No. 18-48
Summer 2018

MERCATUS GRADUATE POLICY ESSAY

PUBLIC, PRIVATE AND, IN-BETWEEN: THE POLITICAL ECONOMY OF ROADWAY MANAGEMENT

by Nick Zaiac

MERCATUS CENTER
George Mason University

Abstract
Section 1033 of the Dodd-Frank Act mandates banks provide consumers' transaction data online. Consumers have since given third-party financial service application access to this data electronically, sparking a legal question over what parties have rights to this transaction data. This paper will use a Coasian lens to show that giving data access and sharing rights to both banks and consumers would provide the most economically efficient outcome given current regulatory constraints. This approach is most likely to maximize the welfare of all the economic stakeholders in this debate: consumers, banks, and third-party financial service applications.

Author Bio
Danielle Barden received an MA in economics from George Mason University, and is an alumna of the Mercatus MA Fellowship program. She is currently an economist at the Environmental Protection Agency. Danielle holds a BS in finance from the University of Northwestern - St. Paul. She previously interned for the American Enterprise Institute and the Joint Economic Committee.

Committee Members
Anne Hobson is a Program Manager for Academic and Student Programs at the Mercatus Center at George Mason University.
Thomas Hogan, Ph.D., is a fellow in Rice University's Baker Institute for Public Policy
Brian Knight is the Director of Innovation and Governance and a Senior Research Fellow at the Mercatus Center at George Mason University.

Acknowledgements
Special thanks to my committee members for their continued guidance and support throughout the process of writing this paper. Your contributions helped refine and develop my initial research into a product that would have otherwise been impossible. Additional thanks goes to Neil Chilson, whose knowledge of data rights and privacy literature were invaluable.

Table of Contents

I. Introduction

The past decade has brought large changes to consumer financial services. In the wake of the Dodd-Frank Act, banks and regulators worked to adjust to a new regulatory landscape. While Dodd-Frank attempted to fill perceived holes in the financial system, it neglected to anticipate how innovations would affect financial services. In recent years, financial services applications, such as Mint, gained popularity among consumers, providing needed data aggregation services. Since these applications began to solicit user-credentials for bank accounts, financial institutions have had to develop policies to allow or disallow third-party access. While it seems consumers have a right to access their online transaction data, banks have voiced concerns over unsafe screen-scraping practices. This prompted the Consumer Financial Protection Bureau (CFPB) to solicit comments from the financial community on how best to regulate third-party services in light of Dodd-Frank.

II. Economics of Privacy

As scholars have grappled with the effects of innovation, disagreements have formed over how best to assign and protect data rights. Some, like Warren Samuel and Louis Brandeis, argue that data created by, or referencing someone, should belong to that person.[1] Others such as Hal Varian argue that data should be treated like any other tradable asset.[2] Contemporary scholarship on privacy rights falls into three major categories: privacy as a basic right, consumer ownership of data, and ownership of data based on economic efficiency.

[1] Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." *Harvard Law Review* Vol. 4, No. 5 (December 1890): 193–220. https://doi.org/10.2307/1321160.
[2] Varian, Hal R. "Economic Aspects of Personal Privacy," in *Internet Policy and Economics: Challenges and Perspectives*, edited by William H. Lehr and Lorenzo Maria Pupillo, pages 101–109. Second Ed. New York: Springer, 2009.

Perspectives on Privacy

The tradition arguing for consumer ownership of personal information derives from Samuel Warren and Louis Brandeis' seminal 1890 article "The Right to Privacy." With the advent of technology such as cameras and recorders that easily captured images and conversations that would have been previously inaccessible to society at large, the authors felt that a fundamental right to privacy was being violated.[3] Warren and Brandeis argued that information gleaned from personal conversations or in a private context, such as a conversation between friends overheard in a cafe, belonged to the speaker. This right "to be let alone" is not an extension of a person's self-ownership; rather, Brandeis and Warren argued that privacy is a right itself.[4] The idea that privacy is a right itself, independent from any other right, is a key distinction of this school of thought. Later economic and legal articles arguing for consumer's right to their data would later rely on Brandeis and Warren's defense of privacy, making it the second-most cited law review article of all time.[5]

A second perspective views privacy as a derivative of property rights, belonging to the owner, unlike the privacy fundamentalism of Brandeis and Warren. In her 1975 article, Judith Jarvis Thomson argues that privacy is one element in a bundle of property rights. Within the context of the ownership of a picture, for example, is the positive right to invite another to share it with you, as well as the negative ability to exclude another person from looking at it.[6] In this vein of reasoning, scholars argue that personal information is a kind of property for the

[3] Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." *Harvard Law Review* Vol. 4, No. 5 (December 1890): 193–220. https://doi.org/10.2307/1321160.
[4] Ibid., 205.
[5] Shapiro, Fred R. and Michelle Pearce. "The Most Cited Law Review Articles of All Times." *Michigan Law Review* 110, no. 8. (2012): 1483–1520. https:// repository.law.umich.edu/mlr/vol110/iss8/2.
[6] Thomson, Judith Jarvis. "The Right to Privacy." *Philosophy and Public Affairs* 4, no. 4 (Summer 1975), 297. https://www.jstor.org/stable/2265075.

consumer, with certain rights that accompany it. In his 1967 work *Privacy and Freedom*, Alan Westin makes this argument saying, "Personal information, thought of as the right of decision over one's private personality, should be defined as a property right, with all the restraints on interference by public or private authorities and due-process guarantees that our law of property has been so skillful in devising."[7] Applied to data in more recent years, this viewpoint has popularized legal reforms to protect consumer data, such as the European Union's General Data Protection Regulation's data portability and the right to be forgotten.[8] Ultimately, for those who take the second perspective on privacy, data belongs to the person to whom it refers, though the rights associated with the property may change.

