the U.S.

## B. AUSTRALIA

Largely inspired by the initiatives of the U.K. / E.U., policy-makers in Australia have undertaken significant steps on data portability. A report issued by the Australian Parliament envisioned a framework in which new regulation would empower the Australian Securities and Investments Commission to both require banks to share data and also prescribe the method for doing so, namely, standardized API-based architecture.[45] More specifically, the Australian Parliament Report recommended that banks "be forced to provide open access to customer and small business data by July 2018."[46] To do so, the Australian Government would amend the Australian Securities and Investments Commission Act 2001 and, if required, the Privacy Act 1998, to empower the Australian Securities and Investments Commission to develop a binding data sharing framework for Australia's banking sector that makes use of APIs and ensuring that appropriate privacy safeguards are in place.

## C. INDIA

While the Indian government has not yet enacted any specific legislation aimed at creating data portability rights,[47] over the past decade it has made attempts to strengthen rights of consumer data protection. The Indian government has taken on an array of technical initiatives that will help to make data portability possible in the future. For example, the government established the Unique Identification Authority of India ("UIDAI"), which provides a unique ID, called "Aadhaar"[48] to all residents.

---

[45] This varies slightly from the bifurcated approach in the U.K. / E.U., in which regulatory reform mandating banks to share data and the overhaul of data-sharing methods will be conducted in separate, albeit complementary paths.

[46] "Review of the Four Major Banks (Second Report)."

[47] But there is proposed legislation that includes a right to data portability. *See* "The Personal Data Protection Bill, 2018"; *see also* Palanisamy and Nandle, "Understanding India's Draft Data Protection Bill."

[48] Aadhaar is a 12-digit numerical code issued by the Unique Identification Authority of India (UIDAI) and is used to establish a person's identity on the basis of demographic and biometric information.

Since Aadhaar's launch, 270 million bank accounts have been opened in India,[49] and the Reserve Bank of India's deputy governor has pushed banks to allow customers to move between banks without having to change their account numbers.[50] The ambitious and controversial government-backed initiative "India Stack" utilizes the data from Aadhaar to create open programming interfaces that are available to developers, allowing them to verify their customers' identities, signatures, and important documents like school records against the biometric database.[51] The Indian Supreme Court recently upheld the overall validity of Aadhaar, but also ruled that individual Aadhaar numbers could not be used by private entities to identify individuals without consumer consent—it held that doing so would run contrary to a fundamental right to privacy.[52]

## D. SINGAPORE

When it comes to open banking initiatives, Singapore has been a leader.[53] As early as 2014, the government's Smart Nation Singapore drove the adoption of new digital technologies, starting with open data and payments.[54] In 2016, Singapore's central bank, Monetary Authority of Singapore, published a comprehensive roadmap—Finance-as-a-Service: API Playbook—which set a "gold standard" for regulatory advice on the topic in Asia.[55] Singapore has also set up a regulatory sandbox to encourage innovative financial products and services to be developed within a well-defined space.[56]

In late 2017, the government built an API Exchange to serve as a centralized data-sharing platform.[57] This Exchange allows government agencies across the city to

---

[49] Garret, "India Is Likely To Become The First Digital, Cashless Society," June 28, 2017.

[50] Sharma, "RBI Pushes for Bank Account Number Portability, Banks Wary."

[51] *See* Stacey, "India Begins Building on Its Citizens' Biometrics."

[52] Chandrachud, Justice K.S. Puttaswamy (Retd.) & And. V. Union of India & Ors.

[53] The International Data Corporation puts Singapore first for open banking readiness in the Asia-Pacific. *See*, Araneta and Agrawal, "Readiness of Asia/Pacific Markets for Open Banking."

[54] This initiative includes building its Smart Financial Sector "where technology is used pervasively in the financial industry to increase efficiency, create opportunities, allow for better management of risks." "FinTech Sandbox."

[55] "Finance-as-a-Service: API Playbook."

[56] "Overview of Regulatory Sandbox."

