HARVARD Kennedy School
MOSSAVAR-RAHMANI CENTER
for Business and Government

THE NEW FRONTIER OF CONSUMER PROTECTION: FINANCIAL DATA PRIVACY AND SECURITY

Marshall Lux
Matthew Shackelford

March 2020

M-RCBG Associate Working Papers Series | No. 135

The New Frontier of Consumer Protection: Financial Data Privacy and Security

March 2020

Marshall Lux

Research Fellow, Mossavar-Rahmani Center for Business and Government, John F. Kennedy School of Government, Harvard University

Senior Advisor, The Boston Consulting Group

marshall_lux@hks.harvard.edu

Matthew Shackelford

Research Assistant, Mossavar-Rahmani Center for Business and Government, John F. Kennedy School of Government, Harvard University

Master of Public Policy Candidate and David M. Rubenstein Fellow, John F. Kennedy School of Government, Harvard University

Master of Business Administration Candidate, Harvard Business School

matthew_shackelford@student.hks.harvard.edu

Abstract

This working paper focuses on the US regulatory framework for consumer financial data privacy and security. It begins with a discussion of the foundational definition of financial data and a review of existing federal regulations impacting the treatment of financial data. The paper then turns to a reflection on recent state-level legislative and regulatory efforts regarding consumer data protection, including the California Consumer Protection Act of 2019 and the Colorado Protections for Consumer Data Privacy Act of 2018, as well as proposed changes that contain unique provisions or requirements. We detail a cross-effort analysis of the key issues and tradeoffs that policymakers must resolve when designing the regulatory framework for consumer financial data privacy and security, focusing primarily on the impacts on consumers, businesses, and societal innovation. The paper concludes with our proposal of the Comprehensive Consumer Financial Data Act, which is holistic federal legislation that establishes the Consumer Financial Data Bill of Rights, simplifies the existing web of regulations to reduce business frictions, and fosters innovation for privacy- and security-focused technologies and financial products.

Acknowledgements

We are deeply grateful for the support of the Mossavar-Rahmani Center for Business and Government at The Harvard Kennedy School, and in particular from John Haigh and Scott Leland. We are also grateful to acknowledge the helpful insights of Caroline Louveaux, Gerti Dervishi, James Catlin, Jim Maloney, Mark Monaco, Mike Marcus, Ronald Green, Steve Freiberg, Tony Castagna, Venkat Chary, and Zubin Mogul. All errors are our own.

CONTENTS

Introduction

Information has always been central for the provision of financial services. Beginning with such basic concepts as a borrower's name or a business's account balance, the role that data plays in the optimal functioning of the financial system has grown over time, particularly as modern information technology began to be adopted by financial institutions. This inclusion of data into financial decision-making has had significantly positive effects on the industry and on consumers by expanding the availability of credit,[1] enabling smarter risk management,[2] and vastly increasing convenience.[3] In the payments industry, there were ~$660 trillion in transactions processed in 2017 alone, with the size and speed of them enabled largely by data and technology.[4] In short, the principal driver of recent structural changes in financial services has been the availability and use of financial data in ways that have largely created value for users and providers of such services.

However, the explosion of financial data has also generated an important negative side effect for consumers by increasing the threat posed by a possible lack of privacy and security for that data. As the scope and power of financial data have increased, concerns from consumer privacy advocates have been elevated into the public discourse, with 97% of consumers saying

[1] Federal Reserve Bank of St. Louis, "Credit Market Debt Outstanding," FRED, accessed January 27, 2020, https://fred.stlouisfed.org/series/TCMDO.
[2] Paola Cerchiello and Paolo Giudici, "Big Data Analysis for Financial Risk Management," *Journal of Big Data* 3, no. 18 (2016), https://journalofbigdata.springeropen.com/articles/10.1186/s40537-016-0053-4.
[3] Jay Clayton, "The Evolving Market for Retail Investment Services and Forward-Looking Regulation - Adding Clarity and Investor Protection While Ensuring Access and Choice" (US Securities and Exchange Commission, May 2, 2018), https://www.sec.gov/news/speech/speech-clayton-2018-05-02.
[4] Boston Consulting Group, "An Interactive Guide to Global Payments," January 11, 2019, https://www.bcg.com/publications/interactives/global-payments-interactive-edition.aspx.

that they are somewhat or very concerned about their data privacy.[5] The potential for data misuse by corporations or pilferage by malicious actors has rightly focused attention on the steps being taken by both the private and public sectors to ensure that consumers are appropriately protected from harm while continuing to promote useful innovation within the industry.

To commence our research into this important topic, we lay out an overview of the existing financial data landscape. We start with an examination of what information should be considered financial data, leveraging critical attributes possessed by all data to define the scope of our inquiry. We specifically focus on financial data due to the extraordinary power of this information in consumers' lives while recognizing that other types of data could similarly benefit from our discussion and some of our proposals. Our view is that financial data should be comprised of any information concerning an individual being utilized in a financial process or that is inherently financial in nature regardless of the organization processing it, recognizing that the potential negative implications of financial data, should it be misused or stolen, do not depend on the underlying firm. This scope is critical to making sure that consumers are adequately protected, even as non-financial companies become more heavily involved in the provision of financial services, and that all firms compete on a level playing field.

We continue our groundwork by examining the long-standing federal laws and regulatory frameworks that apply to the protection of consumer financial data in the United States. From 1970 to 1999, the federal government built a web of regulations that govern how financial firms engage with consumer data, with a mixture of positive and negative consequences. The Bank Secrecy Act of 1970 (BSA) and the Fair Credit Reporting Act of 1970 (FCRA) both deal with the types of financial data that companies are permitted to collect and the purposes for which they can utilize them.[6,7] The Right to Financial Privacy Act of 1978 (RFPA) increases the protections that individuals have against government access to their data,[8] while the Gramm-Leach-Bliley Act of 1999 (GLBA) specifies requirements for the internal and external handling of consumer financial data by companies.[9] Taken together, these laws play critical roles in determining the protections that consumers currently enjoy as well as the key areas where such defenses may be lacking. In particular, the definition of financial data is not consistent across these regulations, meaning that certain protections have irregular coverage. Given the current state of federal regulation about financial data, it's clear that a significant update is necessary to ensure the continuation of existing consumer protections in the ever-changing technology landscape and to expand consumer rights in relation to the collection, treatment, use, and deletion of their financial data.

In pursuit of new ideas for the financial data regulatory framework in the US, we turn to an examination of recent efforts to improve consumer data privacy and security at the state level. The passage of the California Consumer Privacy Act of 2019 (CCPA) and the Colorado

---

[5] Gary Sterling, "Nearly All Consumers Are Concerned About Personal Data Privacy, Survey Finds," Marketing Land, December 4, 2019, https://marketingland.com/nearly-all-consumers-are-concerned-about-personal-data-privacy-survey-finds-272129.

[6] US Office of the Comptroller of the Currency, "Bank Secrecy Act (BSA)," accessed January 2, 2020, https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html.

[7] US Congress, "The Fair Credit Reporting Act," 1681 15 USC § (1992), https://epic.org/privacy/financial/fcra.html.

[8] US Federal Reserve, "Federal Reserve Consumer Compliance Handbook - Right to Financial Privacy Act," January 2006, https://www.federalreserve.gov/boarddocs/supmanual/cch/priv.pdf.

[9] US Federal Deposit Insurance Corporation, "FDIC Consumer Compliance Examination Manual - Gramm-Leach-Bliley Act (Privacy of Consumer Financial Information)," June 2016, https://www.fdic.gov/regulations/compliance/manual/8/viii-1.1.pdf.

Protections for Consumer Data Privacy Act of 2018 (CPCDPA) kickstarted a national discussion regarding the most effective approach to take to better consumer protections.[10,11] Given their utilization as the foundation for other passed or proposed legislative efforts that have since followed, the consumer rights and business requirements enshrined in these pieces of legislation have become the core of political arguments about financial data privacy. It's also important to note that several proposed bills have deviated significantly at times from the CCPA and the CPCDPA, including the state-level New York Privacy Act (NYPA) and Massachusetts S120 (S120) and the federal-level Consumer Online Privacy Rights Act (COPRA) and Consumer Data Privacy Act (CDPA), though the federal efforts have been largely neglected thus far.[12,13,14] We also examine the distinctions between legislative efforts, which are more stable and far-reaching, and regulatory rule changes, which are more specific and flexible, by looking at the New York Department of Financial Services 23 NYCRR 500 (DFS 500) rules.[15] Ultimately, the survey of these efforts serves to illuminate many of the current ideas and proposals in the consumer data privacy space to better inform future policymaking.

We then take a broader view to look at the categories of impacts that financial data privacy legislation has on key stakeholders. Specifically, we focus on consumers, businesses, and societal innovation as the important principals in the discussion of tradeoffs when constructing such efforts. Ideally, regulatory efforts pertaining to financial data would maximize consumer rights and protections, minimize business implementation and compliance costs, and strengthen incentives and systems for innovation that drives society forward. However, practically, we must make tradeoffs between these constituencies when designing governmental oversight. We look at the rights that are likely to be most beneficial to consumers, such as the Right to Know or the Right to Non-Discrimination, and compare them to the changes that would be required in business practices and relationships in order to achieve implementation.[16] We examine the impact that increased consumer rights are likely to have on the availability of data to companies, particularly smaller startups, and the product and insurance innovation that is being incentivized in part by increased government requirements. In sum, we aim to concisely catalog the impacts with which policymakers should be most concerned when building regulatory frameworks for financial data privacy.

Lastly, we construct a comprehensive proposal for federal legislation, dubbed the Comprehensive Consumer Financial Data Act (CCFDA), to model our optimal set of consumer rights and business requirements, balancing the appropriate tradeoffs. Starting with the dire need to harmonize regulations across the state and federal levels, we detail a Consumer Financial Data

---

[10] California Legislature, "California Consumer Privacy Act of 2018," 1798.100-1798.199 California CIV 1.81.5 § (2018), https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

[11] Colorado State Legislature, "Colorado Protections for Consumer Data Privacy Act of 2018," 6 Colorado Revised Statutes § (2018), http://leg.colorado.gov/sites/default/files/2018a_1128_signed.pdf.

[12] Kevin Thomas, "New York Privacy Act," Pub. L. No. S5642 (2019), https://www.nysenate.gov/legislation/bills/2019/s5642.

[13] Cynthia Stone Creem, "An Act Relative to Consumer Data Privacy," Pub. L. No. S120 (2019), https://malegislature.gov/Bills/191/SD341.

[14] National Law Review, "Comprehensive Federal Privacy Law Still Pending," January 22, 2020, https://www.natlawreview.com/article/comprehensive-federal-privacy-law-still-pending.

[15] New York State Department of Financial Services, "23 NYCRR 500: Cybersecurity Requirements for Financial Services Companies," February 2017, https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf.

[16] Boston Consulting Group, "Readiness for Data Privacy: California Consumer Privacy Act & Related Regulations," July 2019.

Bill of Rights that recognizes the treatment of data as the property of consumers and the government's obligation to protect those rights. Notably, we include both privacy and security as cornerstones of our legislation, given the heavily interrelated nature of these concepts for the full protection of consumer data. Our legislation is structured to focus on principles within the legislative text but assign to regulatory agencies, most predominantly the Consumer Financial Protection Bureau (CFPB), the power to create regulatory rules to enforce requirements on firms in order to fulfill consumers' financial data rights. We strongly urge Congress to take up the CCFDA to both increase consumer protections and decrease the costs to businesses of navigating the existing web of financial data regulations at multiple levels of government. We further believe that this simplification will serve as a boost to innovation by shifting power back to smaller firms and incentivizing the creation of systems that incorporate privacy and security by design and the growth of the cyber liability insurance market.[17,18,19]

Given the centrality of financial data to the daily lives of consumers in the US and elsewhere, it is critically important to ensure that financial data regulations are appropriately robust and flexible. While the current regulatory framework contains gaps in protection for consumers and places a significant regulatory burden on businesses, we believe that comprehensive federal legislation on financial data privacy and security can simultaneously achieve the goals of strengthening consumer rights and streamlining compliance for firms.

The Financial Data Landscape

Since the inception of the modern financial system, consumer financial data has been an integral part of the functioning of the industry. However, what likely began as a simple record of deposits has grown into an ecosystem of corporations and governments that collect, maintain, and base decisions off data regarding everything from insurance contracts and home ownership to credit scores and daily transactions.

The scope of what constitutes financial data and the context behind the current role that it plays in modern life are the foundation upon which proposed changes should and will be examined. For this paper, we below provide bounds on the definition of financial data and recount a brief history of financial data regulation in the United States, focused on the elements still relevant to today's landscape.

What Is Financial Data?

Questions surrounding the scope of financial data have plagued corporations and regulators alike since concerns about its utilization and safety first arose. In some instances, financial data is straightforward to categorize and delineate as the data is being directly applied to or derived from a financial event. For example, in the case of a particular credit card transaction made by an individual and being processed by a card issuer, details such as the credit

[17] Boldon James, "CCPA - The New Law Delivering GDPR-Style Privacy to California," accessed January 4, 2020, https://www.boldonjames.com/ccpa-compliance/.
[18] John Noltensmeyer, "CCPA Overview: Understanding Compliance," TokenEx, August 15, 2018, https://www.tokenex.com/blog/understanding-compliance-california-consumer-privacy-act.
[19] Jeffrey Raskin, "Consider Enhancing Cyberliability Insurance Policies to Align with CCPA: Part 1," September 24, 2019, https://www.morganlewis.com/blogs/healthlawscan/2019/09/consider-enhancing-cyberliability-insurance-policies-to-align-with-ccpa-part-1.

card number, the Address Verification System (AVS) information, and the merchant ID are clearly pieces of financial data.[20]

However, the lines begin to blur when referring to information utilized in a non-financial context. While an individual's home address is certainly financial data when it is being used for an online purchase (in other words, a financial transaction), is that status different when the address is utilized by a magazine distributor for postal purposes? The specific purpose for which information is used can vary widely despite the underlying data being mostly or entirely the same and possessing identical potential.

Furthermore, as technology has developed, the scope of data that can be relevant to financial decision-making has significantly increased. In years past, institutions processing a financial event might have been limited to information provided by an individual that was of a direct financial nature. However, as a multitude of data sources have become digitized and made broadly available, corporations have recognized that these sources contain data that can fine-tune financial decision-making. For instance, in the case of the consumer lending industry, companies are now, in some cases, utilizing data sources such as the age of email accounts or the history of telephone numbers to try to detect fraudulent loan applications more readily.[21] While the age of an email address might not be directly financial in nature, whether it should be considered as financial data in this context because it is being used to make a financial decision, namely the issuance of credit, is fundamentally unclear.

Additional complications stem from the fact that financial data can be relevant to different types of subjects and be processed by a wide variety of corporations and other entities. Financial data concerning the workings of a business may not be equivalent to that regarding an individual's financial status in terms of the concerns, risks, and uses that are relevant. Then, that data can be held closely by one organization or distributed widely to many who perform disparate processes on it. Almost any type of organization could, at some time, be in a position to possess and process financial data, and the categories of organizations with a particular dataset can also change over the lifetime of the data. Should the processor of the data be relevant to our view of what financial data is?

Critical Attributes of Financial Data

The above questions all raise essential definitional issues concerning financial data. These issues must be resolved individually in order to appropriately define the scope of what financial data is and how we should think about it. Collectively, the answer to these questions will form the foundation of our understanding of financial data.

Specifically, four critical attributes exist that combine to provide the groundwork of the definition of financial data:

- Data type
- Data utilization
- Data subject
- Data processor

[20] Worldpay Editorial Team, "How Credit Card Processing Works," July 10, 2019, https://www.worldpay.com/en-us/insights-hub/article/how-credit-card-processing-works.

[21] Marshall Lux and Guillaume Delepine, "Revolution in Data: How New Technologies Are Upending Borrowing" (Harvard Kennedy School Mossavar-Rahmani Center for Business & Government, February 2019), 19, https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/working.papers/107_BigData.pdf.

Data type refers specifically to the dichotomy between data that is directly financial in nature, such as a bank account number or an individual's income information, and that which is not inherently financial but could be relevant in financial contexts, such as the history of a person's telephone number when applying for a loan, as mentioned previously. In the former case, the data is linked inextricably to finance, while, in the latter, the data is merely financialized under particular circumstances. Determining if and when certain data types should be included as financial data will be an integral component of our working definition.

Data utilization focuses on the particular task or process in which a piece of data is being leveraged. As with data type, there exists a delineation in data utilization between financial and non-financial applications. An example of a financial application is applying for a credit card, while non-financial applications for individuals run the gamut from applying to a college to registering the warranty on one's television. Certain utilizations of data might never warrant the inclusion of said data into the scope of financial data, while others might always demand it. In particular, the intersection of data type and data utilization will prove especially critical in determining the appropriate classification of data as financial.

Data subject deals with the entity that the data concerns or is about. Data subjects can be individuals, corporations, governments, non-profit charities, social clubs, or any other association of people. This attribute is specifically relevant to the definition of financial data because said data could potentially be very different in nature across types of subjects. For instance, an individual's income is generally considered private information and, given that nature, is likely to be considered financial data. However, a public corporation's net income is a matter of quarterly financial reporting and thus does not, in all likelihood, meet the same standard of financial data.