The third perspective views personal information as property, but believes ownership should be designated based on economic efficiency, rather than the person about whom the information refers. Scholars in this tradition differ from the second perspective in that they see privacy as a commodity that can be traded. Foundational to this perspective is George Stigler and Richard Posner's works on the economics of privacy. Stigler argues that privacy can lead to asymmetric information, resulting in resources inefficiently invested.[9] When differences among people are suppressed, people are either uniformly treated at the average or biased against based on visible distinctions.[10] Similarly, Posner described the exchange of private information about a person, or "prying," as an intermediate good aimed at reducing information disparities. Because this information is valuable both to the person to whom it refers and to others, Posner speculates

[7] Alan F. Westin. *Privacy and Freedom* (New York: Ig, 1967), 324.
[8] Official Journal of the European Union, *General Data Protection Regulation*. L 119, vol. 59. 4 May 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF.
[9] Stigler, George J."An Introduction to Privacy in Economics and Politics." *Journal of Legal Studies* 9 (1980): 623–644.
[10] Ibid., 630.

that property rights could incentivize trade. Property rights can also incentive investment in long-term ideas, such as trade secrets.[11]

For Posner, ownership should be given to the party that values the information most highly, as long as they cannot impose substantial costs on the other party.[12] This is illustrated in the example of the U.S. Census, which has information critical to research and government operations but is worth little to each individual household. Additionally, because precautions are taken to remove identifying information from the data, the transaction costs are low for participants. Therefore, it is the most economically efficient for the U.S. government to possess ownership of the census dataset, rather than have ownership be distributed among each individual household.

Hal Varian added to the scholarship on property rights and privacy in his 1996 essay "Economic Aspects of Personal Privacy," in which he explores the costs and benefits of the sale of consumer information. While consumers may be able to determine the price at which they will sell their personal information, they are unable to foresee the externalities resulting from the resale of their information to a third party. These externalities could take the form of irrelevant offers as sellers search for customers, categorized by Varian as "excess search costs."[13] Varian clarifies that spam results from too little public information about buyers with which to discriminate. The seller of a consumer's information to a secondary buyer has little incentive to ensure the original consumer's preferences align with the buyer.[14] Varian argues that consumer contracts could reduce externalities by putting conditions on the exchange, constraining the

[11] Posner, Richard A. "Privacy, Secrecy, and Reputation," *Buffalo Law Review* 28, no. 1 (1979): 1–55.
[12] Ibid.
[13] Varian, Hal R. "Economic Aspects of Personal Privacy," in *Internet Policy and Economics: Challenges and Perspectives*, edited by William H. Lehr and Lorenzo Maria Pupillo, page 102. Second Ed. New York: Springer, 2009.
[14] Ibid., 103.

resale of customer information or banning it altogether on a case-by-case basis. Ultimately, Varian believes that property rights should generally be given to the party that would minimize overall transaction costs.[15]

Though information is often spoken of as having a single owner, data is rarely created by a singular entity. Everything from internet browsing data to credit card transactions are created in partnership with another party. Even offline, information could have multiple stakeholders. In a commercial context, data is co-produced by a consumer and a company's technology that creates a service and tracks the actions taken.[16] Because this data would not exist without both parties participation, it seems that both the consumer and the co-creator should have at minimum joint access rights to the data.

Challenges to the Property Perspective

Although referring to information as property can be a helpful way of talking about a bundle of rights associated with information, some scholars have noted its limitations. A crucial distinction is that information is nonrivalrous unlike tangible property.[17] Similarly, information can be almost costlessly replicated.[18] Though these qualities of information make it more costly to regulate data as property, it is possible. In his 1996 paper "Markets and Privacy," Kenneth Laudon proposes a data property rights system much like a commodity exchange. People could list private information such as medical and educational data in the exchange, which would be

[15] Ibid., 107.
[16] Ng, Irene Cl. "Can You Own Your Personal Data? The HAT (Hub-of-all-Things) Data Ownership Model." (working paper, University of Warwick, Services Systems Research Group Working Papers series no. 02/18, 2018).
[17] Varian, Hal R. "Economic Aspects of Personal Privacy," in *Internet Policy and Economics: Challenges and Perspectives*, edited by William H. Lehr and Lorenzo Maria Pupillo, pages 101-109. Second Ed. New York: Springer, 2009.
[18] Rayna, Thierry. *Understanding the Challenges of the Digital Economy: The Nature of Digital Goods* Communications & Strategies, no. 71, 3rd Quarter 2008 (September 2008): 13–16, https://ssrn.com/abstract=1353583.