[57] Basu, "Inside Singapore's Plans to Share Data across Agencies."

share data securely through APIs. Unlike the E.U.'s GDPR rollout, officials in Singapore gave no timeline for compliance or adoption, but so far banks in Singapore have been adopting the measures steadily because of the opportunities they see with the new technology.[58]

## IV. BUILDING A POLICY FRAMEWORK FOR PORTABILITY

As we move toward ownership of one's financial data, we need clearer rules for secure data portability that will protect privacy and ensure meaningful consent. Giving consumers ownership over their own data with a secure means to move it or share it with others will promote competition for financial services. Portability will empower consumers to better manage their financial lives with new tools for budgeting, saving, and investing. There are several questions that need to be addressed when building a framework for data portability; the following sections describe conceptual, technical, and legal considerations related to building such a framework.

### A. CONCEPTUAL: ENVISIONING A "LAYERED" APPROACH TO CONSUMER AUTONOMY

Rather than conceive of consumer autonomy as a monolithic concept, it might make more sense to think of it as a theme that underpins various aspects of the consumer financial services experience. Data ownership and portability raise questions about personal identity verification, time-bound and use-specific consent to enhance privacy protections, data security and integrity, and consumer protections. Achieving data portability will involve different challenges and policy trade-offs, and the proposed, non-exhaustive, categories below are examples of how a layered approach might help to address these wide-ranging issues.

One layer might involve developing standards for account number portability, allowing customers to switch their financial institutions while still retaining account details, including direct deposit and automatic payments, without the need to move such deposits and payments manually. A portable financial account number could enhance consumer autonomy, choice, and competition.[59]

A second aspect of consumer autonomy and portability could involve implementing unique consumer identifiers or ID verification that makes it easier to authenticate individuals. The need for identification is strongest in the developing world. As mentioned above, India, for example, has taken strides in this direction through its Aadhar program, which aims to provide all residents within the country with their own unique identification.[60] Globally valid identifiers would assist in promoting

---

[58] Rothwell, "The Brave New World of Open Banking in APAC: Singapore."

[59] *See, e.g.*, Barr and Valenti, "It Shouldn't Be So Hard to Dump Your Bank."

[60] *See supra* III.C.

cross-border remittances while enhancing anti-money laundering and anti-terrorist financing policies. Even in the U.S., low-income and immigrant populations often have difficulty establishing identity and face exclusion from the financial system as a result.

A third layer might focus on how to strike a balance on the issue of consumer consent—more autonomy should come with more ability to restrict how data is used. As discussed below in Section IV.C.1, options such as limiting consent to a particular timeframe or use might allow better consumer control over privacy without restricting innovation and access that comes with "big data" analytics. Closely related to privacy, any consumer autonomy initiative needs to build in strong data security protections to prevent theft, fraud, or other unauthorized uses.

A fourth layer involves substantive consumer protections to prevent abusive and predatory practices. We need to ensure that moves towards consumer autonomy are meaningful and real, not opportunities for the financial sector to take advantage of consumers. That means using behaviorally informed approaches to financial regulation.[61]

Lastly, we need to consider the interaction between state and federal law in regulating data use. Take the recent example of California, which passed one of the most stringent data protection laws in the country—loosely comparable to Europe's GDPR.[62] Among other changes, the law gives residents the right to prohibit the sale of their own data. It is set to go into effect in 2020, and because of California's role in the tech industry, other states will likely look to it as a leader.[63] There is a set of technical complications with California law that may make implementation quite difficult unless there are amendments to several key provisions. If other states develop their own versions of data privacy laws, moreover, there might be different, incompatible provisions leaving consumers vulnerable to loopholes and businesses liable for many different forms of compliance. Data portability between and among states in an efficient and secure way is essential. Yet experimentation at the state level is critical to making progress on consumer autonomy, given the stymied state of efforts at the federal level.

---

[61] *See* Barr, Mullainathan, and Shafir, "Behaviorally Informed Regulation."

[62] Vartabedian, "California Passes Sweeping Data-Privacy Bill." At a high level of generality, California's data privacy law and GDPR have similarities, but in reality, they are quite different. The two provide for different rights, obligations, and exceptions—so much so that compliance with one will not ensure compliance with the other. Moreover, even on its face, California law presents key implementation challenges.