Data processor concerns the individual or organization that is possessing and/or manipulating the data in question. While it may be tempting to label the data processor as the "data owner," the concept of data ownership is a hotly debated question in legal and policy discussions that will be delved into further through the course of this paper. Thus, for simplicity's sake, it is more advantageous to use the term data processor to refer to the entity that is holding the data and, in some cases, running tasks or making decisions on the basis of said data. For instance, in a situation where an individual is applying for a credit card, the data processor would be the credit card company that holds the individual's data and inputs the data into the application algorithm for a decision. The key question is whether the type of organization serving as the data processor is relevant to the classification of the underlying data as financial or not.

A Working Definition of Financial Data

In its broadest form, based on the four critical attributes, financial data could be any piece of information that is directly or tangentially tied to a historical transaction or a potential future transaction regardless of the data subject or the data processor. At first glance, this scope may seem appropriate in order to avoid incorrectly classifying data as non-financial in nature. But, in practice, such a definition is so all-encompassing that it ultimately proves useless for setting reasonable bounds on the dataset so that it is relevant to the task at hand. Arguably, the data in all of the prior examples would fit into this definition, rendering the scope nearly infinite.

Alternatively, the definition of financial data could be kept very tight by limiting it to information about an individual that is directly financial in nature and utilized for a specific financial purpose by a financial institution. While this definition captures the data that is most particularly and clearly in scope for financial data, it potentially ignores some use cases where data should be treated with the care of financial data, given the sensitivity of the utilization or processor, despite not meeting these strict guidelines.

In the spirit of both practicality and applicability, this paper will adopt a definition of financial data that combines various aspects of the critical attributes defined above:

Financial data is a piece of information where:
(a) its subject is an individual or closely related individuals such as a family (data subject), and
(b) it is either:
(i) directly tied to a financial account, transaction, or an individual's personal finances (data type), or
(ii) involved in a financial process (data utilization).

To note, the entity that possesses and/or processes the data (data processor) is not relevant to the classification of the data as financial or otherwise.

A few key aspects of our working definition of financial data stand out.

First, it only applies to data about individuals. This should not be construed to suggest that data about corporations, governments, or other organizations is not important. But, when discussing consumer protection, the data that is relevant to the conversation is that which has individuals as its subject. For that reason, this paper will confine itself to a discussion of individual data.

Next, the definition above incorporates an intersection of data with respect to data type and data utilization. This is done in recognition of two realities. First, data that is directly financial in nature is always financial regardless of the specific use case. Thus, even if this data is being used in a non-financial context, it should continue to be defined as financial data. Second, processes that are financial in nature can utilize many types of data. While some of the data being leveraged may not be traditionally financial in nature, it should nonetheless be classified as financial data when it is being utilized for an explicitly financial purpose. The combination of these two factors results in data that is either inherently financial in nature or that is being utilized in a financial manner obtaining the classification of financial data.

Lastly, the working definition of financial data is agnostic to the individual or organization serving as the data processor. This choice is made in deliberate recognition of the state of business in the modern economy where nearly every entity is involved in financial activities of some variety, even if that activity is as straightforward as processing credit card transactions. Rather than expending time and energy attempting to fit companies into some sort of arbitrary classification regarding the existence or level of financial activity within their boundaries, it is far more practical and, frankly, accurate to include all entities serving as data processors in the scope of financial data.

As will be delved into in more detail, the definition of financial data given here lays the foundation for further exploration of how this data is created, maintained, utilized, and secured in the modern economy as well as what changes or reorganizations are currently being

contemplated or should be considered moving forward. It will be important when looking at these proposals to consider how, if at all, they reflect or alter the definition of financial data and what implications that may have for consumers, businesses, and governments.

Existing US Financial Data Regulation

Now that a firm definition of financial data has been established, it is beneficial to catalog existing policies and regulations regarding financial data in the United States to understand the status quo of the financial system and the players within it. In their own particular ways, each of these pieces of legislation has a continuing impact on how financial data is treated in the US, either through collection guidelines, maintenance requirements, or utilization restrictions. Understanding how they fit together and what areas remain uncovered is essential to analyzing how potential future policy changes would impact the financial data landscape.

Facets of the Effects of Legislation on Financial Data

Comparing the impacts of multiple pieces of legislation is often a tricky affair. For that reason, it is important to ensure that our examination of existing US financial data regulations occurs on an even footing, utilizing standard attributes that delineate the most important effects that such policies can have. The below attributes and their definitions represent a comprehensive evaluation of policies dealing with financial data pertaining to a particular individual:

- Retention: how much data can be kept by an organization
- Specificity: how specific or granular the data collected and retained can be
- Breadth: how broad the types of data collected and retained can be
- Security: how secure the collection and retention of data must be
- Government Access: whether and how the government can access the data
- Third-Party Access: whether and how third-parties can access the data
- Individual Access: whether and how the individual can access the data

By relying on these facets of legislative impact, we can get an accurate sense of the current regulatory landscape as well as examine the potential changes proffered by specific proposals. The latter examination will be critical to shaping future growth in the US economy and financial sector.

Bank Secrecy Act of 1970 (BSA)

The BSA was passed by Congress in 1970 with the goal of reducing money laundering in the United States.[22] Specifically, it was meant to prevent money or other assets from being hidden in or illicitly transferred through domestic or foreign financial institutions.

In order to accomplish this task, the BSA placed several requirements on financial institutions.[23] First, all financial institutions are required to keep records of all cash purchases of securities in an attempt to track asset masking. Second, these institutions must report individual

[22] US Internal Revenue Service, "Bank Secrecy Act," accessed January 2, 2020, https://www.irs.gov/businesses/small-businesses-self-employed/bank-secrecy-act.
[23] US Office of the Comptroller of the Currency, "Bank Secrecy Act (BSA)."

transactions over $10k as well as any other suspicious activity, including patterns of behavior, to the government.

The changes in bank policies and data management practices brought about by the BSA have had a number of broad impacts on the financial data landscape. The data being collected by financial institutions increased in both specificity and breadth, and these institutions were retaining data for a significantly longer period of time. In addition, the government's ability to access financial data increased dramatically due to both the recordkeeping and active notification requirements included within the legislation.

The applicability of the BSA's requirements was broad but limited to traditional financial institutions. Specifically, all domestic and foreign banks operating in the US, as well as savings associations, were subject to the standards set by the BSA. These institutions were obligated to build out internal processes to ensure compliance with the requirements and were subject to potential fines or legal action if found in violation. While individuals within these institutions could be held personally liable for infractions, in practice, successful cases brought by regulators have tended to center on institutions.[24]

Overall, the BSA was a major expansion in the role that financial data plays in modern regulatory practice and the economy more broadly.

Fair Credit Reporting Act of 1970 (FCRA)

The FCRA regulates the collection of credit information on individuals as well as the access that individuals have to their own credit reports.[25] The legislation is meant to set fair standards for the information collection processes of credit rating agencies and increase transparency in the industry to the consumer level.

With this goal in mind, the FCRA, like the BSA, contains requirements for financial institutions, specifically the credit rating agencies.[26] There are multiple limits placed on the types of information that the credit agencies can collect, and the FCRA permits individuals to dispute items included on their credit reports. Furthermore, the legislation limits the ability of credit rating agencies to sell credit-related data to third parties for their own purposes. Finally, it requires that all data except for information about bankruptcies be deleted after seven years to allow for readjustments of a consumer's credit profile over time.

In contrast to the BSA, the FCRA reduces both the retention of consumer financial data and the breadth of its collection through the deletion and scope limitation requirements. While the access that third parties have to this credit-related data is significantly reduced by the legislation, the effect is the opposite on individual access as people now have guaranteed access to their own credit reports.

However, a key delineation between the BSA and the FCRA pertains to the types of financial institutions to which they are applicable. While the scope of the BSA comprises all domestic and foreign banks conducting operations in the US, the FCRA applies only to

[24] Elkan Abramowitz and Jonathan Sack, "Bank Secrecy Act Prosecutions: Why Few Individuals Are Charged," *New York Law Journal* 252, no. 43 (September 2, 2014), https://www.maglaw.com/publications/articles/2014-09-02-bank-secrecy-act-prosecutions-why-few-individuals-are-charged/_res/id=Attachments/index=0/Bank%20Secrecy%20Act%20Prosecutions%20Why%20Few%20Individuals%20Are%20Charged.pdf.

[25] US Consumer Financial Protection Bureau, "A Summary of Your Rights Under the Fair Credit Reporting Act," accessed January 2, 2020, https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

[26] US Congress, The Fair Credit Reporting Act.

"consumer reporting agencies," which specifically refers to entities that "assembl[e] or evaluat[e] consumer credit information … for the purpose of furnishing consumer reports to third parties."[27] Thus, the institutions covered by these pieces of legislation are actually largely distinct, with the BSA covering banks and the FCRA covering credit rating agencies such as Equifax, Experian, and TransUnion.

Ultimately, the FCRA resulted in a reduction of the role that financial data has in the lives of individuals due to the restrictions on collection, retention, and reselling, while granting transparent access to view it.

Right to Financial Privacy Act of 1978 (RFPA)

The RFPA limits the ability of the federal government to access non-public financial records, specifically those held by financial institutions concerning their customers, and lays out clear procedures that the government must follow in order to obtain access to this information.[28] The legislation was passed by Congress in 1978 in response to *United States v. Miller*, which was a 1976 Supreme Court case that held that individuals had no constitutional right to privacy for financial information held by financial institutions.[29]

As an amendment to the BSA, the RFPA had a more limited impact on consumer financial data privacy than prior pieces of legislation because it focused specifically on the privacy of individual data with regard to access by the federal government. While the legislation was certainly instrumental in ensuring that "financial institution customers [have] a reasonable amount of privacy from federal government scrutiny,"[30] it did not have a wide-ranging impact on any aspects of financial data privacy other than government access. However, to the extent that the RFPA represents a "statutory Fourth Amendment protection for bank records,"[31] it is nonetheless impactful.

The scope of the RFPA is identical to that of the BSA: all domestic and foreign banks operating in the US as well as savings associations. In contrast to the BSA, however, it's important to note that the RFPA did not place significant incremental requirements on financial institutions other than the need to keep records of requests from the federal government for individual financial data. Rather, the onus was on the federal government to follow due process requirements, including obtaining the customer's permission or a warrant (or similar legal document) prior to requesting data from financial institutions and to provide written documentation certifying compliance with the requirements of the RFPA.[32] For that reason, the RFPA should be viewed as impacting the public sector far more than the financial institutions of the private sector.

In summary, the RFPA restricts government access to individual financial data to ensure a right to privacy for consumers from government scrutiny, thus reducing the role or, at least, increasing the acquisition costs of financial data in government proceedings.

---

[27] US Congress.
[28] US Federal Deposit Insurance Corporation, "FDIC Consumer Compliance Examination Manual - Right to Financial Privacy Act," June 2006, https://www.fdic.gov/regulations/compliance/manual/8/viii-3.1.pdf.
[29] Electronic Privacy Information Center, "The Right to Financial Privacy Act," accessed January 2, 2020, https://epic.org/privacy/rfpa/.
[30] US Federal Reserve, "Federal Reserve Consumer Compliance Handbook - Right to Financial Privacy Act."
[31] Electronic Privacy Information Center, "The Right to Financial Privacy Act."
[32] US Federal Reserve, "Federal Reserve Consumer Compliance Handbook - Right to Financial Privacy Act."

Gramm-Leach-Bliley Act of 1999 (GLBA)

The GLBA, also known as the Financial Services Modernization Act of 1999, is far-reaching legislation that made significant changes to the financial regulatory structure in the US, including the repeal of part of the Glass-Steagall Act of 1933 that prevented the conglomeration of commercial banks, investment banks, and insurance companies.[33] But the key changes of relevance for this discussion concern new requirements involving consumer financial data privacy for financial institutions.[34]

Specifically, there are two categories of requirements placed on financial institutions with regard to any personally identifiable financial information (PIFI): safeguards and privacy.

The Safeguards Rule "requires financial institutions to have measures in place to protect and keep secure the consumer information they collect."[35] This includes a specific information security plan that is regularly updated and validated, as well as any additional steps that might significantly threaten the safety of customer information.

The Privacy Rule necessitates the provision of "policies on [the] sharing of personal financial information"[36] to consumers in order to inform them of any potential uses that the company might have for their data. Furthermore, companies are required to notify consumers of instances outside of those policies that might result in consumer data being distributed to third parties. In such instances, companies must provide the potential for the customer to opt out.

The key aspects of consumer financial data privacy focused on by the GLBA are third-party access and security. In particular, the GLBA is aimed at limiting the proliferation of data without the customer's knowledge or consent, through either intentional or accidental means. The Privacy Rule pertains to the former situation, where the company collecting data is purposefully sharing it with a third party for some business or monetary reason, while the Safeguards Rule sets standards for data security within financial institutions to attempt to prevent situations where consumer data is released to unauthorized parties either by accident or as a result of a malicious attack. In contrast to the BSA, FCRA, and RFPA, the provisions of the GLBA do not have a significant impact on data retention, specificity, or breadth, nor on the rights of the government or individuals to access financial data.

Of all the legislation discussed thus far, the GLBA has, by far, the broadest scope in terms of the businesses to which it is applicable. Whereas the BSA applies only to domestic and foreign banks operating in the US, the GLBA applies to any entity that "is engaging in activities that are financial in nature or incidental to such financial activities … includ[ing] banks, securities brokers and dealers, insurance underwriters and agents, finance companies, mortgage bankers, and travel agents."[37] In theory, this definition could be viewed as incorporating many types of companies, particularly in the modern age as technology and finance become further

[33] Joe Mahon, "Financial Services Modernization Act of 1999, Commonly Called Gramm-Leach-Bliley," Federal Reserve History, November 12, 1999, https://www.federalreservehistory.org/essays/gramm_leach_bliley_act.
[34] US Federal Deposit Insurance Corporation, "FDIC Consumer Compliance Examination Manual - Gramm-Leach-Bliley Act (Privacy of Consumer Financial Information)."
[35] Sara Jodka, "More Companies Must Comply with the Gramm-Leach-Bliley Act, But Don't Know It. Are You One of Them?," September 2017, https://www.dickinson-wright.com/news-alerts/more-companies-must-comply-with-the-gramm-act.
[36] Electronic Privacy Information Center, "The Gramm-Leach-Bliley Act," accessed January 2, 2020, https://epic.org/privacy/glba/.
[37] US Federal Deposit Insurance Corporation, "FDIC Consumer Compliance Examination Manual - Gramm-Leach-Bliley Act (Privacy of Consumer Financial Information)."

intertwined. In practice, regulators have generally focused on more traditional financial institutions for the purposes of enforcing the requirements of GLBA. However, as policy discussions regarding consumer data privacy have become more prevalent, the regulatory community appears to be reevaluating this scope, with tech-oriented companies potentially under increased scrutiny.[38]

Overall, the GLBA aims to increase the protections for consumer financial data held by financial institutions, specifically in relation to the attributes of third-party access and security, and the legislation has the potential to impact a broad swath of institutions so long as they are engaging in financial activities at some level.

Consistency of Financial Data Definitions

It's worth noting that these four pieces of legislation – the BSA, FCRA, RFPA, and GLBA – take markedly different views of what constitutes financial data to be regulated. The BSA and the RFPA view financial data as any information regarding a transaction at a banking institution, while the FCRA applies to data at credit rating agencies. The GLBA takes the most expansive view by including in its scope any entities engaged in providing a financial service, not only traditional domestic and foreign banks.

To be fair, some of the distinctions in the definitions of financial data in these bills are driven by the fact that they are simply regulating different activities. For instance, the driving force behind the gap in the definitions utilized by the BSA/RFPA and the FCRA is the fact that the FCRA is focused on credit decisions for consumers, while BSA and RFPA are intent on reducing money laundering.

However, there are also distinctions that do not appear to be appropriate. As an example, if anti-money laundering is a goal of the government's financial regulation, why are entities other than traditional banks excluded from the requirements of the BSA/RFPA? One might imagine that a scope more similar to that of the GLBA might be better at serving the government's desired outcome of reducing money laundering.

For that reason, we will aim to consistently compare the definitions of financial data included in existing or proposed legislation to the ideal standard definition that we previously created in this paper to understand whether any distinctions are the result of legitimate legislative purpose or are simply outdated, overly narrow considerations. In the case of the BSA/RFPA, the definitions utilized are too constricted to traditional financial institutions, likely because they haven't been appropriately updated to the standards of the modern economy. For the FCRA, by contrast, the definition, while narrow, seems appropriate as the legislation is solely meant to affect behavior in the credit rating agency industry. The GLBA has the definition that is most consistent with the standard outlined in this paper, though even it does not include non-financial data captured in a financial process, perhaps due to the unexpected rise of big data in financial decision-making in recent years.

One critical element to be considered for proposed or future legislation is how it defines financial data and how that definition aligns with existing regulations and the gold standard previously outlined. The scope of the definition will be essential for determining the ultimate impact of the legislation on businesses and consumers.

[38] Jodka, "More Companies Must Comply with the Gramm-Leach-Bliley Act, But Don't Know It. Are You One of Them?"