distributed into groups for sale. Following the purchase of a basket of information, depositors would receive a share of the revenue from their listing. While this system would create strong rights protection, it fails to address the unique aspects of data privacy. As Pamela Samuelson argues in her 2000 paper "Privacy as Intellectual Property," while a consumer could willingly trade their information to company A, they may not want company A to sell their information to company B.[19] By selling the right to their information, they concede any control over who owns it and how it is used. Although scholars have tried to remedy this problem with data property rights by asserting that property rights can be modified and restricted, they acknowledge that the transaction costs on this would be immense.[20]

Apart from the traditional privacy debate, which breaks down based on allocation of property, some scholars believe that while the economic framework highlighting the benefits of information exchange is helpful, data should not be regulated as property. Samuelson proposes treating information privacy rights as similar to trade secrets, with established norms of disclosure. As a company may reveal their trade secrets to a business consultant in order to benefit from their services, a patient may disclose information to a doctor in order to receive care (1153).[21] In both these cases, the purpose and terms of the disclosure are understood by both parties. Samuelson argues that licensing is a better way of regulating our implicit assumptions about how data should function-- shared with a chosen party for a specific reason.[22] In this model, contracts between parties would regulate how the information being traded is used.

[19] Samuelson, Pamela. "Privacy as Intellectual Property?" *Stanford Law Review* 52, no. 6, (2000): 1138, https://www.jstor.org/stable/1229499.
[20] Leesig, Lawrence. "Privacy as Property." *Social Research* 69, no. 1. (Spring 2002): 247–269. https://www.jstor.org/stable/40971547.
[21] Samuelson, Pamela. "Privacy as Intellectual Property?" *Stanford Law Review* 52, no. 6. (2000): 1125–1173. https://www.jstor.org/stable/1229499.
[22] Ibid.

Additionally, if the recipient of personal information desired to share it, they would need to receive rights to sublease the information. Varian gives an example of what this kind of contract could look like:

> Check here if you would like your name distributed to other parties who will provide you with information about computer peripherals until December 31, 1998. After that, name and address will be destroyed. In exchange, you will be paid $5 for each list to which your name and address is distributed.[23]

Varian argues that a leasing model, based on the idea that personal information has similar economic incentives to a trade secret, would give consumers more control over their data while lowering the transaction costs and definition problems of property.

Coase and Rights Allocation

Assuming the third perspective on personal information, in which privacy can be owned or leased, the Coase Theorem provides a helpful framework in determining which party should receive ownership rights. In his seminal 1960 article "The Problem of Social Costs," Ronald Coase argued that without transaction costs, the initial distribution of property rights would not matter.[24] When confronted with externalities, parties would negotiate towards an economically efficient outcome. Coase illustrates this principle by analyzing the case of Sturges v. Bridgman.[25] In this case, a doctor moved into the same neighborhood as a confectioner. After some time conducting business without issue, the doctor built a consulting room next to the confectioner's

[23] Varian, Hal R. "Economic Aspects of Personal Privacy," in *Internet Policy and Economics: Challenges and Perspectives*, edited by William H. Lehr and Lorenzo Maria Pupillo, pages 104. Second Ed. New York: Springer, 2009.
[24] Coase, R. H. "The Problem of Social Cost." *The Journal of Law & Economics* 3. (Oct., 1960): 1–44. https://www.jstor.org/stable/724810.
[25] Ibid., 9–10.

kitchen. However, the doctor was unable to utilize the room due to the noise and vibrations produced by the confectioner plant. When the doctor sought a legal remedy, the court decided that the doctor could prevent the confectioner from using the machinery causing the disruption. Coase asserts that this problem could have alternately been solved through a payment from the confectioner to the doctor, perhaps to insulate his walls. Alternately, had the confectioner won the suit, the doctor could have stopped the confectioner from using his machinery by paying him an amount equal to his loss in profit from the halted business. To Coase, both parties cause the damage: "If we are to attain an optimum allocation of resources, it is therefore desirable that both parties should take the harmful effect (the nuisance) into account in deciding on their course of action."[26] In a perfectly efficient market, the assignment of property rights and liability is insignificant—parties will negotiate to create an economically optimal outcome.

Our market, however, is not costless; rather, negotiating can be extremely costly, preventing transactions from occurring that would have otherwise taken place.[27] Suppose the doctor had proposed paying his neighbor to cease using machinery as Coase suggests. Time would be spent by both the doctor and the confectioner considering what each of their affected businesses was worth. More time might be spent negotiating to get to a price both parties are happy with. Additionally, more resources could be spent ensuring the neighbor upholds their share of the bargain. If the terms of the agreement are broken, there will be expenses involved with either convincing or coercing a neighbor to stick to their word. Therefore, while negotiating at an informal level seems to be the most efficient option for the rights to be distributed between the doctor and confectioner, further inspection shows it to be fraught.

[26] Ibid., 13.
[27] Ibid., 15.