[63] California was also a first mover on a data-breach notification law in 2003, which all states eventually followed. *See* Hoofnagle and King, "Security Breach Notification Laws: Views from Chief Security Officers."

## B. TECHNICAL: CONSTRUCTING AN "OPEN BANKING" PLATFORM

Policy-makers and the consumer financial services sector could work together to create an "open banking" platform based on standardized APIs, akin to the standard being implemented in the U.K.[64] Already, the financial sector has come together to promote a technical standard for an API through the Financial Services Information and Analysis Center (FS-ISAC), creating a new Financial Data Exchange (FDX).[65] This industry standard now needs to be complemented with a policy process that includes meaningful input from consumer advocates as well as FinTech sector firms, to develop an API standard that could replace screen-scraping and credential-sharing while also ensuring fair competition, open access, consumer protection, privacy and security, and at bottom, real consumer autonomy. The following describe the preliminary steps that would need to be taken:

### 1. Congressional Action

The first step could be for Congress to call on the Federal Reserve Board and the CFPB, both of which have important duties relevant to payment systems reform, to issue joint rules to implement reform within a specified time-frame. Many of the required steps can be taken with existing authorities, but the political will to act, and quickly, is lacking.

### 2. Official report or guidance laying the blueprint for the platform

The financial sector, technical experts, consumer advocates, and agencies overseeing this process should all work together to lay the blueprint for building the platform, culminating in a comprehensive report answering the following questions:

- Standardization: What are the specifications and rules addressing the data along with the technical and security aspects that need to be standardized?
    - Data standards: What are the rules by which data are described and recorded? (e.g. agreements on representation, format, definition and structure)
    - API standards: What are the specifications that inform the design, development and maintenance of an API? (e.g. architectural design, resource formats, documentation and versioning)
    - Security standards: What are the security aspects of the API specification?
- Scope: What is the scope of data to which the aforementioned standards apply? For example, consumers need access not only to their basic account data, but

[64] For more information on the U.K. initiative, see "What is Open Banking?"

[65] *See* FS-ISAC, "Financial Industry Unites to Enhance Data Security, Innovation and Consumer Control."

also to information about fees and rates and how those fees and rates apply to their own experience. This was the motivating factor behind inclusion in the Dodd-Frank Act of Section 1033, which provides consumers with the right to access their account information in machine-readable format. Yet there are important questions regarding how to incorporate purchase data—key to understanding financial usage patterns—without unnecessarily expanding the reach of regulation to generalized merchant activity.

- Governance: Who ultimately decides what will be adopted as the data, API, and security standards?
- Intellectual Property: How should the intellectual property created during the development and use of the open banking platform (codes, software, reference data, etc.) be treated under intellectual property law?
- Licensing: How should use of the open banking platform be licensed? How should permissions and access rights be defined?
- Developer resources: What kinds of developer resources are necessary to deliver a sustainable open banking platform?

### C. LEGAL: ADDRESSING PRIVACY, SECURITY AND LIABILITY ALLOCATION ISSUES

In tandem with the conceptual and technical issues of security, privacy, scope, consumer protection, and governance, there are multiple legal issues to address on the way to achieving data portability, such as issues like liability, data security, privacy, and consent. This section does not comprehensively cover each issue, but instead illustrates some of the legal questions that might arise in key areas.

#### 1. Regulating data use by FSPs: Consent and Control

When data is shared with third parties, there is no easy way for consumers to control all of their shared financial data. As Federal Reserve Governor Lael Brainard observed during a Keynote at a recent conference at the University of Michigan, "there's an increasing recognition that consumers need better information about the terms of their relationships with [data] aggregators, more control over what is shared, and the ability to terminate the relationship."[66] Consumers often do not fully know the terms of agreement with an FSP. As a recent U.K. study following their Open-Banking Initiative found, even if consumers expressed privacy concerns, speed and convenience often trumped these concerns—consumers relied more often on user ratings or a blind belief that regulations would protect them.[67] The amount of

[66] Brainard, "Where Do Consumers Fit in the Fintech Stack?"