Summary of Existing Legislation

The BSA, FCRA, RFPA, and GLBA form the foundation of financial data regulation at the federal level in the US. Together, they provide the rules and requirements that govern the breadth and specificity of financial data collection, the security and retention of that data, and the access that certain entities, including the government, third parties, and individuals, can have to it.

All place distinct requirements on different institutions and operate on unique views of the concept of financial data. Moving forward, it will be essential to understand how new legislation might add to or change the regulations that currently exist for businesses and the protections that they offer – or, in some cases, don't provide – for consumers.

Recent Efforts Impacting Financial Data Laws

Across the country, there has been renewed debate in recent years regarding consumer data privacy and its associated regulation. Many consumers have had an awakening regarding the data that they are giving to companies, particularly tech firms, and the use to which it is being put by those companies. According to a 2018 survey of Americans conducted by SAS, a data analytics firm, 73% of consumers report increasing concerns regarding data privacy, with 66% saying that they've undertaken specific actions to increase their privacy and security.[39]

This shift in public attitudes from accepting to questioning has also manifested in legislative agendas. While there has not yet been any significant action taken at the federal level, a significant portion of state legislatures have passed or been considering legislation pertaining to consumer data privacy. According to a 2019 review by Boston Consulting Group (BCG), 25 states have considered revised data privacy legislation since 2018, with at least nine passing updated laws as a result.[40] Furthermore, multiple regulatory agencies at the state level have enacted or considered changes to regulatory rules pertaining to data privacy and security, providing a complement to proposed legislative action.

Thus far, these efforts have, at times, pursued markedly different goals and had significantly disparate impacts across states. Some have attempted to address problems of more limited applicability, such as concerns specific to children or broadband internet service providers, while others have taken a broad view of these issues by incorporating all citizens of their particular state.[41] Within their chosen scope, data privacy proposals have also differed with respect to the requirements or recommendations applied to individuals and businesses.[42] Some of the pieces of legislation have been incremental upgrades to existing laws, while others have completely reworked existing rules or imposed relatively restrictive mandates with which it may be difficult for companies to comply.

---

[39] Beth Negus Viveiros, "Data Privacy Concerns On Rise" (Chief Marketer, December 12, 2018), https://www.chiefmarketer.com/data-privacy-concerns-on-rise-report/.

[40] Boston Consulting Group, "Readiness for Data Privacy: California Consumer Privacy Act & Related Regulations."

[41] Boston Consulting Group.

[42] Cynthia Brumfield, "11 New State Privacy and Security Laws Explained: Is Your Business Ready?," CSO Online, August 8, 2019, https://www.csoonline.com/article/3429608/11-new-state-privacy-and-security-laws-explained-is-your-business-ready.html.

The following discussion will detail the changes either enacted or proposed at the state level with comparison both to each other and to the existing pieces of federal consumer data privacy legislation described previously. This examination will serve as the foundation for analyzing the impacts that these pieces of legislation are likely to have on the financial industry and consumers. It will also suggest how policy recommendations are to move forward in the most productive fashion for individuals, businesses, and the government alike.

Enacted Laws

We'll begin the discussion with the laws that have been passed and/or enacted at the state level since the end of 2017. These pieces of legislation represent the vanguard of the burgeoning movement to fundamentally alter the way consumers interact with their data and the companies that collect and process it. In some cases, businesses have already had to change their practices to comply with these laws, and there is not an immediate end in sight to the forthcoming transitions.

Furthermore, as additional states and the federal government begin to contemplate legislation in the realm of consumer data privacy, these already-enacted laws have, in many cases, served as a guide to legislators and regulators for their own changes. As will be shown, this has resulted in many similarities among the state-level legislative and regulatory modifications that have been contemplated thus far. However, just as striking are the instances where there is significant disagreement, even direct conflict, between requirements being considered.

California Consumer Privacy Act of 2018 (CCPA)

The CCPA was passed in June 2018 after an effort by California citizens to include a ballot referendum on consumer data privacy and went into effect on January 1, 2020.[43] The requirements are applicable to any business that operates at any level in California[44] and:

1. Has $25mm or more in revenue; or
2. Transacts the personal information of 50,000+ individuals; or
3. Gets 50%+ of its revenue from selling personal information

The broad sweep of the CCPA has the effect of imposing five high-level categories of consumer rights and business requirements on almost any significant corporation in the US and around the world.[45]

Category	Consumer Right	Business Requirement
Transparency	• Right to access data • Right to know what data is collected and disclosed	• Notice of data collection and receipt
Consumer Control	• Right to opt out of sale of personal data	• Data portability

[43] John Stephens, "California Consumer Privacy Act," American Bar Association, July 2, 2019, https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_9/.
[44] Stephens.
[45] Boston Consulting Group, "Readiness for Data Privacy: California Consumer Privacy Act & Related Regulations."

	• Right to deletion	
Commercial Fairness	• Right to non-discrimination in service and price based on exercise of privacy rights	• N/A
Responsiveness	• N/A	• Responses to customer requests within 45 days
Stewardship	• N/A	• Implementation of reasonable data security measures • Training of employees on data privacy requirements and responsibilities

The rights and requirements in the CCPA are based largely on the European General Data Protection Regulation (GDPR), passed in 2016,[46] and serve the purpose of bolstering consumer rights throughout the data lifecycle and placing incremental obligations on businesses with regard to data treatment. Because of the expansiveness of the changes incorporated, the CCPA is widely viewed as a paramount shift in consumer data protection, both in California and, because of the breadth of business applicability, in the US.

Delving deeper into the rights granted to consumers by the CCPA, the consumer gains significant power over his/her data from initial collection to final deletion. Consumers have a right to know what types of data are being collected about them, what specifically that data is, and how it's disclosed to other parties. They have the right to opt out of a sale to a third party and to the deletion of their data by the original collector. Consumers must be treated equally by companies, including given the same price for services, regardless of whether they choose to exercise these rights. From start to finish, the CCPA aims to put consumers in the driver's seat regarding the collection, utilization, and maintenance of their data, which has the side effect of increasing the data privacy and security requirements with which businesses must comply.

In addition to consumer rights, the CCPA places several incremental obligations on corporations. Companies must notify consumers when they collect data from them or receive it from another entity. Businesses need to ensure that consumer data is portable from the consumer's perspective, which, in the case of the CCPA, means that data access requests are in a standardized, intelligible format for consumers. Importantly, the CCPA did not go so far as to require import portability, which would force companies to take consumer data exporting from other businesses and incorporate it into their internal databases and processes and is a key provision of GDPR.[47] For consumer requests regarding data actions, such as access requests or deletions, companies are required to respond within 45 days to ensure timeliness. Lastly, businesses must provide good data stewardship through data security measures and employee trainings on data privacy and security. Overall, the CCPA's requirements on companies focus on fulfilling the consumer rights previously outlined and ensuring data security even in operations where the consumer might not be directly involved.

[46] PricewaterhouseCoopers, "Your Readiness Roadmap for the California Consumer Privacy Act (CCPA)," accessed January 2, 2020, https://www.pwc.com/us/en/services/consulting/cybersecurity/california-consumer-privacy-act.html.
[47] PricewaterhouseCoopers.

In addition to consumer rights and corporate requirements, the definition of data is essential to the impact of the CCPA on financial data privacy. Up front, it should be noted that the CCPA is not specific to financial data. It incorporates any form of consumer data that "identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[48] Thus, the CCPA's definition is significantly broader than that of the prior financial data legislation that we have described.

For our purposes, we will focus exclusively on the CCPA's impact on financial data as we have defined it, and, by that metric, the CCPA is the first wholly inclusive piece of legislation thus far reviewed. It incorporates individual financial data in all circumstances and non-financial data utilized in a financial transaction with little regard to the entity involved, save for the size requirements previously outlined. However, it must be noted that the CCPA contains a specific carve out for consumer data already covered by existing federal legislation, including GLBA and FCRA in the case of financial data, to avoid legal issues regarding supremacy and pre-emption.[49] Thus, the CCPA explicitly excludes financial data being utilized for financial purposes as that is already covered by the GLBA.

The impact of the CCPA is comparable in many ways to that of prior financial data privacy legislation, but also carries some unique twists. On access, the CCPA is primarily focused on increasing the access of individuals to their own data through the right to access and decreasing third-party access through the right to opt out, while government access is not affected. The CCPA serves to increase data security through the corporate requirements on data policies and training, providing an incremental bulwark against intrusions or thefts. Regarding retention, the CCPA primarily leverages the right to deletion to decrease the maintenance of data not essential for ongoing business or as required by law. While not an explicit limit on retention, the right to deletion allows consumers to gain direct control over the longevity of their data. Lastly, the CCPA does not place any particular restrictions on the specificity or breadth of consumer data that can be collected. However, it does so through a market mechanism by establishing the consumer right to know what types of data are being collected and forcing companies to provide upfront notification of this information.[50] In all likelihood, this proactive notification will cause some consumers to prioritize the acquisition of a company's services in part based on the scope of data being collected, which will provide market incentivization for companies to narrow the specificity and breadth of what they collect. If nothing else, the tradeoff inherent in collecting an incremental data field between business purpose and potential loss of consumers will now be more prevalent in corporate prioritization meetings.

For now, the impact of the CCPA on financial data privacy is significant, given the expansion of consumer rights and the implementation of stringent requirements on businesses, but limited to data that falls outside the scope of existing legislation such as the GLBA and FCRA. Thus, the immediate impact on financial data privacy has two similar but distinct flavors: incorporating non-financial data utilized in financial transactions at all businesses, and explicitly bringing into scope data at non-financial businesses that have de facto operated as if they are not

---

[48] California Legislature, California Consumer Privacy Act of 2018.

[49] Seamus C. Duffy, Meredith C. Slawe, and Julia Ann Busta, "United States: Divergent State Privacy Laws Show Need for Federal Solution," Mondaq, August 23, 2019, http://www.mondaq.com/unitedstates/x/840000/Data+Protection+Privacy/Divergent+State+Privacy+Laws+Show+Need+For+Federal+Solution.

[50] Boston Consulting Group, "Readiness for Data Privacy: California Consumer Privacy Act & Related Regulations."

subject to GLBA requirements (though looser interpretations of the law suggest that they are). For the first, companies leveraging non-financial data for transactions will need to determine how best to align their processes to adequately protect both financial data under GLBA and non-financial data under CCPA. For the second, these businesses may require massive uplifts to meet CCPA standards, particularly if they were operating in a manner free of oversight previously. In either case, the impacts based on the reading of the law are only made murkier by the legislation's oversight mechanism, the office of the California Attorney General.[51]

The CCPA's impact is further heightened because it has been leveraged by multiple other states in drafting their own pieces of privacy legislation. As will be shown, the CCPA is the foundation upon which additional modifications have been added to construct requirements for other jurisdictions. We will seek to cover examples where other states have taken markedly different paths from the CCPA. However, even those line up significantly with California's norm-setting legislation. In short, as businesses seek to comply with the CCPA, they will find that some other states have followed California's lead, while others have charted their own course.

Colorado Protections for Consumer Data Privacy Act of 2018 (CPCDPA)

The CPCDPA was passed by the Colorado State Legislature unanimously in May 2018 and came into effect in September of that year.[52] It is significantly narrower in scope than the CCPA as it deals primarily with data security and the proper disposal of data;[53] however, it contains incremental provisions that place significant requirements on businesses above those in the CCPA. Thus, it is an interesting example of data legislation that is focused far more on security than privacy and should be considered through the lens of what alternative data privacy and security frameworks could be.

The CPCDPA is primarily concerned with only two consumer data rights, secure treatment and appropriate deletion,[54] and it manifests these rights through requirements that it places on companies. First, businesses must have reasonable procedures for the handling and security of data and must additionally ensure that any third parties to which it transmits data have appropriate procedures as well. This is a significant incremental burden as compared to the CCPA, which does not require companies to verify that their third parties have good security measures in place.

Second, companies must have written policies to handle the disposal of both paper and electronic data.[55] This requirement differs in both the scope and the level of prescription from the CCPA. The CPCDPA extends data protections to non-digital media such as written documents or applications, and, rather than setting the standard for security at reasonable measures as the CCPA does, the CPCDPA specifically requires a written set of policies for data disposal. The former requirement could impose significant excess burdens beyond the CCPA on companies,

[51] Stephens, "California Consumer Privacy Act."
[52] The Gazette, "New Law Puts Colorado at the Top for Consumer Data Protection," March 22, 2019, https://gazette.com/sponsored/new-law-puts-colorado-at-the-top-for-consumer-data/article_fcfb33ae-4c11-11e9-94d1-0b5d51de9ac2.html.
[53] Boston Consulting Group, "Readiness for Data Privacy: California Consumer Privacy Act & Related Regulations."
[54] Boston Consulting Group.
[55] Colorado Office of the Attorney General, "Colorado's Consumer Data Protection Laws: FAQ's for Businesses and Government Agencies," accessed January 2, 2020, https://coag.gov/resources/data-protection-laws/.

particularly on more legacy firms that might use a mix of non-digital and digital media. The latter requirement, while not necessarily massively incremental to the requirements of the CCPA, imposes a specific prescriptive solution on firms in a way that the CCPA does not.

Third, the CPCDPA requires firms to conduct investigations of any security breaches of which they are aware and provide notification within 30 days to impacted consumers and, if the number of consumers impacted is greater than 500, the Colorado Attorney General.[56,57] This goes well beyond the requirements of the CCPA in both aspects. The obligation to perform an investigation of security breaches, as with the requirement for a specific set of written data disposal policies above, showcases the prescriptive nature of the CPCDPA as compared to the CCPA. It's arguable that the CCPA stewardship standards would likely require investigations of security breaches all the same, but the obligation is made explicit in the CPCDPA. Furthermore, the notification requirement is structured such that the company must publicize that a breach occurred within the relatively tight timeframe of a month, while no such notification is required by the CCPA.

The CPCDPA, in contrast to the CCPA, is focused far more on data security and potential breaches than on privacy. In fact, there are no specific requirements regarding data retention, specificity, breadth, or access included in the CPCDPA. Rather, it is solely focused on the data security element, particularly in the wake of high-profile hacking incidents such as the Equifax breach.[58]

Further, the CPCDPA takes a very narrow view of data. As with the CCPA, the CPCDPA is not solely concerned with financial data. However, it defines the relevant dataset to be personally identifiable information (PII) within a limited range, including Social Security numbers, passwords, biometric data, and passport numbers, among others.[59] It excludes any other types of data that could be equally identifying for individuals, particularly in the context of the financial industry. Similar to the CCPA, the CPCDPA includes a carveout for data that is already included in federal regulations, such as the GLBA, meaning that the incremental requirements placed on financial institutions are minimal at best.

Because the data scope is relatively limited with associated carveouts for other regulations, the largest impact of the CPCDPA will be felt by non-financial businesses for which data regulation did not already exist. Specifically, these companies' data security practices may require significant revamps in order to achieve compliance with the CPCDPA's requirements. However, over time, the prescriptions laid out by the CPCDPA will be fulfilled with only the ongoing breach notification requirement for businesses.

The CPCDPA provides a useful example of what security-focused data legislation might entail for businesses as opposed to the privacy-led CCPA. Because of the distinctions in focus, differences abound between the laws, and coming into compliance with both, such as would be necessary for companies operating nationally, could prove to be a challenge requiring significant time, effort, and investment.

---

[56] Boston Consulting Group, "Readiness for Data Privacy: California Consumer Privacy Act & Related Regulations."
[57] The Gazette, "New Law Puts Colorado at the Top for Consumer Data Protection."
[58] Electronic Privacy Information Center, "Equifax Data Breach," accessed January 2, 2020, https://epic.org/privacy/data-breach/equifax/.
[59] Colorado State Legislature, Colorado Protections for Consumer Data Privacy Act of 2018.

Proposed Legislative Bills

Having seen two examples of starkly different data privacy and security laws passed recently at the state level, we now turn our attention to states that continue to consider what updated data legislation might look like for them. At least 16 states are currently considering new legislation, and a significant majority of them are examining bills that are materially similar to the CCPA or CPCDPA.

However, there are also examples of state legislation still being considered that incorporate significantly different consumer rights or business obligations. For companies that operate across state boundaries, these disparities could pose important conflicts that they will need to resolve in order to continue going about business as usual. States that have not yet passed legislation have the opportunity to learn from those that have gone before. But these learnings can potentially lead to legislative differences of varying magnitudes. How, when, and whether these differences are resolved (or simply managed) will have significant implications for how businesses operate in the US moving forward.

New York Privacy Act (NYPA)

The NYPA is a bill currently being considered in the New York State Senate that, in many respects, is similar to the CCPA.[60] It involves many of the same consumer rights and business obligations and strikes a familiar line on the definition of data in scope for regulation, namely any information that could identify an individual or household. For that reason, we will not discuss each tenet in a fashion repetitive to the discussion of the CCPA.

However, there are critically important differences between the NYPA and the CCPA that merit discussion. First, the NYPA applies to any business regardless of size or scope,[61] which differs markedly from the CCPA, which requires a relatively substantial number of consumers or annual revenue in order to mandate a firm's compliance. Under the NYPA, any entity, from a local bodega to a multinational corporation, could be subject to the law's data privacy and security requirements. The incremental burden placed on small businesses by the NYPA, as compared to the CCPA, would be significant, particularly given the lack of spare resources that many small businesses have to devote to additional regulatory compliance.