This example demonstrates that rights will only be reallocated to the party who most values them when the potential benefits of transferring them exceed the transaction costs. Ownership and liability matters a great deal. Given this state of affairs, Coase argues the following:

> In these conditions the initial delimitation of legal rights does have an effect on the efficiency with which the economic system operates. One arrangement of rights may bring about a greater value of production than any other. But unless this is the arrangement of rights established by the legal system, the costs of reaching the same result by altering and combining rights through the market may be so great that this optimal arrangement of rights, and the greater value of production which it would bring, may never be achieved.[28]

Legal ownership has a substantial effect on production possibilities. In the case of *Sturges v. Bridgman*, the confectioner was prevented from using his machinery altogether, resulting in a benefit to the doctor and an unknown loss for the confectioner. The court's decision effectively ended the confectioner's business due to the doctor's ownership of the land, likely producing an unspecified financial loss for the city, at least until the confectioner was able to relocate or find quieter machinery. This story demonstrates the magnitude of the effect ownership allocation can have on business. All potential solutions to assigning rights have costs; in Coase's view, the task of the law is to minimize them.[29]

The next section of this paper will apply the discussion of privacy and ownership to the debate surrounding Section 1033 of the Dodd-Frank Act. It will provide an introduction to the policy, the stakeholders, and potential rulemaking actions that have been proposed. Finally, the

[28] Ibid., 16.
[29] Ibid., 19.

policy solutions will be analyzed based on their ability to minimize the transaction costs in trading ownership rights.

III. Section 1033: An Introduction

Section 1033 of the Dodd-Frank Act requires financial product and service providers to make any records kept about a consumer's information electronically accessible to that person. These records include "information relating to any transactions, series of transactions, or to the account including costs, charges, and usage data."[30] They do not include algorithms, such as the ones used to calculate consumers' credit scores, information collected for fraud prevention, or other information covered by additional laws. The Act also encourages banks to make this transaction data available online in "machine readable files."

As banks increasingly gave consumers access to their banking data online, companies such as Mint began providing financial services to consumers, leveraging machine-readable banking data to offer services such as budgeting. These services often provide aggregation services, allowing consumers to view multiple accounts at once. Initially, these third-party financial service companies utilized screen-scraping services to gather transaction information, simply requiring consumers to enter their bank or credit card username and password. As these applications gained popularity, banks and other financial institutions grew concerned with the security risk screen-scraping posed, both for the consumers utilizing these financial applications' services and banks' institutional security.[31] Because of this, financial institutions voluntarily developed application programming interfaces (APIs) through which consumer transaction data

[30] Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, § 929-Z, 124 Stat. 1376, Section 1033. Consumer Rights to Access Information. 1871 (2010) (codified at 15 U.S.C. § 78o).
[31] Fuchs, Meredith and Andres L. Navarrete, *Capital One Comments RFI Regarding Consumer Access to Financial Records*, Capital One, 2017, https://www.regulations.gov/document?D=CFPB-2016-0048-0042.

could be accessed more securely.[32] Financial Data Exchange (FDX), a nonprofit whose members include many major banks, applications, and data aggregators, is working to standardize the API used for consumer financial data. This system ensures that consumer login information is not transferred to third-parties. Rather, after entering their credentials, consumers are transferred to their bank's server and given the option to choose what types of data they want to share with the personal finance application.[33] Major banks have started to roll out online dashboards where users can tailor their data sharing with applications using this API.[34] Unfortunately, this security measure is not in place for applications or data aggregators that are still using screen-scraping methods, widely viewed as unsecure for both the consumer and banks.[35] Additionally, consumer advocates have voiced concerns that banks will restrict access to the data accessible to third parties through the API.[36]

Although advances are being made to protect consumer data, security risks remain. It is difficult for consumers to determine what method applications are using to gather their data. Additionally, they may be unaware of what financial data they are agreeing to share with an application outside of the FDX API. Despite an industry-wide move away from screen-scraping, there is nothing preventing fintechs from using this method. Ultimately, consumers are capable of sharing their financial data with any service, secure or otherwise. Banks argue that the regulatory paradigm of consumer-permissioned data sharing has made them liable for a potential

[32] Crossman, Penny, "Big Banks, Aggregators Launch Group to Hash out Data-Sharing Issues," *American Banker*, October 18, 2018, https://www.americanbanker.com/news/big-banks-aggregators-launch-group-to-hash-out-data-sharing-issues.
[33] Ibid.
[34] Octavio Blanco, "Consumers Get More Control Over the Banking Data Shared With Financial Apps," *Consumer Reports*, November 10, 2019, https://www.consumerreports.org/privacy/consumers-get-more-control-over-banking-data-shared-with-financial-apps/.
[35] Ibid.
[36] Daniel Döderlein, "BankThink Fintechs' Defense of Screen Scraping is Shortsighted," *American Banker*, September 7, 2017, https://www.americanbanker.com/opinion/fintechs-defense-of-screen-scraping-is-shortsighted.

security breach.[37] Consumer advocates respond by saying that consumers are protected from any liability resulting from a data breach under existing financial regulations.[38] In a controversial move, the Clearing House rolled out a model agent for banks to use when data sharing with startups, placing the liability in case of a data breach on the recipients.[39]

In sum, the current regulatory climate regarding bank transaction data is uncertain. Consumers, unaware of this ambiguity, are willingly sharing their credentials with third party financial services. Banks, unable to prevent their customers from sharing security credentials, have begun to cooperate with these third party applications and data aggregators to create secure APIs, minimizing their exposure to risk. Despite these steps, conflicting legislation and guidance has made it unclear who has the rights for transaction data. The CFPB will be responsible for providing guidance on Dodd Frank Section 1033, determining what parties are allowed to make decisions about consumer transaction data.