[67] *See* Whitley and Pujadas, "Report on a Study of How Consumers Currently Consent to Share Their Financial Data with a Third Party." The study offered three dimensions that it found affected informed consent: FSP practices regarding how terms and conditions are presented, individual behavior including attitudes toward privacy, and the social context including consumers' attitudes toward their regulatory environment

information people can pay attention to is limited,[68] which should affect the way we think about effective regulation. Given consumers' behavioral tendencies when operating technology in fast-paced and contextually complicated environments, there may need to be more incentive to exercise control over their right to data and keep an eye on their data.[69] Consider also that as financial technology changes, so too might expectations of privacy regarding what kind of financial information is "normal" to share.[70] These normative expectations affect how much consumers care to manage their data privacy.

Issues of consent are further complicated in the realm of financial data sharing because there is no central way for consumers to view every entity that has permission to access their data.[71] Even if a consumer cancels an account with an FSP, the length of time that the company can hold onto that consumer's financial information varies depending on the contract. There should be additional and affirmative consent whenever a consumer's data is used for any purpose other than the product or service he or she signed up for, and time limitations on use based on particular need.

As long as FSPs adhere to their own terms of use, U.S. laws generally do not prohibit selling or licensing access to consumer data. Such access can be for almost any purpose or duration and, with exceptions under the GLBA, often without notice. Without laws in place, this leaves consumers to trust companies not to misuse the data—a trust that may lessen after scandals such as Cambridge Analytica.[72] What is more, there is no straightforward path to regulatory solutions to improve the process for consent. Although there is, for example, an "opt-out" provision in the GLBA,[73] the

---

[68] *See* Barr et al., 2012, note 6, at 442.

[69] "Digital Privacy Rights Require Data Ownership."

[70] For example, a recent article about a researcher's analysis of more than 200 million public Venmo transactions. She was able to glean information about drug use and eating habits based on publicly available transaction information. *See* Solon, "Venmo." This kind of information about payments seems highly intrusive.

[71] *See* "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation." *See also* Asrow and Brockland, "Liability, Transparency and Consumer Control in Data Sharing: A Call to Action for Financial Services Providers and Regulators."

[72] *See* Langevin, "Facebook Case Demonstrates Gaps in Data Ownership Laws."

[73] *See* FTC, "How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act," at 8-11. The Act requires that financial institutions notify their customers of their information sharing practices and inform them of their right to "opt-out" if they do not want their information shared with certain third parties. Although GLBA outlines an opt-out system, it is not clear that data aggregators are covered under the provision because they do not have "direct consumer relationships", and in any event the opt-out is weak consumer protection.

provision is highly unlikely to matter for most consumers who cannot be expected to understand what it means to opt-out of 3rd party data sharing. Section 1033 of the Dodd-Frank Act provides the right to data access, but says nothing about retracting data once shared.

There needs to be a robust process to achieve more informed consent from consumers, to better facilitate understanding about how their data is being used and how long it will be used for. Disclosures have proven a weak consumer protection tool,[74] and clicking "I agree" does not add much more by way of informed consent. Rather, FSPs should provide an opt-in system for consumers to more easily manage the scope and substance of their shared financial lives; there should also be an easy way to stop sharing data and request that non-aggregated formerly shared data is deleted, unless necessary for fraud protection or legitimate credit determinations.[75] Another related solution is to make data sharing time-limited. As mentioned, current privacy laws put the burden on consumers to "opt-out" of access by their service providers. Regulators should consider flipping the paradigm of "opt-out" on its head and having FSPs disclose to consumers how exactly their data will be used, requiring opt-in to specified uses for specified times. This paradigm could lead to more informed time- and use-specific consent protocols; the consumer would only give consent to share data for a limited amount of time, after which data would be deleted unless necessary for market functioning or research. In addition to time-limited consent, putting limits on the substance of data shared will be critical. Such limits would mean that FSPs only obtain the minimum amount of data needed for the purpose that the consumer has authorized. A key consideration on the other side is the need to retain data for market functioning, such as credit bureau reporting, which requires ongoing positive and negative data on both individual consumers and the market as a whole. Indeed, innovations using artificial intelligence and machine learning, requires ongoing availability of such individualized aggregate data.