Second, the enforcement mechanism for the NYPA has significantly broader scope than that of the CCPA. While the CCPA rests that power in the California Attorney General, the NYPA grants the consumer the right to sue a company directly over violations of the statute, which, in some ways, crowdsources enforcement of the law. In short, any consumer who has a complaint about compliance with the NYPA has the right, under the law, to sue the offending company, which is known as private right of action.[62] A similar stipulation in the original version of the CCPA was struck out after significant lobbying by industry groups that argued that the provision would lead to myriad nuisance lawsuits. While such a concern may be hyperbolic, taking the combination of private right of action with the lack of any applicability criteria, as

[60] Thomas, New York Privacy Act.
[61] Issie Lapowsky, "New York's Privacy Bill Is Even Bolder Than California's," *Wired Magazine*, June 4, 2019, https://www.wired.com/story/new-york-privacy-act-bolder/#:~:targetText=The%20New%20York%20Privacy%20Act%2C%20introduced%20last%20month%20by%20state,privacy%20before%20their%20own%20profits.&targetText=The%20New%20York%20Privacy%20Act%20bears%20some%20similarity%20to%20the%20California%20law.
[62] Lapowsky.

outlined above, would indicate that a business of any size in New York could find itself the subject of frivolous lawsuits, which could be significantly damaging to small businesses in the state.

The NYPA does not differ from the CCPA on many material dimensions concerning privacy and security; however, the enforcement element is crucial to understanding the distinctions between the laws. The NYPA would bring all businesses, particularly the smallest, in scope and allow consumers to individually sue companies for potential violations of the law. The implications of these changes as compared to the CCPA remain to be seen. On one hand, the expanded scope and increased enforcement could result in fewer privacy issues slipping through the cracks; however, on the other, they could lead to a significant hindrance for the types of businesses least equipped to handle incremental burdens. If not refined prior to passage or handled properly by regulators and the courts, the NYPA could pose an existential operational risk to small businesses in New York and beyond.

Massachusetts S120 (S120)

S120 is a bill introduced in the Massachusetts State Senate entitled "An Act Relative to Consumer Data Privacy" that bears many similarities to the CCPA, with several key distinctions.[63] As with the NYPA, we will focus on two of these differences: a non-waivable private right of action and an expansive definition of whose data is covered by the legislation.

Similar to the NYPA, S120 gives consumers the right to pursue civil legal action against companies over data privacy concerns, which is known as the private right of action.[64] However, the standards used in S120 result in a much broader set of capabilities for consumers to act against companies. First, the private right of action is non-waivable, meaning that any agreement between consumers and companies to remove the applicability of this right would carry no legal significance. While consumer advocates believe that including the right as non-waivable prevents companies from bullying consumers into giving up their power, industry groups argue that such a right would lead to a promulgation of class-action lawsuits on behalf of many consumers who would otherwise have willingly waived their right of action.[65]

Second, under the proposed law, consumers could bring civil lawsuits against companies without being required to show that any actual personal harm occurred regarding their data privacy. In legal terms, consumers would automatically have standing in a civil court, which would remove a significant barrier that companies normally use to halt data privacy-related lawsuits, given the complexity of proving harm in such a case. Consumer groups believe that granting automatic standing is an important way to shift power over data privacy from companies to consumers, while firms believe that not requiring consumers to prove harm will lead to a plethora of frivolous lawsuits. Both the non-waivable nature and the automatic grant of standing of the private right of action mean that S120 contains the broadest consumer rights of all the reviewed pieces of legislation for legal recourse against companies that, based on the law, violate consumer data privacy standards.

---

[63] National Law Review, "Massachusetts Consumer Data Privacy Bill Could Dramatically Expand Class Action Litigation Risk," May 21, 2019, https://www.natlawreview.com/article/massachusetts-consumer-data-privacy-bill-could-dramatically-expand-class-action.

[64] Stone Creem, An Act Relative to Consumer Data Privacy.

[65] National Law Review, "State Legislature Hears Concerns About Proposed Massachusetts Consumer Data Privacy Bill," October 11, 2019, https://www.natlawreview.com/article/state-legislature-hears-concerns-about-proposed-massachusetts-consumer-data-privacy.

As with other legislation concerning data privacy, S120 defines the data to which it is applicable, and, in many respects, its scope is in line with the CCPA. One key difference, however, is the definition of "consumer"; in other words, the definition of whose data is relevant. S120 utilizes the definition of "a natural person who resides in the Commonwealth," with an exemption for data about a business's employees.[66] The CCPA utilizes this formulation as well but broadens the exemption to include other types of business-to-business interactions or transactions that might include data on the employees of a partner firm. By doing so, the CCPA is differentiating between two types of data relationships: those where an individual is a true consumer of a business's activities and has their data sold to another business for commercial purposes, and those where an individual is employed by a business and has their data transferred to another business as part of the scope of their employer's role. An example of the former might be a person with a Facebook account having their attributes sold to a third-party advertiser, while an example of the latter would be an employee whose employer sends their personal information to a third-party 401k administrator. The CCPA only covers the former, while the wording of S120 includes both situations. Notably, both pieces of legislation exempt an employer holding the data of its employees from their requirements.

In the areas of both the private right of action and the types of individual-business relationships in scope, S120 is more expansive and aligned in the interests of individuals at the expense of businesses. The distinctions that S120 highlights are critical to consider for comprehensive data privacy legislation to understand the balance that will result between consumers and firms.

Regulatory Rules Changes

The final category of recent efforts affecting the treatment of financial data stems from the executive, rather than legislative, branch of state governments: changes in regulatory rules by state agencies. While largely more limited in scope than legislative changes, due to the nature of the separation of powers in US state governments, they are nonetheless important and, in some cases, have been finalized and implemented far more quickly.

Regulatory changes are particularly relevant for financial data privacy, as compared to consumer data privacy more broadly, because regulators in many states and at the federal level have possessed some authority over the protection of financial data for a long time. Thus, many bodies are able to accomplish the changes they would like for financial data under existing powers and regulatory structures rather than wading through the legislative process. That is not to say that legislative changes are unimportant for financial data (quite the opposite, as we have seen), but that regulatory rule changes can generally have greater impact on financial data at this point than on consumer data broadly.

New York Department of Financial Services 23 NYCRR 500 (DFS 500)

DFS 500 was adopted in February 2017, taking effect in March 2019, by the state-level regulatory body for financial institutions in New York. Like the CPCDPA, DFS 500 was focused primarily on cybersecurity and data storage practices rather than on data privacy.[67] Given that it was issued by DFS, the rules only applied to financial institutions operating in the state of New

[66] Stone Creem, An Act Relative to Consumer Data Privacy.
[67] Brumfield, "11 New State Privacy and Security Laws Explained: Is Your Business Ready?"

York, though the scope of data was unlimited within those firms.[68] The overarching goal of the rules was to ensure that financial institutions meet a certain set of minimum cybersecurity requirements for their data, given the importance of the data that they collect and utilize.

DFS 500 places several prescriptive requirements on regulated entities under the heading of establishing a comprehensive cybersecurity program at each firm. Companies must designate a Chief Information Security Officer (CISO), report data breaches to the firm's board of directors, and run penetration testing on their systems.[69] In addition, companies are required to design policies to limit data access within the organization to only those who need it for commercial purposes and must use multifactor authentication for external access to the internal network.[70] Finally, companies must establish written policies for data security in their interactions with third parties, including requirements that the third parties must meet in order to be eligible to do business with the firm. While the stated goal of DFS 500 is to "not be[] overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances,"[71] the net result is a mostly formulaic list of requirements that financial firms must meet to continue operating in New York.

Given its focus on the security aspect of data, DFS 500 is most similar to the CPCDPA. However, there are three key distinctions that constitute critically important decisions by its drafters and have a material influence on the regulation's impact.

First, DFS 500 is significantly more prescriptive than the CPCDPA, which, in turn, is more prescriptive on security issues than other legislation such as the CCPA. The resulting tradeoff from being more prescriptive is between ensuring compliance with what regulators believe to be the optimal course of action presently and maintaining flexibility to adapt as technologies, strategies, and risks change in the future. All else being equal, DFS 500 would provide less flexibility to the firms that it applies to than would CPCDPA. However, this concern is affected by the difference between the CPCDPA as legislation and DFS 500 as regulatory rules/guidance. Because DFS 500 originates from a regulatory agency within the Executive Branch, it is likely far easier and more timely to make adjustments as concerns evolve within the industry than it would be to amend the law through the legislature. For that reason, the prescriptive nature of DFS 500, as compared to other data privacy efforts, seems more reasonable as flexibility is less of a concern.

Second, DFS 500, unlike other legislation, is specific to the financial industry as it originated from New York's financial regulatory agency. In addition to allowing the rules to be more specific to the concerns and needs of the financial industry in particular, narrowing the scope of applicability to financial firms further enhances the likelihood that the rules will be sufficiently flexible to adapt to new threats moving forward. Instead of having to draft updated regulations with all possible businesses and consumer types in mind, DFS will only need to consider the interests of the financial industry and financial consumers, which will likely accelerate and simplify the process and allow for deeper and more nuanced collaboration between firms, relevant individuals, and the regulatory agency. While restricting the scope of the

[68] New York State Department of Financial Services, "23 NYCRR 500: Cybersecurity Requirements for Financial Services Companies."
[69] Brumfield, "11 New State Privacy and Security Laws Explained: Is Your Business Ready?"
[70] New York State Department of Financial Services, "23 NYCRR 500: Cybersecurity Requirements for Financial Services Companies."
[71] New York State Department of Financial Services.

rules to the financial industry obviously diminishes their overall impact, it allows far greater flexibility and specificity in tackling the issues most relevant to financial firms.

Lastly, DFS 500 considers all non-public information to be relevant under its rules.[72] Thus, almost all data within a financial firm is subject to these regulatory requirements, which is significantly more expansive than the PII threshold of the CPCDPA. In particular, it includes information about individuals that would not, by itself, be identifying, and information related to the business's operations that is unrelated to individuals that would not be covered by other pieces of legislation. This difference is driven by the goal of DFS 500 to implement an enhanced cybersecurity posture at New York financial institutions, as opposed to that of the CCPA, CPCDPA, and others like them to protect consumers. In short, consumer protection is a side effect of DFS 500 rather than its purpose.

Ultimately, DFS 500 presents interesting questions that must be considered for data privacy and security-related regulation, including whether it is optimal to utilize the legislative or executive branches of government, how tailored an effort should be to a specific industry, and what the underlying goal is for the effort and how that affects its scope.

Summary of Recent Financial Data Privacy Efforts

In response to increased public awareness and pressure about consumer data privacy and security, state governments across the US have been pursuing the implementation of new regulatory changes and legislation that alters how businesses and consumers interact, what rights consumers have with respect to their data, and what requirements businesses must meet to continue operations. Such states are, to quote Justice Brandeis, taking advantage of "one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country."[73] In doing so, these states have made a plethora of unique decisions about the implementation method, scope, and content of new rights and requirements that can serve as a useful window for analyzing disparate impacts on consumers and businesses and determining more optimal solutions moving forward.

Regarding the appropriate implementation method, the two options available for policymakers at a particular level of government are new legislation and changes to regulatory rules. New legislation has the advantage of allowing for more sweeping change to occur, particularly in jurisdictions that do not currently have significant regulatory structures in place, while regulatory rule changes can occur more quickly, can adapt more readily over time, and, depending on the specific agencies involved, can be more finely tuned to relevant industries.

Decisions around scope fall into three categories: data, business type/industry, and consumer. First, policymakers must determine what types of data are considered covered by the regulation, and this can have a significant impact on both the protections offered to consumers and the compliance costs imposed on businesses. The appropriate resolution of this tradeoff may also depend on the overarching goal of the regulation as certain types of data will be more relevant for privacy considerations over security concerns, or vice versa.

Second, two themes have emerged within consumer data privacy and security regulatory efforts regarding the businesses that are considered in scope: the size and the industry. Some efforts have excluded firms below a certain size (either in terms of customer base or revenue in

[72] New York State Department of Financial Services.
[73] Louis Brandeis, New State Ice Co. v. Liebmann (US Supreme Court March 21, 1932).

most cases) to avoid imposing unbearable costs on small businesses. This decision comes with the inherent tradeoff that a consumer's PII is not significantly less dangerous in the possession of a small company than in that of a large company. Furthermore, some regulations have been applied only to specific industries, while others apply broadly. While obviously less impactful, regulations that focus on an industry allow for more nuanced and flexible rules to be drafted, such as rules that have applied specifically to financial firms. Finally, policymakers must decide the scope of who qualifies as a consumer. While perhaps the most "natural" definition consists of individuals unaffiliated with a business consuming or purchasing that business's services or goods, some legislation has taken a more expansive view to include employees of other companies with which a firm might engage. While most regulation has avoided tackling concerns around data that a business has on its employees, there are legitimate questions to be asked about whether this category of individuals should also be included in data privacy efforts.

The last (and perhaps largest) set of decisions for policymakers concerns the content of the regulation, and there are four main elements that must be determined. First, existing regulatory efforts have tended to focus primarily on either privacy or security. While some have attempted to include both, one of the two foci has tended to dominate the purpose of the effort, with the other providing support to this primary aim. Second, the elements of data privacy and security efforts can be broadly sorted into two categories: consumer rights and business requirements. The balance between the two, as well as electing whether a right or a requirement is likely to be more effective in reaching a particular goal, is a critical task for policymakers to achieve the best outcomes for consumers, businesses, and the government alike. Third, concerning consumer rights, policymakers must decide how expansive these rights should be in changing the status quo balance of power. In general, increasing consumer rights will come at a cost for business, so this tradeoff must be managed to optimize overall welfare. Fourth, with regard to business requirements, the level of prescription of the regulatory effort must be decided involving the tradeoff between ensuring compliance with the goals of lawmakers and regulators presently and maintaining adaptability moving forward as risks, technologies, and best practices evolve.

Category	**Key Decision**	**Options**
Implementation Structure	• What policy mechanism should be used to generate change?	• Legislation (ex. CCPA) • Regulatory rules (ex. DFS 500)
	• Should the regulation be rules-based or principles-based?	• Rules-based (ex. CCPA) • Principles-based (ex. GDPR)[74]
Scope	• What data is relevant to regulate?	• Only traditionally defined PII (ex. CPCDPA) • All identifiable information (ex. CCPA) • All non-public information (ex. DFS 500)

[74] UK Information Commissioner's Office, "Guide to the General Data Protection Regulation (GDPR): The Principles," accessed January 20, 2020, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/.

	• What business types or industries are included?	• Only financial firms (ex. DFS 500) • Only companies of a given size (ex. CCPA) • All businesses (ex. NYPA)
	• Who is a consumer?	• An individual utilizing a firm's commercial activities (ex. CCPA) • Another firm's employees (ex. S120) • A firm's employees
Content	• Should privacy or security be the focus?	• Privacy (ex. CCPA) • Security (ex. CPCDPA)
	• What's the appropriate balance of consumer rights and business responsibilities?	• Focus on consumer rights (ex. NYPA) • Balance between both (ex. CCPA) • Focus on business responsibilities (ex. DFS 500)
	• How expansive should consumer data rights be?	• Focus on consumer empowerment (ex. NYPA) • Expand rights comparatively incrementally (ex. CCPA)
	• How prescriptive should business data requirements be?	• Stipulate explicit requirements where possible (ex. DFS 500) • Focus on high-level guidelines (ex. CPCDPA)

When designing consumer data privacy and security legislation, policymakers should make these decisions carefully while weighing the tradeoffs involved and understanding the interrelation of many of these elements. In analyzing the impact of existing financial data legislation and regulatory rules, as well as determining the optimal policy decisions for financial data regulation, we will consider these decisions to be the building blocks from which actual and expected outcomes are derived.

Resulting Effects of Changes to Financial Data Regulation

Prior to examining what form and function optimal financial data privacy and security regulations might take, it's critical to more concretely understand the impacts that have been and will likely be felt in the financial industry from previous changes to these rules. While the prior section dealt primarily with the theoretical nature and content of recent legislation, bills, and regulatory rules, we must also examine the realized consequences, both intentional and accidental, for relevant stakeholders to understand whether particular policymaking decisions appear appropriate in retrospect and to determine areas for iterative improvement.

Rather than articulate the effects of individual pieces of legislation, a thematic examination by stakeholder is more relevant to draw out important conclusions for future policymakers. In particular, financial data regulatory efforts tend to inherently generate tradeoffs between businesses and consumers, and the positive balance in these tradeoffs is critical to

ensure that the normative goals of policymakers and society more broadly are being met as well as possible. However, financial data regulations also generate significant externalities regarding innovation that impact the government and society, and it's important to understand which measures are creating positive externalities to be maximized and which are associated with negative externalities to be avoided.

We will examine the impacts on businesses, consumers, and innovation in turn while drawing out areas where significant gains for one constituency appear to come at relatively minor cost for another, representing a net benefit for society, as well as segments where the imposed costs are material for a stakeholder with smaller commensurate advantages. It's critical to note that classification into either category is not necessarily indicative of whether policymakers should pursue a particular measure regarding financial data regulation, as such a determination can only be made in line with the specific democratically informed goals of the jurisdiction considering the action. However, a clear understanding of the practical impacts on relevant constituencies imposed by these efforts in financial data regulation should nevertheless serve as a key input into the decisions of policymakers, if only to ensure comfort on their part with the tradeoffs being imposed on society.