IV. Stakeholders: Banks, Consumers, and Financial Service Applications

There are multiple parties at play involved in the application-based financial services industry. Consumers and banks create the transaction data as the bank records the consumer's activity. Additionally, the service being utilized by the consumer has an interest receiving the consumer's transaction data. While it is possible to delineate among the actual applications and the services that are providing the data aggregation (these are not always the same), as far as Section 1033 is

[37] *Request for Information Regarding Consumer Access to Financial Records; Docket No. CFPB-2016-0048*, Consumer Financial Protection Bureau, 2016, https://www.regulations.gov/docketBrowser?rpp=25&so=DESC&sb=commentDueDate&po=0&dct=PS&D=CFPB-2016-0048.
[38] Lauren Saunders, *Request for Information: Consumer Access to Financial Records, Docket No. CFPB-2016-0048*, National Consumer Law Center, 2017, https://www.regulations.gov/document?D=CFPB-2016-0048-0072.
[39] "Big Banks Want to Make it Easier to Share Consumer Data with Startups," *American Banker*, November 12, 2019, https://www.americanbanker.com/articles/big-banks-want-to-make-it-easier-to-share-consumer-data-with-startups.

concerned, the ambiguity seems to be in the relationship between the banks and consumers. Because of this, I'll be referring to the applications as well as the aggregators together.

Banks

Before further analyzing the details of the bank's claim on consumer transaction data, it is important to consider a few regulations that influence financial institution's perspective on this issue. First, the Truth In Lending Act (TILA) created statutes regarding standardization and disclosure in consumer credit. Regulation Z, or C.F.R. 1026, implements TILA's directives and describes what kind of information financial service providers are required to make accessible to their consumer.[40] The required disclosures include information such as account transactions or how the financial service providers have used the consumer's non-public information. Second is the Gramm-Leach-Bliley Act of 1990.[41] The law requires that financial institutions disclose what information banks are collecting from consumers, as well as giving consumers the opportunity to opt-out of their information being shared with outside companies.[42] While there are a few exceptions to consumer's ability to opt-out, such as information necessary to conduct business or marketing agreements, consumers largely have the option to prevent their information from being shared with other institutions. Third, the Office of the Comptroller of Currency (OCC) released Bulletin 2013-29, giving direction to banks regarding their relationship to third-party vendors. Bulletin 2013-29 states the following:

> The OCC expects banks to perform due diligence and ongoing monitoring for all third-party relationships. The level of due diligence and ongoing monitoring, however, may

[40] Truth in Lending Act of 1968, Pub. L. No. 90-321, 82 Stat. 146 (2019).
[41] Gramm-Leach-Bliley Act of 1990, Pub. L. No. 106-102, 113 Stat. 1338 (1999).
[42] Federal Deposit Insurance Corporation, *Your Rights to Financial Privacy*, August 2003, https://www.fdic.gov/consumers/privacy/yourrights/.

differ for, and should be specific to, each third-party relationship. The level of due diligence and ongoing monitoring should be consistent with the level of risk and complexity posed by each third-party relationship. [43]

The legal ambiguity regarding who is responsible for protecting financial data, financial institutions or third parties, puts banks in a precarious position when making relationships with third-party financial service companies, especially those that are consumer-permissioned, such as Mint. There is consumer pressure to cooperate with third party financial services, but they may be on the regulatory hook for monitoring the security of these services. Fourth, a 2018 Department of Treasury report argued that the definition of *consumer* in Dodd-Frank covers agents acting on behalf of the consumer.[44] Because of this, they recommended that the CFPB require banks to cooperate with consumer-permissioned services.

In sum, these laws state a few things. First, financial institutions are required to give consumers access to their transaction data in machine-readable files as far as the Dodd-Frank Act is considered. Second, consumers are allowed to request to have their information removed from being sold by financial institutions, with a few business-related exceptions. Third, banks are ultimately responsible for monitoring the security of their relationships with third-party vendors. Finally, paradigm for banks' liability regarding third party services is governed by conflicting agency guidance and little regulation.

Consumers

[43] Office of the Comptroller of the Currency, *Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29*, June 2017, https://www.occ.gov/static/rescinded-bulletins/bulletin-2017-21.pdf.

[44] Department of the Treasury, "A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation," E.O. 13772, July 2018, https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation.pdf.

Too many consumers, the answer to the debate over who owns their transaction data seems obvious—it belongs to them. Few consumers think about the liability banks might face when they provide their security credentials to applications such as Mint. Rather, a consumer might wonder whether or not a financial service application is trustworthy and stores data securely. This concern is valid because there is a chance a consumer could be on the hook for transactions. In its public comment on Section 1033, the Consumer Financial Data Rights Group (CFDR) cited the Electronic Fund Transfer Act, which states that if consumers allow a third-party to initiate monetary transfers, and the third-party abuses this authorization, the consumer is liable unless they report the incident to their bank.[45] In contrast, The National Consumer Law Center's public comment contradicts this reading of the Electronic Fund Transfer Act, saying that Regulation E protects consumers from bad actors.[46] The law's ambiguity regarding financial application liability creates uncertainty for consumers, who have fewer resources than banks to investigate potential security threats.