2. Creating a more effective system of liability allocation

The current means of allocating liability for unauthorized transactions is inefficient and confusing; resolution depends on negotiation and resolving complicated factual issues. The following lists possible ways to streamline the process and deliver more clarity to the stakeholders:

- Joint fact-checking and monitoring efforts: Both banks and FSPs can work together, in terms of effort and cost, to improve fact-checking and monitoring procedures so that when fraudulent transactions occur, it becomes easier to pinpoint the cause of that breach.
- Ordered system of reimbursement and loss-shifting contractual arrangements: Banks and FSPs can consider implementing a system of reimbursement and loss-shifting contractual arrangements such as those used by payment

[74] *See, e.g.*, Issacaroff, "Disclosure, Agents, and Consumer Protection."

processing organizations. While this approach might bring greater certainty, it could be limited by the fact that some FSPs have limited capital from which to provide reimbursements.

- Mitigate risk with insurance: Banks and FSPs can coordinate with insurance agencies to tailor solutions that cover liability for unauthorized or fraudulent transactions, which might save time and effort required to conduct fact-checking or negotiating reimbursements.

At the end of the day, consumers will rely on their banks to protect them against fraud and unauthorized transactions, and the law should protect the reasonable expectations of consumers in that respect.

## V. CONCLUSION

The financial system is not currently well designed to meet the needs of households, and its very structure reduces competition, decreases efficiency, and undermines our basic sense of fairness. There are many ways we need to reform the financial system, but one important component includes a focus on enhancing consumer autonomy. A greater focus on the human beings the financial sector is supposed to serve would lead to greater control over their own financial data. Such consumer autonomy would include enhanced privacy protections, stronger data security liability incentives, meaningful consumer protections, globally accepted identification, and portability, so that consumers could more readily switch bank accounts. Better access to one's own data and usage patterns would better enable budget management, would increase competition in banking, helping to lower fees—especially after-the-fact "gotcha" contingent fees, and would improve the quality of financial services. Together with reforms to our payment system and funds availability rules, these steps would go a long way towards making the financial system truly work for all of us.

## BIBLIOGRAPHY


Andriotis, AnnaMaria, Michael Rapoport , and Robert McMillan. "'We've Been Breached': Inside the Equifax Hack." *Wall Street Journal*, September 18, 2017, sec. Business. https://www.wsj.com.

"A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation." U.S. Department of the Treasury, 2018.

Alpert Gladstone, Julia. "Data Mines and Battlefields: Looking at Financial Aggregators to Understand the Legal Boundaries and Ownership Rights in the Use of Personal Data." *J. Marshall J. Computer & Info. L.*19 (2001): 313, 317.

Antle, Karl. "Banking Perspectives: The Looming Battle over Customer Data." The Clearing House, 2016. https://www.theclearinghouse.org.

Araneta, Michael, and Anuj Agrawal. "Readiness of Asia/Pacific Markets for Open Banking." IDC Perspective, May 2018. https://www.idc.com.

Asrow, Kaitlin, and Beth Brockland. "CFSI's Consumer Data Sharing Principles: A Framework for Industry-Wide Collaboration." Center for Financial Services Innovation, October 2016.

Asrow, Kaitlin and Beth Brockland. "Liability, Transparency and Consumer Control in Data Sharing: A Call to Action for Financial Services Providers and Regulators." Center for Financial Services Innovation, September 2017.

"Banking and Finance – The ODI." Accessed November 1, 2019. https://theodi.org.

Barocas, Solon, and Andrew D. Selbst. "Big Data's Disparate Impact." *Calif. L. Rev.*104 (2016): 671, 684–85.

Barr, Michael S., Sendhil Mullainathan, and Eldar Shafir. "Behaviorally Informed Regulation." In *Behavioral Foundations of Public Policy*, 440–64. Princeton: Princeton University Press, 2012.

Barr, Michael, and Joe Valenti. "It Shouldn't Be So Hard to Dump Your Bank." American Banker, November 4, 2016. https://www.americanbanker.com.

Basu, Medha. "Inside Singapore's Plans to Share Data across Agencies." *GovInsider*(blog), May 19, 2017. https://govinsider.asia.

Betterment. "Betterment: The Smart Money Manager | Save. Invest. Retire." Accessed November 2, 2019. https://www.betterment.com.

