THE ROLE OF INDIVIDUALS IN THE DATA ECOSYSTEM:

Current debates and considerations for data protection and data rights in the United States

FINTECH EDGE SPECIAL REPORT

FEDERAL RESERVE BANK
OF SAN FRANCISCO

The Role of Individuals in the Data Ecosystem: Current debates and considerations for individual data protection and data rights in the U.S.

Author
Kaitlin Asrow, Fintech Policy Advisor, Federal Reserve Bank of San Francisco

Publication Date
June 3, 2020

Acknowledgements
The author would like to acknowledge the following individuals for their contributions to this research:

Symposium Partners
- Melissa Koide, FinRegLab
- Kelly Thompson Cochran, FinRegLab
- Aaron Milner, FinRegLab

Paper Reviewers
- Kelly Thompson Cochran, FinRegLab
- Jonah Crane, Klaros Group
- Douglas Elliott, Oliver Wyman
- David Medine, Consultative Group to Assist the Poor
- Andres Wolberg-Stok, Citi
- Chi Chi Wu, National Consumer Law Center

The author would also like to thank the following individuals from the Federal Reserve Bank of San Francisco for their invaluable contributions to the final paper:

Anna Baram, Avery Belka, Brian Walker, Caroline Pao, Cynthia Course, Marshall Eckblad, Mitchell Lee, Mongkha Pavlick, Santa Ram Susarapu, Steve Wertheimer, Walter Yao, Irina Yugay

Table of Contents

COVID-19 Impacts and Considerations

The global COVID-19 pandemic has caused unprecedented disruption and change in every aspect of our lives. In spite of these changes, efforts to consider data governance frameworks for the United States (U.S.) appear even more relevant.

Since early 2019, the Federal Reserve Bank of San Francisco has engaged in focused research to understand data as a complex policy area, with a particular focus on the potential roles of individuals in the data ecosystem. This effort has culminated in the white paper, "The Role of Individuals in the Data Ecosystem: Current debates and considerations for individual data protection and data rights in the U.S." The majority of the paper was completed prior to the COVID-19 crisis therefore considerations relative to the pandemic are not explicitly addressed. Despite this, many of the data governance concepts that are presented for consideration and discussion remain directly relevant.

In particular, the current crisis has highlighted the tensions that can occur between individual preferences and societal preferences with regard to data; the importance of broad data protection; and the value of data portability and digital infrastructure.

HEALTH AND DATA IMPACTS

To contain the spread of the virus, public health officials have indicated that it is essential to track infected, and potentially exposed individuals.[1] Technology, and the collection and use of data, can facilitate this, but it can also expose individuals to privacy and security risks both now and in the future. Many countries are using mobile phones, and mobile phone applications, to gather a range of data including GPS locations, phone-to-phone proximity, and individual daily health status.[2] The full impact of these data activities is still unknown, however two essential challenges have already surfaced that underscore issues and concepts raised in the paper.

The first challenge is that for both digital contact tracing and the reporting of health status, it is more effective[3] if a majority of the population participates. Unfortunately, many Americans report that they are unlikely to voluntarily take part in this kind of data collection.[4] This tension highlights the larger issue raised in the paper, of when individual rights around data, such as consent to collection, could come into conflict with other policy goals.

The second challenge that has surfaced thus far is that the information being collected and used in the pandemic response is particularly sensitive, such as health status, and can be challenging to anonymize, or disassociate from specific individuals.[5] This second challenge underscores the importance of strong data protection requirements across entities that incorporate both cybersecurity and internal conduct expectations, a concept raised in the paper.

ECONOMICS, DIGITAL LIVES, AND DATA IMPACTS

To facilitate the economic response to the pandemic there has been a clear and pressing need to make data available quickly and securely for consumer authentication and loan underwriting. Furthermore, COVID-19 has highlighted the importance of effective digital infrastructure to facilitate economic responses such as stimulus payments to individuals, and to enable increasingly digital lives. Unfortunately, these needs have exposed a lack of standards and processes for sharing information, and the limitations of aging technical systems.[6] The value of data portability processes, as well as adequate infrastructure, are also issues raised in the paper.

Currently, there are not standardized systems and policies in the U.S. for moving data quickly and securely between diverse financial service providers in order to facilitate activities such as lending and payments. The paper delves into the potential of data portability as right for individuals, as well as the value of consistent and secure systems to facilitate such a right.

During the COVID-19 crisis there have been reports of individuals, primarily in rural and marginalized communities, that do not have the internet access or computing resources necessary to work or attend school remotely.[7] As lives become increasingly digital it is essential to consider how the U.S. will create, update, and maintain adequate digital infrastructure for everything from baseline needs such as internet access, to more complex systems such as facilitating payments. The importance of digital infrastructure to support both data rights and data protection is emphasized in the paper.

ESSENTIAL COVID-19 DATA CONSIDERATIONS

In addition to the issues and concepts raised in the paper, COVID-19 raises additional questions:

Where does increased data collection have the greatest opportunity to help? There is limited evidence that using data to monitor locations or proximity at the individual level is effective at identifying those who may have been exposed to the virus, compared to traditional contact tracing.[8] More work is needed to determine which types of data are actually necessary and effective.

Which entity/entities will be doing the actual data collection, and for what purpose? Currently, the most important consideration is determining which entities have the capacity to engage in these activities immediately and securely. For the U.S. that capacity rests largely in the private sector. Unfortunately, today there are limited avenues to hold private companies accountable for data security and conduct.

What rights will individuals have relative to data collected and used during the pandemic? This pandemic highlights the tension between individual agency and broader societal needs. An important distinction can be made between limiting choices now, and still providing them in the future. There may be opportunities to provide individuals with rights that can enable them to

review data collected and take actions—such as having data deleted—at a later date, even if those options are not available today.

How do we build data systems for the crisis that can be monitored, and reconsidered after it is over? The data systems that are built to deal with the pandemic today do not necessarily need to define U.S. data governance in the future. Once the pandemic has subsided, the country can hopefully learn from these crisis efforts, as we endeavor to make changes and build more permanent governance frameworks. Some companies[9] have already developed voluntary data conduct guidelines for the pandemic, and these standards, along with consistent security approaches could be used as starting point for future systems.

MOVING FORWARD

While data governance may understandably be a lower priority when lives are at risk, using data for the benefit of citizens and to help the U.S. weather this pandemic can happen in tandem with individual data protection and data rights.[10] The country has an opportunity to examine the role of data under these current challenging circumstances, even as it assembles guardrails and infrastructure that can help respond more quickly and confidently in the future.

Executive Summary

We are living in a time of immense technological change, driven in part by our ability to capture data, convert it into new information, and use that information to inform decision-making, automate activities, and develop new products and services. This use of data, and the insights that it can provide, are impacting every aspect of our lives. Today, information is fueling massive business growth and helping individuals by enabling more personalized experiences, providing visibility into complex relationships such as financial services and health, and aiding in decision-making.[11]

Unfortunately information is also used to manipulate actions, exploitatively target people, discriminate on improper grounds, and open once intimate spaces up to unforeseen dissection and analysis.[12] These benefits and risks are increasing as more data are collected and used,[13] and they directly affect every person in the U.S., and therefore the country as a collective whole. The global COVID-19 pandemic has further emphasized this tension. As society seeks new ways to track and monitor the virus, and as even more daily activities become digital, concerns around privacy and data security continue to grow.

A range of stakeholders and policymakers are acknowledging the need to more proactively balance the benefits and risks of this data explosion,[14] and there are robust conversations occurring across the country around the potential for improving and expanding U.S. data governance regimes.[15]

An essential question that weaves through this dialogue is the role of individuals themselves in judging these benefits and risks, and managing data directly.

Terms such as “control”, “choice”, and “ownership” over data are increasingly being used to describe the roles that individuals could play in this ecosystem. These words underscore a shared acknowledgment that there is inherent value in individuals playing a role relative to data, but a fundamental question remains around what type, and what amount, of individual management is actually reasonable to expect in such a large and technically complex ecosystem. There are also questions regarding what needs to change within technology systems to make management choices and control truly meaningful.

Currently, information related to each of us is constantly collected and used, and there is often little we can truly do about it.[16] The most meaningful action that individuals can take around data today may be to avoid using digital services at all. However, this potentially cuts people off from the benefits of personalization, improved efficiency, and necessary activities such as school and work.[17] Individuals themselves are increasingly aware of this reality, and report feeling a lack of

both protection and control with regard to data, while still acknowledging the value of information for creating innovative products and services.[18]

Creating a U.S. data governance regime that more deliberately balances benefits and risks and creates an enhanced role for individual choice and autonomy is an exciting proposition and may be more necessary than ever,[19] but it is also uniquely challenging. This kind of undertaking would affect individuals and businesses across the county, and requires careful consideration of issues concerning privacy, cybersecurity, innovation, inclusion, domestic competition, international trade, and more.[20]

The Federal Reserve Bank of San Francisco (SF Fed) has undertaken research, policy analysis, and stakeholder outreach throughout 2019 to help provide a nuanced and neutral perspective on the issues described above, with a particular focus on the potential roles of individuals themselves. **It is the goal of this report to help examine the complexity of data as a policy area and offer data governance concepts for consideration and further discussion.** Another contribution of this work is to offer consistent terminology that can be used to describe data governance goals moving forward.

This research builds upon a number of public and private efforts that have offered common principles for data governance, including work from the Consumer Financial Protection Bureau (CFPB),[21] the American Law Institute (ALI),[22] the Financial Health Network,[23] the Consultative Group to Assist the Poor (CGAP),[24] the World Economic Forum (WEF),[25] and others.[26] Of particular importance to this work was a symposium hosted by the SF Fed and FinRegLab, a nonprofit innovation center that tests new technologies and data to inform public policy and drive the financial sector toward a responsible and inclusive financial marketplace. This symposium, entitled, "The Role of Consumers in the Data Ecosystem" took place on November 4 - 5, 2019.[27] The event provided a forum to test and refine some of the ideas considered as part of this research. While the Symposium contributed to the concepts in this report, the detail and analysis stand alone as a larger project.

The analysis and recommendations presented in this report should *not* be interpreted as opinions of symposium partners, advisors, or participants, reviewers of this report, the Federal Reserve Bank of San Francisco, or the Board of Governors of the Federal Reserve System.

This report contends that while control over data has the potential to empower individuals and create new benefits, that concept alone cannot address the full range of challenging, and intersecting policy issues that the data ecosystem gives rise to.

In particular, there is an important distinction between enabling individuals to manage data, and expecting them to take action as a form of protection or to achieve other policy goals.

The paper is presented in two parts. Part 1 is intended to unpack and analyze many of the key debates and challenges that have been raised relative to individuals' role in the data ecosystem. Based on the analysis in each section, **key takeaways are offered that focus on benefiting and protecting individuals**, while highlighting particular legal and technological complexities to keep in mind.

REFRAMING FROM "DATA OWNERSHIP" TO "DATA RIGHTS"

It is easy to say we should "own" data about ourselves, but creating legal and administrative structures for individual "ownership" of data would be exceptionally complex. Furthermore, **an ownership framework that treats data primarily as a commodity, or in monetary terms, could have negative consequences for other policy goals. A shift is proposed away from the framing of "ownership", and instead towards a broader concept of "data rights".**

THE LIMITATIONS OF INDIVIDUAL CONSENT

Notice and consent regimes are broadly used in the United States to give individuals a role relative to data, but given the complexity of technology and the volume of digital interactions today, it places too heavy a burden on individuals to protect themselves. This regime is profoundly broken and there are significant challenges to improving it. One potential approach is to move away from detailed consent and introduce a "legitimate purpose" requirement across all data activities. To meet a legitimate purpose requirement, data activities would need to be necessary for the product or service requested, and not be harmful to the individual.

THE CRUCIAL CHALLENGE OF EQUALITY

The benefits and risks of data collection, processing, and use occur differently across diverse populations and therefore data protection and data rights will impact individuals differently. More research is needed to understand the needs and preferences of diverse populations relative to data, and to explore systems that could customize experiences and reduce management burdens across individuals. A particular focus on populations already under-represented in the design of, and access to, digital technology is especially warranted.

BALANCING INDIVIDUAL RIGHTS AND COLLECTIVE GOALS

There are a multitude of policy goals that interact with data and information. Siloed approaches to data governance that focus only on one policy objective may inadvertently interact with other goals and considerations. A multi-disciplinary, multi-sector approach to the creation and implementation of data governance can help reveal and address these policy intersections.

CURRENT U.S. DATA GOVERNANCE

U.S. laws that include data governance elements can yield important lessons about the effectiveness of particular approaches and where changes may be warranted in policy design and implementation going forward. **There are gaps in protection and confusing overlaps across current U.S. data governance laws. A broad, baseline approach to data governance could help address these issues.** There is also the potential to accomplish shorter-term improvements while larger structures are developed.

Part 1 seeks to demonstrate that while agency is important to respect the dignity and diverse needs of individuals, there are limitations to individual data control as a tool given the complexity of digital interactions today, and in light of other policy considerations. Part 2 of this report strives to address these tensions through a two-sided data governance framework that includes both individual data protection and individual agency through active data rights. The scope of this idea is broader than any current Federal, State, or sector-based regulation, and is intended to be a conceptual design that can serve as a base for further refinement and adaptation.

THE FOUNDATION: INDIVIDUAL DATA PROTECTION

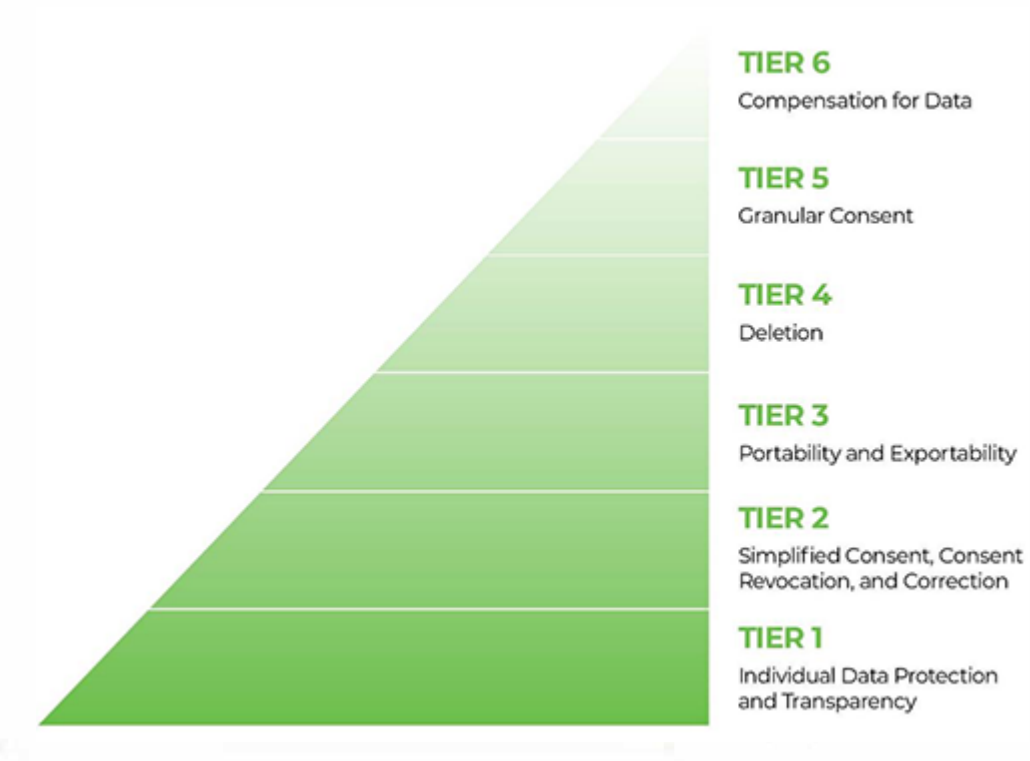
It is challenging, and maybe impossible, to quantify the exact risk that data can pose to individuals. Harm from data can come from external attacks or internal misuse of data by companies. Entities that use data, and how those data are used, blend across traditional sectoral and regulatory boundaries, and techniques used to "de-identify" data in order to protect individuals are largely ineffective. To address these realities, **a comprehensive data protection structure is proposed that would apply to all entities that collect, process, and use data. This structure would specify both security and conduct standards, such as a legitimate purpose requirement, and would extend protections to cover "de-identified" data.** The goal of this proposal is to create a clear, navigable, and baseline ecosystem for all entities, and to enable the subsequent active data rights framework. An essential premise of individual data protection is that **individuals should not need to take any affirmative actions, or exercise any 'rights', in order to experience data protection.**

A PROPOSED SPECTRUM OF ACTIVE DATA RIGHTS

Building upon the foundation of individual data protection, enabling individuals to directly act on information related to them can improve well-being, and may stimulate innovation, inclusion, and competition across markets. However, those considerations must be balanced with other social and policy goals, and an acknowledgment of how active data management on the part of individuals could create new cognitive, time, and resource burdens. To address these considerations **a bundle of active data rights is proposed that is structured into tiers that vary the rights available to individuals across circumstances.** Certain rights are foundational and apply across all situations, and others vary based on the intellectual property that entities

contribute, how close data activities are to the original legitimate purpose of collection, and the risk of certain data and data formats.

Figure 1. A Spectrum of Data Rights
The pyramid base applies more broadly, while the availability of rights is reduced in subsequent tiers to account for other policy considerations.



TECHNOLOGY AND BUSINESS MODELS TO SUPPORT INDIVIDUAL DATA RIGHTS

While a broad framework for individual data protection and active data rights can help change the current data landscape for individuals and businesses, there is also **a need for new market-based innovation and business design that can support these data governance structures**. Ideally governance structures can both incentivize these evolutions, and benefit from them.

Across all of the analysis and ideas presented in this paper, there are common barriers to achieving broad changes to data governance: (1) complexity across current and future systems, (2) tensions with existing law and precedent, and (3) limitations to what technology can accomplish for data management today. Because of this, more collaboration and research are needed across all of the elements of individual data protection and active rights described in this paper.

This report, and the concepts within it, are intended to stimulate conversation and provide a forward-leaning set of ideas to be vetted and refined collectively. The SF Fed looks forward to continuing to explore the potential for broad data governance in the United States.

Project Scope, Definitions, and Background

Scope

The collection, processing, and use of information has become so expansive that traditional sectoral and regulatory boundaries are blurring. While the mandate of the SF Fed is rooted in financial services this paper is framed broadly across all U.S. contexts. Given the history of data governance within financial service laws, and the multitude of domestic[28] and international conversations[29] around data related to this sector, this research provides examples from financial services, but that is not intended to confine the conversation. Parallel issues, and conversations are arising across many sectors and jurisdictions, and taking a broad approach to this topic has the potential to stimulate learning and innovation.[30] However, while it is the hope that this research can apply more broadly, additional work is needed to test the relevance of these ideas for other sectors.

The ideas put forth in the report are intended to apply to all organizations that handle data, both public and private, and any data related to individuals that are used for a commercial or public purpose. The discussion does not consider data that are gathered for an individual's personal use, such as a list of friend's addresses.[31]

Definitions

A variety of terms related to data, data governance, and data rights have been used interchangeably as this debate has evolved in the U.S. A secondary goal of this report is to establish a shared language, and understanding, around the terms used to describe data governance and individual control.[32]

This paper uses the term "individual" for the majority of the discussion, in lieu of the terms "consumer" or "customer". These terms are often used with an expectation of a direct commercial relationship between a company that is handling data and the individual to which the information relates, however a significant portion of data collection and handling occurs among entities without a direct or meaningful connection to the affected individuals. Examples of this include service providers, large unseen data brokers,[33] and arguably many websites that are visited simply for information or enjoyment. Thus, the term individual is intended to avoid embedding assumptions about direct relationships and to focus on natural persons in order to create a collective understanding. Furthermore, information about individuals can be intimately tied to dignity and concepts of personhood, and the term "individual" is intended to remind readers of this sensitive linkage. The section of the report that deals with existing law, *Current U.S. Data Governance*, will revert to using the terms "consumer" and "customer" for clarity when used as terms of art under existing statutes. Many of the same concerns that apply to individuals may also apply to small business owners, but that was not the primary focus of this project and

more research is needed to assess the extent to which the concepts presented in this report could apply to small business more broadly.

The term "agency" is used across this report to indicate an individual's ability to take action, and as a synonym for active data rights. The elements of individual agency around data that are discussed and considered for this paper include the concepts listed below. These reflect various active data rights that have been provided to individuals in both domestic and international contexts to date, but there may be other actions available to individuals that have not been conceptualized, or codified anywhere yet.

- Visibility into information to be collected; and previously collected
- Visibility into how information will be used; and the subsequent impacts of those uses
- Initial and ongoing consent for collection, processing, and use
- Revocation of consent for collection, processing, and use
- The ability to review for, and request the correction of, data errors and omissions
- One-time porting of data between entities, or provision directly to individuals
- Ongoing transfers of data between entities
- Deletion of held data

Data discussed in the paper are broadly defined as any information related to an individual that are used for a commercial or public purpose. As will be discussed in subsequent sections, this includes *both* "identified" data and "identifiable" data, despite the fact that much of current U.S. law only applies to "identified" data. Furthermore, this report takes a broad approach to what is classified as "identifiable" data. An example of "identified" data is information, such as income, attached to information that is unique to individuals, such as a name or social security number. Name and social security number are examples of unique pieces of information that are typically called "direct identifiers". "Identifiable data" is a broader category that refers to any pieces of information that could reasonably be associated with a particular individual.[34] For example, if a data set contains information about income, job title, and job address, there is a limited group of individuals that that information likely relates to. Given the large number of data breaches that have occurred,[35] it is reasonable to assume that even data that does not include "direct identifiers" can be combined with information from other sources in order to identify specific individuals.

The phrase "data collection, processing, and use" is used interchangeably with the umbrella term "data activities". Both of these are meant to capture the breadth of actions that entities may take around data. Data collection refers to the initial creation, or capture, of data about an individual whether through entry onto a form, tracking through technology, or other means. Examples of data processing include standardizing data into a consistent format, performing analysis on it, and the storage of data for future uses. Data use refers to the eventual product or service that the

data are enabling, such as a credit decision. These terms are also intended to align with the term data "processing" used in Europe's General Data Protection Regulation (GDPR), defined as, "operations performed on personal data such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".[36]

The phrase "data governance" is used broadly across the report to indicate any formal policy or market-based structures that direct, enable, or prohibit data activities. References to "stakeholders" in this report refers broadly to policymakers, researchers, and leaders across regulation, legislation, market entities, academia, advocacy, and beyond.