Importantly, we will focus in this analysis on impacts from legislation and regulation in the context of the standard definition of financial data outlined previously in this paper. Thus, while certain efforts may have a very broad scope, we will only reference the impacts that those rules have on the treatment of financial data. Consistent with our definition, this will include both traditional financial businesses and non-financial corporations that are possessing or processing financial data. For the purpose of completeness regarding the financial industry, we will also highlight select cases where non-financial data at financial firms is impacted by changes in laws or regulations.

Impacts on Businesses

Companies are arguably the stakeholder that is most directly impacted by financial data regulations, as they are the entities onto which policymakers impose requirements and against which consumers will pursue their newfound rights. Given this dynamic, one would intuitively expect that businesses would have the highest costs to bear and the smallest amount to gain from financial data regulations, and, to a certain extent, this logic is borne out in reality. However, there are interesting effects of these new regulations across industries and when considering business-to-business relationships that may, over the long term, create boons for creativity and stability that ultimately serve firms well.

Additionality of Requirements

While the business requirements and consumer rights included in the most recent round of financial data legislation and regulatory rules may be significant in breadth, it's critical to remember that they do not exist in a vacuum devoid of prior attempts at regulation. Particularly in the financial industry, the landscape contains a plethora of rules and laws that already govern how firms procure, process, and handle their data, such as the GLBA, FCRA, and others.

Because of the pre-existing foundation of data regulations for financial businesses, the incremental burden from laws like the CCPA is relatively small compared to that for companies like tech firms that are starting from a zero-regulation baseline. For data within financial firms

that is covered under a prior regulation such as the GLBA, the CCPA contains an explicit carveout that excludes this data from the regulation in order to ensure that no conflicts exist between the CCPA and federal legislation. Thus, it is only data not in scope for existing regulations at financial companies that is subject to the CCPA and similar laws.

In order to ensure compliance with the CCPA on the limited dataset for which it is relevant, financial firms are primarily pursuing the complementary solutions of building out compliance functions and creating or purchasing new technology tools.[75] Due to the nature of the financial industry, many firms have elected to rely on compliance personnel who are already on staff to determine the path forward on regulatory implementation, while others have turned to external consultancies to handle the planning, recordkeeping, and systems work associated with the transition.[76]

After preparation and documentation, the biggest technological hurdle for financial firms has been data management and tracking in order to comply with the new consumer rights within the CCPA for data access, portability, and deletion. Specifically, financial firms need to track identifiable information within their systems, regardless of the complexity or age of their databases and processes. Once the firms know where their consumer data is, they must be able to extract it in a consumer-readable format, serve it to consumers upon request, and, most complicated from a technical perspective, delete the data, subject to the legality of doing so under other regulations.[77] Both of these solutions impose monetary costs on a business, with the majority of outlays coming at the outset for planning and system installation but with continuous upkeep and, if purchasing third-party software, subscription costs indefinitely. Furthermore, businesses will need to devote resources to training the appropriate employees to use the systems and respond to customer requests in the manner mandated by the CCPA. Based on an estimate completed by Berkeley Economic Advising and Research, the average firm will incur an annual cost of ~$10k to fulfill these obligations under the CCPA, though this estimate is not industry- or size-specific.[78] For companies that must purchase a third-party solution for data management, it is likely that the subscription costs charged by the third party will exceed this expected cost.

For non-financial companies that process financial data, the costs of compliance are affected by two incremental factors that have uncertain effects. Unlike financial firms, these companies are less likely to have significant data infrastructure in place to track and categorize financial data as they were not previously subject to data privacy regulations such as the GLBA. Thus, it is possible that compliance costs for operational and technological upgrades will be higher as there will be less of a foundation on which to build. However, this factor is countered to some degree by the relative dearth of regulatory complexity for non-financial firms. Such firms only need to be concerned about complying with the CCPA or other similar legislation, while financial firms must contend with multiple pre-existing federal laws that complicate their

[75] Scott Woepke, "California Consumer Protection Act (CCPA) and Its Impact for Financial Services Companies. Are You Prepared?," August 12, 2019, https://www.acxiom.com/blog/ccpa-and-its-impact-for-financial-services-companies/.
[76] Boston Consulting Group, "Readiness for Data Privacy: California Consumer Privacy Act & Related Regulations."
[77] Mark Davies, "CCPA Is Coming January 1. Is Your Bank Ready?," May 15, 2019, https://digitally.cognizant.com/ccpa-coming-is-your-bank-ready-codex4675/.
[78] Berkeley Economic Advising and Research, LLC, "Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations," August 2019, 24–27, http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.

compliance efforts. Depending on how a financial business's systems are structured, it might end up having to run two parallel data compliance structures, one for the GLBA and one for the CCPA, whereas non-financial firms will only need one set of processes.[79] For these reasons, the relative difference in costs between financial and non-financial companies is difficult to fully determine and will likely vary on a case-by-case basis.

Altering Business-to-Business (B2B) Relationships

A significant focus of recent legislative efforts impacting financial data is on the distribution of consumer data to third parties, given the complexities and conflicts of interest that arise in such relationships regarding the protection of consumer privacy. The goal of legislation like the CCPA or the CPCDPA on the topic of third parties is twofold: to ensure that consumers are aware their data is being distributed or sold to third parties, and to make the originally-collecting business responsible in some respects for the behavior of the third parties to which they give consumer data.

Regarding the former, firms are providing notifications to consumers when data is collected about them to inform the consumers about companies to which the data will be transmitted and allowing the ability to opt out as required by the CCPA. After the CCPA went into effect, many websites began requiring consumers to either accept their terms and conditions when first visiting the site or select the "Do Not Sell My Personal Information" button to opt out of third-party data distribution.[80] As of now, it is unclear whether many individuals are actually opting out of this sale and what effect those opt-outs are having on the underlying businesses. It is certainly possible that, if consumers begin exercising this right frequently, certain business models that rely heavily on the transmission of data to third parties to provide services or generate revenue may have to be adjusted or become entirely unsustainable.

In response to such an occurrence, certain businesses could be forced to shut down. Another interesting possibility could be that mergers between tech firms become more attractive in order to remove the "third party" nature of the relationship. Put another way, firms could eliminate the risk that consumers hinder their business model by opting out of third-party data sharing by simply acquiring those third parties to bring the associated functions in-house, and consumers are not able under the current version of the CCPA to opt out of specific internal data uses as long as they are disclosed.

With respect to the latter part of the legislative goal for third-party relationships of shifting more responsibility to the originally collecting business, recent efforts like the CPCDPA have focused on ensuring that the originally collecting firm is responsible for the information security posture of companies to which they sell consumer data. This has led many businesses to conduct information security reviews of their partner firms on a regular basis in order to fulfill the regulatory requirements. For financial firms, this topic is less impactful as such practices are already commonplace due to prior regulatory efforts such as the GLBA.[81] However, for non-

[79] Anna Fridman, "What Financial Institutions Need to Know About the CCPA," October 4, 2019, https://www.law.com/therecorder/2019/10/04/what-financial-institutions-need-to-know-about-the-ccpa/?slreturn=20200004211855.
[80] Los Angeles Times Staff, "Seeing Those Opt-Out Messages About Your Personal Information on Websites? Thank California's New Privacy Law," *Los Angeles Times*, January 2, 2020, https://www.latimes.com/california/story/2020-01-02/california-consumer-privacy-act-do-not-sell-my-info.
[81] NuHarbor Security, "Third-Party Security in the Financial Services Industry [Infographic]," June 28, 2016, https://www.nuharborsecurity.com/third-party-security-in-financial-services-infographic/.

financial firms that process financial data, this requirement could be more onerous due to its novelty, forcing such firms to quickly become more closely intertwined in their business practices with third parties. Overall, the expected impact of this requirement is more hand-in-glove coordination between businesses and their third parties, with the occasional uptick in acquisition activity to eliminate risks associated with failing to adequately oversee or have a material say in third-party risk standards.

Complying Across Jurisdictions

A key issue for both domestic and multinational firms is understanding and implementing the best methodology to comply with requirements across multiple jurisdictions. As we have previously detailed, there are pre-existing legal requirements for financial firms at the US federal level, and many of these recent data privacy regulatory efforts stem from state governments, of which approximately 25 have passed or are currently considering some form of updated data legislation.[82] This is not to even mention the regulations in other countries and jurisdictions around the world, with GDPR from the European Union being the most notable.[83]

Within this web of regulations across boundaries, it can be very difficult for even the largest financial firms to comply with all the restrictions and requirements. Firms must devote significant resources to achieving and maintaining compliance, as previously discussed, and a lack of clarity within regulations is amplified when that confusion extends across state or national boundaries. For instance, there remains confusion for US financial institutions regarding which ones need to comply with GDPR,[84] and similar questions are being asked for small financial and fintech firms as they grow and expand in relation to the CCPA.[85]

While most states have followed the example of the CCPA when passing their own pieces of legislation, given California's relative importance in the American economy and its first-mover advantage, not all have matched CCPA requirements line for line, as we saw during the review of recent state-level regulatory efforts. For that reason, industry groups have strongly lobbied for Congress to pass federal consumer data privacy legislation that updates the existing federal standards, such as the GLBA and FCRA, and preempts the state efforts to regulate data privacy at that level of government, with concerns expressed that "inconsistent and duplicative requirements … could potentially disrupt financial transactions and the financial system."[86]

Multinational firms are likely able to absorb the costs of multi-faceted regulatory compliance. In general, these companies have elected to comply with the most stringent portions of each jurisdiction's mandates across the board to eliminate the risk of accidental non-compliance. However, such a requirement is likely to disproportionately impact nascent firms,

[82] Boston Consulting Group, "Readiness for Data Privacy: California Consumer Privacy Act & Related Regulations."
[83] European Union, "What Is GDPR, the EU's New Data Protection Law?," accessed January 4, 2020, https://gdpr.eu/what-is-gdpr/.
[84] Penny Crosman, "Large U.S. Banks Scramble to Meet EU Data Privacy Rules," American Banker, April 16, 2018, https://www.americanbanker.com/news/large-us-banks-scramble-to-meet-eu-data-privacy-rules.
[85] Trulioo, "CCPA Compliance - A Guide for Fintech," August 14, 2019, https://www.trulioo.com/blog/ccpa-compliance/.
[86] James Ballentine, "American Bankers Association Response to Data Privacy Inquiry from the Senate Committee on Banking, Housing, and Urban Affairs," March 15, 2019, https://www.banking.senate.gov/imo/media/doc/Data%20Submission_American%20Bankers%20Association%20(ABA)1.pdf.

such as fintech startups, that seek to grow across jurisdictions but do not have the workforce or fiscal resources to be consistently updating their systems and processes to comply with the latest financial data privacy regulations. One possible solution is to anticipate future growth and build systems from the start to comply with the strongest requirements of all possible jurisdictions, and some technology providers are developing plug-and-play white-label solutions using this approach.[87] That being said, it is likely that some smaller companies will simply be unable to shoulder the burden of the web of jurisdictional regulations but would be able to comply with a single federal (or even multilateral) standard.

Liability for Data Misuse and Breaches

Under the pre-existing data privacy regime of the GLBA, financial institutions could be held liable via regulatory fines for data breaches due to "allegedly insufficient data security policies."[88] Under regulations like the CCPA, the liability scheme is materially similar, with the California Attorney General able to enforce fines on companies that violate the requirements.[89] Thus, the impact on financial firms for their own actions regarding consumer data is minimal as the liability only increases to include data not covered by the GLBA.

For non-financial firms handling financial data, the change in liability is more significant as there is no current regulatory liability for these companies. The CCPA fundamentally alters the liability framework for non-financial firms in their internal handling of data.

However, the most significant change in liability driven by the CCPA and similar legislation stems from the inclusion of the actions of third parties in the scope of a firm's liability. While there is some ambiguity in the law, a company's act of sharing consumer data with a third party could make the company liable for any misuse of data by the third party.[90] This is massive expansion of liability for both financial and non-financial firms that could significantly alter how these firms consider sharing financial data with other companies in order to optimize their business models. Suddenly, there is a significantly larger incentive for companies to perform all possible functions in-house rather than farming them out to third parties in a manner that might actually be more optimal from the perspective of leveraging the competitive advantages of different firms.

At a minimum, this change will likely result in greater cooperation between partner firms. The CCPA stipulates that companies can put in place specific legal agreements to remove the expansion of this liability, but those agreements place restrictions on the actions of the third party.[91] It will also increase incentives for financial firms to acquire their third parties in order to take greater control over data privacy and security in the operation, given that the firms will be assuming liability anyway under the CCPA. Overall, the inclusion of liability for third-party actions, as with other changes previously discussed, is likely to increase the interconnectedness of firms with their third-party partners.

---

[87] Boldon James, "CCPA - The New Law Delivering GDPR-Style Privacy to California."
[88] Bernard J. Kornberg, "Banks Face Unique Liability for Data Breaches Under the Gramm-Leach-Bliley Act," Severson & Werson, March 7, 2018, https://www.severson.com/banks-face-unique-liability-for-data-breaches-under-the-gramm-leach-bliley-act/.
[89] Stephens, "California Consumer Privacy Act."
[90] David Navetta et al., "CCPA FAQs Part 3: Litigation, Regulatory Actions and Liability," Cooley Cyber/Data/Privacy Insights, October 1, 2019, https://cdp.cooley.com/ccpa-faqs-part-3-litigation-regulatory-actions-and-liability/.
[91] Navetta et al.

Regulatory Risk in Mergers and Acquisitions

The final impact on businesses of recent changes to financial data regulations is a result of the increase in liability for firms as previously described but relates to potential mergers or acquisitions. Companies utilizing financial data have increased regulatory risk due to the CCPA, CPCDPA, and similar legislation, and this liability does not disappear if a company is acquired by another firm. Rather, that liability, similar to other types of liability, travels to the acquiring company upon completion of the acquisition.[92]

Thus, for any company acquiring another firm that processes financial data, there is incremental risk that must be considered and accounted for. Furthermore, particularly in the early years of compliance with new regulations, the processes and systems within target firms to handle data privacy and security will need to be top-notch to convince potential acquirers that they are not accepting unnecessary liabilities. This will likely front-load compliance costs on firms that would otherwise be attractive acquisition targets in an attempt to remain so for potential strategic and private equity acquirers. In a similar vein, there will be acquirers who suffer from unexpected liabilities due to CCPA breaches within target firms that were not recognized at the time of purchase.

Impacts on Consumers

The intended beneficiaries of these legislative and regulatory efforts around data privacy and security are American consumers. Primarily, the benefits provided to consumers come in the form of new rights regarding the status and use of their personal data, both financial and otherwise, with these rights placing related requirements of various degrees on businesses. Some of these rights are expansive and will fundamentally alter the data relationship between consumers and businesses, while others are less impactful, either by design or due to the conflicting nature of some business requirements across different pieces of legislation. We will focus on the three most important rights afforded to consumers by the recent data privacy efforts and discuss their impacts, particularly where there are disparities between the intended and actual results due to unforeseen factors.

Rights to Know and Access

At its most basic, a key concern for privacy advocates prior to recent legislative efforts was the lack of transparency in data collection by businesses. While there were some companies that told consumers what types of data were being collected on them, such disclosures were often significantly limited in scope or done on a voluntary basis by forward-thinking businesses with little to directly lose from doing so.

However, under the CCPA and similar legislation, firms must disclose to their customers what types of data are being collected, what uses that data is being put to, and to whom that data

[92] Alex Barthet, "Mergers and Acquisitions and Successor Liabilities: The Deal Is Done, but the Liability Lives On," The Lien Zone, March 31, 2010, https://www.thelienzone.com/mergers-and-acquisitions-and-successor-liabilities-the-deal-is-done-but-the-liability-lives-on/.

might be sold or disclosed, which, collectively, are broadly referred to as the "Right to Know."[93] Furthermore, the CCPA requires that companies provide consumers with the ability to know exactly what data the firm maintains on them within the categories of data that the company collects, which is referred to as the "Right of Access."[94] Together, these two newfound consumer rights aim to vastly increase transparency for consumers when making decisions about whether to engage with a particular business, both at the outset and during the course of the commercial relationship. Simply, the goal is to aid consumers in making informed, rational choices in their consumption of goods and services that involve the collection or maintenance of personal data.

Regarding financial data, these rights will result in some consumers being surprised at the types of data currently being collected about them and the uses to which the data is being put. Particularly relating to relationships with third parties, there will be increased awareness of the linkages that exist in seemingly simple business services and the types of commercial functions for which consumer financial data is being leveraged that are currently abstracted away from individuals.

For instance, several B2B firms exist to provide financial data and account aggregation services to fintech companies that service consumers. Specifically, these firms build plug-and-play technology solutions for fintech startups to source data from consumer financial accounts to enable the provision of services. While the consumer is largely aware of the immediate service being provided by the fintech startup, they may be less cognizant of the fact that the actual sourcing of their financial data to enable the service is being done by a third party. Furthermore, they are likely unaware that the third party retains their current financial account information and access to future updates largely unrelated to the initial provision of services by the fintech startup, and that these data aggregation firms then perform analytical services using consumer data to generate insights that are then sold back to fintech startups to better target other customers and understand consumer behavior.[95]

For B2B companies that operate "behind the scenes" from consumer-facing applications or businesses, the impacts of the Rights to Know and Access are going to necessitate more significant changes in consumer messaging, technological capabilities, and strategic approach. This is driven by the simple reality that consumers are likely to have been less aware of their presence and purpose previously, which will necessitate greater efforts by these firms to fully disclose their data collection and usage practices and justify their business models. Furthermore, the process of providing data access for consumers will possibly be more convoluted given the B2B operational nature of these businesses, despite their possession of consumer data. For B2B firms that handle consumer financial data, the Rights to Know and Access will present a unique challenge of adding consumers as a direct stakeholder and judge regarding their business practices and requirements.