Despite regulatory uncertainty, many consumers have signed up for financial service applications. In 2016, Mint reported that they had over 20 million users.[47] Their services include investment tracking, transaction data aggregation among multiple banks, budgeting, and more. Although there is little information on the effectiveness of these financial service applications, surveys show a potential market for them. In a Nielsen Mobile Wallet Report, 28 percent of consumers using mobile banking strongly agreed that using budgeting applications had helped

[45] Steven Boms, CFDR Group Response to Consumer Financial Protection Bureau Request for Information Regarding Consumer Access to Financial Records. *Consumer Financial Data Rights Group,* 2017, https://www.regulations.gov/document?D=CFPB-2016-0048-0034.
[46] Lauren Saunders, Data aggregator CFPB RFI, *National Consumer Law Center*, 2017, https://www.regulations.gov/document?D=CFPB-2016-0048-0072.
[47] Kim Tracy Prince, "Mint by the Numbers: Which User Are You?" *MintLife* (blog), Intuit, April 6, 2016, https://blog.mint.com/credit/mint-by-the-numbers-which-user-are-you-040616/.

changed their spending habits.[48] A 2019 survey found that 59 percent of Americans are not tracking their spending, and two-fifths have never had a budget; additionally, among Americans who utilize credit cards, the average number of cards is 3.7.[49] Another finance application and website, Credit Karma, provides aggregated transaction information as well as information on customers' credit scores and insights into how to improve their financial health.[50] Given both a lack of attention paid to personal finance and the number of accounts Americans are using, financial service application aggregation and tracking services seem to fill a vital service for consumers. Because of this, consumers are latching onto financial aggregation services, with varying levels of awareness towards the security of these services.

Third-Party Applications

Third-party applications are a bridge between consumers and banks. Although they may not always directly provide aggregation services, they utilize the aggregated data to provide trends on consumers' personal finance. This piecemeal information, which alone is worth little, is used both as a product for consumers as well as an advertising tool. By itself, consumer transaction data is worth little, but aggregated data provides a powerful opportunity for service provision and advertisement. Applications such as Mint can get a full picture of an individual's income and spending habits, rather than the slice to which a bank has access. Therefore, many comments submitted to the CFPB's public comments period argued for consumer ownership of data, paired

[48] "Don't Fear the Reaper: Tax Day is Coming, But Mobile Banking is Helping Consumers Balance Their Books," The Nielsen Company, April, 8, 2015, https://www.nielsen.com/us/en/insights/article/2015/dont-fear-the-reaper-tax-day-is-coming-but-mobile-banking-is-helping-consumers/.
[49] "How Many Cards Does the Average Person Have?" *The Ascent, A Motley Fool Company*, November 15, 2018, https://www.fool.com/the-ascent/credit-cards/articles/how-many-credit-cards-does-the-average-person-have/.
[50] Sumeet Ajmani, *Credit Karma Response to Consumer Financial Protection Bureau Request for Information Regarding Consumer Access to Financial Records Docket No.: CFPB-2016-0048,* Credit Karma, 2017, https://www.regulations.gov/document?D=CFPB-2016-0048-0049.

with an industry-created standard for transferring information, as proposed by the Center for Financial Service Innovation (now renamed the Financial Health Network).[51] The Network's set of principles proposes a collaborative system that sets expectations for what, when, and how data will be transferred. These principles highlight the benefits of API agreements among banks and data aggregators while acknowledging that these bilateral agreements may hinder consumer access.[52] Ultimately, they recommend collaboration among business utilizing financial data and regulators in order to achieve an innovative framework that benefits consumers. While many financial institutions recommend the adoption of APIs for security reasons, data aggregators voiced concerns that this could stifle innovation and access.[53] While all parties involved seem open to cooperation, there is mutual skepticism about the motives of the other and the resulting effects on the consumer.

V. Alternatives for Section 1033 Rulemaking

With the three stakeholders' interests in mind, it is possible to consider the CFPB's regulatory alternatives. While there are certainly more than three potential solutions, for the purposes of this paper, I will simplify them into three possible courses of action.

Solution 1: Banks Own Data.

[51] "Understanding Consumer Data Sharing and Financial Health," *The Financial Health Network*, https://finhealthnetwork.org/research/consumer-data-sharing/.
[52] Ibid.
[53] Ryan Christiansen, *Finicity Response – Consumer Access to Financial Records Docket No. CFPB-2016-0048*, Finicity, 2017, https://www.regulations.gov/document?D=CFPB-2016-0048-0064; Steven Boms, *Yodlee RFI Response Final*, Envestnet Yodlee, 2017, https://www.regulations.gov/document?D=CFPB-2016-0048-0033; Meredith Fuchs, Andres L. Navarrete, *Capital One Comments RFI Regarding Consumer Access to Financial Records*, Capital One, 2017, https://www.regulations.gov/document?D=CFPB-2016-0048-0042.

Given this regulatory environment, banks are hesitant to give consumer-permissioned third-parties access to their data. Unfortunately, it is difficult for banks to stop applications like Mint, since they are able to use consumer's credentials to access data. Though banks have cooperated with these application-based companies to set up APIs to protect consumers, they are wary of the consequences they might face if there was a security breach.[54] Until this point, the CFPB, the government agency tasked with interpreting the Dodd-Frank Act, had not provided regulatory guidance regarding who has rights to the consumer data. However, in November 2016, the CFPB called for comments on Section 1033.[55] Among the respondents were banks and other financial institutions, representing a variety of perspectives. Compass Bank said that although third-party data sharing can provide benefits to consumers, banks cannot be responsible for screening an unlimited number of third-parties.[56] Additionally, Compass asserted that banks should be able to deny to enter into a relationship with a third party. The Consumer Bankers Association echoed this concern, noting that in the past, the CFPB has held banks accountable for the actions taken by outside service providers and citing the OCC's Bulletin 2013-29.[57] At present, there is little clarity over whether banks are required to cooperate consumer-permissioned financial services. Overall, financial institutions' concerns as presented in the CFPB's request for comments revolved around potential liability for a breach of security resulting from consumer-permissioned, third-party access.