The difference between "privacy", "individual data protection", and "active data rights": The term privacy is frequently used together, or interchangeably with other ideas such as data protection and data rights. For the purposes of this report, and the broader data governance dialogue, the concepts are defined, and differentiated in the following ways:

Privacy: Defined as "the quality of being apart from observation or intrusion". This term first appears in English common law[37] and was focused primarily on defining areas where an individual was free, and separate, from the state. Stemming from this concept, privacy was declared a human right by the United Nations following the state-led atrocities of World War II.[38] In the U.S. the Constitution does not explicitly provide for a right to privacy,[39] but the courts have established a broad precedent for privacy that covers everything from libel,[40] protection from government action, to Roe v. Wade.[41] Despite its breadth, this precedent still focuses primarily on protecting privacy from intrusions by the state or other individuals.

As businesses are increasingly able to collect, process, and use data, the concept of privacy has been expanded to also consider being apart from observation or intrusion by a company or non-governmental entity.

While the concept of privacy is powerful in its familiarity and history, it is increasingly challenging to make actionable. Many interactions with technology, by their nature generate data about individuals which could be considered observation or intrusion. It is also unclear when various activities, such as automated decision-making, may cross the line into "intrusion". This ability to constantly observe individuals, and intervene at moments of decision-making, has powered innovation and benefit, but it is challenging to clearly define when data activities become intrusive and objectionable. In this new world of constant observation, additional terms and clarifications are helpful in articulating what it means to truly have "privacy".

Individual data protection: The *data security and conduct expected from business* with regard to information collection, processing, and use. Individuals do not need to take direct or affirmative actions in order to experience data protection.

Active data rights: *Actions that individuals have a right to take* with regard to information collection, processing, and use. Individual rights are supported by, and occur in addition to, data protection.

Drawing a distinction between data protection and active data rights borrows from the philosophical distinction between positive and negative liberties.[42] The concept of negative liberty (protection) is the idea that individuals have a right to be free from interference, in this case risk and harm relative to data. Positive liberty (rights) is the idea that individuals will be entitled to act independently, in this case asserting various forms of control over data.

An example of the distinction between protection and rights is the difference between legal prohibitions on certain data activities and an individual providing consent to permissible uses of information. This distinction is important but does not suggest that these are mutually exclusive concepts. In fact, individual data rights often cannot be truly actionable and safe without imposing some direct requirements on companies. **Combining individual data protection with active data rights creates a policy framework that may help to achieve a broadened, more actionable form of privacy for digital interactions.**

Background

It is part of the mission of the Federal Reserve System to promote the stability of the financial system, contain systemic risk, ensure the safety and soundness of financial institutions, and promote consumer protection.[43] Data, and the information derived from data, create both value and risk for individuals and businesses, and therefore, the economy. Given the scale and speed at which data are collected and leveraged today, the SF Fed seeks to facilitate an ongoing dialogue on these issues in order to better understand current and potential future systemic impacts to the U.S. In addition to the economy-wide impacts of data, two issues that are directly affecting supervised financial institutions are the developments around individual data control and portability structures,[44] and required compliance with new privacy laws.[45]

Navigating a path forward among such complex issues requires a collective approach between private and public entities and across sectors and disciplines. In an effort to facilitate this broad collaboration the SF Fed and FinRegLab,[46] a nonprofit innovation center that tests new technologies and data to inform public policy and drive the financial sector toward a responsible and inclusive financial marketplace, co-hosted a symposium on November 4 – 5, 2019 entitled, "The Role of Consumers in the Data Ecosystem". This event drew together 130 experts from regulation, consumer advocacy, for-profit entities, and academia, with experience across financial services, health, education, and international contexts. The symposium was a culminating event for this broader research project and explored the considerations and tradeoffs around individuals taking a more active role in managing data. Discussions covered topics such as balancing protection with individual agency, legal concepts of ownership, the challenge of informed consent, diversity and disparate impact concerns, and tensions between societal and individual goals.

This report is not a summary of that event. Instead it captures the foundational research that fueled the symposium discussions, and integrates the rich, interdisciplinary discussions from the

event into the analysis of the research and the subsequent ideas. Specific elements from the event that influenced this report are highlighted below.

- The Data Symposium started with a focus on individual agency, but there was an acknowledgement that agency alone is not enough. A framework for individual data protection is needed as well.
- Participants felt that data protection needed to balance reducing risks for individuals, with enabling ongoing use of data for innovation and research.
- A variety of experts found the framing of individual data "ownership" challenging. A key element of this discussion was the reality that data are jointly created with businesses.
- There was wide acknowledgment of the drawbacks to the current system of notice and consent. The idea of "legitimate purpose" test for data activities was discussed relative to its use in international contexts.
- There was broad consensus that frameworks for data protection and individual agency could not be developed by only the private or public sectors. This must be a combined effort.
- Gaps and complexity across current U.S. data governance laws were unpacked and debated.

Overall, the Data Symposium drove deeper and broader considerations for this research, and while many of the recommendations in this report were not specifically discussed during the event, it served as inspiration.

The Emergence of the Data Economy: Risks, Opportunities, and Challenges

By 2025, the sum of all digital data ever created globally is expected to reach 175 zettabytes, up from 40 zettabytes as of 2019, 1 zettabyte as of 2012, and 5 exabytes as of 2000.[47] To store all of that information in 2025, the world would need 23 stacks of CD-ROMs, each tall enough to reach from the Earth to the Moon.[48]

Industries vary in their contributions to this data explosion[49] and their use of the information produced. Across a growing number of economic sectors businesses increasingly need to generate, access, analyze, manage, and store data to stay competitive. The inherent potential of data can be seen in large market valuations for companies primarily driven by the number of users, rather than profitability.[50] Even in traditional industries, digitization of information is causing substantial creative disruption by reducing costs and barriers to entry, enabling greater tailoring of products and services, and providing new ways to predict and manage risks. New technology companies that depend on new forms and flows of information are growing rapidly.

For example fintech companies have grown from only 5 percent of the personal loan market in 2013, to 38 percent of the market in 2018.[51]

Individuals are also clearly participating in both the production, and consumption of data. Today 81 percent of Americans report owning a smartphone,[52] and nearly 70 percent own "smart" products such as internet connected doorbells or virtual assistants.[53] Over the next five years individuals' average daily digital interactions are expected to rise from 700 to nearly 5,000,[54] and many of those interactions will likely include the collection and sharing of data. Furthermore, individuals are increasingly generating data not only in the use of physical devices, but just by traveling in public and company spaces. Digital billboards are in use that identify phones that pass by and collect data from them,[55] and audio and visual recordings are increasingly being taken as we go about our daily lives, and are then packaged and sold to opaque buyers.[56] This revolution is creating new norms around pervasive data collection and broad uses of information, and while it is providing benefits to business and individuals, there is growing concern about its emerging risks.

The financial services industry, which has always been an information-dependent sector, is both a microcosm and an amplification of these trends and tensions. Financial services providers have been deploying data-based analyses for decades, even centuries, to calculate risk and return around lending, investments, and other products. The speed, scale, and reach of these tools were limited by the format of the information during early stages of digitization, but advances in technology have changed that. Improved electronic data access and other technical innovations are increasing the predictive accuracy, speed, and efficiency of data processes, as well as permitting increasing product personalization. At the same time, these activities are raising new versions of long-standing policy concerns around bias, privacy, safety, and stability. For example, use of data that omits certain populations or reflects the results of previous biased decision-making may lead to inaccurate credit predictions, improper biases, and exclusionary pricing.[57] There are also sharp disagreements around the risks and opportunities of data flowing between entities that sit outside of traditional financial supervision.[58] This has prompted discussion of what should lie within the regulatory perimeter, and how technology activities should be supervised.

Over the past 50 years, industry and policymakers have worked to keep up with the evolving issues presented by exponential rates of data generation and usage. As this revolution has accelerated, stakeholders have focused on two primary and interrelated concepts to manage the risks and opportunities of data: protection and individual agency.

Concepts of both individual agency and individual data protection, were first introduced in the U.S. in 1970 under the rubric of Fair Information Practices (FIP) presented within federal agency reports.[59] The original FIPs touched on the active rights of transparency or visibility into data activities, consent, correction, and the broad concept of protection. These concepts are part of this report's framework of active data rights. The approach of the original FIPs also highlights the

long-standing acknowledgement that these concepts are interrelated and it is more effective to address them together than separately.

In 1973 the Advisory Committee on Automated Personal Data Systems presented the FIP concepts to the Secretary of Health, Education, and Welfare. The FIPs remain relevant today, but since their development there has been significant technological change that has made some rights, such as consent, more difficult to achieve, and driven the need for new rights, such as data portability. The original FIPs stated that:

- There must be no personal data record keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about them is in a record and how it is used.
- There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

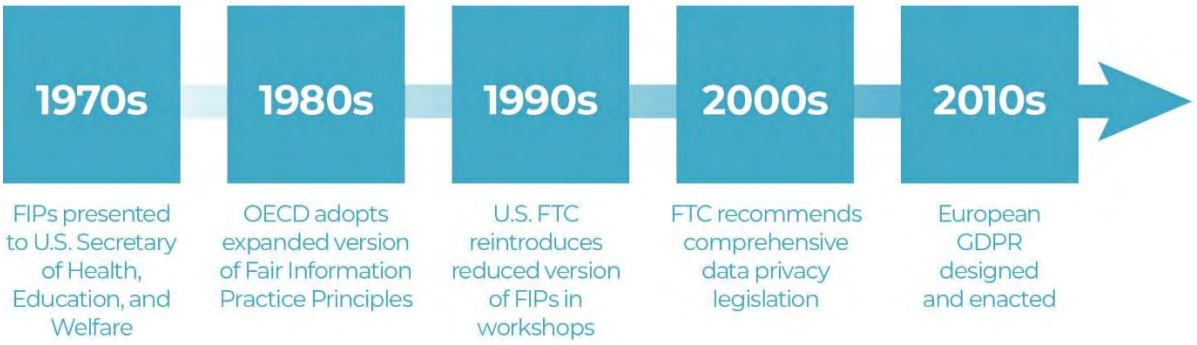
Reference[60]

The FIPs were the first discussion of standardized concepts such as transparency, consent, and security for the digital economy. The proposed FIPs were partially adopted into federal law in the U.S. through regulations such as the Fair Credit Reporting Act (FCRA) of 1970,[61] the Privacy Act of 1974,[62] the Health Insurance Portability and Accountability Act of 1996,[63] and the Gramm-Leach-Bliley Act of 1999.[64] These laws did not incorporate FIPs comprehensively but instead adopted select elements. For example the sector-specific approaches in finance and healthcare incorporated more elements of protection into statutes, but varied their provision of rights. Outside of specific laws, the Federal Trade Commission (FTC), through a series of public workshops in the 1990s,[65] encouraged the use of disclosures and seeking consent for data activities, and these became the primary forms of agency available to individuals in digital interactions. The broad use of notice and consent will be discussed in more detail in this report's section on *The Limitations of Individual Consent*. This piecemeal approach to the adoption of FIPs has resulted in a U.S. data protection system with a limited scope of applicability based on sector and entity type, and a lack of actionable data rights.[66]

Outside of the U.S., the FIP concepts gained greater traction, starting with efforts by the Organization for Economic Cooperation and Development (OECD). The OECD recommended Fair Information Practice Principles (FIPP) in 1980 that added detail and specificity to the original concepts.[67] These principles spread throughout the world and most recently have served as the foundation for broadening data governance frameworks in Europe, Australia, India, and beyond.

New frameworks such as GDPR, the Australian Consumer Data Right,[68] and constitutional privacy protections in India[69] have now established even broader concepts of data protection and individual agency that go beyond what the OECD proposed. These new governance regimes create a new baseline to consider relative to information practices.

Figure 2. Introduction of Fair Information Practices Concepts Globally



Both the increasing pace of data innovation and these new international responses are driving interest in revisiting comprehensive data governance in the U.S. There is a recognition that the sectoral focus of current laws is breaking down as the borders between business types and data types erode, and that existing U.S. frameworks do not support the current digital needs of individuals and innovators. Furthermore many U.S. entities with global footprints are already implementing data governance laws based in other jurisdictions.

This growing focus on U.S. data governance has manifested in a variety of ways. On the government side there has been a spate of activity, albeit much of it disjointed. Fifty states, D.C., and a number of U.S. territories have passed laws requiring notice to individuals if personal data has been breached.[70] In 2010, following the financial crisis, section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act established the right of individuals to access digital financial records.[71] In 2012, the Obama administration attempted to create a privacy bill of rights, but it was never taken up by Congress.[72] Most recently, California introduced the California Consumer Privacy Act (CCPA) which incorporates some of the newer information practices introduced overseas, like the right to deletion.[73] Other states are watching CCPA implementation and considering their own actions.[74] Data privacy is clearly on the minds of the 116th Congress,[75] which has introduced seven largely bi-partisan bills[76] that touch on data privacy in some way. A wide range of non-governmental stakeholders has also created an array of data governance proposals.[77] Trade associations, consumer advocates, academics, and more have produced white papers, principles, and legislative proposals, and have even formed entirely new entities to deal with this data revolution.[78]

While this level of activity speaks to the importance and urgency of U.S. data governance, the impact to date has largely been more inconsistency and uncertainty. The responses by Federal

and State regulators and legislators are contributing to fragmentation and complexity around what information, entities, and individuals are covered under various laws. Industry efforts are laudable but are encountering competitive and coordination roadblocks. As the U.S. continues to iterate on this patchwork of potential solutions, technologies that enable faster and more extensive data activities continue to evolve, a handful of companies are establishing increasing dominance across digital and physical commerce,[79] and other countries are developing their own competitive technologies and regulations. These realities complicate the evolution of U.S. data governance.

This history and the current challenges require a nuanced yet comprehensive approach. Although many stakeholders share broad conceptual goals for improving data protection and individual rights, they often disagree over the detailed tradeoffs, policy tools, and implementation standards. As reliance on data continues to deepen and expand across countries and sectors, policymaking will need to be bold, and incorporate a deep understanding of context and potential impacts. The U.S. is an exceptionally innovative and persistent country and these characteristics are needed for a fundamental shift in how the country approaches data.

PART 1: ANALYSIS

Reframing from "Data Ownership" to "Data Rights"

The increasing focus on individual data control in the U.S. has evolved into calls for direct "data ownership".[80] The focus on the term "ownership" likely stems from how data are treated by companies in business relationships. Data are treated as an asset by many firms,[81] and technology companies are amassing vast profits through data collection, processing, and use. Many of these companies reinforce an "ownership" narrative by highlighting that their services are free because customers are choosing to exchange data rather than money.[82] If data are already treated as an asset by businesses, and we are told that it has a tradeable value for us, it is a natural leap to think about data related to individuals as something they can "own" like property or money. The concept of "ownership" also resonates because it typically provides legal protections, like the rights that property owners have against intrusion into a home,[83] and gives individuals the freedom to generate value directly, like the ability to invest money, or rent out property.

Individuals themselves also use the phrase "my data" when referring to information related to themselves. Clearly there is a notion that information is part of us, and therefore should come with some legal weight that imparts protections, control, and potentially tradability. While this report agrees with the sentiment of legally protecting individuals, and providing forms of

individual control over data, the use of the term "ownership" to describe our relationship with data is challenging for a number of reasons.

- The structures that govern and enable some ownership, like tangible property, benefit from the fact that those assets are physical and cannot be copied. It is easier to control something physical. These characteristics do not exist with data, which makes implementing and enforcing traditional concepts of "ownership" more complex.
- How data are generated and managed is unique. Almost every piece of data has multiple parties involved, and most individuals need ongoing involvement from entities in order to transform data into usable information. Furthermore the term "ownership" can imply a level of responsibility for the maintenance and care of assets. Managing data systems in order to assert that level of care at the individual level is not technologically feasible today, and would require the involvement of other entities. While existing ownership constructs do offer opportunities for joint ownership and shared responsibility between individuals and entities, this kind of system would be particularly complex given the unique characteristics of data.
- A system that is primarily focused on data as an individual commodity that can be monetized, could create incentives that result in unequal experiences and treatment across groups and unintended social consequences.

This section will examine the challenge of implementing individual ownership frameworks for data, and analyze the potential consequences of doing so in more detail.

Because of these challenges, a shift is proposed away from the concept and terminology of "data ownership", and instead towards the development and implementation of "individual data protection" and "active data rights". Using this framing instead of "ownership" does not negate the inherent relationship between individuals and data, or the value of information for individuals, business, and society. Instead this provides a broader framing that does not stem from existing legal structures, and acknowledges the inherent complexity of data as an intangible resource that is shared between individuals, businesses, and the broader society.

Individual data protection: The *data security and conduct expected from business* with regard to information collection, processing, and use. Individuals do not need to take direct or affirmative actions in order to experience data protection.	***Active data rights***: *Actions that individuals have a right to take* with regard to information collection, processing, and use. Individual rights are supported by, and occur in addition to, data protection.

The Challenge of Creating Ownership Systems for Data

Existing legal structures of property ownership are a complicated initial framework to use when considering data governance. While some aspects of these long-standing systems are conceptually appealing, significant resources would be needed to adapt them to the nature of digital information, and some elements of ownership may actually impeded other policy goals.

The set of rules that apply to ownership of physical property like objects and land can't be applied in their entirety because it is not as easy to exercise physical control over electronic data. It is easiest to own something physical because control can be asserted directly on the asset, rather than having to depend on technology, intermediaries, or complex systems. When physical possession is broken apart from ownership it becomes much harder to define and to exercise control. There are scientific arguments that data are physical, though microscopic, and therefore they can be directly analogous to ownership of physical property.[84] Despite this argument any physical manifestation of data would be almost imperceptible and turning data into something that can be physically confined or controlled by individuals themselves depends entirely on technology to differentiate and control data that "belong" to an individual, and mechanisms to monitor those data as they flow among diverse businesses.

There are still significant benefits to managing, tracing, and reporting on data but this will be much easier to achieve on an aggregate, institutional level, rather than organizing a system that expects each individual to maintain and care for data separately.

There are examples of intangible "owned" assets, such as financial instruments (e.g., stocks) or intellectual property (patents, trademarks, and copyrights). These systems of intangible ownership are often complex markets with established legal and technological structures. Furthermore, these intangible assets are typically owned or managed by knowledgeable individuals, or professional intermediaries, who are well versed in the legal structures and remedies to protect, monitor, prevent impairment of, and maximize asset values. The copyright model is used today for information shared between businesses such as branding and design. Many consent forms on websites and mobile applications extend that model to individuals by seeking a perpetual license to collect and use information related to that individual. Business to business licensing of intangible assets typically has a limited purpose and frequency. Applying these complex systems to data about individuals is challenging because "licensing" can occur hundreds of a times a day, and entrenches a responsibility on individuals to understand, and agree to the purpose for this licensing. Individuals cannot participate as an equal party in these kinds of complex negotiations, especially across the huge volume of digital interactions. These issues will be discussed in more detail in a later section of this paper, *The Limitations of Individual Consent*.

In addition to data being functionally intangible, it is also challenging to assign the term 'own' to information because it is **non-rival, meaning that it can be used by multiple entities at the same time, without reducing the utility for any of those parties**.[85] There are two types of non-rival goods, public goods and club goods, which are differentiated by whether you can exclude other parties from using them.[86] Data can be endlessly copied, so there are limited ways to stop companies from retaining and using data if they received it at any point. This is another barrier to individuals asserting unique control as a part of ownership. In order to exclude other parties from using data that they previously had access to, individuals must again, rely on complex

governance and technical systems to monitor and prevent companies from copying and retaining data against their wishes.

Even without the additional complexity of intangibility and non-rivalry, ownership as a construct always requires administrative and legal mechanisms to create definitions, protections, and governance and enforcement systems. While many of these systems will still be necessary under a system of individual data protection and active data rights, the frameworks proposed in this report are designed to assign primary responsibility for maintaining data and overseeing its appropriate use to the institutions that handle the data, rather than placing the primary burden on each individual to protect themselves.

Consequences of Data Ownership Systems

Even if technical and legal systems could be developed to enable data to be directly controlled and traced, and its usage limited directly by individuals, other consequences could arise from applying, and implementing an ownership construct, especially one that emphasizes tradability or monetization of data.

The framing of "ownership" is easiest to apply when assets belong solely to one individual or entity. While there are concepts of joint ownership in existing property law, they are challenging to adapt to this context. Almost every piece of digital information about an individual is generated through an interaction between that person and multiple businesses. Businesses create the technology that enables data to be recorded and collected, and they transform data into usable, and actionable information. Everything from capturing information digitally, like a name, to performing human or machine analysis, requires investment on the part of businesses and much of that activity would not be possible for individuals to accomplish independently. Furthermore to keep using data over time it needs to be stored, transferred, and protected. While data are still intimately tied to an individual, entities play essential roles in the creation and use of information. For these reasons it would be challenging to demarcate when data are "owned" solely by an individual, and when one, or more companies could reasonably claim a stake in that ownership based on their fundamental contributions. Additionally, while much of this data activity is done to provide specific products or services, safe innovation with data can be positive for companies and individuals. Depending on how it is executed, differentiating "ownership" across all of the parties who are involved in this ecosystem could limit the incentive and/or ability for companies to create new intellectual property. The U.S. Supreme Court has identified this tension of shared interest in ruling that data are business records[87] and also that individuals retain rights within those business records.[88] A related ambiguity of "joint ownership" is data that relate to multiple individuals. Examples of this include joint financial accounts, peer-to-peer transactions, and technologies that observe public spaces such as new digital doorbells.