On the Right to Access, it is important to note, as has been previously discussed, that the recent legislative efforts contain carveouts for data whose access is already covered by pre-existing federal legislation.[96] This is particularly relevant for credit data under the FCRA, where

---

[93] Jones Day, "California Consumer Privacy Act Guide," 2018, 7, https://www.jonesday.com/-/media/files/publications/1/01/california-consumer-privacy-act-guide/files/california-consumer-privacy-act-guide-gdpr-handout/fileattachment/california-consumer-privacy-act-guide-handout.pdf.

[94] Boston Consulting Group, "Readiness for Data Privacy: California Consumer Privacy Act & Related Regulations," 2.

[95] Plaid, "Company Overview," accessed January 19, 2020, https://plaid.com/company/.

[96] Boston Consulting Group, "Readiness for Data Privacy: California Consumer Privacy Act & Related Regulations," 6.

annual disclosure opportunities for consumers are already required by law. For this data, the Right to Access in the CCPA and similar pieces of legislation will not change the underlying rights of consumers to access it, resulting in more limited access for consumers to data covered under the FCRA than for other types of financial data. This sort of delineation between segments of financial data is driven not by fundamental differences in the data, but by the reality of split levels of government in the US. This discrepancy is something that future federal data privacy legislation should aim to rectify and standardize.

Right to Deletion

Under recent legislative efforts such as the CCPA, consumers gain the Right to Deletion, which requires a firm to delete all data associated with the requesting consumer so long as the data is no longer essential to the completion of a pre-existing transaction or contract with the consumer.[97] Ostensibly, this right allows consumers to force a company to forget what the firm knows about them should the consumer no longer wish to be a customer of that company, which grants the consumer more direct control over their data, particularly how long it remains in the hands of firms. For instance, if a company commences using consumer data for a new business line in which a customer doesn't wish to be involved, the customer now has the right to actively remove their data from the firm's purview, whereas previously, customers likely had no recourse when the company moved to leverage their data for purposes not originally specified.[98] In short, the goal of the Right to Deletion is to complete the consumer's control over the full lifecycle of their data from the time they elect to give it to a company to the moment they decide that the firm should no longer be in possession of it.

However, for financial data, there is a key exception to the Right to Deletion related to regulatory overlap. As in other instances, requirements of pre-existing federal legislation regarding data retention would conflict with the Right to Deletion under the CCPA and similar legislation if it were not for specific carveouts in these recent legislative efforts for other legal requirements.[99] For instance, the BSA requires that financial institutions maintain certain transaction records for at least five years for the prevention of money laundering.[100] In such a case, there is a direct conflict not only between these two pieces of legislation but more broadly between two legitimate governmental purposes, namely, the anti-money laundering in the BSA and consumer protection in the CCPA. Such tradeoffs are more pronounced with financial data than with other types of data because of the significant potential of financial data to be utilized both harmfully, such as when companies unfairly leverage consumer data to their advantage, and to prevent or correct harm, including when authorities identify and intervene in money laundering. This double-edged nature of financial data will necessitate regulators and legislators to take great care when deciding what situations are optimal to enhance consumer control through the Right of Deletion and what areas are best left without this capability.

It is also important to note that there is some ambiguity in the CCPA and other recent efforts regarding the Right of Deletion in relation to third-party data transfer. Stringent consumer

[97] Jones Day, "California Consumer Privacy Act Guide," 9.
[98] Yoni Bard and Scott Bloomberg, "United States: CCPA: The (Qualified) Right to Deletion," July 30, 2019, http://www.mondaq.com/unitedstates/x/831300/Data+Protection+Privacy/CCPA+The+Qualified+Right+To+Deletion.
[99] Bard and Bloomberg.
[100] Federal Financial Institutions Examination Council, "BSA/AML Manual: Appendix P," accessed January 19, 2020, https://bsaaml.ffiec.gov/manual/Appendices/16.

advocates would like the company that originally gave consumer data to a third party to be responsible for ensuring that the third party deletes the data upon a consumer's request, creating a chain of deletion responsibilities across firms. However, many companies are interpreting the CCPA to require only the notification of consumers that their data has been transmitted to a third party and the notification of third parties that the customer has requested the deletion of their data.[101] It would then, depending on the specific legal interpretation, be the responsibility of the third party to delete the data, or the responsibility of the consumer to follow up with the third party directly to submit a deletion request. From a consumer rights perspective, it is obviously more advantageous for regulators to enforce the former approach where companies are responsible for the daisy chain for deletion because it reduces the burden on consumers. However, there are others who argue that placing responsibility on one corporation to enforce specific actions in another would be a step too far for data privacy efforts, particularly regarding financial data where a complex web of requirements exists. It is likely that this dispute will be adjudicated as enforcement bodies begin to take actions against firms allegedly in violation of these new legislative requirements.

Rights to Opt Out and Non-Discrimination

The final set of critical consumer rights provided by recent legislative efforts is comprised of the Rights to Opt Out and Non-Discrimination. The Right to Opt Out gives the customer the right to opt out of the sale of personal data to third parties, though, notably, it does not give customers the right to institute a blanket prohibition on data distribution to third parties.[102] Specifically, data that is transferred between companies pursuant to a service contract that meets certain guidelines does not count as data sold and is, thus, not subject to the Right to Opt Out.[103]

The Right to Non-Discrimination is tied closely to the Right to Opt Out as it provides that consumers cannot be excluded from service provision or charged different prices for similar services because they exercise their privacy rights.[104] The only situation when companies can charge different prices to consumers who exercise their privacy rights disparately is when the price differential is directly tied to a difference in the value of the data that the consumer did or did not elect to provide or enable the company to utilize internally.[105]

The impact on businesses of these rights is likely to be a decrease in profitability for certain activities that rely on the sale of financial data to third parties. Under the CCPA, a consumer now has the right to opt out of that sale of data while maintaining access to services that the company provides, which will have a negative effect on profits.

For consumers, these rights increase their ability to control the use of their data by the companies to which they give it and protect them from unfair business practices associated with exercising their privacy rights, which is a significant boon for consumers. However, there may be knock-on effects for consumers in terms of paying higher prices for or losing access to financial services such as credit if opt-out rights are exercised without an understanding of the

[101] Jones Day, "California Consumer Privacy Act Guide," 9.
[102] Jones Day, 10–11.
[103] Clarip, "CCPA Right to Opt Out for the Sale of Personal Information," accessed January 19, 2020, https://www.clarip.com/data-privacy/ca-consumer-privacy-act-right-opt-out/.
[104] Boston Consulting Group, "Readiness for Data Privacy: California Consumer Privacy Act & Related Regulations," 2.
[105] Jones Day, "California Consumer Privacy Act Guide," 12.

tradeoffs. For financial credit providers, having access to more information is likely, though not guaranteed, to result in being able to provide a lower price for credit access for a particular customer. Thus, if a customer exercises the Right to Opt Out or Right to Deletion when trying to access services such as these, it is likely that the customer will receive a higher price or rate to do so. While this may be an acceptable tradeoff for some consumers, there are concerns about the degree to which consumers will fully understand the implications of their privacy decisions on the economics of their financial transactions. For that reason, it is critical for policymakers to balance the consumer benefit provided by having these data rights and the effects that such rights might have on the ability or willingness of firms to provide financial services to customers at a low price or rate.

Impacts on Innovation

The final area to consider regarding the impact of data privacy legislation as it pertains to financial data does not concern a specific set of stakeholders. Rather, it is critical to understand the impacts of these legislative and regulatory efforts on innovation as it pertains to the development and implementation of new ideas that add value for society more broadly. Perhaps counterintuitively, the impact on innovation of these changes is not necessarily negative in all areas or for all players. Rather, it appears to be of a mixed nature that should be closely examined to determine their overall net impact and, more specifically, their effects on particular types of players within the financial industry.

Consumer Willingness to Share Data

As consumers have become more broadly aware of the negative externalities that widespread data sharing can have, consumer willingness to share data with companies has declined in the past few years.[106] In general, consumers are less willing to part with their data in return for benefits than before, with only 22% of individuals willing to trade "financial information" for a personalized advertising experience, as opposed to 20% for a generic experience.[107] This speaks to both the high value that consumers place on their financial data and the significant mountain that companies must climb to convince customers to part with their financial data by providing significant benefits for doing so. With the introduction of the Right to Opt Out and other privacy rights, as previously described, consumers are likely to become stingier, rather than more freewheeling, with their data.

Now, research shows that there are two primary methods for companies to convince consumers to part with their data. The first is to build trust. Surveys show that the biggest determinant by far of whether a consumer is happy to share data with a firm is whether the consumer trusts the organization.[108] This can also be enhanced by providing increased transparency to consumers about why data is being collected and the associated policies around

[106] Heidi Tolliver-Walker, "Survey: Consumers' Willingness to Give Up Personal Data Is Waning," November 20, 2019, http://whattheythink.com/articles/98437-survey-consumers-willingness-give-personal-data-waning/.
[107] Tolliver-Walker.
[108] Greg Sterling, "Survey: 58% Will Share Personal Data Under the Right Circumstances," June 20, 2018, https://marketingland.com/survey-58-will-share-personal-data-under-the-right-circumstances-242750.

its use.[109] The second method is to provide material increased value to the consumer through the collection of data. The next-most important factors determining the willingness of consumers to submit their personal data to a company pertain to the services to which they will gain access or the increased product quality that they will receive based on the increased level of data disclosure.[110]

However, these methods to entice elevated consumer willingness to part with their financial data – building trust and providing value – create a disparity between different sizes and stages of financial services companies. All else being equal, it is easier for a large, well-established company to have trust and provide immediate value to a consumer than for a nascent fintech startup. For that reason, we would expect that consumer attitudes toward sharing data will disproportionately and negatively impact smaller and lesser-known firms that have less brand equity with consumers or that are still developing their service offerings.

This likely propensity for consumers to be more willing to give their data to large firms will have a negative impact on the innovation that is generated through the creative destruction that startups in the financial industry represent. Given that smaller firms are more productive at generating innovation on a per-employee basis, the net impact of this dichotomy in consumer behavior is likely to be negative on overall innovation, and these legislative efforts exacerbate this difference by enhancing consumer power to withhold data from firms.[111] While this may serve consumers well with regard to their rights, the long-term impact of decreased innovation may be a price too steep to pay.

Industry-Derived Interpretations for Compliance

As with many previous regulatory efforts, leading financial firms are driving the effort to standardize legal interpretations for compliance with new pieces of legislation such as the CCPA. These efforts serve the purpose of raising nuanced issues that only some players may have noticed, involving industry experts, lawyers, and other parties in discussions, and providing enforcement cover for institutions that participate and ultimately implement the recommendations.

However, such efforts tend to be dominated by the largest institutions, as one might expect. This can lead to situations where smaller firms that are covered by the regulation are not materially consulted when designing rules or responses that might disproportionately impact them. Then these smaller companies must decide whether to follow the recommendations of the standardization effort, incurring potentially unfair costs, or expose themselves to increased enforcement risk by implementing solutions and interpretations that are more advantageous to them but are outside of the "norm" established by the industry leaders.

Thus, this regulatory effort will disproportionately impose costs on smaller firms that are likely to be startups innovating in the financial space, which will distract them from their core purpose of creating positive change. For that reason, innovation is likely to be negatively

[109] Robert Williams, "Accenture: More Consumers Willing to Share Data When There's Transparency," October 17, 2019, https://www.marketingdive.com/news/accenture-more-consumers-willing-to-share-data-when-theres-transparency/565195/.
[110] Sterling, "Survey: 58% Will Share Personal Data Under the Right Circumstances."
[111] Anthony Breitzman and Diana Hicks, "An Analysis of Small Business Patents by Industry and Firm Size" (Rowan University, November 2008), iii, https://rdw.rowan.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1011&context=csm_facpub.

impacted due to the desire for industry-wide interpretations to be made in response to these legislative and regulatory efforts.

Enforcement Concerns

One key concern raised by the CCPA and similar pieces of legislation is the nature of the enforcement mechanism utilized. In the case of the CCPA, enforcement powers are placed in the office of the California Attorney General, while for others such as the proposed NYPA, a private right of action expands the enforcement mechanism to include lawsuits from consumers.[112,113] These differing mechanisms introduce two important concerns: inconsistency of enforcement and relevance of enforcement.

Regarding inconsistent enforcement, resting the powers of enforcement in the Attorney General's office as the CCPA does means that violations will be channeled through an organization that must also be concerned with many other tasks and responsibilities. The broad mandate of the Attorney General's office may lead to variations between lenient and strict enforcement as the office provides lesser or greater time and effort to the CCPA specifically. This issue might not result if enforcement powers were given to a regulatory agency with a significantly narrower mandate to tackle data privacy concerns in particular. Inconsistency is important because it generates uncertainty for businesses, which is likely to hamper investment in long-term innovation or improvements.

The relevance of enforcement is also a concern for legislation that includes a private right of action. While this provision significantly increases the power of consumers, it potentially subjects businesses to repetitive or frivolous lawsuits that could take resources and energy away from core business growth and innovation. In particular, the impact of these lawsuits is likely to be more severely felt by smaller businesses like startups, given their relative lack of a cushion to absorb civil suits.

Thus, there are significant concerns associated with the enforcement mechanisms of the CCPA and similar pieces of legislation that they could lead to inconsistent and irrelevant enforcement against companies, resulting in decreased innovation by these firms as they deal with the uncertainty and costs that would result from enforcement. For that reason, regulators must determine a better path forward for enforcement to reduce uncertainty and ensure the appropriate balance between consumer rights and business growth.

Cyber Liability Insurance Policies

As mentioned previously, not all innovation impacts of these regulatory and legislative efforts are negative, and a key bright spot for innovation surrounds cyber liability insurance policies. For several years, the cyber liability insurance industry has been getting bigger due to the increasing number of cyberattacks on companies and the growing importance of data in company operations.[114] With the introduction of the CCPA and other such pieces of legislation, this trend has only accelerated, primarily to handle the liability imposed by the CCPA in case of data misuse or breach. While this might intuitively be viewed as a deterrent to innovation, this

[112] Stephens, "California Consumer Privacy Act."
[113] Lapowsky, "New York's Privacy Bill Is Even Bolder Than California's."
[114] Andrew Granato and Andy Polacek, "The Growth and Challenges of Cyber Insurance," Chicago Fed Letter #426, 2019, https://www.chicagofed.org/publications/chicago-fed-letter/2019/426.

development is actually aiding innovation in the insurance market to develop new types of coverage and standardize insurance offerings across companies and providers.[115] Due to the passage and implementation of these regulations, greater market pressure is being exerted on insurers to provide substantive value through these policies, and more financial firms and startups are gaining cost-effective access to them.

While there is some negative impact on smaller financial businesses because such policies are likely more necessary for these firms than they were prior to the CCPA, overall, the innovation that is occurring in the cyber liability insurance industry is allowing more startups to gain access to this protection, decreasing risk to their core operations from data issues and incentivizing them to implement best practices in order to obtain these policies. Thus, a key positive innovation impact of the CCPA and similar legislation is to spur development and affordability in the cyber liability insurance industry, which increases certainty on the part of businesses when they seek to pursue innovative solutions to financial problems.

Commercial Incentivization of Privacy by Design

The final impact on innovation is also a positive development for long-term, sustainable growth of financial technologies. Specifically, the CCPA and other similar pieces of legislation incentivize firms and technology providers to implement privacy by design in their business strategies, systems, and processes. While this might impose some upfront costs, as previously discussed, it also spurs innovation in thinking about new ways of doing business to ensure that privacy-related issues are prioritized and included from the outset of projects and the development of new businesses. This is leading to fundamentally new ways of doing business in the financial industry, particularly as fintech firms determine how best to adapt to the regulatory environment.

On the technology side, companies are responding to this market opportunity by developing a host of white-label data management solutions to be purchased by firms subject to the CCPA, including financial companies.[116] In the long run, this will result in greater data privacy and security due to the concentration of resources in a smaller number of companies that design these types of systems and lead to market-wide cost savings by lowering the number of misuse or breach incidents. Several technology providers are also working on the problem of data transfer under the CCPA regime and innovating through the use of tokenized data formats to ensure compliance with the regulation while continuing to enable secure data transfer between companies.[117]

Overall, while the CCPA and other similar legislation place incremental requirements on businesses, the market is responding to this challenge by creating space for innovation in data privacy and security systems and business models. Long term, this innovation will lead to societal benefits from a financial industry that is more secure, more technologically advanced, and better at ensuring the privacy of consumer financial data.

[115] Raskin, "Consider Enhancing Cyberliability Insurance Policies to Align with CCPA: Part 1."
[116] Boldon James, "CCPA - The New Law Delivering GDPR-Style Privacy to California."
[117] Noltensmeyer, "CCPA Overview: Understanding Compliance."