---

[54] Meredith Fuchs, Andres L. Navarrete, *Capital One Comments RFI Regarding Consumer Access to Financial Records*, Capital One, 2017, https://www.regulations.gov/document?D=CFPB-2016-0048-0042.
[55] Bureau of Consumer Financial Protection, "*Request for Information Regarding Consumer Access to Financial Records*," 2016, https://www.regulations.gov/document?D=CFPB-2016-0048-0001.
[56] Rita Eads-Milazzo, *Re: Request for Information Regarding Consumer Access to Financial Records ("RFI") Docket No. CFPB-2016-0048*, Compass Bank, 2017, https://www.regulations.gov/document?D=CFPB-2016-0048-0040.
[57] David Pommerehn, *Re: Docket No.: CFPB-2016-0048 / Document No.: 2016-28086 - Request for Information Regarding Consumer Access to Financial Records*, Consumer Bankers Association, 2017, https://www.regulations.gov/document?D=CFPB-2016-0048-0050.

Solution II: Consumers Own Data.

Consumer advocates have nearly unilaterally agreed that that banking customers should have the right to both access and utilize their transaction information in financial service applications.[58] Some argue that because transaction data refers to the private affairs of a consumer, they should have ownership of this information. Policies bolstering consumer data rights have been implemented on a broader scale in the European Union (EU) with the General Data Protection Regulation (GDPR). In the case of GDPR, consumers have a right to know what information a company is collecting about them, restrict a company's access to sensitive information, transfer their data, as well as destroy collected data in some cases.[59] In the United States, states have become increasingly interested in privacy regulations, the most notable example being the California Consumer Privacy Act, which goes into effect in 2020.[60] These laws clarify and expand consumer rights regarding business' collection, management, and destruction of their data. Unfortunately, the adoption of competing state data laws would effectively put a tariff on business in certain states.[61] On a federal level, the Senate has proposed multiple privacy bills. [62]

In terms of the current state of financial data regulation, however, the terms have already been set. Consumers and banks each have designated rights as a result of Dodd-Frank. Consumers have the clear right to access their data in a machine-readable form and constrict

[58] Joseph Jerome, "*RE: Improving Data Privacy, Protection and Collection Practices in Financial Data*," (The Center for Democracy & Technology, March 15, 2019), https://cdt.org/insights/letter-to-us-senate-on-improving-data-privacy-protection-and-collection-practices-in-financial-data/.
[59] Mark Kaelin, "GDPR: A Cheatsheet." *TechRepublic*, (May 2019), https://www.techrepublic.com/article/the-eu-general-data-protection-regulation-gdpr-the-smart-persons-guide/.
[60] California Consumer Privacy Act of 2018, S 1121, (23 September 2018). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121.
[61] Jennifer Huddleston, "State Should Think Twice About Data Privacy Policy Making" *The Bridge*, February 21, 2019, https://www.mercatus.org/bridge/commentary/states-should-think-twice-about-data-privacy-policy-making.
[62] Cameron F. Kerry, "Game on: What to make of Senate privacy bills and hearing." *The Brookings Institution*, December 3, 2019, https://www.brookings.edu/blog/techtank/2019/12/03/game-on-what-to-make-of-senate-privacy-bills-and-hearing/.

banks from selling their data. Alternately, banks have the right to sell unrestricted consumer data. Given this paradigm, the regulatory framework currently prevents consumers from having exclusive ownership of their financial data.

Solution III: Leasing model

In the case of bank transaction data, consumers are opting to utilize technology operated by banks to conduct their financial affairs. Bank transaction data could include information about a variety of financial products, ranging from savings account withdrawals to credit card purchases. Though consumers could choose to make purchases with cash or save their money under a mattress, they are utilizing a financial institution due to preferences of safety, ease of use, or a variety of other reasons. In exchange, consumers have consented to allow the financial institution a slice of their privacy—a peek into their financial state. Although the data they produce by shopping or depositing money into an account refers to them, it is produced in cooperation with the bank. Both the bank and the consumer are legally allowed to access the transaction information, and banks are required to publish this data online.

However, there are legal protections for consumers from their personalized financial data being shared by banks without their permission. A financial institution could not, for example, share a consumer's transaction data with their employer without a clear legal reason. In this way, the situation between financial institutions and consumers resembles co-leasers.[63] Neither party has property rights over the data—a consumer could not restrict the bank from accessing their account's transaction data. Likewise, a consumer can restrict banks from selling their personal transaction data if they opt-out after reading the privacy policy. Both sides have permissioned

[63] Varian. Hal R. "Economic Aspects of Personal Privacy."

uses as well as restrictions of the use of the data. The current legal framework for data sharing may leave either party unsatisfied. For example, perhaps a consumer with a strong preference for data rights would be inclined to buy the rights to their data, profiting from the use of their data. Conversely, a bank could be inclined to restrict consumers from utilizing other financial services, forcing the consumer into utilizing their exclusive services. Despite these challenges present in the financial data legal environment, consumers and banks are able to have some control over financial data.