Furthermore, even if systems were developed to differentiate when data "belong to" individuals versus a businesses, information is most valuable in aggregate.[89] For a direct "ownership" system

with a goal of commoditizing and monetizing data individually, value generation would need to be tracked over time, aggregated, technologically tied to individuals, and after all of that it may not represent a significant amount of money. As discussed above, these kinds of individual systems would be exceptionally complex to develop. There is a potential for intermediaries to step in and develop the technology and systems for all of this, but it would be essential that their incentives are aligned with the individual. For example, unaligned intermediaries could try to sway individuals to sell data at lower prices. Additionally, paying intermediaries directly to act in individual's interest could be inaccessible for many. Concepts for these kinds of intermediaries have been proposed,[90] but they do not address the issues of incentives and socio-economic differences that could play out in system of individual data monetization. The potential of intermediaries will be discussed in more depth in a later section of this paper titled, *The Crucial Challenge of Equality*. There have also been proposals for "data dividends" that could be provided to individuals as compensation for data collection, but many of these ideas center on taxes that would be levied on companies, and then the government would redistribute those funds to individuals. These models don't necessarily assume individual data "ownership", and take a more collective approach.[91]

In addition to the risk that a direct ownership model could limit innovation incentives, and would not actually provide a significant opportunity for individuals to generate value individually, there is a risk that a marketplace for individual data sales could allocate resources in a way that would be suboptimal for other social considerations. As described above, data are non-rival and challenging to exclude others from. This places data in the category of public goods, and there is a long-held view that markets fail at effectively allocating these types of resources.[92] Some scholars even explicitly define data as public goods because information about individuals can be used to extrapolate about other individuals, and therefore it can both benefit and harm everyone collectively, like the environment.[93] For example, if enough individuals within a certain demographic group share, or "sell" information, it can be used to profile or target others, even if they did not directly share or "sell" information about themselves.[94] There are those who take this a step further and use the term "data pollution" to describe the unintended harms of individual data use, and misuse, on social interests and institutions.[95] It is also unclear how financial incentives around the sale, or retention, of information as an "owned" asset could impact social considerations such as public research. Certain populations sharing more information than they otherwise would because of monetary incentives could lead to unexpected variations in the representativeness of data sets and new potential biases.

Creating a marketplace for data as tradeable, "owned" personal assets could also result in the risks and benefits of data not being evenly distributed among individuals directly involved with this kind of system. Businesses may value information about individuals differently. For example, if an individual has a high-net worth, details about their shopping preferences may be more valuable to businesses wishing to sell them products. A market for selling individual's information could lead to price variation that would impact populations of people differently. That variation

could be positive and provide disadvantaged populations with new revenue, but it could also result in lower values for poorer populations. Additionally there could be an incentive to sell information to gain income, while higher-wealth populations are able to retain more control and privacy over their information.[96]

While equality and complexity absolutely need to be considered with individual data protection and active data rights frameworks as well, this report argues that the unknown incentives and allocations that individual monetization of data could introduce is more challenging to address. Without the introduction of financial incentives, there is evidence that individual agency and control in determining the right balance of benefits and risk relative to data can provide a larger public benefit than either business or government unilaterally determining where information flows.[97] This highlights the importance that individual agency can play within a data governance framework without the need to create monetary incentives.

More research is needed to fully consider the universe of benefits and risks to direct individual "ownership" and monetization of data, but these ideas must be carefully considered in light of the challenges and potential negative interactions described above. If a limited market for individual data can be safely managed from both a legal and technological standpoint, there remains a potential to compensate individuals, on a smaller scale, directly or indirectly for data. Services that offer a safe exchange for data could be more accessible to the poorest populations, and there are examples of these kinds of exchanges today. For example when individuals are paid to take surveys, or offered subscription models where advertisements are removed. There are even new models emerging that blend these concepts and pay individuals to see advertising.[98] Data clearly have value, but assigning that value at the individual level, across all data would be complex and could create unintended consequences. The value of information also extends to business and society as a whole, which is underappreciated if it is defined solely as an individual asset.

The Limitations of Individual Consent

In addition to conversations around the potential for data "ownership" and what that could mean, another important debate around individuals playing direct roles with regard to data is the effectiveness of seeking individual consent to perform data activities.

A system of "notice and choice" has been used broadly in the U.S. since the advent of the World Wide Web itself in the 1990s.[99] In the mid-90s the Federal Trade Commission held a series of workshops and hearings to explore privacy concerns that were raised by the collection of personal information online.[100] These efforts highlighted the Fair Information Practices, described earlier, but also focused on entity self-regulation in the new digital ecosystem. Notice and consent were encouraged as a form of self-regulation by the FTC, and this system also provided a stronger mechanism through which to regulate privacy. The federal government has very

limited authority over activities related to information collected digitally by companies. The FTC Act[101] prohibits unfair or deceptive practices, and if a company discloses digital activities, but then does not comply with their own disclosure, it provides an immediate avenue for enforcement. Thus, encouraging notice and consent gave the FTC a new avenue through which to consider, and enforce the FIPs.

Building upon this history, in 1998 the FTC provided a report to Congress about the state of online privacy. The report continued to call for self-regulation, but noted that industry was not developing effective disclosures, and companies were not actually following the practices that were disclosed.[102] The report indicated that there was a need to implement the FIPs across the market and that the agency saw no evidence of an effective self-regulatory system. This resulted in the 1998 Children's Online Privacy Protection Rule (COPPA).[103] The FTC also provided Congress with a formal recommendation to implement federal data privacy legislation in 2000, but it was subsequently withdrawn.[104] Interestingly, certain sector-specific laws predate this era, such as the Fair Credit Reporting Act (FCRA) and do not rely on consent. Other laws such as the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm–Leach–Bliley Act (GLBA) were developed in this same time period and incorporate a greater emphasis on consent. These laws will be discussed in more details the upcoming section on *Current U.S. Data Governance*.

Notice and consent systems, either mandated or used as a form of self-regulation, place an expectation of responsibility on the part of individuals to monitor and respond to a company's data activities. **Choice is valuable to individuals and deeply interwoven into current law, but there are significant limitations to its ability to indicate preferences and it cannot be relied upon as a form of data protection.** This section will delve into the challenges of gathering and interpreting individual preferences for both protection and agency through consent mechanisms. Because of these limitations, this report proposes deliberate governance structures that define acceptable data practices, reducing the role of consent broadly, and improving the process for informing individuals and collecting consent when it is necessary.

The Current State of Consent

Today as long as companies adhere to their own disclosures, and individuals accept those disclosures, there are few limitations on what entities can do with data.[105] This has enabled businesses to monetize information in ways that are significantly removed from the original purpose for which data were collected.[106] Additionally, companies that want to demonstrate that they use more secure and protective data practices can struggle to communicate, and thus differentiate themselves, on these important metrics. While it is currently the responsibility of each individual to refuse products and services if they are uncomfortable with data practices, evidence shows that the disclosures that describe companies' activities are typically not read by individuals, and when they are read, they are rarely understood.[107]

Individuals are not able to engage effectively with disclosures for a variety of reasons: Information is often frustrating to access, and the paths and prompts to do so are presented inconsistently across entities. Disclosures appear in different locations and are presented at different times. Frequently, a consent request appears next to only a notification that a disclosure is available, forcing individuals to navigate to another location to read the actual disclosure. Laws have created some standardization in the presentation of disclosures in the financial services industry, which speaks to the value of consistency, but those efforts have been largely considered ineffective.

If individuals are able to find disclosures, they are almost impossible to understand for a variety of reasons. Disclosures are typically too long to reasonably read, with some researchers estimating that 25 full days are needed to read every disclosure for the websites visited by an individual over a year.[108] That estimate does not account for mobile-phone applications, and the increasing ubiquity of internet connected devices that also collect significant amounts of information.[109] If individuals find, and elect to take the time to read every disclosure, the content would be largely incomprehensible. Tests show that readability scores for common disclosures are lower than dense philosophical texts, and even lawyers would struggle to understand them.[110] In addition to using jargon, and legal phrasing, information about activities and practices are typically described in vague terms such as for "business purposes" or "service improvement", which could span a huge spectrum of activities. These terms provide minimal clarity on what is truly necessary for the use case or whether the potential data risks to individuals are worth that use. The length, density, and opaque language of disclosures are not designed for individual consumption. They instead provide regulatory compliance, legal coverage, and in some cases can enable entities to maximize their ability to use data.

Finally, if individuals did understand the complexity and density of disclosures, there is no opportunity to negotiate for different terms of the relationship. Notice and choice is typically a contract of adhesion,[111] meaning that the only option that an individual has if they do not agree with the outlined terms is to not use the service at all. Given the prevalence of these binary take-it-or-leave-it contracts across digital services, individuals either essentially have to cut themselves off from digital product and service options, or have to spend significant resources to identify and vet the alternatives that are more protective.[112]

Given these realities, it is not surprising that surveys show many individuals have largely given up trying to manage their data privacy and security. A Deloitte survey found that 90 percent of individuals accept the terms of consent without reading them.[113] Clearly, individuals do not, and likely cannot, read the disclosures they are presented before making digital decisions and, even if they do, they cannot actually act upon their preferences. Therefore, the United States' broad system of notice and choice is neither informed nor participatory.

Despite the barriers to providing informed and meaningful consent, consumer surveys still indicate that people want to receive information and play a role in managing information.[114] The

tension between this desire for control and the lack of engagement with disclosures and consent (the primary mechanism individuals have to assert control) is commonly referred to as the "privacy paradox".[115] As researchers have explored this tension it has become clear that beyond the readability and accessibility of disclosures, there are additional factors that are causing this disconnect between individuals saying they want control, but not engaging.[116] These factors will be discussed below. Given the potential of individual agency to help allocate data as a resource, and the important preference reported by individuals to be involved in this ecosystem, **it essential to both respect individuals' desire for control and choice, while acknowledging the challenges and limitations to truly providing that.**

The Challenge of Improving Consent

Consent is heavily influenced by the digital context and format in which it is presented. Research has shown that is easier for individuals to interact with, and consent to, binary choices rather than complex choices, but granular consent is more effective at revealing preferences.[117] When choices are presented to individuals, they are commonly opt-out rather than opt-in decisions, and research has demonstrated repeatedly that individuals rely on default settings and rarely proactively opt-out of presented activities.[118] Evidence has also shown that the ways in which consent requests are phrased can change responses, and digital context, such as the professionalism of a website, can have unexpected effects. For example, researchers found that individuals were *more* likely to disclose sensitive information if the digital presentation was less professional, while more professional-looking websites cued them to think about potential risk.[119] This dynamic could result in consent being more easily obtained by entities without a strong focus on privacy, while individuals may avoid engaging in positive data relationships with more secure companies. Other research has demonstrated that even small implementation choices, such as where consent appears on an individual's screen, can influence their ultimate choice more than the content of the disclosure itself.[120]

In addition to the digital context in which disclosure and consent are displayed, choices are also heavily influenced by human psychology and the physical environment, such as time pressures. There is a phenomenon known as "information avoidance", and while individuals may express a preference for more information, they can easily get overwhelmed and start to avoid details altogether that run contrary to their preferences.[121] There are also phenomena that have been identified in social science research such as "risk discounting", "optimism bias", and the desire to take the path of least resistance. Risk discounting refers to the struggle for individuals to calculate risks in the future.[122] Optimism bias is the tendency for individuals to over anticipate positive outcomes, and under anticipate negative outcomes.[123] If disclosed information is hard to find, read, or understand, or it runs contrary to an individual's preferences, the disclosure may be ignored in favor of simply accepting the terms.

As mentioned above, attempts to standardize disclosure information about data activities to make it more accessible, such as the financial model privacy disclosure created by eight financial regulators, have been largely ineffective.[124] The model disclosure does not go into depth around the complexities of how entities use and share data, it still allows for dense and vague language, and it does not address the realities of human behavior. Researchers found that use of the model forms could actually result in less transparency when companies only included required information, simply omitted information, or in some cases just copied the forms sample text. The model forms were at times effective in demonstrating differences among company practices, but comparing differences and selecting among them was sufficiently difficult that researchers created their own interactive website to help individuals review practices.[125]

Thus, even if companies are using disclosures to be transparent and distinguish themselves through high quality data security and conduct, there is no easy, or demonstrably effective way to signal those things to individuals. Behavioral science research indicates that individuals seek transparency and prefer more information,[126] but the combination of cognitive realities, broad and dense disclosure language, and the complexity of technology and data systems means individuals have no way of effectively judging entity practices.

An Alternative to Consent - Legitimate Purpose Requirement

For the reasons outlined above, some stakeholders are considering a baseline legitimate purpose requirement for the collection, processing, and use of data that would apply *prior* to an entity performing any activity on data or establishing a relationship with individuals, and could not be superseded by consent. **This paper defines legitimate purpose as requiring that any data related to an individual that are collected, processed, and used are necessary for the specific product or service that is being requested, and that those activities do not create disproportionate risk to the individual.** The expectation is that this requirement would cover all entities engaged in data activities, and would be part of a comprehensive individual data protection framework. This framework is described in more detail under the section titled, *The Foundation: Individual Data Protection.* Complying with legal requirements and sharing data as part of essential business partnerships would be treated as necessary for the specific product or service, but secondary and tertiary uses of information, such as building new products and monetizing data outside of the original use case, would require additional compliance and communication steps. A necessity standard is not intended to be overly restrictive, and an example of the potential breadth can be found in Europe's updated Payment Service Directive (PSD2). Under PSD2 certain partnerships are considered a necessary part of doing business, and the directive creates a clear, but limited role for these entities as silent parties, without leaving the burden on individuals to determine whether different business relationships are truly necessary.[127]

The concept of an underlying legitimate purpose requirement across all activities is distinct from GDPR which outlines multiple lawful bases for processing information.[128] Lawful bases under GDPR include consent, legal requirements, or "legitimate interest" of the entity collecting, processing or using information.[129] The primary distinction of legitimate purpose is that consent alone would not be a lawful basis for data collection, processing, and use. Additionally, legal requirements would be captured within the definition of legitimate. "Legitimate interest" under GDPR is similar to the legitimate purpose requirement described here, but there are also important differences. "Legitimate interest" is more broadly defined, and centers on the interests of the entity as long as those meet certain criteria. The first criteria is the most important, which is whether the company has a legitimate interest in the activity being completed. This focus on the entity's interest means that generating revenue could be considered legitimate.[130] The additional criteria include whether the data activity is necessary to effectuate the entity's legitimate interest and whether the entity's interest is overridden by the interests or fundamental rights and freedoms of the data subject. Since GDPR places the criteria of "interest" first, that means that the subsequent necessity test is also broadened. For example, if monetizing data is considered in the interest of an entity, then any activities performed to complete that sale of data would be considered necessary. The legitimate purpose requirement considered here instead focuses on the safety, and necessity of the activity for the individual, instead of the entity. This shift inherently narrows the scope away from tangential activities such as resale of data for generating revenue, which may be unnecessary for providing the product or service itself. But, the legitimate purpose requirement would include activities such as fraud prevention which creates safety for individuals, and can also fall within GDPR's "legitimate interest" definition. Legitimate purpose also focuses more heavily on mitigating risks for individuals, rather than asking entities to balance their interests against an individual's. A similar baseline approach to requiring a legitimacy or purpose test prior to consent has also been proposed in India[131] and New Zealand,[132] with some variations.

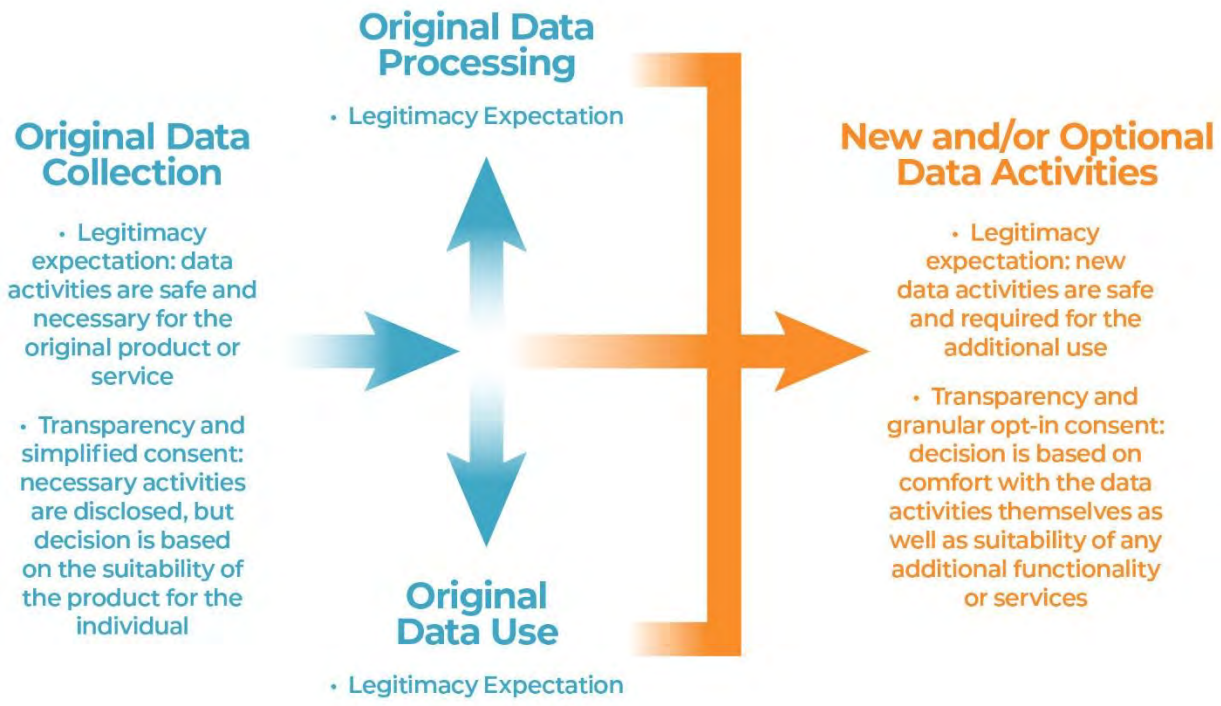
The Consultative Group to Assist the Poor (CGAP) recently released a report[133] suggesting a legitimate purpose requirement, and echoing many of the sentiments in this analysis. There are some differences between that proposal and the one offered here. CGAP suggests that de-identified data would not fall within a legitimate purpose requirement, while this report takes the position that given the shortcomings of current anonymization technology, "de-identified" data related to an individual should not be treated differently until processes are demonstrably improved. The challenges of anonymization will be examined in more depth in Part 2 of this report under, *The Foundation: Individual Data Protection*. Another key difference is that CGAP proposes that entities only be permitted to use data in ways that are in the "interest" of the individual. The "interest" of the individual can be interpreted narrowly to mean that the activities would not be harmful, or could be interpreted more broadly to mean that activities benefit the individual in some way. As will be discussed in more detail in the upcoming section, *The Crucial Challenge of Equality*, it is challenging to define where benefit truly accrues with regard to data uses, and what is in the best interest of each individual. Given this challenge, this research

proposes a slight variation to CGAP's proposal, by not explicitly requiring that the legitimate purpose requirement rise to the threshold of a broad definition of "interest" or benefit to an individual, but instead focuses only on the thresholds of safety and necessity.

As discussed above, there is still value in engaging individuals in data decisions, and given how integral concepts of choice are to U.S. legal structures, it is likely beneficial to retain forms of consent within a bundle of active individual data rights. With a legitimate purpose requirement the role of consent could be greatly reduced across the large volume of daily, and more standardized, digital interactions. For example, for activities that are safe and necessary for the original product requested, a consent prompt could focus solely on the benefits and suitability of the product, instead of expecting individuals to review and accept details about the data activities themselves.

If entities want to collect data that is not necessary for the requested product or service, or want to use previously collected data in new ways, a more granular form of opt-in consent could be used that provides additional context around new activities. This more granular form of consent could enable new value generation from data, but in a way that engages individuals more directly in that additional exchange. New activities would still need to be safe for individuals, and be limited to what is necessary for the new purpose. Additionally, any consent that is provided could not override the legitimate purpose requirement for either original or new activities.

Figure 3. Two Forms of Consent with Legitimate Purpose



These two forms of consent could help highlight for individuals the point when information is moving away from original, expected activities, while reducing the volume and complexity of consent for more standard, ubiquitous activities. This also allows for previously collected information to be leveraged for new innovation, while creating a clearer separation between activities necessary for the original product or service, and additional activities a company may want to engage in for their own interests and benefit. These forms of consent will be discussed in more detail in Part 2 of the report within the section, *A Proposed Spectrum of Active Data Rights*.

There remains a risk that individuals would not engage with these secondary, granular forms of consent, and entities would default to using this version of consent to broaden the activities they could perform with limited oversight by individuals. This highlights the importance of retaining a legitimacy expectation that requires activities to be safe for individuals across all activities, but more research is needed to determine when consent is most appropriate, and how to offer that to individuals in a more meaningful way.

Where consent remains, clear, actionable, and concise language should be prioritized, rather than vague or generic descriptors.[134] It also may be beneficial to separate out information that is provided for transparency, from information that can help individuals with no technical or legal backgrounds make decisions. Information, such as security protocols and legal relationships, can be available for individuals to review, but few have the knowledge or time to use that in decision making. There are efforts underway around the globe to leverage design principles for communication,[135] and transparency initiatives are being developed in business contexts[136] that could potentially be leveraged for individuals to create a common language and understanding around digital practices.

This section proposes a foundation of legitimate purpose that would replace the current system of "privacy self-management" through notice and choice, but significantly more detail is needed around the design, implementation, and oversight of such a requirement. The design of a legitimate purpose requirement could range from principles-based guidance with only enforcement to incentivize compliance, to prescriptive menus, techniques, and relationships that are deemed acceptable and directly supervised through reporting and examination. There could also be a role for an entity, or agreed upon process, that reviews proposed activities and attests to their legitimacy. While not directly analogous, standards such as International Organization for Standardization (ISO)[137] could be used as models. The FCRA is an example of a law that limits the use of data (credit reports) to permissible purposes without the need for individuals to monitor this activity through consent, though purpose limitations are not imposed on the reporting agencies that compile the information in the first place, only on the entities who subsequently use the information. The law also layers on individual consent for additional uses of credit reports beyond their original intended purpose. Lessons from this law, and its approach, will be discussed in more detail in the section titled, *Current U.S. Data Governance.* Any kind of final design should incorporate reasonable avenues to address unique situations and new product

requirements. This approach may limit the ability of firms to quickly innovate with large compiled data sets, but it relieves the burden currently placed on individuals to engage, understand, and effectively judge the appropriate balance of risks and benefits across the breadth of the digital ecosystem.