Optimal Regulatory Framework for Financial Data Privacy and Security

Throughout this discussion, we have focused on the theoretical scope of financial data and delved into the most relevant legislative and regulatory efforts that impact the treatment of financial data and the balance of power between consumers, businesses, and societal innovation. Having analyzed the realized and anticipated impacts of these policies, we now turn attention to our proposal for the optimal regulatory framework to support the privacy and security of consumer financial data, taking into account lessons from the existing rules and suggesting some additional novel elements.

Our goal is to recommend the best path forward on financial data regulation, focusing on the structure, scope, and content of such an effort. We aim to take a holistic view of financial data, to understand the tradeoffs between certain constituencies implied by policy choices, and, ultimately, to articulate a clear vision for how to reconcile the important nuances in financial data. While there may be short-term costs for some stakeholders associated with our proposal, we believe that our approach is the optimal long-term solution for financial data privacy and security in the US to increase consumer protections, to safeguard sustainable business growth, and to boost innovation in the economy.

Implementation Structure

Before looking at the scope and content of any potential regulatory effort, it's critical to determine the most appropriate structure to achieve lasting efficacy. For our proposal, we will leverage a comparison of the approaches taken by previous policies, namely legislation and regulatory rules, to propose a hybrid approach that involves both legislative bodies and executive agencies. Furthermore, we will look at balancing guiding principles and prescriptive rules in regulatory design to promote the optimal mix of effectiveness and flexibility.

The Power of Federal Legislation

One of the most pressing issues in current US financial data regulations is the convoluted tapestry of existing state and federal legislation and policies. As we have seen, a plethora of regulations from all levels of government apply to different aspects of the financial industry, and these rules can often be at cross purposes or result in murky outcomes. Put simply, this state of affairs is inefficient for businesses and results in, at best, a patchwork of consumer protections.

Therefore, our proposal consists of one comprehensive piece of federal legislation relating to financial data privacy and security regulation, tentatively titled the Comprehensive Consumer Financial Data Act (CCFDA), to replace existing federal policies and override conflicting state legislation. While this approach would require significant work to fully craft the legislation to ensure optimal outcomes and consistency where appropriate with prior structures, it provides two massive benefits that ultimately prove convincing.

First, this approach reduces the significant regulatory burden associated with compliance with various regulatory regimes at different levels of government. Instead of having to determine how all of these policies fit together and needing to comply with multiple jurisdictions, businesses would only need to focus on one piece of legislation for financial data regulation. The decrease in uncertainty and complexity will lead to lower compliance costs and fewer barriers to entry for firms as well as an increased willingness to invest in new and existing business lines.

Second, the CCFDA will eliminate disparities that currently exist in how the same data is treated in disparate contexts or at different types of companies. In the present regulatory framework, pieces of financial data are not handled consistently based on the type of institution holding the data, the source of the data, or the business purpose of the data, despite the fact that, from a consumer's perspective, there is no material difference in the damage the data can do if it is misused or stolen. For example, a Social Security number held by a credit reporting agency is not fundamentally different when it is held by a tech company in terms of its usefulness to a malicious actor, but the regulatory oversight of the number in those two situations is remarkably divergent. Furthermore, the ultimate victims of this divergence are consumers themselves, as bad actors can exploit these differences to target the areas with the weakest protections.

Thus, it benefits all three of our major stakeholder categories – businesses, consumers, and societal innovation – to pursue a comprehensive approach at the federal level to establish one clear set of guidelines and rules for financial data privacy and security.

The Necessity of Regulatory Agencies

While federal legislation is best to produce a comprehensive regulatory framework that can learn from the lessons of prior efforts while superseding them, the implementation, including the creation of highly specific rules, should be the purview of federal regulatory agencies. This reasoning is primarily driven by the need for flexibility and specificity in the application of the new regulatory framework to firms in the industry but is also done partially to maintain some continuity with existing regulations.

Regarding specificity and flexibility, the CCFDA will need to be implemented for many different types of firms, including some non-financial companies, and changed over time as businesses and concerns around their handling of data develop. While it would be technically possible to pass legislative updates every time a change is necessary, such a process would be extremely cumbersome and subject to broader policy gridlock. For that reason, the particulars of implementation, as well as the power to partially alter rules, should be left to regulatory agencies in order to remove impediments to positive innovation in the future.

There is also an argument to be made that the involvement of regulatory agencies is optimal, given their existing expertise in implementing and enforcing the current suite of financial data regulations. Multiple agencies, from the CFPB to the Office of the Comptroller of the Currency (OCC), are part of the regulatory framework at present, and the existing knowledge base and relationships in these agencies should not be discounted.[118,119] The initial implementation and ongoing maintenance of the new framework will be made easier by leveraging the existing agencies, though it should be noted that it would be optimal, at a minimum, to reduce the number of agencies involved in the regulation. Given the focus on consumer financial data of this regulation, it would be logical to pick an agency like the CFPB, which is already focused on consumer financial issues, to spearhead the framework. However, the CCFDA is not necessarily limited to implementation by one agency or another.

[118] US Consumer Financial Protection Bureau, "A Summary of Your Rights Under the Fair Credit Reporting Act."
[119] US Office of the Comptroller of the Currency, "Bank Secrecy Act (BSA)."

Principles and Rules

The final concern regarding the structure of the CCFDA pertains to the balance between principles-based and rules-based regulation. While certain data regulatory efforts like GDPR have adopted principles-based approaches, others like the CCPA have been based on explicit rules included in the legislation.[120,121] In general, principles-based regulations tend to be more resilient over time because the underlying implementation can be more flexible as technologies develop and facts change, while rules-based regulations are more effective in the short term at achieving the specific policy aims of legislators given the explicit nature of requirements.

Since both types have their uses, our approach combines principles and rules in order to realize specific aims while promoting long-term flexibility. Specifically, we advocate for a focus on principles within the text of the CCFDA, such as the inclusion of a Right to Know for consumers, to be discussed in more depth in the Content section, without explicitly detailing how businesses are required to act in order to achieve this consumer right. However, rule-making power would be delegated by the legislation to the appropriate regulatory agencies, given their expertise and ability to be flexible over time, in much the same way that the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 delegated specific rule-making to regulatory agencies, most notably the Federal Reserve, after laying out principles and high-level categories of requirements.[122]

The goal of this approach is to simultaneously establish immutable principles that must be respected and adhered to in the long term to provide increased consumer financial data protections, while enabling high-level adaptation and implementation that make the most sense for specific types of firms to preserve innovation over time. Thus, the CCFDA should primarily articulate the principles most relevant for financial data privacy and security, to be expanded upon in the Content discussion, and dictate the regulatory agencies responsible for implementing specific rules to fulfill the principles of the legislation and maintaining both the coherence of and adherence to these rules in the long term.

Scope

Now that the structure of the CCFDA has been detailed, our discussion turns to the appropriate scope of the legislative effort. We will look at the breadth of data that should be included under the purview of the CCFDA, including both the type and subject, to set the boundaries of applicability for this legislation.

Focus on Financial Data

Our proposal leverages the definition of financial data that we described previously in this analysis to detail the data that should be included under the CCFDA. As a reminder, our definition is as follows:

---

[120] UK Information Commissioner's Office, "Guide to the General Data Protection Regulation (GDPR): The Principles."
[121] Boston Consulting Group, "Readiness for Data Privacy: California Consumer Privacy Act & Related Regulations."
[122] US Congress, "Dodd-Frank Wall Street Reform and Consumer Protection Act" (2010), https://www.govinfo.gov/content/pkg/BILLS-111hr4173enr/pdf/BILLS-111hr4173enr.pdf.

Financial data is a piece of information where:

(c) its subject is an individual or closely related individuals such as a family (data subject), and

(d) it is either:

(iii) directly tied to a financial account, transaction, or an individual's personal finances (data type), or

(iv) involved in a financial process (data utilization).

To note, the entity that possesses and/or processes the data (data processor) is not relevant to the classification of the data as financial or otherwise.

Our reasons for focusing exclusively on financial data as defined above are twofold. First, financial data holds unique power and risks for consumers as compared to other types of data. While a family vacation picture is certainly meaningful personal data, financial data can be used in a variety of applications that have significant impacts on modern life. For that reason, we believe that it is a sufficiently important type of data to be given a specific framework within the broader context of data regulation.

Second, we have intentionally developed a broad definition of financial data, relative to those included in previous regulatory efforts, to cover all data that could be relevant to an individual's financial life. Therefore, while the CCFDA is limited to financial data, the scope of that definition is actually relatively expansive, even as it is the appropriate scope to ensure consistency in consumer protections and the treatment of businesses.

It is critical to underscore that the scope of companies that will be included in the CCFDA would be significant, as the definition of financial data is agnostic to the type of firm that possesses the data. This will be a major shift from prior regulatory efforts in the financial data space that were limited to financial institutions. However, as previously discussed, this change is necessary due to the reality that the power of financial data is not dependent on the industry of the business possessing or utilizing it.

The Natural Definition of Consumers

For the purposes of the CCFDA, there is one restriction that we must place on the above definition of financial data pertaining to the types of business-individual relationships that it covers. Specifically, the definition includes all relationships that an individual might have with a business, which includes both consumerism and employment. While it is certainly important to be cognizant of the data involved in the relationship between an employer and an employee, we desire for our proposal to focus specifically on consumer financial data privacy and security, utilizing the "natural" definition of consumers, which pertains only to business-individual relationships where an individual is utilizing or purchasing the goods or services of a firm with which the individual has no employment relationship. Thus, the CCFDA is concerned with financial data only when it is associated with a consumer as described here.

Content

As the structure and scope of the CCFDA have now been described, we turn our attention to the content of this legislative proposal with a focus on, as previously discussed, the principles and high-level rules that should be included. We will first look at the inclusion of privacy and/or security, then describe the consumer rights that we believe to be optimal to firmly establish consumers' ownership of their financial data. Then, we will discuss the appropriate treatment of the business requirements and liability structures necessary to actualize those consumer rights and the enforcement mechanisms to maintain their realization over time.

Privacy and/or Security

As we have seen with existing pieces of legislation, there is a tendency for data regulation to focus predominantly on either privacy or security, most demonstrably evident in the differences between the CCPA and the CPCDPA, though it should be noted that the CCPA does contain some security provisions. However, we believe that the distinctions between data privacy and security have been overemphasized in these efforts. Rather, in reality, privacy and security are two sides of the same coin: privacy provides for the protection of information from internal misuse, and security focuses on the protection of information from external pilferage. In short, privacy and security are heavily interrelated, and diminishments in either generally adversely affect the other.

For that reason, the CCFDA contains provisions covering both privacy and security to ensure strong postures from corporations on these elements. Our approach seeks to enumerate consumer rights that impact both areas as currently defined, requiring businesses to make investments and changes to improve them proportionately. While some rights will seemingly pertain more to one than the other, we believe that consumers will only truly be protected when both are given the weight that they deserve.

The Basis for Consumer Rights

Prior to delving into the specific consumer rights that we propose including in the CCFDA, it is important to discuss a critical theoretical basis for the government providing rights to consumers regarding their financial data. Dating back to Locke, the principle that part of the government's role in society is to protect the individual's property rights has been largely accepted in market-based economies.[123] While the exact limits of this power have been the source of many political debates in the US and elsewhere, the underlying principle rings largely true. We believe that an individual's data should be rightfully treated as an individual's property, given that it is sourced from and generated by that individual; yet, the current regulatory framework for consumer financial data does not grant many rights to individuals in handling, maintaining access to, or protecting their data.

In our view, the foundational insight behind the CCFDA, as well as other recent legislative and regulatory efforts around consumer data, is to recognize that a person's data is their property and that the person should, by extension, have certain rights regarding that property, with government enumeration and enforcement of those rights if necessary. Thus, we

[123] John Locke, *Second Treatise of Government*, 1689, 16, https://www.earlymoderntexts.com/assets/pdfs/locke1689a.pdf.

have structured our proposal's core principles around a detailing of these consumer rights with respect to their financial data while recognizing that business requirements, liability structures, and enforcement mechanisms will be necessary to ensure the realization of these rights.

Consumer Financial Data Bill of Rights

In line with the stated goal of focusing primarily on principles in the CCFDA, with specific rule-making largely delegated to the regulatory agencies charged with implementation and enforcement, we have developed the following Consumer Financial Data Bill of Rights to fully enumerate the rights that consumers should be granted with respect to their property in the form of financial data:

1. Right to Know
2. Right to Access
3. Right to Deletion
4. Right to Opt Out of Third-Party Sales
5. Right to Non-Discrimination from Exercise
6. Right to Reasonable Distribution
7. Right to Prudent Security

In constructing our proposal, we have borrowed rights and concepts from existing legislative and regulatory efforts, most pertinently the CCPA. Specifically, the first five rights in our Bill of Rights are largely consistent with their framing in the CCPA. The Right to Know and the Right to Access focus on increasing transparency for consumers by entitling them to know in advance what types of data are being collected and for what purpose, as well as to access the data that a company maintains on them. The Right to Deletion centers on the consumer's ability to maintain control over data in the long term and request the removal of their data from a company, so long as the data is no longer necessary for an ongoing contract between the company and the consumer. The Right to Opt Out of Third-Party Sales serves the purpose of empowering consumers to prevent unwanted monetization of their data and further incentivizes businesses to develop new revenue models that are not dependent on the sale of customer data. The Right to Non-Discrimination from Exercise ensures that consumers cannot be denied services by companies simply for utilizing their powers under the first four rights, with the exception that businesses can charge disparate prices if there is an underlying change in value to the data provided or available due to exercise.

It's important to note that, while these first five rights are primarily aimed at increasing consumer privacy, they also have positive security implications as they give consumers more knowledge about the data that they are sharing, allow consumers to sunset data, and will likely have a negative impact on third-party distribution of data through sales.

The goal of the final two consumer rights – the Right to Reasonable Distribution and the Right to Prudent Security – is to fully enumerate implied social contracts between consumers and firms possessing or processing their data. Specifically, there is a legitimate expectation on the part of consumers that businesses to which they give their financial data will exercise reasonable restraint in distributing that data and provide for prudent security measures to protect that data. While these may seem obvious, we believe it is critical to recognize these rights as essential to appropriate consumer data protections and, by extension, place requirements on firms to take measures to realize them.

The primary implications of these final two rights are to change how businesses handle their data both internally and externally. The Right to Reasonable Distribution places a burden on firms to not permit parties access to consumer financial data if there is no legitimate business reason for them to have it. This will incentivize the development and maintenance of internal and third-party controls on data handling and permissioning that will protect both consumer data privacy and security.

The Right to Prudent Security involves a similar burden in that it necessitates the adoption of an appropriate security posture by firms with both their internal systems and their third-party relationships. We expect this right to lead to increased investment in cybersecurity measures and audits on the internal front, along with cybersecurity standards and reviews for third parties with which firms engage.

It's critical to note that neither of these rights automatically implies that firms are to be held responsible if consumer financial data is distributed to someone who shouldn't have it or is breached by malicious actors. We specifically include the standards of "reasonable" distribution and "prudent" security to recognize the reality that some firms could find themselves the subject of data mishaps despite taking all relevant precautions and investing in state-of-the-art systems. Thus, we leave it up to the regulatory agencies and their associated enforcement mechanisms to determine the difference between an unfortunate accident and corporate negligence when taking action against firms for issues regarding consumer financial data privacy and security. However, we believe that the specific enumeration of these two rights is essential for institutionalizing the existing consumer expectation that corporations are taking appropriate actions and measures involving the distribution and protection of their financial data.

Aligned Business Requirements and Liabilities

As discussed previously, our structuring of the CCFDA would largely leave specific rule-making to the regulatory agencies involved in its implementation and enforcement. However, it is prudent to discuss the expected results of this rule development process and their impact on business requirements and liabilities.

Business requirements would be designed with the goal of fulfilling one or more consumer rights and could be tailored to match the realities of specific industries or types of companies. In the initial development phase, firms would likely provide feedback to regulators on draft proposals to aid them in the construction of rules that achieve the desired consumer right(s) at minimal impact to the firms and broader societal innovation. After the first implementation, rules could be updated by regulators as appropriate when changes occur in various industries or technologies or when there is a realization that a mistake was made in a prior round of rule drafting. This flexibility would greatly increase the viability of the CCFDA in the long run and ensure that shifting consumer sentiment or business realities could be reflected if appropriate.

Regarding business liabilities, the CCFDA would relegate liabilities to inappropriate actions that occur within a particular firm. By doing so, companies would not be legally liable for every single action taken by third parties to which they transmit consumer financial data, as is the case in some situations today. However, there would still be liability assumed by the originating company upon a misdeed by a third party – if it is determined that the third party possessed the consumer financial data due to a failure on behalf of the originating company to maintain the Right to Reasonable Distribution or the Right to Prudent Security. For instance, if

an originating company failed to perform a reasonable security audit on a third party, that company could be held liable for a breach at the third party. We believe that this distribution of liability, focused on the final two rights in the Consumer Financial Data Bill of Rights, represents a reasonable solution to a problem that has long caused uncertainty for firms that possess or process consumer financial data.