VI. Policy Implications of the Coasian Approach to the Economics of Privacy

In Coase's framework, the government's role is to minimize transaction costs in assigning ownership and liability. In his mind, there is no neutral ownership assignment: "The real question that has to be decided is: should A be allowed to harm B or should B be allowed to harm A? The problem is to avoid the more serious harm."[64] To Coase, any assignment of ownership is a decision about how to use economic resources.[65] With this in mind, I will analyze the proposed solutions to Section 1033 according to their ability to minimize transaction costs.

Both bank-owned and consumer-owned financial data would be accompanied by large transactions costs associated with trading ownership. In the first case, there is a large disparity between financial institutions access to knowledge and resources to navigate laws governing consumer finances. With this disparity would come high transaction costs for consumers seeking to utilize their financial data outside of the institution's purview, preventing consumers from granting permission to third parties to access their transaction data. Although banks would still

[64] Coase, R. H. "The Problem of Social Cost." *Journal of Law & Economics* 3 (October, 1960): 2. www.jstor.org/stable/724810.
[65] Ibid., 27.

be required to provide consumers machine readable copies of their transaction data, consumers would need to find alternatives to financial applications to analyze their spending habits.

In the case of the second solution, consumers would have ownership rights over their transaction data. Consumers would have the right to trade, share, or delete their financial data, as well as opting-out of financial institution's ability to benefit from their data. Unfortunately, this regulatory framework, while championing consumer rights, would burden financial institutions with the responsibility of securing customers' data without the ability to profit from the collection of it. This profit incentive is what drives the creation of new financial services and allows banks to allocate more resources toward securing data.

Finally, there is the third solution, in which both the bank and the consumer have the right to use transaction data in predetermined ways. Rather than traditional ownership rights, leasing rights limit the use rights of both the bank and the consumer. Both the financial institution and the consumer would have the right to access and share data, but neither would be allowed to destroy the information or restrict either party from it. The leasing model is also better equipped to address the co-produced nature of transaction data, in which the financial institution and the consumer are dependent on the other for the data creation. The current legal framework governing financial institutions places restrictions on the ways consumer transaction data can be used, similar to Varian's hypothetical subleasing example. Ultimately, this regulatory paradigm would minimize the need to trade ownership right of data, with both parties able to utilize the information without limiting access to the other. A data leasing framework protects consumers' use of their transaction information while giving financial institutions the opportunity to benefit from data collection.

Although the leasing model addresses many of the concerns brought up by the public comments regarding Section 1033, there are remaining concerns. Consumers would continue to be allowed to utilize unsecure third-party applications for their finances, putting banks at risk. However, banks can continue to provide services for their consumers to verify the trustworthiness of an application. As major players such as Wells Fargo, Citi, Bank of American, and Chase roll out dashboards giving consumers control over their data, it will become more pressing for third parties to adopt standard API practices. While this movement towards bank-controlled data access has prompted concerns about financial data being restricted, the leasing model gives the consumer the right to access and share their data, forcing banks to make this data available to third parties.

Ultimately, the co-leasing model minimizes the need for the exchange of data rights. Consumers have the ability to share their financial data with other services. Financial institutions are allowed to continue sharing customer information (unless otherwise instructed by consumers) but are required to cooperate with consumer-permissioned third parties. Since both parties are involved in the creation of transaction data, they each have access and sharing rights. Both are able to profit from their information, with banks selling consumer data, and consumers sharing their data with third parties in exchange for financial services. Neither party is given sole ownership of the data or able to exclude the other from benefiting from their leasing rights. In moving away from the traditional ownership rights model, the need for costly rights exchange has been minimized.

VII. Conclusion

Coase highlighted the important role assigning rights has in economic productivity. He wrote the following in "The Problem of Social Costs":

> One arrangement of rights may bring about a greater value of production than any other. But unless this is the arrangement of rights established by the legal system, the costs of reaching the same result by altering and combining rights through the market may be so great that this optimal arrangement of rights, and the greater value of production which it would bring, may never be achieved.[66]

The success of the market depends on the initial assignment of rights and liability. Financial data differs from traditional property due to its nonrivalrous nature.[67] Additionally, transaction data is produced by a customer in conjunction with a bank, making it difficult to assign ownership to either party. Given the regulatory environment that requires banks to make transaction data available to consumers and protects customers from negligence, the co-leasing model is the best of the policy alternatives. With both financial institutions and customers able to access and share transaction data, this model removes the need for the exchange of data ownership.

Future research could explore how burgeoning financial data management systems impact how consumers interact with their banks. These systems could create the opportunity for more robust and seamless leasing permissions. Additionally, these systems could create the distinction between aggregator and service more crucial to consumers.

---

[66] Ibid., 16.

[67] Will Rinehart, "Hearing on Data Ownership: Exploring Implications for Data Privacy Rights and Data Valuation," *Testimony Before Committee on Banking, Housing, and Urban Affairs*, October 29, 2019, https://www.banking.senate.gov/imo/media/doc/Rinehart%20Testimony10-24-19.pdf.