"Big Data: A Tool for Inclusion or Exclusion?" Washington, DC: Federal Trade Commission, January 2016.

Bolotin, Louise ed. "The Open Banking Standard." Open Bank Working Group, 2016. https://www.scribd.com.

Lael Brainard, "Where Do Consumers Fit in the Fintech Stack?" at "FinTech Risks and Opportunities: An Interdisciplinary Approach", a conference sponsored by the University of Michigan. Ann Arbor, Michigan, November 16, 2017. www.federalreserve.gov. *See also*, Keynote Address, YOUTUBE, https://www.youtube.com.

"Budget Tracker & Planner | Free Online Money Management | Mint." Accessed November 2, 2019. https://www.mint.com.

Chandrachud, D. Y. Justice K.S. Puttaswamy (Retd.) & And. V. Union of India & Ors., No. 424 (August 24, 2017).

Cocheo, Steve. "Open Banking, Present and Future - Banking Exchange," May 15, 2018. https://www.bankingexchange.com.

"Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation." Washington, DC: Consumer Financial Protection Bureau, October 18, 2017.

"Consumer-Authorized Financial Data Sharing and Aggregation: Stakeholder Insights That Inform the Consumer Protection Principles." Washington, DC: Consumer Financial Protection Bureau, October 18, 2017.

Crosman, Penny. "Wells Fargo's Bid to Vanquish Screen Scraping." American Banker, June 7, 2016. https://www.americanbanker.com.

Data Protection Act 1998 (n.d.). https://www.legislation.gov.uk.

"Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach." U. S. Government Accountability Office, September 7, 2018.

GOV.UK. "Data Sharing and Open Data in Banking: Call for Evidence." HM Treasury, January 28, 2015. https://www.gov.uk.

"Digital Privacy Rights Require Data Ownership." *Financial Times*, March 21, 2018. https://www.ft.com.

Dimon, Jamie. "Dear Fellow Shareholders," April 6, 2016. https://www.jpmorganchase.com.

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance), Pub. L. No. 32015L2366, OJ L 337 (2015). http://data.europa.eu.

"Ensuring Consistent Consumer Protection for Data Security: Major Banks vs. Alternative Payment Providers." The Clearing House, August 2015. https://bpi.com.

"Finance-as-a-Service: API Playbook." The Association of Banks in Singapore & The Monetary Authority of Singapore, n.d. https://abs.org.sg.

Smart Nation Singapore. "FinTech Sandbox," January 29, 2019. https://www.smartnation.sg.

FS-ISAC. "Financial Industry Unites to Enhance Data Security, Innovation and Consumer Control," October 18, 2018. https://www.fsisac.com.

Garret, Olivier. "India Is Likely To Become The First Digital, Cashless Society." Forbes, June 28, 2017. https://www.forbes.com.

Hirschey, Jeffrey Kenneth. "Symbiotic Relationships: Pragmatic Acceptance of Data Scraping." *Berkeley Tech. L. J.*29 (2014): 895.

Hoofnagle, Chris, and Jennifer King. "Security Breach Notification Laws: Views from Chief Security Officers." Samuelson Law, Technology & Public Policy Clinic, UC Berkeley School of Law, December 2007. https://www.law.berkeley.edu.

Hope, Bradley. "Provider of Personal Finance Tools Tracks Bank Cards, Sells Data to Investors." *Wall Street Journal*, August 7, 2015, sec. Business. https://www.wsj.com.

Federal Trade Commission. "How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act," July 2, 2002.

Issacaroff, Samuel. "Disclosure, Agents, and Consumer Protection." *J. of Institutional and Theoretical Economics*167, no. 56 (2011).

Langevin, Jim. "Facebook Case Demonstrates Gaps in Data Ownership Laws." The Hill, March 30, 2018. https://thehill.com.

Maarec, Adam D., Christopher M. A. Chamness, and Brian J. Hurh. "Consumer Financial Data Aggregation & the Potential for Regulatory Intervention." Lexology, June 7, 2017. https://www.lexology.com.