The Data Privacy Principles recently released by the American Law Institute highlight that there may be a challenge to a legitimate purpose requirement in the U.S. because lower courts have upheld an expectation of free flows of information under the First Amendment as commercial speech. This issue was also raised in a challenge to the constitutionality of FCRA, but the Supreme Court declined to take the case.[138] Limiting flows of information to a lawful basis is codified in the constitution of the EU, but the ongoing debate in the U.S. around whether information activities are protected as free speech by businesses[139] could create additional challenges to incorporating this concept here. Despite this setback, the American Law Institute also recommends limiting the use of data for downstream activities unrelated to the original collection purpose.[140]

The Crucial Challenge of Equality

Defining the scope and nature of potential requirements like legitimate purpose, as well as the appropriate role for individual agency, is especially challenging given the diversity of U.S. citizens. Some groups may experience outsized benefits from the use of digital services, while others may be exposed to unique risks through the collection and use of data. The idea of active data rights is particularly attractive because it allows for diverse individuals to customize their digital use and footprint. But, because digital interactions impact populations differently, it is important to examine whether there are barriers to exercising broader active data rights if they were to be established. This section will address the challenges of actually using active data rights, and will analyze whether well designed intermediaries could play a role in making individual agency more accessible across diverse populations.

New data and new digital technology, particularly in financial services, are seen as an opportunity to better support underserved populations.[141] But while the use of technology to reduce cost, or enable free services, is commonly cited as enabling more equitable access, there is a lack of sufficient research on the preferences of diverse preferences to accurately judge what tradeoffs those populations want to make. In fact new international research indicates that assumptions, such as poor individuals preferring to trade data for services rather than pay more, may be incorrect.[142]

Simultaneously, disadvantaged groups may experience outsize harms as a result of data activities and are faced with structural barriers to using technology for their own benefit. The most immediate risks of data loss and misuse, such as identity theft and predatory targeting, happen disproportionately to already disadvantaged groups.[143] These kinds of data harms also

typically require time and resources to resolve, which can compound their impact.[144] Some groups, such as women[145] and immigrants[146] also experience unique, and heightened risks with regard to certain data, such as location or citizenship information.

Technology can reinforce existing racial, gender, and socio-economic biases as well. Evidence reveals bias occurring in everything from physical sensors[147] and photo recognition technology[148] that do not register darker skin tones, to machine learning algorithms that taught themselves to penalize women based on historical resume pools.[149]

Technology itself is also not equally accessible to all people.[150] Educational attainment, which is closely associated with socio-economic status, is positively correlated with more digital knowledge[151] and higher-income Americans have more devices through which to access digital services[152] and therefore more tools for data control. These factors taken in combination indicate that while disadvantaged populations may benefit from the collection, processing, and use of data, they also face more risks and larger barriers to using and navigating technology. Therefore, **if individuals are given more agency over data, there need to be implementation systems that overcome structural barriers to actually using those tools**. It is also not surprising that underserved populations typically seek more government intervention in reasonable oversight standards for data protection.[153]

All of this underscores the importance of both appropriately calibrating broad-based individual data protection across different risks, as well as enabling data rights in the U.S. that work for diverse needs and preferences. If the design of cybersecurity, conduct standards, and systems that support active data rights are tied to an average of U.S. experience and preferences, we risk excluding populations that have the most to both gain and lose.

Calibrating Active Rights in Addition to Protection

Effectively calibrating individual data protection that addresses populations with varying sensitivities is challenging, but the larger challenge may be creating systems for acting on data rights that are equally accessible to diverse populations.

As discussed in the previous section, *The Limitations of Individual Consent*, individuals commonly desire information and choice, but struggle to effectively act on it. Populations with less access to education and technological resources may therefore be at an even greater disadvantage in understanding, and acting upon information. This dynamic could be exacerbated if active rights, such as the ability to request, correct, or delete information, are implemented without accounting for the cognitive and resource management burden that this could place on individuals. In particular, **if systems are not consistent, and do not work together, it requires a much greater effort to manage information and take actions**. While individuals have limited active data rights in the U.S. today, there are some opportunities to proactively request information, delete certain records, or request corrections. These

opportunities are due to a patchwork of Federal, State, and international laws, and positive business practices, but that means that individuals need to understand and navigate these different realms if they wish to exercise particular rights, or take advantage of increased protections, that are available under various regimes. Furthermore, if individuals want to take available actions, such as using new data dashboards or requesting access to information, they have to do so separately across every entity, with no consistent interfaces or tools. The systems in place today for controlling data require a high-level of digital literacy and resources, which may make them inaccessible to most people, and put certain groups at a particular disadvantage.

In addition to the fact that actively exercising data agency can be resource-intensive, the unique privacy sensitivities of certain groups, such as immigrants, may make them cautious about using new rights at all. For example, individuals may be reluctant to exercise rights to move information between entities if they are not confident that their data will be protected during and after transfer. This highlights the importance of data protections that work in tandem with well-designed systems that enable active data rights across different needs.

The challenge of enabling the actual use of data rights across disconnected systems, and accounting for diverse needs and bandwidths, raises the potential for intermediaries that can act on behalf of individuals.

The Potential of Intermediaries

A number of ideas have been proposed that could act as a layer between entities and individuals. Some of these proposals were designed with specific markets in mind, such as advertising, and may be intended to replace the need for detailed policymaking around data protection and active rights. Other concepts could help supplement a data policy framework in order to create more individual customization and reduce management burdens. This section will discuss the challenge of relying solely on intermediaries in lieu of broader structures, while also considering which concepts could be used in tandem with policy to help address diverse needs.

FIDUCIARY MODELS - SHIFTING THE RESPONSIBILITY OF CARE

There have been a number of proposals to create a fiduciary duty for companies that handle data.[154] This could be either a legal, or ethical, responsibility for entities to act in a prudent and trusted manner towards individuals that they engage with, meaning they show care and thought for the future impacts that data activities could have. Expecting companies to show care towards individuals could lead to more product personalization, and suitability considerations for entities that have a direct relationship with individuals, as well as for large middleware, data-focused firms, such as aggregators. Fiduciary models are a familiar structure, appearing in health, legal, and financial relationships, and this duty of care can be mandated by law, or may be self-described and variable. The nature of many current data-based business models can make self-enforced fiduciary responsibilities challenging, though there may still be value in considering

how businesses can voluntarily identify, and align activities to the best interests of individuals, in addition to upholding individual data protection and enabling active data rights.

Allowing firms to define how they can best work on behalf of individuals could leave positive room to customize approaches to diverse populations, but it is difficult to define what is truly in the best interest of individuals or what is "suitable". Recalling an example used earlier, assumptions that lower income individuals prefer lower product prices over data protections may not be the case for all groups.[155] Additionally, many of the incentives of data-centric business models, such as targeted advertising which depends on significant data collection and sharing among parties, may run directly contrary to an individual's preference to limit those activities. This puts companies in a challenging, and fraught position. They would be expected to constantly decide between the beneficial interest of the company and what is most suitable for individuals.

There may be more natural alignment between the services of doctors and lawyers and the preferences of their patients and clients, than between businesses whose revenue is based on wide-spread data collection and use, and privacy-seeking individuals.[156] But even in cases where interests seem more aligned, such as healthcare, formal restrictions have been necessary in situations where incentives are at odds, such as doctors owning labs and testing facilities while prescribing those services.[157] Finally, as discussed in the section, *The Limitations of Individual Consent*, individuals are at an inherent disadvantage in understanding digital contracts and have limited ability to truly negotiate for better terms. Variable approaches to a self-defined and enforced fiduciary obligation would put the burden on individuals to determine whether a company's concept of "best interest" aligns with their own.

Given these challenges, a broad data protection responsibility placed on all entities may provide a more consistent path forward than depending on variable, or self-declared fiduciary standards. As discussed earlier, it is also challenging to require a judgment around product benefits or suitability. It may make sense to impose consistent fiduciary duties by law on entities who play a specific role in helping individuals determine the suitability of particular data activities, but given the diversity of business models and the complexity of data impacts, the legitimate purpose standard could be a more helpful generalized baseline. If a fiduciary expectation was consistent, formalized, and did not require a beneficial determination, it would more closely resemble the proposals presented in this report.

TRUST MODELS – POOLING PREFERENCES

Another proposed intermediary model is "data trusts"[158] or "data cooperatives"[159] which bring together groups of individuals with similar preferences. These models can help individuals distribute the burden of understanding, and acting upon data choices among a community, and some of the proposed examples use collective bargaining power to help individuals capture more direct value for data.

As discussed in the earlier section, *Reframing from "Data Ownership" to "Data Rights"*, data have more value in aggregate. In some trust designs, a group of individuals could pool data related to themselves and therefore increase their aggregate value, creating a stronger position for negotiation and potential sale. Though as described earlier, direct sale of data by individuals raises a number of concerns. A different trust design, focused more on helping individuals manage their privacy settings with companies, could enable individuals to self-select into groups with similar privacy preferences, and have designated trustees take actions on their behalf.

Similar to the design of trusts in financial services, and fiduciary obligations, there remains a core challenge of aligning the goals of the intermediary layer with those of the individual. A data trust would require management, technology, and sustainable funding. If individuals themselves were required to collectively pay for the trust, it could exclude populations who do not have the funds to contribute. If the trust is funded in a different way, then it is important that those interests do not run contrary to the goals of participants. Some groups[160] are exploring existing cooperative models such as labor unions to identify how governance could work for this kind of design.

CENTRALIZED MODELS – NEW INTERMEDIARIES

A final model considered in this research are centralized intermediaries that would be distinct from both the entities who engage in data activities (fiduciary model), and individuals coordinating among themselves (trust model). Centralized models could create standardized mechanisms for using active data rights, enabling individuals to take action in one place instead of across multiple entities. Centralized models could also be used to store and protect data, and even consolidate it for use in public research and to facilitate competition. This kind of model could be either a public or private entity, but there are public examples in a number of countries. The Indian Government's digilocker[161] enables individuals to store government benefits data in a publically provided system and then recall it when needed. The European Union is considering creating a "central market for data" to enable innovation and competition.[162] These centralized functions are a blend of directly enabling individuals and capturing broader social benefits of data. A core challenge of centralized systems though is that they rely on a single entity that can be attacked or corrupted. Private centralized intermediaries are also challenging for the reasons discussed previously, creating aligned incentives and making it accessible to all groups is difficult.

All of these models have the potential to take some burden off of individuals when exercising active data rights and could help customize approaches to account for unique needs, but they are dependent on effective design and aligned incentives. Relying solely on intermediaries instead of comprehensive data protection and active data rights framework may not be an effective path forward given the challenges discussed above. There are efforts underway across the world[163] though to understand the potential roles for different institutions and intermediaries around data. These concepts can also be modified or combined with each other to help mitigate their risks while providing more management support to individuals.

Unfortunately, it is unlikely that any of these approaches can fully address the challenge of equality across diverse data preferences and experiences. **Clearly the design of a comprehensive data governance system needs to be attuned to differing risks and bandwidths of a diverse population, and there are benefits to considering how entities can participate alongside individuals to act upon data rights**. Additionally, figuring out how to incorporate equality and diversity into data governance does not need to be a perfectly linear process. There are strong existing civil rights and antidiscrimination laws that could be incorporated, and brought to bear within a comprehensive individual data protection and active data rights framework as a first step.[164] There are opportunities to learn from international experiences, and **as broad laws, such as CCPA, come into effect, special attention should be paid to how these policies impact diverse groups**. More research is also needed to understand the unique experiences of different populations and uncover areas where disparate impacts could occur from data collection, processing, and use. This kind of research could include an assessment of differing views on the scope of protection and definitions of legitimate purpose across different populations in the U.S.

Balancing Individual Rights and Collective Goals

As a country we have many policy goals intended to improve outcomes for individuals, the economy, and for society as a whole. Similar to the challenge of balancing data protection and active rights across diverse needs, policymakers will need to consider the potential interactions between broad data governance and other societal goals such as competition, innovation, and stability. Promisingly there are also situations where policy goals could work in tandem with each other to achieve even better outcomes. A report by Oliver Wyman titled, "Data Rights in Finance: Key Public Policy Questions and Answers"[165] explores these dynamics in financial services, though many of these tensions and opportunities exist across sectors. This section builds upon that work through a multi-sector approach that incorporates the distinct concepts of individual data protection and active data rights.

Evidence suggests that approaches to data policy that focus only on narrow goals could have suboptimal effects. For example, policymakers and citizens may limit the amount of information that can flow in order to achieve more privacy for individuals, which in turn could reduce opportunities to improve financial inclusion and competition. Maintaining large flows of information to feed innovation may improve the global competitiveness of U.S. technology, but it could also have cybersecurity risks, concentration risks, and stability implications for the country. It is important to acknowledge and weigh the potential externalities of data governance across policy areas in order to identify areas for harmonization, mitigate negative impacts, and ensure we are triangulating to the desired outcome. There is also hope that advancements in anonymization techniques and privacy-enhancing technologies could help reduce some of the

tensions around collecting and using data for market and public benefits, while still upholding individual protection and agency.

Competition

While data are inherently non-rival and can be used by many entities at the same time, the lack of consistent expectations around data practices has led to huge variations across sectors and companies in the ability to collect, store, and leverage information. The technological capacity to perform data activities, and access to large amounts of stored data can impact the speed and quality of innovation and growth across the country, [166] and they can give companies a significant competitive advantage.[167]

The ability for individuals to port data from one entity to another, both as a one-time occurrence and through ongoing flows, is seen as an avenue to increase competition by addressing this variable access to data across companies. This was a clear goal of the United Kingdom's concept of Open Banking which creates a system of sharing information between financial institutions and other kinds of service providers.[168] An active right to data portability, and Open Banking structures, streamline opportunities for individuals to switch providers and ideally makes data more accessible for businesses. Unfortunately, this promise of competition depends heavily on individual awareness of, and confidence in, new systems for moving data. As discussed in the earlier sections, *The Limitations of Individual Consent* and *The Crucial Challenge of Equality*, it is difficult for individuals to judge data activities and their potential impacts, and exercising agency rights requires attention and resources, especially as new systems like open banking are introduced.

Until better forms of communication are developed, and tools are available to help individuals make judgments and take actions, new data rights such as portability, and transfer structures such as open banking, may not meaningfully increase competition. The United Kingdom also acknowledges that individual engagement with their Open Banking system is necessary to achieve competition goals.[169]

At the company level, new innovators also face a challenge in breaking into new markets because they often need initial access to large amounts of aggregated, representative data to develop models and products before beginning to service individual customers. Thus, because large technology companies in the U.S. have amassed so much information, new entrants are unlikely to catch-up through one-off permissioned transfers of data alone. [170] Sectoral laws, like in financial services, have limited the flows of certain sensitive information to date, and therefore portability could have a greater competitive impact in those cases. But the reality of dominant companies and sectoral variations raise the potential of using other forms of data governance in tandem with portability. Data transfers to new entities raise security and conduct concerns, therefore data protection expectations across all companies is crucial to creating confidence in these systems. Other active data rights, such as transparency and deletion, could also work in

tandem with portability to increase competition. To chip away at dominant market positions there could be a multi-pronged approach of 1) minimizing future data collection through stricter expectations, such as legitimate purpose, 2) providing individuals with the agency to delete and transfer information, and 3) creating systems whereby new innovators can safely and efficiently access and use data. Despite the potential of these tools to increase competition, the infrastructure of large technical companies to collect, process, and use information is heavily entrenched in the digital ecosystem,[171] and data governance alone may not be able to change that.

There is also the potential that data governance could create new hurdles for competition. Young companies would be faced with new, stricter expectations, while older companies, who did not need to comply with these frameworks originally, now have significantly more resources to do so. This situation is unfortunately the reality of evolving policy, and therefore it is important to consider whether certain expectations could be tiered for early-stage companies to enable them to reach scale, while still maintaining robust individual data protection. Alternatively though, new data governance frameworks can incentivize better data hygiene and management practices at an earlier stage, which can reduce the need for large, resource intensive overhauls later on in a company's development.[172] Clear and equal data protection requirements across companies can also have a positive impact on competition by enabling more relationships among different kinds of firms by reducing the need for be-spoke, intensive partner vetting in sensitive sectors such as financial services.[173]

While certain active data rights, such as portability, transparency, and deletion could play a positive role in competition, they are not a panacea for concentrated market power. The discussion above also indicates that a bundle of both protection and rights used together can be more effective than a focus on a single right of portability. Finally, it is important to consider tiered and proportional requirements based on the riskiness of activities and scale, but as will be discussed in Part 2 of this report, *The Foundation: Individual Data Protection*, quantifying risk is challenging, and exempting any entities from protection requirements should be limited and carefully considered.

Innovation

Closely tied to competition goals, society can strive to foster innovations that can improve the lives of individuals. An example of this is online and mobile banking, which have enabled greater access to financial services as computer and telephone technology has evolved. Large-scale data collection, processing, and use have undisputedly driven innovation across multiple sectors in the U.S., but to date that has not been balanced with data protection and individual agency. The challenge for policymakers going forward is to find ways to preserve flexibility for innovation while adopting more deliberate and secure safeguards.

Introducing new data protection standards around security and conduct, as well as active data rights, will inevitably shift some financial resources from growth to compliance, and these changes will impact the data resources available for developing new products and services. This highlights the need to foster innovation in tandem with data policy. Some innovation, and new business opportunities, may be directly stimulated by new compliance requirements[174] or through growing demand for new privacy-protective tools and products. It is also important to take into account existing business rights such as intellectual property that can incentivize experimentation. While individual data rights may serve certain policy goals, there are some elements of data control, and opportunities, that may need to remain with businesses in order to promote ongoing innovation. Considerations around what these elements could be will be discussed in Part 2 of the paper.

Research

Stricter requirements and new hurdles to accessing data pose similar challenges for not-for-profit private and public sector research, as they do for innovation. Furthermore, it is extremely important for societal research goals to have accurate, and representative information about individuals. For example there are long-standing gaps in the collection of information about women[175] and minorities,[176] which could be helped by expanding data collection, processing, and use in ways that respect diverse preferences. Unfortunately, the introduction of more restrictions on the collection and use of data, and active data rights, such as deletion, could also exacerbate certain populations being under or over represented in data sets.

For these reasons there have typically been carve outs in data laws such as CCPA and GDPR, that enable certain entities to use information with fewer restrictions if it is for public benefit. These kinds of carve outs are understandable, but it is also important to maintain high-quality security and conduct across all entities. Given the heightened risk that certain populations have relative to data, it is essential for individuals to feel protected across data activities conducted by both private and public entities. There also may be cases where some active data rights, such as deletion, may need to be limited where there is demonstrable public benefit, like the census.

The tension between data activities for public benefit, and individual protection and choice, again raises the importance of continuing to explore technologies that can reduce the risks of data breach and misuse through more permanent “de-identification”. Public and non-profit entities have limited resources to comply with a strict protection regime across all data activities, but if more reliable tools can be developed for anonymization and encryption, then the challenges that new data governance expectations could pose to both innovation and research could be mitigated. The potential of these technologies will be discussed in more detail in the section titled, *Technology for Individual Data Protection*.

Security

Entities face constant cyber-attacks,[177] and this is only increasing as more products and service become digital. Because of this reality, cybersecurity has been fundamental to data governance over the years and it is essential to maintain that as new systems are introduced. There is a concern that focusing on individual data rights such as portability, could lead to a proliferation of data across new, less-secure entities, which could create more opportunities for external attacks. Evidence suggests that a strong focus on data protection across entities can counter this risk. For example Europe has seen improvements in data management processes, cyber hygiene and incident reporting across entities that collect, process, and use data since the implementation of GDPR.[178] There is also hope that the current focus on privacy can push U.S. companies to improve their technologies and systems, which could positively interact with the innovation and competition goals discussed earlier.[179] This, again, reinforces the importance of individual data protection as a foundation for a subsequent regime of individual data rights, if security is to be maintained as a foundational policy objective.

Social and Systemic Risk

In addition to increased data flows, stemming from a narrower focus on a right to portability, potentially creating a more challenging cybersecurity landscape, there could be larger social and financial-system risks to not taking a broad approach to the design and management of new data governance systems.

Today, broad unchecked data collection, processing, and use has created social tensions and risk, such as the rise of "misinformation" across social media platforms.[180] This is an example of the ability for "data pollution",[181] referenced in the earlier section, *Reframing from "Data Ownership" to "Data Rights,* to degrade trust in public systems.

Another systemic challenge related to data is the complexity of the infrastructure and business relationships that underpin the ecosystem, and the speed and scale at which data, and the associated risks of breach and misuse, could propagate. Currently the network of entities that may interact with information about individuals is vast, and each relationship is governed by a unique contract which imparts differing standards. A report by the United Kingdom Information Commissioner's Office found that a single website visit can result in an individual's data being shared with hundreds of organizations.[182] At some point, this complexity becomes too much for the average person or institution to understand, and therefore the risks may be impossible to identify or manage. As demonstrated by the U.S. financial crisis, it is necessary for regulators to understand complex systems, and more standardized structures can help with risk monitoring.

While data pollution and complexity represent large-scale risk, there are also risks in particular sectors that could accumulate, and have an impact on traditional concepts of stability. Certain use cases for information that are foundational to the financial system, such as credit

underwriting, require representative and accurate data to perform effectively. Individual data rights, such as deletion, may need to be limited in cases like this, where omissions or removed information could directly impact the safe provision of credit. Conversely, specific use cases, such as underwriting, could also be greatly improved by expanded and improved avenues for individuals to provide new information, review existing information and correct inaccuracies. This again highlights the complexity of creating broad data governance systems, and the importance of integrating sector-specific requirements.

A final tension related to systemic risk is that it is inherently more difficult to regulate many different kinds of companies. Pro-competition policies can make monitoring and supervision more challenging because business models and approaches become more diverse, and stricter compliance requirements can give rise to more external service providers that play essential functions for businesses.