Consistency in Enforcement

As a final measure, we aim to utilize enforcement mechanisms for the CCFDA that are as consistent as possible. As we saw with the CCPA and the NYPA, the utilization of a state Attorney General's office or the private right of action can lead to negative consequences such as uncertainty within firms and potentially devastating costs from civil suits for small businesses. Because of those realities, the CCFDA relies on the enforcement mechanism preferred for many federal financial regulations: action by regulatory agencies. The CCFDA will leverage the agencies that are responsible for rule-making and implementation to enforce business requirements and take action against companies that are found to be in violation of the enumerated consumer rights.

We believe that this method of enforcement will lead to a more holistic approach that is consistent across firms and appropriately recognizes the disproportionate burden that can fall on smaller firms, negatively impacting innovation. Given that firms will be involved in discussions with regulators from the beginning of the process to design the rules associated with the CCFDA, we would expect that relying on these agencies as the enforcers will lead to fewer unexpected outcomes for businesses that are trying to legitimately operate in a manner consistent with these new consumer rights.

The Expected Impact

Overall, we expect that the impact of the CCFDA will be greater long-run stability for businesses, stronger consumer rights and protections regarding financial data privacy and security, and increased innovation to build business models and systems with these concerns in mind from the ground up. However, we recognize that there will be short-term pains associated with this approach. Foremost, the CCFDA will be replacing a plethora of existing regulations, so care will need to be taken by legislators and regulatory agencies to ensure that no unnecessary discontinuities exist between current and new requirements. In addition, short-term costs will be borne by companies that need to make significant investments in new technologies, systems, and processes to comply with the anticipated requirements, particularly non-financial firms that currently find themselves largely without restrictions when they handle financial data. Lastly, it is likely that there will be a learning curve on the part of consumers to understand these new rights with regard to their financial data, so changing impacts may be seen over time as a consensus emerges about how best to exercise them.

That being noted, we firmly believe that the CCFDA is the optimal regulatory framework for consumer financial data privacy and security. We strongly recommend that the US Congress undertake the process necessary to realize the vision of the CCFDA for the betterment of American consumers, businesses, and society over the long term.

Conclusion

Consumer financial data privacy and security are essential for the protection of consumers and the continued functioning of the US financial system. Without them, trust in the financial system would be quickly eroded, causing the economy to grind to a standstill. As it currently stands, the US regulatory framework for financial data contains many deficiencies in consumer protection and carries significant compliance costs for firms due to the complex, interlinked nature of a myriad of state and federal regulations. While legislative attempts at state-level solutions, such as the CCPA and CPCDPA, are a promising start to rectifying some of these issues, particularly with regard to consumer rights, the optimal solution is to pursue comprehensive federal legislation that incorporates prior federal rules on financial data and significantly simplifies the regulatory approach for financial data protection.

Doing so would ensure that consumers are truly treated as the rightful owners of their data, with all the appropriate associated rights, and would simultaneously lower the regulatory burden on companies through the harmonization and clarification of business requirements. Furthermore, American innovation would be spurred through the relative empowerment of small businesses and the increased incentivization of privacy- and security-first technologies and financial products. Utilizing this exhaustive approach, the US regulatory framework for financial data will truly empower American consumers with their legitimate rights and enable companies to tackle the largest innovation challenges to come.

Works Cited

Abramowitz, Elkan, and Jonathan Sack. "Bank Secrecy Act Prosecutions: Why Few Individuals Are Charged." *New York Law Journal* 252, no. 43 (September 2, 2014). https://www.maglaw.com/publications/articles/2014-09-02-bank-secrecy-act-prosecutions-why-few-individuals-are-charged/_res/id=Attachments/index=0/Bank%20Secrecy%20Act%20Prosecutions%20Why%20Few%20Individuals%20Are%20Charged.pdf.

Ballentine, James. "American Bankers Association Response to Data Privacy Inquiry from the Senate Committee on Banking, Housing, and Urban Affairs," March 15, 2019. https://www.banking.senate.gov/imo/media/doc/Data%20Submission_American%20Bankers%20Association%20(ABA)1.pdf.

Bard, Yoni, and Scott Bloomberg. "United States: CCPA: The (Qualified) Right to Deletion," July 30, 2019. http://www.mondaq.com/unitedstates/x/831300/Data+Protection+Privacy/CCPA+The+Qualified+Right+To+Deletion.

Barthet, Alex. "Mergers and Acquisitions and Successor Liabilities: The Deal Is Done, but the Liability Lives On." The Lien Zone, March 31, 2010. https://www.thelienzone.com/mergers-and-acquisitions-and-successor-liabilities-the-deal-is-done-but-the-liability-lives-on/.

Berkeley Economic Advising and Research, LLC. "Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations," August 2019. http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.

Boldon James. "CCPA - The New Law Delivering GDPR-Style Privacy to California." Accessed January 4, 2020. https://www.boldonjames.com/ccpa-compliance/.

Boston Consulting Group. "An Interactive Guide to Global Payments," January 11, 2019. https://www.bcg.com/publications/interactives/global-payments-interactive-edition.aspx.

———. "Readiness for Data Privacy: California Consumer Privacy Act & Related Regulations," July 2019.

Brandeis, Louis. New State Ice Co. v. Liebmann (US Supreme Court March 21, 1932).

Breitzman, Anthony, and Diana Hicks. "An Analysis of Small Business Patents by Industry and Firm Size." Rowan University, November 2008. https://rdw.rowan.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1011&context=csm_facpub.

Brumfield, Cynthia. "11 New State Privacy and Security Laws Explained: Is Your Business Ready?" CSO Online, August 8, 2019. https://www.csoonline.com/article/3429608/11-new-state-privacy-and-security-laws-explained-is-your-business-ready.html.

California Legislature. California Consumer Privacy Act of 2018, 1798.100-1798.199 California CIV 1.81.5 § (2018). https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

Cerchiello, Paola, and Paolo Giudici. "Big Data Analysis for Financial Risk Management." *Journal of Big Data* 3, no. 18 (2016). https://journalofbigdata.springeropen.com/articles/10.1186/s40537-016-0053-4.

Clarip. “CCPA Right to Opt Out for the Sale of Personal Information.” Accessed January 19, 2020. https://www.clarip.com/data-privacy/ca-consumer-privacy-act-right-opt-out/.
Clayton, Jay. “The Evolving Market for Retail Investment Services and Forward-Looking Regulation - Adding Clarity and Investor Protection While Ensuring Access and Choice.” US Securities and Exchange Commission, May 2, 2018. https://www.sec.gov/news/speech/speech-clayton-2018-05-02.
Colorado Office of the Attorney General. “Colorado’s Consumer Data Protection Laws: FAQ’s for Businesses and Government Agencies.” Accessed January 2, 2020. https://coag.gov/resources/data-protection-laws/.
Colorado State Legislature. Colorado Protections for Consumer Data Privacy Act of 2018, 6 Colorado Revised Statutes § (2018). http://leg.colorado.gov/sites/default/files/2018a_1128_signed.pdf.
Crosman, Penny. “Large U.S. Banks Scramble to Meet EU Data Privacy Rules.” American Banker, April 16, 2018. https://www.americanbanker.com/news/large-us-banks-scramble-to-meet-eu-data-privacy-rules.
Davies, Mark. “CCPA Is Coming January 1. Is Your Bank Ready?,” May 15, 2019. https://digitally.cognizant.com/ccpa-coming-is-your-bank-ready-codex4675/.
Duffy, Seamus C., Meredith C. Slawe, and Julia Ann Busta. “United States: Divergent State Privacy Laws Show Need for Federal Solution.” Mondaq, August 23, 2019. http://www.mondaq.com/unitedstates/x/840000/Data+Protection+Privacy/Divergent+State+Privacy+Laws+Show+Need+For+Federal+Solution.
Electronic Privacy Information Center. “Equifax Data Breach.” Accessed January 2, 2020. https://epic.org/privacy/data-breach/equifax/.
———. “The Gramm-Leach-Bliley Act.” Accessed January 2, 2020. https://epic.org/privacy/glba/.
———. “The Right to Financial Privacy Act.” Accessed January 2, 2020. https://epic.org/privacy/rfpa/.
European Union. “What Is GDPR, the EU’s New Data Protection Law?” Accessed January 4, 2020. https://gdpr.eu/what-is-gdpr/.
Federal Financial Institutions Examination Council. “BSA/AML Manual: Appendix P.” Accessed January 19, 2020. https://bsaaml.ffiec.gov/manual/Appendices/16.
Federal Reserve Bank of St. Louis. “Credit Market Debt Outstanding.” FRED. Accessed January 27, 2020. https://fred.stlouisfed.org/series/TCMDO.
Fridman, Anna. “What Financial Institutions Need to Know About the CCPA,” October 4, 2019. https://www.law.com/therecorder/2019/10/04/what-financial-institutions-need-to-know-about-the-ccpa/?slreturn=20200004211855.
Granato, Andrew, and Andy Polacek. Chicago Fed Letter #426. “The Growth and Challenges of Cyber Insurance.” Chicago Fed Letter #426, 2019. https://www.chicagofed.org/publications/chicago-fed-letter/2019/426.
Jodka, Sara. “More Companies Must Comply with the Gramm-Leach-Bliley Act, But Don’t Know It. Are You One of Them?,” September 2017. https://www.dickinson-wright.com/news-alerts/more-companies-must-comply-with-the-gramm-act.
Jones Day. “California Consumer Privacy Act Guide,” 2018. https://www.jonesday.com/-/media/files/publications/1/01/california-consumer-privacy-act-guide/files/california-consumer-privacy-act-guide-gdpr-handout/fileattachment/california-consumer-privacy-act-guide-handout.pdf.

Kornberg, Bernard J. “Banks Face Unique Liability for Data Breaches Under the Gramm-Leach-Bliley Act.” Severson & Werson, March 7, 2018. https://www.severson.com/banks-face-unique-liability-for-data-breaches-under-the-gramm-leach-bliley-act/.

Lapowsky, Issie. “New York’s Privacy Bill Is Even Bolder Than California’s.” *Wired Magazine*, June 4, 2019. https://www.wired.com/story/new-york-privacy-act-bolder/#:~:targetText=The%20New%20York%20Privacy%20Act%2C%20introduced%20last%20month%20by%20state,privacy%20before%20their%20own%20profits.&targetText=The%20New%20York%20Privacy%20Act%20bears%20some%20similarity%20to%20the%20California%20law.

Locke, John. *Second Treatise of Government*, 1689. https://www.earlymoderntexts.com/assets/pdfs/locke1689a.pdf.

Los Angeles Times Staff. “Seeing Those Opt-Out Messages About Your Personal Information on Websites? Thank California’s New Privacy Law.” *Los Angeles Times*, January 2, 2020. https://www.latimes.com/california/story/2020-01-02/california-consumer-privacy-act-do-not-sell-my-info.

Lux, Marshall, and Guillaume Delepine. “Revolution in Data: How New Technologies Are Upending Borrowing.” Harvard Kennedy School Mossavar-Rahmani Center for Business & Government, February 2019. https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/working.papers/107_BigData.pdf.

Mahon, Joe. “Financial Services Modernization Act of 1999, Commonly Called Gramm-Leach-Bliley.” Federal Reserve History, November 12, 1999. https://www.federalreservehistory.org/essays/gramm_leach_bliley_act.

National Law Review. “Comprehensive Federal Privacy Law Still Pending,” January 22, 2020. https://www.natlawreview.com/article/comprehensive-federal-privacy-law-still-pending.

———. “Massachusetts Consumer Data Privacy Bill Could Dramatically Expand Class Action Litigation Risk,” May 21, 2019. https://www.natlawreview.com/article/massachusetts-consumer-data-privacy-bill-could-dramatically-expand-class-action.

———. “State Legislature Hears Concerns About Proposed Massachusetts Consumer Data Privacy Bill,” October 11, 2019. https://www.natlawreview.com/article/state-legislature-hears-concerns-about-proposed-massachusetts-consumer-data-privacy.

Navetta, David, Megan Donohue, Nathaniel Cooper, and Christian Lee. “CCPA FAQs Part 3: Litigation, Regulatory Actions and Liability.” Cooley Cyber/Data/Privacy Insights, October 1, 2019. https://cdp.cooley.com/ccpa-faqs-part-3-litigation-regulatory-actions-and-liability/.

Negus Viveiros, Beth. “Data Privacy Concerns On Rise.” Chief Marketer, December 12, 2018. https://www.chiefmarketer.com/data-privacy-concerns-on-rise-report/.

New York State Department of Financial Services. “23 NYCRR 500: Cybersecurity Requirements for Financial Services Companies,” February 2017. https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf.

Noltensmeyer, John. “CCPA Overview: Understanding Compliance.” TokenEx, August 15, 2018. https://www.tokenex.com/blog/understanding-compliance-california-consumer-privacy-act.

NuHarbor Security. “Third-Party Security in the Financial Services Industry [Infographic],” June 28, 2016. https://www.nuharborsecurity.com/third-party-security-in-financial-services-infographic/.

Plaid. “Company Overview.” Accessed January 19, 2020. https://plaid.com/company/.
PricewaterhouseCoopers. “Your Readiness Roadmap for the California Consumer Privacy Act (CCPA).” Accessed January 2, 2020. https://www.pwc.com/us/en/services/consulting/cybersecurity/california-consumer-privacy-act.html.
Raskin, Jeffrey. “Consider Enhancing Cyberliability Insurance Policies to Align with CCPA: Part 1,” September 24, 2019. https://www.morganlewis.com/blogs/healthlawscan/2019/09/consider-enhancing-cyberliability-insurance-policies-to-align-with-ccpa-part-1.
Stephens, John. “California Consumer Privacy Act.” American Bar Association, July 2, 2019. https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_9/.
Sterling, Gary. “Nearly All Consumers Are Concerned About Personal Data Privacy, Survey Finds.” Marketing Land, December 4, 2019. https://marketingland.com/nearly-all-consumers-are-concerned-about-personal-data-privacy-survey-finds-272129.
Sterling, Greg. “Survey: 58% Will Share Personal Data Under the Right Circumstances,” June 20, 2018. https://marketingland.com/survey-58-will-share-personal-data-under-the-right-circumstances-242750.
Stone Creem, Cynthia. An Act Relative to Consumer Data Privacy, Pub. L. No. S120 (2019). https://malegislature.gov/Bills/191/SD341.
The Gazette. “New Law Puts Colorado at the Top for Consumer Data Protection,” March 22, 2019. https://gazette.com/sponsored/new-law-puts-colorado-at-the-top-for-consumer-data/article_fcfb33ae-4c11-11e9-94d1-0b5d51de9ac2.html.
Thomas, Kevin. New York Privacy Act, Pub. L. No. S5642 (2019). https://www.nysenate.gov/legislation/bills/2019/s5642.
Tolliver-Walker, Heidi. “Survey: Consumers’ Willingness to Give Up Personal Data Is Waning,” November 20, 2019. http://whattheythink.com/articles/98437-survey-consumers-willingness-give-personal-data-waning/.
Trulioo. “CCPA Compliance - A Guide for Fintech,” August 14, 2019. https://www.trulioo.com/blog/ccpa-compliance/.
UK Information Commissioner’s Office. “Guide to the General Data Protection Regulation (GDPR): The Principles.” Accessed January 20, 2020. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/.
US Congress. Dodd-Frank Wall Street Reform and Consumer Protection Act (2010). https://www.govinfo.gov/content/pkg/BILLS-111hr4173enr/pdf/BILLS-111hr4173enr.pdf.
———. The Fair Credit Reporting Act, 1681 15 USC § (1992). https://epic.org/privacy/financial/fcra.html.
US Consumer Financial Protection Bureau. “A Summary of Your Rights Under the Fair Credit Reporting Act.” Accessed January 2, 2020. https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.
US Federal Deposit Insurance Corporation. “FDIC Consumer Compliance Examination Manual - Gramm-Leach-Bliley Act (Privacy of Consumer Financial Information),” June 2016. https://www.fdic.gov/regulations/compliance/manual/8/viii-1.1.pdf.

———. “FDIC Consumer Compliance Examination Manual - Right to Financial Privacy Act,” June 2006. https://www.fdic.gov/regulations/compliance/manual/8/viii-3.1.pdf.
US Federal Reserve. “Federal Reserve Consumer Compliance Handbook - Right to Financial Privacy Act,” January 2006. https://www.federalreserve.gov/boarddocs/supmanual/cch/priv.pdf.
US Internal Revenue Service. “Bank Secrecy Act.” Accessed January 2, 2020. https://www.irs.gov/businesses/small-businesses-self-employed/bank-secrecy-act.
US Office of the Comptroller of the Currency. “Bank Secrecy Act (BSA).” Accessed January 2, 2020. https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html.
Williams, Robert. “Accenture: More Consumers Willing to Share Data When There’s Transparency,” October 17, 2019. https://www.marketingdive.com/news/accenture-more-consumers-willing-to-share-data-when-theres-transparency/565195/.
Woepke, Scott. “California Consumer Protection Act (CCPA) and Its Impact for Financial Services Companies. Are You Prepared?,” August 12, 2019. https://www.acxiom.com/blog/ccpa-and-its-impact-for-financial-services-companies/.
Worldpay Editorial Team. “How Credit Card Processing Works,” July 10, 2019. https://www.worldpay.com/en-us/insights-hub/article/how-credit-card-processing-works.