Manyika, James, Michael Chui, Peter Groves, Diana Farrell, Steve Van Kuiken, and Elizabeth Almasi Doshi. "Open Data: Unlocking Innovation and Performance with Liquid Information." McKinsey Global Institute, October 2013. https://www.mckinsey.com.

Medha, Basu. "Inside Singapore's Plans to Share Data across Agencies." *GovInsider*(blog), May 19, 2017. https://govinsider.asia.

Montjoye, Y.-A. de, L. Radaelli, V. K. Singh, and A. S. Pentland. "Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata." *Science* 347, no. 6221 (January 30, 2015): 536–39. https://doi.org/10.1126/science.1256297.

Morgan, Robert. "Request for Information Regarding Consumer Access to Financial Records," February 21, 2017. https://www.consumerfinancemonitor.com.

GOV.UK. "Open Banking Revolution Moves Closer," February 2, 2017. https://www.gov.uk.

"Overview of Regulatory Sandbox." Accessed November 2, 2019. https://www.mas.gov.sg.

Palanisamy, Mayuran, and Ravin Nandle. "Understanding India's Draft Data Protection Bill." *Privacy Tracker*(blog), September 13, 2018. https://iapp.org.

Popper, Nathaniel. "Banks and Tech Firms Battle Over Something Akin to Gold: Your Data." *The New York Times*, March 23, 2017, sec. Business. https://www.nytimes.com.

Rainie, Lee, Sara Kiesler, Ruogu Kang, and Mary Madden. "Part 5: Online Identity Theft, Security Issues, and Reputational Damage." *Anonymity, Privacy, and Security Online*(blog), September 5, 2013. https://www.pewresearch.org.

"Request for Information Regarding Consumer Access to Financial Records." Consumer Financial Protection Bureau, 2016. https://files.consumerfinance.gov.

"Request for Information Regarding Consumer Access to Financial Records." *Federal Register* 81 (November 22, 2016): 83806–11.

"Review of the Four Major Banks (Second Report)." House of Representatives Standing Committee on Economics, April 21, 2017. https://apo.org.au.

Rothwell, Graham. "The Brave New World of Open Banking in APAC: Singapore." *Accenture Banking Blog*(blog), September 27, 2018. https://bankingblog.accenture.com.

Schmitz, Amy J. "Secret Consumer Scores and Segmentations: Separating 'Haves' from 'Have-Nots.'" *Mich. St. L. Rev.*1411 (2014).

Sharma, Sahib. "RBI Pushes for Bank Account Number Portability, Banks Wary." Hindustan Times, May 31, 2017. https://www.hindustantimes.com.

Solon, Olivia. “Venmo: How the Payment App Exposes Our Private Lives.” *The Guardian*, July 17, 2018, sec. World news. https://www.theguardian.com.

Spiotto, Ann H. “"Financial Account Aggregation: The Liability Perspective.” *Fordham J. Corp. & Fin. L.* 8, no. 2 (2003): 567–74.

Stacey, Daniel. “India Begins Building on Its Citizens’ Biometrics.” *Wall Street Journal*, February 20, 2017, sec. Business. https://www.wsj.com.

“The Personal Data Protection Bill, 2018,” n.d. https://meity.gov.in.

Vartabedian, Marc. “California Passes Sweeping Data-Privacy Bill.” *Wall Street Journal*, June 29, 2018, sec. Tech. https://www.wsj.com.

Open Banking. “What Is Open Banking?” Accessed November 4, 2019. https://www.openbanking.org.uk.

Whitley, Edgar A., and Roser Pujadas. “Report on a Study of How Consumers Currently Consent to Share Their Financial Data with a Third Party.” London: London School of Economics and Political Science, March 2018. https://www.fs-cp.org.uk.

Wierzel, Kimberley L. “If You Can’t Beat Them, Join Them: Data Aggregators and Financial Institutions.” *NC Banking Inst.*5 (2001): 457, 459–60.

Wisniewski, Mary. “JPMorgan Chase and Intuit Partner to Share Data via API.” American Banker, January 25, 2017. https://www.americanbanker.com.

Wisniewski, Mary. “The Data Access Debate Is About to Get A Lot More Interesting.” *American Banker*, January 27, 2017. https://www.americanbanker.com.