While data governance can increase market complexity, it also has the potential to drive mergers and concentration. For example, Europe has experienced more market concentration in its technology sector in the wake of GDPR implementation.[183] Unfortunately, while a multitude of companies can lead to complexity risk, fewer entities in the market can lead to more interdependency and concentration risk. This indicates that data protection and data rights can have both positive and negative implications for systemic risk, and other policy goals, such as increasing competition, can create new challenges for oversight.

While policymakers likely want to achieve a combination of many social goals, it is essential to understand when those goals may interact, or even counteract, each other. There are clear tradeoffs when creating a data governance framework, but that does not diminish its importance to individuals, and the positive impact that a well-designed, broad system can have for a country.

Current U.S. Data Governance

Today many of the laws that govern the management of data related to individuals at the federal level in the U.S. are focused specifically on the financial services sector. There are also new state laws emerging such as the California Consumer Privacy Act which take a broader perspective, but often carve out data that is already governed by more specific federal statutes.

This section will provide an overview of three major federal financial services laws that include data governance, as well as the CCPA. Each overview starts with the scope of coverage for each law, followed by the data protection requirements, and data rights, that the laws impart. Another important dimension that will be discussed concerns the regulatory approach to supervision and enforcement of these laws, both with regard to direct oversight and under more general expectations governing companies that act as third-party service providers to entities that are

subject to ongoing federal supervision. Because each law uses certain terminology and defines it in specific ways, this section uses those terms in describing the particular legal requirements rather than referring more broadly to "individuals", "entities", and "companies".

In the financial services sector, the main federal laws governing management of data related to individuals were adopted before the emergence of the current data economy and exponential increases in data generation and sharing. For example, the Fair Credit Reporting Act was adopted in 1970, and was subject to a broad general congressional update in 2003. The Gramm-Leach-Bliley Act was adopted in 1999. The Dodd-Frank Act of 2010 adds an important new general right for individuals to access their own transaction and account data in connection with consumer financial products and services, but neither implementation rules or interpretative guidance has been issued by the CFPB.

Each of the federal financial laws has different scopes of coverage as to what data are covered, which firms are expected to comply, and even how the laws define "consumer". Additionally, they each place different degrees of emphasis on empowering individuals to exercise agency over data, versus addressing information security and customer protection concerns by imposing prescriptive requirements and limitations on covered firms. While none of these laws provide a comprehensive framework for individual control similar to European or California data legislation (which will be discussed in more detail in the sections below), they provide helpful examples and lessons about the balance between managing data protection, fairness, accuracy, and broader individual empowerment in the U.S. context.

Figure 4. Comparison of Data Rights Available in Current U.S. Law

	FCRA	GLBA	Dodd-Frank 1033	CCPA
Year	1970, 1996, 2003	1999	2010	2018
Initial Disclosure	✓	✓	✗	✓
Consent	Rarely required	Opt-out right*	Always required	Opt-out right*
Ongoing Transparency	✓	✗	✓	✓
Correction	✓	✗	✗	✗
Deletion	✗	✗	✗	✓
Portability	Not primary focus	Not primary focus	✓	✓

**Only for certain transfers*

Fair Credit Reporting Act (FCRA)

The FCRA was enacted in 1970 and was one of the first U.S. regulations to incorporate concepts of data governance into law. The FCRA is also the broadest of the three financial statutes in terms of its substantive scope. It includes a broad range of topics, including data protection and accuracy expectations, protections in the event of identity theft, required disclosures to individuals, and rights to dispute and correct information.

Coverage Overview: Most Fair Credit Reporting Act provisions apply only to information contained in "consumer reports", which are generally defined as any communication by a consumer reporting agency that includes information bearing on a consumer's creditworthiness, character, or reputation which is used or collected for the purpose of determining the consumer's eligibility for credit, insurance, employment, or other authorized purposes. Thus, some aspects of FCRA reach beyond financial services, and also govern data that is used in connection with employment, housing, and other sensitive decisions. However, such data is only covered if it is contained in a "consumer report" that is compiled by a "consumer reporting agency" as defined under the statute. The law has been interpreted to not apply to de-identified, "anonymized" data only if it is not used for determining eligibility. For eligibility decisions, any data that could be reasonably linked, or "identified", back to an individual is still covered by FCRA.

Where a consumer report is involved, FCRA imposes various limitations and requirements not only on consumer reporting agencies but also on entities that "furnish" the underlying information, and on users of the reports. Consumer reporting agencies are defined broadly to include any party that regularly engages in assembling or evaluating information for the purposes of furnishing consumer reports to third parties, even if they do not think of themselves as a traditional credit bureau. The definition of "consumer reports" depends not just on the nature of the information, but also on the purposes for which it is compiled and used, and the involvement of a reporting agency, in the transmission process. Thus, information that may bear on creditworthiness or character may fall outside the scope of the statute if it is compiled solely, and used solely, for purposes that are not addressed by the FCRA. Additionally, information such as a character reference that is used specifically for credit underwriting, is not a consumer report if it is transmitted directly from the original source to the lender without the involvement of credit reporting intermediary.

FCRA generally defines a consumer as an individual, while using the term "person" more broadly to include individuals, partnerships, corporations, and various other types of entities. Although FCRA does not apply to credit reports about businesses, it has been interpreted to apply in situations in which a lender obtains a personal consumer report about a business owner in conjunction with extensions of commercial credit.

Some FCRA requirements can be enforced by individuals through private lawsuits, while other parts are subject only to enforcement by federal regulatory agencies and state attorneys general.

The CFPB can examine consumer reporting agencies used for financial services that meet specified size thresholds for all FCRA requirements, except for certain rules concerning identity theft "red flags" and records disposal. The CFPB cannot examine activities related to employment or tenant background checks. Banks and credit unions are subject to examination for compliance with furnisher and user requirements, and some non-banks are also subject to CFPB examination for most of the same provisions.

Data Protection and Individual Rights: FCRA requires disclosures on a broad range of topics, but it does not require consumers' consent to collect data in the first instance. Transmission and use of data for purposes that are designated as permissible under the statute also do not generally require consumer permission, with the exception of certain employment-related situations and new rights that allow individuals to place "freezes" on their reports in order to manage concerns about identity theft in the credit context. The law isn't typically thought of as a portability regime, though it does allow consumers to authorize the sharing of consumer reports if they provide written permission to firms, even for purposes that would not otherwise be permitted by the statute. However, the consumer reporting agency is not required to disclose the information even if the firm has written permission and there is relatively little regulatory guidance governing such situations. This differs from European laws such as PSD2 and GDPR which create a requirement to disclose information based on a valid consumer request.

The law provides consumers with a general right to dispute the accuracy or completeness of information in their consumer reports, and helps to facilitate the exercise of this right in situations in which lenders or certain other parties take an "adverse action" based on information in a consumer report, by mandating that individuals be provided with certain disclosures and an opportunity to review the underlying information. It also imposes general requirements on consumer reporting agencies to maintain practices to promote information accuracy, including monitoring and following up on potential data discrepancies. Congress has repeatedly strengthened provisions relating to dispute rights and general accuracy requirements on covered entities, as well as making it easier for consumers to obtain credit scores and their underlying reports outside of adverse action situations.[184] Yet even after these improvements, and amidst increasing concerns about data breaches and identity theft, surveys suggest that the percentage of individuals who exercise their rights to obtain free copies of their consumer reports is well below 50 percent,[185] and general awareness of key facts about credit reports and scoring is actually declining.[186] Despite both conduct standards around data accuracy and the requirements to facilitate correction after an adverse action, accuracy remains a major concern. Studies have indicated as many as one in five consumer reports may contain errors,[187] though that may have improved over time.

Gramm-Leach-Bliley Act (GLBA)

GLBA, also known as the Financial Services Modernization Act, came into law in 1999 as an amendment to the larger Glass-Steagall Act. In contrast to FCRA, GLBA is more narrowly focused on "nonpublic personal information" used in the provision of financial services. The law is divided into two provisions, the safeguards rule and the privacy rule. The safeguards rule imposes information security requirements, while the privacy rule establishes boundaries of data sharing and enables individuals to halt certain activities.

Coverage Overview: GLBA defines "nonpublic personal information" as personally-identifiable financial information that is provided by a consumer to obtain a financial product or service from a financial institution, results from a consumer transaction, or is otherwise obtained by the financial institution in connection with providing the financial product or service. The law has been interpreted to exclude aggregate or de-identified, "blind" data that does not contain personal identifiers such as names, addresses, or account numbers.

GLBA applies broadly to "financial institutions", which are defined as companies that engage in financial activities, as defined under the Bank Holding Company Act. This definition extends beyond depository institutions. Examples of financial activities include securities, insurance, retail banking products, financial advisory activities, and the processing and transmission of financial data. Companies that are not financial institutions in their own right may still be subject to certain requirements when they receive nonpublic personal information from a financial institution.

GLBA information security requirements apply generally to the nonpublic personal information of "customers" that have continuing relationships with a financial institution. The rule can extend to entities where the consumer is not a direct "customer", for example consumer reporting agencies. The privacy disclosure and information sharing requirements apply to consumers (defined as individuals and their legal representatives) who apply for credit or obtain one-time financial products or services (such as a cash withdrawal at an automated teller machine) even if they do not have an ongoing relationship with a financial institution. Both consumers and customers must be obtaining the financial products or services for personal, family, or household use. GLBA does not protect data relating to products and services for small businesses.

Only federal regulatory agencies and state insurance regulators can enforce GLBA. Although banks and credit unions are regularly supervised for compliance with all parts of the statute, non-bank monitoring is significantly more limited. The Consumer Financial Protection Bureau can examine and enforce GLBA privacy and information sharing requirements for those non-bank entities for which it otherwise has supervisory authority, but not for information security safeguards. The Federal Trade Commission has enforcement authority over GLBA safeguards compliance for non-bank financial institutions generally, but has limited staffing and no supervision authority. As discussed below, some non-banks may be examined by federal banking

agencies for GLBA safeguards compliance to the extent that they provide vendor services to banks and credit unions. Overall, there is also a perception that enforcement actions have been limited with regard to the GLBA privacy rule in particular.

Data Protection and Individual Rights: While GLBA is considered a privacy-focused law, it emphasizes data protection, and includes only a limited active right for individuals to opt-out of certain sharing. The law requires that financial institutions adopt "information safeguards" to protect the security of identified data regardless of any action taken by customers. With regard to information sharing between companies, GLBA requires financial institutions to provide notice and an opportunity for individuals to opt out of certain activities, such as marketing by third-parties, while allowing a broad range of additional sharing pursuant to various exceptions listed in the statute. Like the FCRA, consumers can also authorize sharing of their data outside of circumstances that would otherwise be permissible under the statute, but the law is not typically thought of as a portability regime and there is relatively little regulatory guidance governing such situations.

As described in earlier sections, eight federal agencies worked together to develop model forms for disclosing financial institutions' privacy practices. Although the forms have been widely adopted, there is a widespread sense that individuals do not in fact review the materials or meaningfully exercise their opt-out rights. For example, although the law originally required financial institutions to provide annual privacy notice updates to their customers, those requirements have been scaled back in recent years by both federal regulators and Congress due to concerns about compliance burdens and potential information overload for customers. In addition, one study of more than 6000 financial institution privacy notices found that they contained contradictory statements and many did not enable legally-required opt-out options.[188] There do not appear to be any recent generally available statistics on the rate at which consumers opt out of information sharing under GLBA, but among stakeholders it is commonly believed to be less than 5 percent.[189] Additionally, concerns have been raised that the number of exceptions under the law for which information sharing is permitted without notice or an opportunity to opt out, may exceed individual's reasonable expectations.

Despite one of GLBA's basic purposes being to harmonize information security and sharing protections across different types of financial activities, there is a substantial concern that it is not in fact applied consistently across the entire market. For example, with regard to information security requirements, differences have developed between federal agencies that are charged with administering the law to different types of entities. The Federal Trade Commission is currently engaged in rulemaking that would narrow many of these substantive and coverage gaps between non-banks and bank actors.

Dodd-Frank Act Section 1033

Section 1033 was enacted in 2010 as part of the larger Dodd-Frank Wall Street Reform and Consumer Protection Act. This law made broad changes to financial regulation, and in particular Section 1033 created a right for consumers to access transaction and account information concerning consumer financial products or services that they have obtained from a "covered person" as defined by the Dodd-Frank Act.

Coverage Overview*:* Under Section 1033 consumer financial products and services are generally defined to include lending, deposit and payment services, financial advisory activities, providing consumer reports or similar decisioning information for purposes of another consumer financial product or service, and providing financial data processing services to consumers.

The law requires "covered persons" to provide information that can be retrieved in the ordinary course of their business in usable electronic form, upon the request of a consumer, but does not address consumer disclosures, request procedures, or other topics. "Consumer" is generally defined to include not only individuals who are obtaining financial products and services for personal, family, or household purposes, but agents, trustees, and representatives acting on the behalf of such individuals.

Section 1033 directs the CFPB to prescribe "standards … to promote the development and use of standardized formats for information", but the Bureau to date has not issued regulations or clarified whether the law is in effect absent such rules. In 2017, the Bureau issued non-binding principles for consumer data sharing.

Only federal regulatory agencies and state officials can act upon Section 1033. The CFPB and federal banking regulators can examine entities that are subject to their supervision authority for compliance.

Data Protection and Individual Rights: Section 1033 is an important step toward a more robust individual data rights regime because it specifically enshrines the principle that individuals should be able to access transaction and account information in an electronically usable form upon request. However, the statutory provision is quite short, and other than directing the Consumer Financial Protection Bureau to issue rules to promote standardized data formats, it does not provide guideposts for the exercise of this right or address other types of consumer agency over data.

The CFPB's 2017 Consumer-Authorized Data Access Principles[190] provide a more robust discussion of a broader system of protections and rights, but they are non-binding. For instance, they describe the scope of data access by individuals and authorized third parties, list topics that should be fully and effectively disclosed to consumers prior to them providing authorization for data access, call for robust security and accuracy processes, and endorse the provision of

mechanisms that allow individuals to monitor data access, revoke consent, and compel data deletion at their discretion.

California Consumer Privacy Act (CCPA)

The CCPA was passed in June 2018 and went into effect on January 1, 2020. This is the broadest data-focused law in the U.S. today and is specifically focused on increasing individual's agency relative to data.

Coverage Overview: Unlike FCRA and GLBA, which are restricted to certain activities and entities, CCPA applies broadly to for-profit business entities operating in California, subject to certain thresholds of applicability and specific exclusions (including activities governed by FCRA and GLBA).[191]

The for-profit entities covered by the law must do business in California and either collect the personal information of at least 50,000 individuals, households, or devices directly or through third parties, have an annual gross revenue in excess of $25 million, or derive 50 percent or more of their revenue from selling data. There is significant debate as to what constitutes "sale" of data, and while the law defines sale beyond just a monetary exchange, there may be transfers between businesses where an exchange of value is not clearly delineated.

The law applies to any data that identifies, relates to, or can reasonably be associated with an individual or household. This is an expanded definition of covered data relative to most other privacy regimes because it applies to data that is not currently associated to an individual, but could reasonably be re-associated. The law names particular data points that have historically been excluded from the definition of personally identifiable information under other regimes, such as IP address, to illustrate this point. The law also explicitly covers information that has been inferred about individuals. CCPA does exempt "de-identified" information, which is defined as information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to an individual. Businesses that use de-identified information are required to have technical and organizational structures in place to prevent re-identification. The law does not cover data that are subject to other existing privacy laws such as GLBA and the Health Information Protection and Portability Act (HIPAA).

CCPA also defines a broad scope of coverage with regard to "consumers". The law applies to all natural persons who are residents of California, it does not require that individuals are in a business relationship with firms, and protections and rights provided cannot be waived through contract. Given that state residency can be difficult to determine, and would require additional data collection to verify, many entities use the location information of individuals to establish the applicability of CCPA. Overall, many entities report confusion about how the law should be implemented, and this could prompt a broader provision of rights to individuals outside of California as well.

The Attorney General (AG) of California proposed detailed implementation rules for the law and is responsible for its enforcement. If firms fail to comply with CCPA they may be subject to civil penalties imposed by the AG. Individuals can also seek damages for CCPA violations, but this is only allowed when there is unauthorized access and disclosure, exfiltration, or theft of non-encrypted, identifiable information. This ability to seek damages is further limited to data breaches where business "failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information".[192] While situations where individuals can be directly compensated is limited, the law does include a right to statutory damages which means that consumers do not have the burden of proving that they were directly harmed by the event.

Data Protection and Individual Rights: CCPA provides a number of clear individual data rights, and establishes certain conduct standards for businesses. California residents can now request access to the information that a company has collected about them, and as part of that request, they also have a right to know which third parties a company has previously obtained information from, or sold it to. Under the law individuals may also request that entities delete information related to them, but that is limited to identifiable information, and is subject to exceptions, such as certain types of research.

The right for individuals to port data between entities is not independently called out in the law, but companies that respond to access requests electronically are required to provide the information in formats that can be transferred. Individuals can also opt-out of data being sold and for children under the age of 13 parental authorization is required for the sale of data. As described above though, there is debate around what constitutes sale, therefore these rights may not apply to a spectrum of data transfers that occur between entities and do not involve a direct value exchange.

The law imposes a number of conduct standards, including that businesses must disclose on their websites what information they collect broadly, the business purpose of that collection, and any third parties that they sell data to. They must comply with access and deletion requests within a set time-frame, and they cannot change the level of service they provide to individuals in response to those requests. There are a number of additional requirements in the law[193] and within the draft regulations provided by the California AG. The law does allow for businesses to offer financial incentives in order to collect and resell data. While the law prohibits the denial of service, or discrimination based on privacy preferences, the exception that was latter added to the law around financial incentives, enables businesses to try to entice consumers into additional data activities. There are some limitations to this program, but overall these two elements of the law may come into tension in the future.[194]

Additional Relevant Statutes, Laws, and Issues

Third-Party Service Provider Guidance: One further important component of federal financial data protections is oversight of vendors that provide third-party services to banks and other entities that are supervised by the federal banking regulators or the CFPB. The federal agencies have acknowledged that it often makes sense for supervised entities to outsource certain functions to vendors, but the entities retain responsibility for compliance with both safety and soundness and consumer protection laws. Accordingly, supervised entities are expected to develop a comprehensive risk management process for conducting both initial due diligence and ongoing monitoring of their vendors for compliance purposes. The federal agencies have authority under the Bank Service Company Act and the Dodd-Frank Act to conduct their own examinations of vendors, but only with regard to the vendors' activities performed on behalf of, or under the direction of, the entities that are subject to direct primary supervision.

Third-party service provider oversight has helped to substantially reduce risk levels in conjunction with bank outsourcing activities for decades, but stakeholders have raised concerns that in the new digital economy this system is serving a broader data protection oversight function than intended. The expectation that financial institutions hold primary responsibility for data protection across a complex system of varied relationships is a significant responsibility, and has raised competitive concerns around interactions between incumbents and non-bank entities. For example, each federal agency has its own formulation for what types of relationships trigger third-party service provider status, and there are substantial debates about whether data aggregators and other fintech companies that do not contract with banks, but do collect information from them at the behest of individuals, are in fact subject to the guidance.[195] In 2020 the Office of the Comptroller of the Currency (OCC) issued updated guidance on this matter.[196] This guidance clarified that while data sharing may occur with an entity that is not a vendor, or under contract with a bank, financial institutions are still responsible to assess and mitigate the risks associated with data activities. Both supervised entities and third parties can find the expectations of constant downstream, and partner risk management challenging to meet. From the supervised entity perspective, it can be challenging to get sufficient information from third parties about proprietary and highly technical processes to satisfy supervisory expectations, particularly when the third parties are filling a knowledge or expertise gap, or if they are not in a traditional relationship with the supervised entity. From the third parties' perspective, having to satisfy the due diligence and monitoring expectations of multiple supervised entities can be challenging, if not outright prohibitive for small companies. There have also been claims that some banks have imposed overly restrictive vetting requirements, in an effort to reduce the competitive edge of fintech companies that rely on data that is being collected by aggregators.

Other laws that have important implications for data governance in particular contexts include:

- Electronic Fund Transfer Act (EFTA)[197]
- Fair Debt Collection Practices Act (FDCPA)[198]
- Children's Online Privacy Protection (COPPA)[199]
- Equal Credit Opportunity Act (ECOA)[200] and the Fair Housing Act (FHA)[201]

Additionally, with regard to more general commercial activities, the Federal Trade Commission has used its authority to police unfair, deceptive, and abusive acts and practices (UDAAP/UDAP)[202] to take action with regard to both data security and notice and consent, as discussed in the prior section, *The Limitations of Individual Consent*. A large number of states have also adopted general laws requiring notification in the event of data breaches.[203]

As this section outlines, the U.S. does have existing data protection and conduct standards, as well as some codified individual data rights. Unfortunately most of this regulation is limited to specific sectors or geographies, and creates a complexity that is precarious for individuals, and burdensome for businesses and government oversight. There is clear value in creating a foundation of data protection that extends across all entities and individuals in the U.S., and borrows from the positive lessons that the current laws have taught us. Some of these lessons include: the value of clear communication to individuals about what rights are available to them and accessible systems to manage those rights; the importance of consistent monitoring and accountability across entities; and the role that sector-specific protections can continue to play on top of a broader data governance foundation. An overarching effort could also address the inconsistencies in our current system around what data are covered, who is responsible, and which individuals are protected.[204] A broad approach could also streamline conduct expectations around the initial collection of data, and consider how "de-identified" data should be protected given the current ease of re-identification. A baseline for individual data protection and rights would also address the competitive and partnership challenges of risk oversight and liability allocation, incentivize good digital hygiene and technology practices across the country, and create a consistent approach to oversight and enforcement. While a comprehensive data governance framework is developed, it is also valuable to watch and learn from the impact of new laws, like CCPA.

Lessons from Other Industries

Beyond financial services, other sectors are also struggling with data governance, and are working to understand the appropriate role for individuals in the data ecosystem. Healthcare and education are two sectors with existing data governance laws, but similar to financial services, a growing number of stakeholders are acknowledging the need to adapt to changing practices[205] and calling for more individual control. In addition to health and education, sectors ranging from to farming[206] to utilities[207] are also discussing the challenges of data.

Healthcare

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is the most notable legislation governing the management of health data in the U.S. HIPAA predates much of the modern digitization of data, and while it covers information generated by hospitals and health care providers, it specifically excludes data generated directly by individuals.[208] This means that information created through wearable fitness trackers and mobile applications are not covered by the law's protections.

The 2009 Health Information Technology for Economic and Clinical Health Act (HITECH) amended HIPAA in an attempt to modernize legislation in recognition of digitization, but the framework still recognizes "covered entities" based on sector and industry,[209] similar to GLBA. The Department of Health and Human Services issued a Request for Information to explore changes to HIPAA that would make access to health data, as well as sharing and transferability by individuals easier, but there is no suggested extension of covered entities.[210]

Similar to Dodd Frank Section 1033, the **21st Century Cures Act** was passed in 2016 and includes a right for individuals to access medical data from covered entities.[211] The legislation also promotes interoperability between diverse health data management systems which often differ across providers. Unfortunately, only 18 percent of health systems report being familiar with new patient data access rules.[212] Another interesting element of the Cures Act is a focus on helping medical researchers access more data more quickly and securely.

Education

The Family Educational Rights and Privacy Act (FERPA) protects student education records and empowers parents and eligible students to request access to, and corrections on, those records.[213]

Similar to laws in other sectors, FERPA is limited in scope. For example it only applies to schools that receive funds from specific programs within the Department of Education. Therefore, private and parochial schools are generally not subject to FERPA.[214] Similar to the challenge in the finance and health sectors of new technology falling outside of existing regulation, digital education platforms like Coursera or Duolingo are not covered by the law.

Lessons from Outside of the U.S.

In tandem with domestic efforts, structures for data governance are being refined, and created across the globe. The sections below provide an overview of some of the relevant international regulations and proposals, and highlights some of the elements that have been incorporated into this paper.

Europe

The General Data Protection Regulation (GDPR) is a pan-European law that went into effect on May 25, 2018 and is intended to create consistent governance of data privacy across Europe.[215] Data Protection Authorities were established to oversee and enforce the law.

- *Incorporated element*: Blended regulation that both increases data protection and provides individuals with data rights
- *Incorporated element*: A broad scope. Covers all EU citizens, and all entities that handle information related to those citizens

Payment Service Directive 2 (PSD2) is a pan-European directive released on November 25, 2016. This is not a regulation, so detailed governance is left to each European member state. Part of the intent of the directive is to increase competition in the payments market by enabling secure access to payments related data.

India

The Indian Data Protection Bill[216] is a legislative proposal to provide comprehensive data protection to all citizens of India. The bill also establishes a Data Protection Agency to implement the potential new law, and provide oversight.

Aadhaar[217] is a digital identity system for all citizens of India that is integrated with technological capabilities across the Indian government, such a data storage.[218]

- *Incorporated element*: A requirement to disclose the purpose of data activities, and limit additional activities to that original purpose.
- *Incorporated element*: A focus on public technology that can help enable data protection and the use of data rights.

United Kingdom

Open Banking is an effort initiated by the UK Competition and Markets Authority to enact, and expand upon PSD2 legislation. Open Banking describes a system of regulatory oversight, and technical connections, that enable financial data portability.

- *Incorporated element*: Including new entities within an oversight perimeter (Account Information Service Providers and Third Party Service Providers) in order to facilitate secure data portability.
- *Incorporated element*: The importance of developing, and using technical processes to support data rights, such as documenting and tracking consent.[219]

Australia

The Australian Consumer Data Right is an initiative of the Australian Government to improve individual's access to, and control over, data. Implementation rules and processes are currently being developed by the Australian Competition & Consumer Commission.[220]

- *Incorporated element*: Information is seen as a resource for the country as a whole, so governance structures are focused on using that resource more efficiently, and collectively.
- *Incorporated element*: The initiative is intended to cover all sectors of the country.

Brazil

The Brazilian General Data Protection Law (LGPD), published in August 2018, provides both individual data protection and certain data rights. This law is modeled on Europe's GDPR, and also has a broad scope of applicability to all Brazilian citizens and all entities handling information about those citizens.[221]

Canada

The government of Canada is embarking on a review of a consumer-directed finance model, analogous to open banking concepts in the United Kingdom. This type of system would enable financial data portability.[222] Canada has also released a comprehensive digital charter for the country.[223]

These examples represent only a handful of laws and systems that are being developed around the world.[224] For example, countries such as New Zealand and Singapore are creating fundamental infrastructure around digital identity,[225] and Know Your Customer (KYC) utilities,[226] while other countries, such as Japan, are encouraging data portability through non-binding API standards.[227] Additionally, there are efforts underway in Europe to create blended, synergistic approaches[228] to the myriad of policy goals that interrelate with data governance.

While these laws are an essential resource for the development of data governance in the U.S., there are key areas that may warrant divergence. For example, GDPR excludes "anonymous" data from the regime, and maintains consent as a standalone lawful basis for data collection.

This research initiative, and the ensuing symposium design, started with a narrower focus on the agency that individuals could, and potentially should, have with regard to data. Through this work though an important distinction, and intersection, emerged between data protection and individual agency. **An individual taking an active role in directing and managing information related to themselves should not imply that they therefore hold primary responsibility for their own protection relative to data risks**. Based on the research and analysis underpinning this project, Part 2 if this report provides a conceptual structure for a two-sided data governance framework that incorporates both individual data protection and active data rights. In addition to describing this framework, Part 2 includes a brief review of the essential roles that technology and businesses can play in protecting data and enabling the use of active individual data rights.

The Foundation: Individual Data Protection

This section describes the first side of the proposed data governance framework: a foundation of individual data protection in the U.S. that focuses on security and conduct across all entities and data activities in order to facilitate a safe market for information, and to create subsequent opportunities for individual control.

The ecosystem that underpins the collection, processing, and use of information, is increasingly complex,[229] which places individuals at a, potentially insurmountable, disadvantage in understanding and upholding their own protection. As Professor Woodrow Hartzog describes, "data subjects have the fewest resources of every party in the chain of data flows and they are on the wrong side of substantial information and power disparities. While control is an attractive goal in isolation, it comes with a practical and legal "obligation". If you do not exercise that control, you are at risk."[230] As described in the background section, the Fair Information Practices have been a model of data governance since the 1970s and include concepts of both business responsibility and individual agency. Despite leading the development of these concepts, the U.S. has focused on entity "self-regulation" by incorporating the FIPs into reports, guidelines, and model codes,[231] but their use in binding law was limited to only certain sensitive sectors. This has left a broad emphasis on "notice and choice". Furthermore, while the FIPs created a valuable common starting point, they do not address the challenges that individuals face in protecting themselves in increasingly complex data and policy ecosystems.

For these reasons the U.S. may benefit from revisiting its approach to individual data protection. This sentiment is echoed by the American Law Institute (ALI), whose recent privacy principles propose moving away from "privacy self-management", and placing clear and consistent

obligations directly on organizations.[232] As of 2019, the FTC has also repeatedly called for privacy and data security legislation in Congressional testimonies.[233]

While conversations about data protection and privacy have tended to happen separately from calls for increased individual agency, this research suggests that data protection across all entities that handle information could actually be an enabler of increased individual agency, and therefore designing these policies jointly may offer the greatest benefits. Focusing first on concepts of individual control to harness new opportunities, such as the promises of portability to enable innovation and competition,[234] could result in surges of data across both regulated and unregulated entities, elevating risks for everyone.[235] Furthermore, introducing new types of active data rights amidst already fragmented data protection laws will make compliance, and therefore partnerships more challenging, and could lead to less innovation and less competition.[236] Comprehensive data protection structures that apply to all entities that collect, process, and use data could create a clear and navigable ecosystem for businesses, and could enable subsequent individual data rights. The concepts below are an option for the design of a comprehensive policy floor, with opportunities for additional policies to be built upon it at the state and sector levels.

Protection from What?

The first challenge in developing a data protection framework is defining the harms that individuals are being protected from. Some harms stemming from data loss or misuse can be defined, and even measured, but many more are intangible, unmeasurable or both.[237] Harms can also arise from both direct injury, or through the loss of an opportunity. This makes protection particularly challenging, but also even more essential given the unknown nature and scale of potential harms. Governance structures within regulation and business relationships may use definable and measurable harms to quantify and distribute liability, but given that these make up only a portion of the risk, broad structures of oversight and remedy can help mitigate more opaque harms to the extent possible.

Definable harms can arise both from data loss due to external breach, or from the misuse of information by companies internally. If identifying information, or financial account numbers are breached individuals could experience fraud, and direct financial loss. Subsequent harms could include the inability to access credit because of fraudulent activity impacting a credit score, or necessitating a credit freeze. Data misuse by companies internally could result in discriminatory exclusion from opportunities, such as jobs, or targeting individuals with products that prey on their situation[238] and vulnerabilities.[239] While these kinds harms may still be challenging to demonstrate and truly seek remedy for,[240] there are legal systems and existing case law that can be used to compensate individuals for money and time spent to resolve issues stemming from data loss or misuse.

Less definable harms that occur due to data loss or misuse include cognitive stress and familial, social, or employment issues that arise due to the revelation of sensitive information. Research

also indicates that both tangible and intangible data harms can persist over long periods of time,[241] and vary significantly based on individual situations. As discussed in the previous section, *The Crucial Challenge of Equality*, some groups, such as women and immigrants, may experience heightened risk around certain types of data, such as location information. It is challenging to demonstrate and describe these kinds of harms in order to seek remedy, and therefore it may be impossible to make individuals whole if they occur. Furthermore, both the risk of external breaches, and a loss of trust due to internal misuse, creates a resource drain and an environment of mistrust across broader systems and customer relationships.

Broad data protection expectations could reduce cybersecurity risk across increasingly complex business partnerships because one weaker, or less prepared, entity couldn't be exploited to attack partners. This reduced partner-risk could potentially bring down pooled costs such as insurance, and could increase confidence across systems. More secure and trustworthy internal and networked data systems, combined with improved ways to communicate those merits to individuals, could also bring in new customers who may have been previously unwilling to use data-driven products and services due to privacy concerns.[242] For both individuals and business it therefore may be time to bring more focus to mitigating risks in the first place, while making accessible pathways for individuals to seek remedy if harms do occur.

Including Both Security and Conduct

Inadequate data security and internal data misuse by entities may be unintentional or deliberate, and can arise from legacy or poorly managed IT systems,[243] misaligned business incentives, and a lack of clear expectations from regulators. Given this diversity of influences, and the risk of both external attack and internal misuse, **a data protection framework should likely include both cybersecurity and conduct standards**. Cybersecurity standards are the technology and processes devoted to protecting information from external attack or loss.[244] Conduct standards are focused on entities being intentional about their collection, processing, and use of information. This could include processes and mechanisms to identify and monitor the impact that data activities have on individuals, and adjust practices over time.

As discussed earlier, individuals have a limited ability to understand and respond to disclosures about differing cybersecurity and business practices relative to data. Furthermore, both cybersecurity and opaque business practices are credence goods, meaning that even after an individual agrees to certain protection criteria, they have no way of assessing its actual utility until a disclosed event, such as a data breach, occurs. For these reasons, as well as those discussed in the section, *Reframing from "Data Ownership" to "Data Rights"*, current market forces of supply and demand may not be effective in incentivizing appropriate levels of data protection across companies. Comprehensive security and conduct expectations across all entities would ideally improve individual protection, streamline compliance requirements, and create clarity for all parties. Furthermore, it is likely useful to differentiate between security and conduct, while

expecting them to be jointly upheld. For example a popular antivirus software that enables cybersecurity was found to be monetizing and reselling data collected.[245] It is challenging for individuals to weigh these intertwined expectations alone, especially in cases where they may be in tension.

Information security standards for entities have a long history that can be leveraged, including work by the National Institute for Standards and Technology (NIST),[246] Financial Services Sector Cybersecurity (FSSCC) profile,[247] the GLBA safeguards standards,[248] and within industry groups, such as the PCI Security Standards Council.[249] While this history exists, improvements may be necessary in the development and maintenance of technical standards over time. It is also important to determine what baseline level of security is necessary across all entities, and when stricter expectations may be warranted given the diversity of institutions and activities. Conduct standards face similar challenges of proportionality and needing to evolve over time, as well as necessitating the additional complexity of qualitative processes and judgments. This combination of both technical cybersecurity expectations and qualitative conduct standards already exists in financial supervision, and there is growing recognition that it is broadly necessary. For example NIST, has developed a privacy framework to be used in conjunction with their security framework that includes internal policy and process recommendations, though they do not recommend specific approaches.[250]

Conduct standards could include business practices that ensure entities can adequately respond to risks and errors, such as audit schedules and insurance, as well as testing processes for equitable treatment, and having funds available to make individuals whole in the event of harm. Conduct standards in this overarching conception, would include limiting activities to defined concepts of legitimate purposes of data collection, processing, and use. The use of a legitimate purpose standard for initial activities was discussed in detail within the earlier section, *The Limitations of Individual Consent*. Other reasonable conduct standards could include, data retention limitations,[251] establishing processes for reviewing and updating inaccuracies in data, and monitoring data activities and results for biases. Finally, new conduct standards could readily incorporate existing expectations across companies, such as prohibitions on unfair, abusive, or deceptive practices. Conduct standards that weave together proportionality based on the risk of entities and their activities, and processes for reviewing and incorporating new legitimate purposes for collection, processing, and use are essential. Europe and the United Kingdom have worked through a number of similar concepts which could be adapted for the U.S. market and context. For example the UK Information Commissioner's Office has provided a list of processing activities[252] and types of information that pose a higher risk to individuals.[253] They have also developed guidance on how to judge "legitimate interest" as a lawful bases for collecting data under GDPR. While "legitimate interest" is not directly analogous to the legitimate purpose requirement presented here, European regulators have created criteria for testing necessity which can be partially applicable. As an element of conduct standards, the legitimate purpose test would require that activities are both safe and necessary for a particular product or service. A

determination of whether that product or service is useful, or "suitable" for an individual's particular needs would not be the responsibility of the company in this framework. As discussed previously, the concept of a legitimate purpose test is broad enough to capture legal requirements and necessary partnerships, but it is focused on what is necessary and safe for the product or service requested by an individual, not what is in the broader interest of the entity providing that product or service.

This combined security and conduct framework is one way to structure a baseline for organizations, with the potential for more stringent practices and industry-led customization to be subsequently layered on top. It is also essential to build in mechanisms to review and update any standards on a frequent basis to keep pace with changing technology and societal expectations.

Scope of Protection

Traditional boundaries between sectors, partnerships, and customer relationships are breaking down. Firms increasingly use broad pools of information to make decisions,[254] partnerships are both more complex and more necessary,[255] and there are a multitude of companies behind every digital interaction. Even in sectors with data governance laws, such as financial services, the fact that data flows and relationships can involve entities that are not subject to the same degree of direct regulation can result in inconsistent levels of protection. Given these changing dynamics, and mounting calls for more protection across the population,[256] **a foundation of data protection, and its subsequent liabilities, may need to be extended to cover all individuals, and apply to all entities that engage in the collection, processing, and use of data**. This reflects the reality of the data ecosystem as it is today. This expansion is already happening in Europe where PSD2 is bringing new entities into a system of regulatory oversight.[257] As stated above, proportionality is essential, and this concept is not intended to prohibit any businesses or use cases. A broader scope of applicability would still allow for additional sectoral or state expectations to be layered on top.

This breadth would mean that protection is provided to every individual if information related to them is collected, processed or used, irrespective of whether they are in an established relationship with an entity or actively consuming a good or service. This focus on individuals rather than customers or consumers is especially important as technologies increasingly incorporate data collection in their fundamental design, and a vast amount of data handling occurs among companies without a direct relationship to an individual.[258] Furthermore, there are many cases where individuals navigate websites or download mobile applications and do not expect that doing so creates a formal business relationship with an entity. Frequently, individuals may simply be seeking an answer to a question, or browsing among options. While cookie banners and consent screens are treated as the initiation of a relationship they typically happen

prior to an individual being able to gather enough information about a product or service in order to make that decision.[259]

The breadth of this concept would also extend across all sectors, entities, and use cases that engage with data (again, subject to potential proportionality). It is increasingly difficult to fit information, and the use of information, into clear sectoral categories. Entities are innovating where there is demand for information and new uses, but when oversight perimeters are defined by the type of entity, such as hospitals, or the type of service, such as the provision of a financial product, it leaves gaps and inconsistencies as innovative products and services enter the market. Businesses are evolving to naturally cross sectoral lines for the benefit of individuals, but doing so may subject them to differing, and potentially inconsistent, standards and expectations across data and business processes. This could create unanticipated incentives to move away from, or towards, certain business models or sectors. Regulating by entity or activity types, even for the newest use cases, is likely to become outdated and confusing quickly, as evidenced by the inability of experts in a congressional hearing[260] to differentiate between data brokers, data aggregators, and consumer reporting agencies, even though these terms are used to define oversight in federal and state law.[261]

Finally, there are layers of relationships among businesses that are governed by bespoke contracts which set variable expectations. An expansion of data protection expectations to cover all entities would incorporate the multitude of unseen parties and relationships that are active, and essential to the data ecosystem and innovation. This expansion could also help negate some of the challenges, and intensive resource requirements for businesses, of constant oversight and monitoring of partner data practices. Covering all entities in a similar manner could create consistent expectations, streamline business relationships, and hopefully encourage partnerships and innovations that cross sectoral boundaries without increasing risks for individuals or the country. And again, while this concept would create a baseline of protection across all entities, there may be use cases, or sectors that warrant additional security or conduct standards where the risks and tradeoffs are more tangible or measurable.

Data Formats

Older U.S. data protection laws apply to only "identified" data, meaning that they are stored in a format where individuals are explicitly associated with relevant data. "Identifiable" data is a broader term used in new laws such as GDPR and CCPA, and includes all data that could reasonably be associated with an individual, even if they are not directly tied to identifiers such as a name or address within a stored data set. **There is growing consensus that an individual data protection regime likely needs to cover both "identified" data, and data that are "identifiable" to an individual**.[262] The formats and types of data that fall within the scope of new data protection laws has been broadening to reflect the failure of so-called "anonymized" data.[263] Data ranging from demographics,[264] to metadata,[265] to location, and much more[266] that is no

longer “identified” to an individual, can easily be reattached to specific people and used to uncover extremely sensitive details about their lives.[267] A deeper examination of “de-identification” began in the 1990’s led by Professor Latanya Sweeney, Ph.D. Dr. Sweeney discovered that data that excluded explicit identifiers (name, address, phone number, etc.) could still be used to identify individuals when combined with other databases, including those that are publically available.[268] At the time of that research she found that 87 percent of the U.S. population could be uniquely identified using only date of birth, gender, and zip code.[269] This statistic has likely only increased as more and more sensitive data sets have been exposed through data breaches.

Despite the reality that almost all information related to an individual is “identifiable” if enough separate pieces of data can be brought together, murky distinctions are still used, such as the term “reasonably linked” to an individual. This reasonability test can create positive incentives for essential, baseline technical protections such as de-identification and encryption, but it must be acknowledged that using these processes cannot fully negate the fundamental risk of collecting, processing and using information in the first place. This report therefore puts forth for consideration a stricter idea that protections cover data in any format, including “de-identified” and encrypted data, if it relates to individuals and can be re-identified within the entity. Ideally, this could work in tandem with security and conduct standards to incentivize companies to limit the amount of data that is collected and processed to what is absolutely necessary for the use case.

A broad scope of protection across both “identified” and “identifiable” data could also potentially help drive the development of new technologies and techniques that can enable more complete, and permanent, anonymization. There are already innovations that move in this direction, by greatly limiting the ability for entities and partners to re-identify, or unencrypt information. These technologies will be discussed in more detail in the upcoming section, *Technology for Individual Data Protection*. Simultaneously though, new advances in quantum computing may make it easier to break traditional encryption.[270] This highlights the need for more research around new technologies with the potential to keep information more secure, and the need to continuously evolve protection expectations to keep pace. Given the ease of re-identification today, this research cautions against reductions in protection expectations simply because data have been “de-identified”, until there are more avenues for technological certainty. This concept is a significant divergence from how current law treats data, and a transition period for entities to reach higher compliance standards, or to incorporate new de-identification techniques would be warranted. Additionally, with everything related to data within this report, it is recommended that governance be iterative and adapt to changing technology and revealed impacts.

Liability and Remedies

The prior sections have focused on reducing risks, but it is also **important to consider the creation of usable systems to make individuals whole if harms do occur**. Liability is a mechanism for allocating the responsibility for remedy across entities, including potentially individuals bearing some responsibility themselves. U.S. consumer protection laws, such as the Electronic Funds Transfer Act (EFTA), contain the concept of negligence and indicate circumstances where an individual can be held responsible for certain harms.[271] As discussed in the earlier section, *The Limitations of Individual Consent*, it is exceptionally challenging for individuals to effectively assess the potential risk of data activities, especially given the multitude of digital interactions and the realities of behavioral science. This current reality, combined with the variation in resources available to diverse groups, makes placing liability directly on individuals fraught. If individuals are expected to hold even limited responsibility in the future, supplemental systems need to be developed that alert individuals about risky entities and activities. For example these systems could provide consistent processes for indicating business compliance, and highlighting variations.

Another important, and challenging area to consider is how to best structure both individual compensation for harms and punitive deterrence mechanisms. Hopefully, the allocation of responsibility across all entities can provide businesses with a clearer understanding of their liability, but there are ongoing debates relative to the effectiveness of private rights of action,[272] arbitration, class action lawsuits, and government fines to both deter risky activities and compensate individuals. While the threat of unexpected legal action may serve as a deterrent, individuals rarely go through arbitration processes.[273] Class action lawsuits can result in limited compensation, especially if harms are difficult to measure, and not immediate, such as the Equifax breach. In cases where actual harms have not yet manifested or are not tangible in nature, class action compensation is often applied equally across all individuals irrespective of potentially varied harms.[274] Simultaneously, direct lawsuits can provide larger, potentially more relevant compensation, but they typically require that individuals demonstrate tangible harm, which as discussed previously, is not always possible. Government fines levied on companies are also problematic. They typically do not provide remedy directly back to the individuals and have been widely cited as lacking impact relative to the size and scope of companies they are levied against.[275] The American Law Institute also recommends that remedies be revisited, and proposes removing the general requirement to demonstrate tangible harm before seeking relief. The institute does not recommend specific approaches but does indicate that everything from enforcement actions, to direct compensation for injured parties be considered. It also notes that anxiety or emotional distress arising from privacy violations may be compensable, under specific court's precedents.[276]

Developing, and enforcing, security and conduct standards for all individuals, and across all entities in the U.S. would be a massive undertaking. Significant research, analysis, and design

resources are needed to implement this kind of option, and anything of this magnitude would likely need ongoing adjustments as impacts are monitored and evaluated over time. This kind of regulation may need to blend prescriptive and principles based approaches to enable both standardization and flexibility. For example there could be bright line expectations in some areas, and others may need to be interpreted on a case by case basis. While these things can be difficult to achieve together, a nuanced approach will likely make the structures more sustainable. It is also important that prescriptive rules are monitored and updated for applicability, and principles-based rules have clear and consistent review and oversight. More collective work is needed to determine how to best structure regulatory oversight and enforcement of the broad protection regime offered in this report. Financial services has long experienced direct supervision, while other sectors only experience regulation or enforcement after issues have become more significant and sometimes public. Both models have benefits and drawbacks as discussed in the earlier section, *Current U.S. Data Governance*. Finally, regulators in other countries, such as the United Kingdom's Information Commissioner's Office, are responsible for overseeing a huge spectrum of companies, and have implemented tools that could be explored here. For example, they require data protection impact assessments to be submitted in certain cases, which enables broader oversight.[277] The ALI also emphasizes the importance of documentation and reporting programs to help monitor compliance with data governance regulations.

The individual data protection framework laid out in this section is one approach among many, and would require the development of additional implementation details. Ideally though, a comprehensive framework like this could lay the foundation for a safe and competitive digital economy far into the future. Finally, and importantly, these protection ideas are not intended to be overly restrictive on the collection, flow, or use of information for the benefit of business growth, society, and individuals themselves. They are about analyzing the tradeoffs between current risks and opportunities, and targeting the right balance in order to achieve individual well-being, while enabling competition and innovation.

A Proposed Spectrum of Active Data Rights

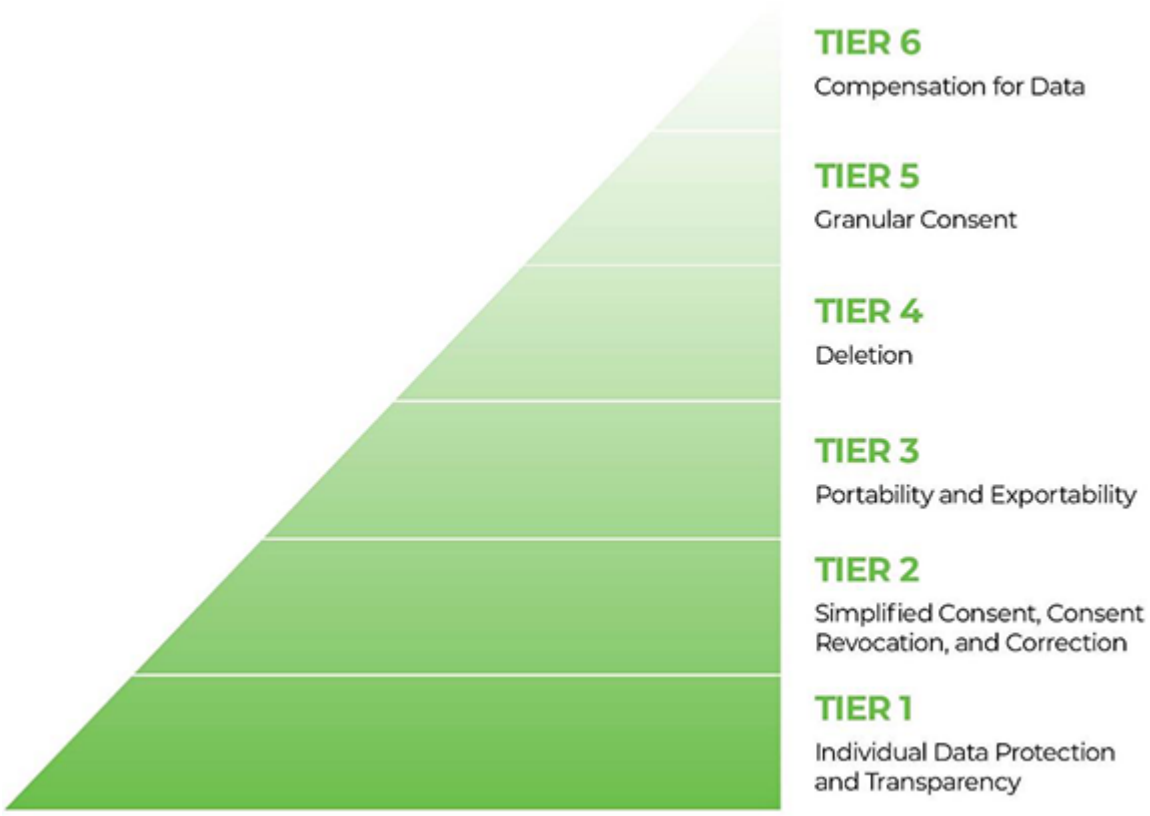
This section outlines the other side of the dual framework imagined by this research: a potential structure for what active data rights in the U.S. could look like. These concepts are intended to sit on top of the individual data protection foundation described above, which safeguards individuals irrespective of any proactive actions they want to take.

The overall structure draws from data rights that have been discussed internationally and domestically over the past four decades, such as active rights to transparency, error correction, portability, deletion, and more. This design varies the rights available to individuals in order to work in tandem with other policy considerations and sector-based requirements. Lessons from

systems that are currently available in the U.S., such as consent, as well as current laws also informs the design. Finally, this model does not assume that more choices and agency are always net beneficial, and instead recognizes that expecting individuals to constantly manage data choices, across the vast amount of daily digital interactions, can strain limited resources.

The concept of providing individuals with rights is foundational to the U.S.,[278] but it has been sporadically discussed and codified relative to technology. The ongoing dialogue around active individual data rights described in the beginning of this report is a huge advantage for developing a comprehensive and effective data governance framework for the U.S., and there is broadening acknowledgment that the time is ripe for a focus on comprehensive rights.[279]

Figure 1. A Spectrum of Data Rights



The graphic above proposes a bundle of rights that would apply across different circumstances. This concept borrows from Maslow's hierarchy of needs[280] in order to describe the interrelation and interdependence of these active rights. The base of the pyramid applies in all situations, while the availability of rights is reduced in subsequent tiers to account for other considerations. This layering also respects the impact that the use of active rights could have on business and research, which are fundamental to innovation, and the use of data for positive societal impacts. Individuals would retain their rights around "de-identified", or "identifiable", data, and there is only a reduction in available rights if companies create internal, technological barriers to re-identification, or if more effective anonymization techniques are developed. The nature of the

rights in each tier are outlined below, followed by additional discussion around the circumstances in which particular rights would or would not apply.

Tiers of Rights

TIER 1 - INDIVIDUAL DATA PROTECTION AND TRANSPARENCY

This first layer of rights is the broadest, and includes the baseline of data protection described in the prior section, as well a right to transparency, or visibility into data activities prior to them occurring, and on an ongoing basis. Data protection, and to some extent transparency, are negative rights rather than positive or active rights, but they are included in this section to provide a comprehensive picture of the proposed governance framework. The rights to protection and transparency are envisioned to apply to all data, activities, and individuals, irrespective of other variations.

While more research is needed on individual preferences around data, a clear theme throughout the research is the desire for transparency into what is being done with information and its potential impact on individuals. Another potential benefit of a consistent and complete requirement on transparency is that it could help create a deeper understanding on the part of individuals, and enable them to take actions that more closely align with true preferences, thereby reducing the incidence of the "privacy paradox" described in the previous section, *The Limitations of Individual Consent*. Important considerations for the right to transparency include how and where individuals will be able to see this information. Building out structures and guidance around this right is necessary so individuals are not alone in navigating and ingesting a new flood of information. For example, transparency is currently fulfilled through individual requests that must be sought out from, and provided by, each entity separately. This system is onerous for all parties. Individuals have no way to standardize and parse data in different formats. European companies have also experienced a number of falsified requests for information that are challenging to navigate while also responding to new, valid requests.[281] Promisingly, there are new dashboards being developed which can provide a more consolidated view into what data have been collected and where they are flowing. These tools could also be leveraged for subsequent layers of rights such as correction and deletion. Unfortunately, these dashboards are still being housed within individual entities and do not currently connect across the universe of data activities to provide a comprehensive picture into what is going on. These tools will be discussed in more detail in the upcoming section, *Technology to Enable Active Data Rights*. A concern has also been raised that a right to transparency would force companies to re-match data to individuals that they otherwise could keep more secure. An option to consider is enabling this right to be fulfilled through both summary information around what has been collected, processed, and used, and by providing full data sets. Summary information may be easier for individuals to interpret and can differentiate the right to transparency from a portability right that would require sending complete data sets. Summary information alone is likely not sufficient though. The FCRA originally only required bureaus to reveal summary information, but

that was deemed unsatisfactory and now full reports are provided.[282] This highlights the need to consider implementation options within each data right layer that can enable individuals to take action in whatever way best suits their needs and capacity.

TIER 2 - SIMPLE CONSENT, CONSENT REVOCATION, AND CORRECTION

This next tier includes a greatly simplified form of consent, the ability to revoke previously provided consent, and the right to correct errors. Simple consent is discussed in more detail in the earlier section, *The Limitations of Individual Consent*, and is intended to minimize the burdens on individuals. Similar to today, individuals would be able to indicate acceptance through simple, binary choices or potentially just by using the product or service. Unlike today though, they could be confident that the digital interaction is safe for them, and any data collected is necessary for the use case. For example, if an individual would like to use a digital map, the right to transparency would enable them to see that the collection and use of real-time location data is necessary for that particular service. They may choose to seek another service that allows for inputting of addresses directly, but in either case they can be confident that data will not be collected until they consent, what are collected is necessary for that service, and they will be protected from harm. The complete bundle of data rights also includes a mechanism for more detailed, granular consent which will be discussed under *Tier 5*. A goal of breaking consent into these two forms is to reduce the management burden on individuals for ubiquitous, daily interactions as much as possible, while still maintaining a role for choice and agency. With both simple and granular consent though, the burden would *not* be on the individual to determine whether the data that are collected and used are limited to what is necessary for the product, or that the activities are safe.

Simple consent could take the form of binary, opt-in agreements, but this would still place some burden on individuals to engage with that prompt every time they use a product or service that requires data. Another option for simplified consent is to make it passive, where an individual is expressing consent just by using the product or service. In this scenario a prompt would only be presented when more granular consent is needed, defined here as when new data are collected or original data are used, for purposes that are not strictly necessary for the original, primary product or service sought by the individual. This kind of approach is possible, but would still come with an expectation of transparency so individuals can see what collection and activities are necessary, before they happen. In the digital map example, services may not be able to default to using location data when the application is first opened, but if there is transparency around data activities and an individual moves forward in using the service, then real-time location could be collected. In some cases, such as websites, certain information like an IP address may need to be collected initially as part of the technological protocol, so passive consent may even be necessary in some cases. **The goal of simplified consent is to allow individuals to make active choices if they would like, but also enabling those that prefer to click-through or not engage, to do so without additional data collection or risk.** This layer of rights is also intended to break apart consent, or the act of making a choice, from transparency,

which is a separate opportunity for individuals to receive and ingest information for many different purposes.[283]

The additional rights that this layer confers are the ability to revoke consent, and the right to correct data errors. An important consideration for these rights is, as always, implementation. A revocation of consent would mean that no additional information is collected, processed, or used by the entity. Revocation of consent should be simple to accomplish for individuals, and ideally could be tied to the right to transparency through a comprehensive platform that can provide both visibility and these elements of control. There may be situations when revoking consent would change the functionality of a product or service, which would need to be made clear to individuals. Deleting previously collected information will be discussed under *Tier 4*. The right to correction would mean that mechanisms are in place for individuals to flag, or dispute errors in data. This also means that there is a responsibility placed on entities, potentially within conduct standards, to verify and respond to correction requests. Verifying that correction requests are legitimate and true is essential to not only maintain accuracy, but also to prevent individuals from cherry-picking, or altering the data available for sensitive cases, such as eligibility determinations.

While it is essential to verify the identity of the individual making the correction requests, it is also important to limit, to the extent possible, collecting additional data for this verification. Reviewing data, making corrections, and authenticating themselves should also not be too burdensome on individuals. The identification and correction of true errors benefits both individuals and businesses, but if systems are not accessible and easy to use, uptake will likely be limited. Ideally the processes for correction can also be tied to the same tools used for transparency and revocation. A balance would need to be struck between providing summary information to fulfill a transparency right in some situations, while providing the necessary detail in other situations to enable granular correction. Finally, the right for individuals to correct errors is distinct from an expectation within conduct standards that entities maintain accurate data, though they are compliments to each other. There may be proactive opportunities for individuals to correct information, but entities would still be expected maintain policies and procedures to monitor and promote accuracy, and investigate evidence of data errors as a normal part of doing business. An individual correcting errors would not imply that a conduct standard of accuracy was not upheld, instead it is a subsequent opportunity to improve.

TIER 3 - PORTABILITY AND EXPORTABILITY

The next tier of rights are portability and exportability. These are separated to indicate two distinct, but equally important elements of the right to move information between entities. Portability indicates a right to transfer data from one business at a single point in time, in order to switch between service-providers or start a new business relationship. Ideally, this enables businesses to compete, irrespective of the length of a relationship, and therefore, of the amount of information they may have collected from individuals. Exportability refers to ongoing transfers of information between two connected entities, both of which have relationships to an individual.

This ongoing transfer right enables new services to connect to information where it is already stored, rather than collecting it separately. This could also reduce the need to copy and store the same information in multiple places by creating the assurance that entities can access the minimum data needed for particular activities at the time that they are needed. Minimizing the amount of data that are created or collected, replicated, and stored can lessen risk to individuals and reduce some of the compliance load on entities. The right to portability and exportability are new additions to the baseline of FIPs, but could serve policy goals around competition, and would hopefully incentivize secure, interconnected relationships between entities. Important considerations for these rights are expectations on the timing and structure of both one-time and ongoing data transfers. It is also important that the timing and format of these transfers align to the necessary use case in order to maximize their value to individuals.

A key distinction of this framework, which will be discussed in more detail below, is that this tier of individual rights is not conferred across all data and activities. The right to portability and exportability would *not* apply to information that has been permanently de-identified within an entity, and is considered non-sensitive. As discussed earlier, there are few ways to permanently accomplish de-identification today, but this carve out is intended to incentivize businesses to develop, and shift to more robust anonymization techniques and implement internal, technical barriers to re-identification. If companies can no longer identify information to individuals internally, then they could not comply with requests to port or export that information. Sensitive data would still be subject to this right, because while sensitive information is ideally kept in secure formats, it may also be important to allow individuals to use the most secure technology available to provide access to this information in new locations, in order to reduce replication and storage. The additional reductions in the availability of this right are around data that are inferred, such as consumer profiles, or algorithms that are trained on data. Individuals would still have transparency into the development and use of inferred information and trained algorithms, and be able to take actions around them, such as consent and correction where relevant, but these types of data have more business resources added to them and therefore could be considered the intellectual property of organizations. Hopefully, excluding these more value-additive data types from the right to portability and exportability can support competition and innovation goals. Individuals themselves could still provide inferred information directly to new entities, but the scale of transfers would be reduced. Additionally, if businesses themselves want to elect to make these categories portable or exportable to other entities they could always differentiate themselves by doing so.

TIER 4 – DELETION

The next layer in this conceptual structure is deletion. This concept is also new to the original FIPs framework, and was introduced in GDPR as the "right to be forgotten". While this right is important, and could potentially help reverse some of the data proliferation that has occurred thus far, this research suggests that there may be value to limiting it based on certain factors. Many financial consumer protection requirements, such as identity verification and fraud monitoring, require the retention of data. Additionally, current technological innovation, such as

machine learning, requires large amounts of data to train predictive models. Some of machine learning models are also designed to retain or revisit[284] original information. Implementing a blanket right to deletion could immediately come into tension with these regulatory requirements, security needs, and valuable innovation. Therefore, in this structure the formal right to delete is limited to instances when data are stored for secondary or tertiary uses of information, but it could apply to primary use cases wherever possible. To further incentivize the development of new technologies that more securely anonymize information, the right to delete would not apply to data that is permanently de-identified within companies, and non-sensitive, but as stated throughout this report, more research is needed to define a more secure threshold for "de-identification".

TIER 5 - GRANULAR CONSENT

As described above, the right to, and expectation that, individuals provide granular consent for proposed data activities is intentionally limited in this framework. While confined to only certain cases, this right would create a detailed level of consent for individuals to proactively opt-in to *only* new uses of previously collected data, or additional data collection that is not necessary for the original product or service. This more intensive form of consent requires additional time and attention on the part of individuals. This friction would only be necessary as data collection, processing, and usage move further away from the primary product or service sought by the individual, and there would still be an expectation that new activities are safe and necessary for the secondary or tertiary purpose. An example of granular consent might be an individual selecting among specific data, or categories of data they are willing to provide for new uses, or selecting among new activities that an entity wants to engage in. Retaining this more intensive form of consent is meant to respond to growing concerns about data activities that are significantly removed from the original product or service requested. In particular, unseen companies extracting value out of data in ways that are not reasonably expected by individuals can feel unfair, and can create mistrust in broader information systems.[285] Introducing friction at this moment is intended to alert individuals to the new activity, and allow them to judge for themselves whether the additional activities and value exchange are reasonable. Introducing this type of consent and additional friction is meant to retain the potential to innovate with data, but with more individual involvement.

There is still the potential that individuals will just click-through granular consent requests, which is why, again, consent is meant to work in tandem with the individual data protection foundation. Even in cases where there are downstream uses of information, legitimacy, conduct, and security would still be expected. This is intended to reduce the management burden on individuals by not requiring detailed, granular engagement for more standard digital interactions, while also streamlining business requirements if they are only engaging in primary, necessary activities. More research is needed across both simplified and granular consent to understand how to effectively, and equitability, engage those individuals who wish to participate in these active rights. Furthermore, work is needed to understand how to communicate the

complexity of data activities within both the rights to transparency and granular consent, while still easing the management burden on individuals.

TIER 6 – COMPENSATION FOR DATA

The final potential right is direct compensation for data. As discussed in Part 1 under, *Reframing from "Data Ownership" to "Data Rights*, treating information as a commodity for individuals is difficult to implement and may have unintended consequences if done on a large scale. On a small scale though the concept of paying individuals to provide information or exchanging data for services is not unprecedented. In research contexts individuals are frequently paid to take surveys. In order to mitigate the challenging externalities of large-scale, direct individual compensation for data, this framework limits the right to be compensated to only tertiary uses of information, such as marketing or downstream resale for monetization. Like the idea of granular consent, this right is intended to increase individual agency and choice if information is used and reused for purposes beyond the original product or service they signed up for.

Variation of Rights for Risk and Purpose

This section is intended to provide the necessary nuance and customization required to effectively implement the bundle of individual data rights described above. This part of the framework approaches varying available rights based on three key factors. The first factor is the type of data, defined by how much involvement a business has had in the development of the information itself. The second factor is the distance from the original purpose of collection that an individual would reasonably expect to occur, and the final factor is the relative risk of the data and the format that it is stored in.

Data Type: The types of data outlined here are intended to describe different levels of individual and business contributions that go into creating pieces of information. The types considered are: "provided", "collected", "inferred", and "trained algorithms". "Provided data" refers to information that an individual enters onto a form, or provides directly to an entity. Collected information are data that have been generated through an individual's interaction with technology—this encompasses transaction data from the use of financial products, health data, such as from step or heartrate monitors, or other information that is passively observed about individuals. "Inferred" data is entirely new information, created through proprietary techniques, but based on provided or collected information—this includes a company's proprietary analysis of data, and the insights they gain from that analysis. Examples of this are credit scores or customer profiles. "Trained algorithms" are the models that are created using large stores of provided, collected, and inferred data to identify patterns, make predictions, and much more. The categories of "provided" and "collected" data represent more limited activity on the part of businesses in the actual creation of new information, and are more closely associated with direct actions taken by individuals. Individual rights are strongest with these first two types of information. Inferred data and models that are produced by businesses, have more intellectual property input into them, and therefore some individual rights, such as the rights to portability/exportability and deletion,

may be limited to preserve competition and incentivize innovation. There may be exceptions where inferred data are widely used and shared, such as credits scores, and therefore porting or exporting them to competitors is no longer a business concern, or may even be required by law. There are also categories of data that are inferred by businesses but could still warrant additional rights, such as portability/exportability. An example of this are customized fees that individuals are charged for products.

Fees may be tied to a unique customer profile that a company builds, but the ability to easily share that information can also help individuals compare prices and find better products for themselves. Cases like this warrant additional consideration, but individuals can always provide that kind of data directly to companies rather than porting it between entities directly. Even in cases of more business input though, entities would still be expected to comply with the broader tiers of data rights such as transparency and simple consent. Businesses can also differentiate themselves by providing additional rights to individuals beyond what is suggested in the framework.

Data Purpose: This distinction wrestles with the tensions that have arisen around fair-value exchange for data, and reduces the active management burdens on individuals when data activities are solely in service of the original product or service. Primary uses capture data activities that are necessary to deliver the product, service, or content that an individual is seeking. This definition includes essential business partnerships as well as activities that are necessary to comply with legal requirements. The necessity of those activities and partnerships would be tested through the legitimate purpose expectation described in the section, *The Limitations of Individual Consent*. For these more straightforward and frequent situations, the framework does not provide for certain individual rights in order to reduce the active management expected of individuals.

The focus on primary purposes could also reduce the management burden on companies to provide the higher tier rights, hopefully incentivizing a clear delineation of how, and why, information, processing, and partnerships are needed prior to activities occurring.

Secondary uses of data are defined as tangential to, but not necessary for, the original product or service. An example of this would be developing new product functionality. It is also important for companies to differentiate in partnerships when it is truly necessary to transfer data to new entities. A partnership may be necessary to provide a particular product or service, but transferring data directly to that partner, or them storing that data, may not be necessary. An example of data activity that falls outside of the primary purpose of a relationship and use case would be a partner entity retaining a copy of data provided for a one-time analysis. Creating this distinction is intended to incentivize companies to build partnerships that do not require additional visibility into, and retention of, data, but more research is needed to understand the breadth of data management processes across various service provider relationships, especially as technology evolves.

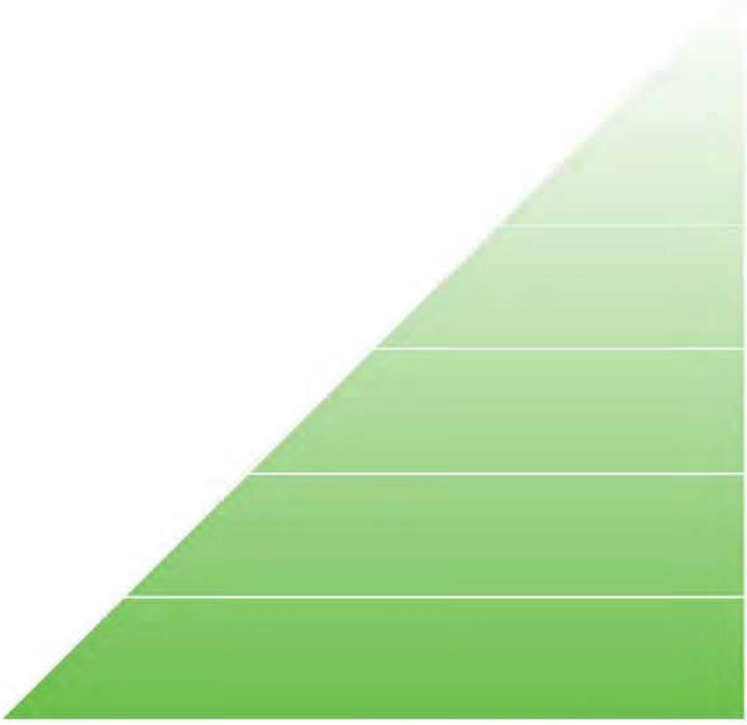
Tertiary uses indicate that data are being leveraged completely outside of the original relationship and intent, such as re-sale to an external, unaffiliated party to generate revenue. Evidence suggests that individuals are primarily concerned about data collection, processing, and use by entities that they are not aware of.[286] The exchange of value becomes more opaque as information transitions away from the entity that an individual first engages with, therefore this layering of data purposes is intended to strengthen rights, and the choices available to individuals as information moves downstream of its original purpose and relationship, without creating explicit prohibitions on activities.

Data Sensitivity: This is divided into only two categories of more or less sensitivity. More sensitive data is the broader category and captures both "identified" and "identifiable" data as well as information that may be deemed especially risky, such as account and routing number or health status. The category of less sensitive data refers to information that is not especially risky, and has been permanently de-identified internally, meaning that the entity cannot relink the data to specific individuals. Today, many companies can re-identify and use data with few restrictions beyond internal process controls, such as employee access levels. Individual rights are reduced for low sensitivity data and formats, and conversely entities retain more control over data. This is intended to create an incentive for entities to use technological barriers to re-identification, instead of process barriers, and ideally reduce the potential for internal misuse of data to harm individuals.

Unfortunately, there is always the potential for data breaches, and malicious, external re-identification of data, despite high-quality cybersecurity and advanced internal de-identification techniques. Therefore, for data to fall within the low sensitivity category, entities would *not* be expected to guarantee that data could not be re-identified in the event of an external breach. Because of the constant risk of external attack and data loss, this category also calls out particularly high-risk information. For information to fall within the low sensitivity category, which shifts the balance of control towards entities, it cannot be high-risk data. This classification of higher-risk data has been done by other countries[287] which could be used as a reference. For example, biometric data, which cannot be changed, could be categorized as high-risk.

Across this report, the more stringent requirement for technical barriers to internal re-identification is not intended to restrict internal re-identification. If data need to be re-identified as part of the necessary use case that is absolutely acceptable—it just comes with a responsibility to provide stronger active individual rights. The goal of this is to create choice for entities: to focus on permanent, verifiable de-identification and the use of less risky information, or the provision of rights such as portability, exportability, and deletion, which necessarily require an association to an individual. Because of the intended permanence of internal de-identification, the framework does not contemplate information moving from the category of less sensitive, and less individual control, to more sensitive and more individual control.

Figure 5. A Data Governance Framework
A summary of how the data rights pyramid could be used in tandem with other considerations around data type, data purpose, and data sensitivity.



TIER 6
Compensation for Data

TIER 5
Granular Consent

TIER 4
Deletion

TIER 3
Portability and Exportability

TIER 2
Simplified Consent, Consent Revocation, and Correction

TIER 1
Individual Data Protection and Transparency

	Data Sensitivity Categories	
Data Types	**More Sensitive** Identifiable or high-risk data	**Less Sensitive** Permanently de-identified and low-risk data
Primary Purposes: Necessary for the product or service, legal requirements		
Provided and collected data	Tiers 1 - 3, 4*	Tiers 1 - 2
Inferred data	Tiers 1 - 2, 4*	Tiers 1 - 2
Trained algorithms	Tiers 1 - 2	Tiers 1 - 2
Secondary Purposes: Product improvements, unnecessary partner transfers		
Provided and collected data	Tiers 1 - 5	Tiers 1 - 2, 5
Inferred data	Tiers 1 - 2, 4 - 5	Tiers 1 - 2, 5
Trained algorithms	Tiers 1 - 2, 4 - 5	Tiers 1 - 2, 5
Tertiary Purposes: Marketing, downstream monetization		
Provided and collected data	Tiers 1 - 6	Tiers 1 - 6
Inferred data	Tiers 1 - 2, 4 - 6	Tiers 1 - 2, 5 - 6
Trained algorithms	Tiers 1 - 2, 4 - 6	Tiers 1 - 2, 5 - 6

**Entities uphold the deletion right unless there is a legal requirement to maintain the data. For example for tax reporting, BSA/AML compliance, a court order, etc.*

This bundle of active data rights is one potential structure intended to balance tradeoffs and align incentives broadly, but additional individual rights may be warranted, or not, depending on particular situations and sector-based needs. This framework strives to strike a balance between principles and prescription, while leaving much of the details open for discussion and refinement by stakeholders. These ideas are intended to evolve through ongoing discussion, and, as ideas are implemented, categories and approaches will likely need to adapt to be effective in practice. Additionally, as has been stated throughout, any data governance should be revisited over time to respond to broad social and market changes. For example, the scope of both protection and rights could be revisited if new anonymization technology are developed, tested, and implemented.

Finally, this concept of data rights is intrinsically linked to data protection, and therefore developing them together is beneficial for the overall approach. For example, areas where alignment is necessary between individual data protection and active data rights include:

- A business responsibility of accuracy and a right to correction. A responsibility for data accuracy may be included as part of a broad conduct standard, and an active right to correction would also enable individuals to flag and correct data where possible. The fact that an individual corrects information does not automatically mean that a company is not meeting an accuracy responsibility.
- A legitimate purpose expectation, and the provision of transparency and consent rights. The details of a legitimate purpose expectation can be part of communication to individuals under their active rights to transparency and within simple or granular consent prompts.
- Conduct expectations around data retention and an active right to deletion. If individuals are aware of reasonable deletion timeframes that are built into conduct standards they may not need to use their active data right of deletion.

Technology and Business Models to Support Data Governance

While this paper offers for consideration broad policy interventions to address data protection and data rights, there is a simultaneous need for both technology and business design that can support and facilitate these kinds of proposals.[288] The frameworks described above are intended to incentivize this kind of innovation while also benefiting from it, and this section explicitly calls out areas where new models and technologies could help facilitate collective data governance goals.

Technology for Individual Data Protection

Technology has transformed many aspects of our lives, and a significant contributor to that innovation has been the ability to gather and leverage new information. While the use of large amounts of data remains valuable, there is a growing movement to explore how data activities can be more deliberate, secure, and private, all while retaining the benefits that new information can provide. There has been an increase in privacy-focused technology to help facilitate compliance in the wake of GDPR and CCPA, as well as a broader conversation around "privacy-enhancing technologies" (PETs) that is driven by increasing market demand and forward leaning companies. There is no uniform definition of PETs, but they are broadly defined as technologies that help achieve the goals of data protection.[289] An important element of PETs is shifting some of the conduct processes away from human implementation, which can be variable and qualitative, and towards consistent and readily auditable technological systems. Encryption is an example of a well-known and long-standing PET. Notable, newer PETs include differential privacy, secure multi-party computation, and homomorphic encryption, among others.[290] These new techniques span two important elements of data protection: de-identification and encryption. De-identification is the process by which data ideally can no longer be associated with an individual, while encryption refers to scrambling or hashing information so it is unintelligible without an encryption key to decode it. Encryption can protect both identified, and de-identified information.

Differential privacy[291] is an anonymization technique that enables businesses to determine, and adjust, the probability of data re-identification. At its core differential privacy inserts fake data among real data, or randomizes information to obscure individual identities. This is distinct from traditional de-identification which removes pieces of real data in order to obscure identities. Differential privacy still allows for analysis to be done on data through averaging information, but data that have been de-identified in this way cannot be re-identified simply by combining data sets. While this technology is not effective for use cases that require identified information, for data processing that only needs averages, such as website improvements, this could be a powerful option.

A related tool is local differential privacy, or on-device analysis.[292] In this process, randomized or fake data are combined with real data before they leave a physical device, such as a cell phone. This means that the company collecting the information never receives the true, identifiable data set. While differential privacy may be more secure if data is lost in an external attack, local differential privacy also creates a barrier to internal misuse of information. This technique is dependent on the availability and quality of physical devices, and it does not prevent problems such as bias stemming from a lack of representative data or algorithm design. Together though, differential privacy, and local differential privacy have demonstrated new methods for more securely de-identifying information, and creating a technological barrier to re-identification of data even internally within an organization. While this is positive for individual data protection,

there are also ethical considerations around the potential need for law enforcement to access true underlying information.[293] More work is needed to delve into these ethical and technological considerations.

Secure multi-party computation is a form of cryptography that involves breaking apart data, and storing and analyzing those pieces in different locations. The goal of this technique is to avoid giving any one party complete access to an identifiable data set.[294] This technique could potentially facilitate partnerships where less data can be shared, but joint work can still be completed for business needs. Technology like this could enable service providers to create value for their clients without the additional risk of copying and storing data directly. Another PET that is commonly highlighted is homomorphic encryption. This depends on advances in computing power, but it enables businesses to perform analysis on encrypted data, and only unencrypt the end result. Typically, data have to be unencrypted in order to perform analysis on it, creating additional risk for breach or misuse during processing activities. With homomorphic encryption, there is a potential that data could be permanently encrypted, and therefore remain anonymous to business partners and even the original company, while still enabling analysis and value to be extracted.

Finally, and importantly, application programming interfaces (APIs) are a technology that can help improve overall data protection. APIs enable software at different firms to connect, and securely share data. This technology allows partners to set clear expectations for what information will pass between them at a particular cadence, while creating a record of that activity. This is in contrast to the data-sharing technique known as screen-scraping, which utilizes software to "read" webpages, and create copies of the information displayed. While both APIs and screen-scraping may create copies of the data being transferred, APIs can provide ongoing connections that negate the need for storage, offer more control to businesses sharing data, and can create digital records to enable oversight of, and compliance with, a data protection framework.

A final, and likely essential, role that technology can play in broad data protection is through automated monitoring of data activities. If technology can be leveraged to record activities, such as tagging and tracing data as they flow between entities, then the resource burden of extending the oversight perimeter across more entities, could potentially be reduced.[295]

Technology to Enable Active Data Rights

Technology can be leveraged to not only facilitate broader, and more effective data protection, it can also be used to make data rights more accessible and actionable for individuals. Current examples of this are platforms, or "dashboards" being developed by banks,[296] and data aggregators[297] that allow for individuals to see what data they have consented to share, and with whom. These kinds of connected services can help support the entire bundle of rights by providing a consolidated holistic view into data activity, and ideally reducing the number of

separate actions individuals need to take across companies. While these services hold promise, they remain limited in their connectivity. A key challenge is that many of these dashboards only give insight into data shared from, or to, the entity providing the dashboard. There is a vast number of additional locations where individual information is collected, but those may not be reflected in dashboards if they are created solely at the entity level. Additionally, the control exerted by individuals within the tools, such as revoking previously provided consent, typically only apply to the entity that provides the platform. For example, if an individual wishes to revoke consent for data activities, a financial institution dashboard can limit the sharing of future information, but cannot necessarily restrict activities on data that have already been provided to other entities. This means that currently data control through these tools is limited to be-spoke technology, connections, and agreements.

Another technical opportunity that could potentially be leveraged to support data rights, in addition to data protection, are digital identities. Verifying who individuals are in digital interactions is essential in financial services, and beyond. Currently, identity is verified at the beginning of a relationship, usually through the collection of multiple pieces of information, including government provided identification. After that initial verification, individuals must be constantly re-identified when they come back to a website or application. Confirming that a new login is the original individual who signed-up is much more difficult in online interactions, and it typically involves matching a significant number of different data points to confirm that it is not only the correct individual, but that it is a human logging in rather than software programmed to imitate real log-ins. Information matching can range from just confirming that the individual possesses the correct username and password that were previously provided to them, to capturing IP addresses, keystrokes, location, and much more. All of this activity requires significant data collection and data storage, and yet fraudulent actors continue to gain access to digital systems. The Financial Crimes Enforcement Network (FinCEN) estimates that there are billions of usernames and passwords, as well as sensitive personal information, currently exposed to fraudulent actors,[298] which can be used to gain access to online accounts.

Due to the complexity and challenge of authenticating an individual's physical identity digitally, there have been a number of systems developed, and proposals for new systems, to create unique digital identifiers. Digital identities can take many forms, but ideally they can limit the need to collect and store increasingly more information in order to authenticate individuals. These systems have been primarily created in two ways: as a centralized utility, or through a de-centralized, distributed ledger, or blockchain.

One of the most well-known centralized digital identity systems today is India's Aadhaar program. The program was designed to be used both physically and digitally, and it was created by gathering demographic and biometric data from every Indian citizen, and then assigning them a unique 12-digit number.[299] Other examples of government-based systems include a digital driver's license, which is being explored by U.S. states,[300] and a national utility in Singapore

to help banks comply with financial Know Your Customer (KYC) regulation.[301] The value of centralizing this kind of identification with governments is that governments typically provide and manage physical forms of resident or citizen identification already, and the incentives between governments and individuals are hopefully aligned around keeping the underlying information secure and confidential. There are also private companies that are exploring how to provide and use centralized digital identities,[302] but more work is needed to understand what scale is needed to not exclude diverse populations, and what the appropriate oversight mechanism should be for such a fundamental system existing outside of the government. The additional challenge with centralized systems is that they create one central point of attack or weakness, and they are vulnerable to corruption.

An alternative to centralized systems is using distributed ledger technology to create digital identities. A number of private entities[303] and consortiums[304] have been established to provide this service, and, while they vary in their design, the underlying concept is that the pieces of information that comprise an individual's identity are stored, verified, and updated on a shared record across a number of different entities. These kinds of systems hold potential because they are not dependent on any one entity for functionality or protection. Another important element of these systems is that they could allow individuals to break apart and share limited pieces of their identity depending on what is needed for particular situations. For example an individual could share a confirmation that they received a particular education degree with an employer, while withholding other information such as their home address. Similar to the challenge of digital identity provided by one company though, these systems need scale to be truly effective. To be a ubiquitous identification system, a strong majority of individuals need to have their identities in the system, and a majority of entities that need identity verification and authentication have to accept the system, otherwise both groups will default to old forms of identification that require constant data collection and use.

Both centralized and distributed identities are still early in their development, and more work is needed to explore the potential of these kinds of systems to both protect individual data and enable active rights. The Federal Reserve Bank of San Francisco is embarking on a follow-on research project focused on the potential of privacy-enhancing technologies and data infrastructure to support data governance.

Aligning Business Models

While data governance principles, and technological innovation, can be developed and disseminated through both public and private efforts, there is an important, and unique, role for the private sector to play in aligning business models more closely with individual preferences around data protection and active data rights. Businesses develop where there is market demand, but that does not necessarily mean direct demand by individuals. In the data ecosystem there is significant demand for information among companies in order to design

better products, market to new customers, and compete with rivals. But this focus on business-to-business demand can drive data activities that are disconnected from individual's own need for data, and their preferences with regard to privacy.

There is a growing role for investors to play in identifying and supporting business models that are more aligned with individuals' preferences, rather than focusing on broad data collection and use for business to business monetization.[305] It is important to examine when entities are making choices on behalf of individuals, such as collecting data without truly informed consent, and when their profits may be dependent on those kinds of systems. More work is needed in the investor community, between partners, and within companies to more clearly identify when profit incentives may run contrary to individual preferences with regard to data.

The current state of data proliferation and unfettered usage is not inevitable, and there is a potential that businesses and systems could default to less data activity, without sacrificing innovation or competition. The private sector, and the funders and organizations that support those businesses, have an opportunity to restructure digital ecosystems[306] to focus more on individual needs for information, rather than opaque revenue generation,[307] and this shift could be beneficial across sectors and policy goals.

Conclusion and Areas for More Work

This report proposes a radical shift in how the U.S. approaches data. For the reasons outlined throughout the paper—the importance of individual agency, the challenge of relying on market forces, the resources required from individuals to engage, the risk of entrenching bias and inequality, and the multitude of interrelated policy goals—it may be time to govern the digital realm more directly. Unfortunately, given the unique complexities of data, effective governance likely cannot depend solely on current law.[308] As this research demonstrates, there is value, and hopefully efficiency, in establishing a consistent baseline of individual data protection across all individuals and entities in the U.S. Furthermore, a complementary active data rights regime could work in tandem with data protection to empower individuals, achieve a number of interrelated policy goals, and help to more closely align the use of information as a national economic resource, with individual wellbeing. As much as possible it is also worth considering what elements of data governance can be harmonized with international systems. Data easily flows across country borders, and harmonizing approaches can be beneficial for trade and global community, but given the wide variation in cultures and government structures, variations across countries may be necessary and potentially inevitable.

The concepts and designs included in this report are not meant to be prescriptive, but rather another step in a broad conversation around the evolution of data governance in the U.S. among policymakers, regulators, market stakeholders, advocates, and researchers. There is growing consensus around many of these concepts,[309] but more work is needed to continue to flesh out the details, and tradeoffs, of implementation.

Specific areas for further work and consideration include:

- How a legitimate purpose expectation would be defined and overseen.
- How much proportionality is warranted and safe within a broadened perimeter of regulatory oversight.
- How to best use supervision versus enforcement tools in data governance. Supervision requires significant resources and expertise, while enforcement means that some harm may have occurred prior to a correction occurring.
- Which forms of remedies (such as a private right of action, fines, etc.) will work best to both reduce data harms, and rectify them if they occur.
- The development of better systems to quantitatively measure the cost of data-related harms to individuals and society.
- The development of better forms of communication and tools for data activities, with a focus on consistency, accessibility, and empowering individuals to act upon rights.
- A deeper exploration around the potential roles for trusted intermediaries, with a particular focus on aligning incentives and making them equally accessible to diverse populations.
- More research on the needs and preferences of diverse populations around technology and data.
- How to integrate policy considerations around the use of algorithms in decision-making into a broader data governance framework. This could take the form of expanding data rights into a consideration of "digital rights".
- The creation of systems to monitor the impact of new laws such as CCPA, in order to incorporate those lessons into broader efforts.
- Further refinement of the concepts presented in this report, and across the data ecosystem, as well as potential codification and implementation. This could take the form of a dedicated task force, an implementation entity, or even a new federal data-focused agency.[310]
- How physical data infrastructure is currently structured, owned, and used; and how that structure could support or impeded policy goals. In addition to research on privacy-enhancing technologies, this is an area where the SF Fed will focus ongoing research.

The COVID-19 global pandemic has further highlighted how essential data governance is to enable society to use information while keeping individuals protected. As the crisis unfolds, and eventually passes, it will be more important than ever to debate and refine the questions and considerations raised in this paper.

The Federal Reserve Bank of San Francisco looks forward to continuing to participate in this ongoing, nation-wide dialogue.

Appendix A - Definitions

Definitions are not intended to be statements of fact, but provide clarity on these terms in the context of this report. Where relevant, definitions have been pulled directly from entity mission statements and materials.

Aadhaar: An Indian national digital identity system based on biometric and demographic data.

California Consumer Privacy Act (CCPA): A California law passed in 2018 which aims to enhance consumer privacy rights and protections for California residents in relation to personal data.

Data access/transparency: The ability or authorization to view what consumer information is being collected, and/or stored, by an entity.

Data consent/permission: A consumer's decision regarding data (could be permission to initially collect or use information, to port data, etc.).

Data dividend: The concept of consumers receiving a cash payment for the use of information related to them.

Data Empowerment and Protection Architecture (DEPA): An initiative by the Indian government to create country-wide data infrastructure for the use and maintenance of consumer information.

Data fiduciary: An entity with a legal and/or ethical obligation to act in the best interest of individual consumers with regard to data.

Data portability: The ability to provide consumer information stored at one entity to another, unrelated, entity. Commonly associated with technical standards to facilitate the provision of information between entities.

Data at rest: Information that is not currently being used by an entity, and is stored in a digital format.

Data in transit: Information that is flowing with a single entity's network, or is flowing in a network between multiple entities.

Differential privacy: The ability for computer systems and algorithms to obscure whether an individual's information was used in a particular output or computation.

Digital identity: Information used within computer systems to authenticate the user that is interacting with those systems.

Digital phenotyping: The identification of human traits through information on the use of, and interaction with, technical devices and platforms. (E.g. website browsers and mobile phones).

Disclosure: Information provided to a consumer regarding entity activities and/or decisions they may be authorized to make regarding those activities.

Distributed ledger technology: An immutable, synchronized digital record maintained through a consortium of entities.

Encryption: A code that is used in place of raw data to obscure, and therefore protect, sensitive information. Typically the code comes with an "encryption key" that enables conversion between the raw and coded data.

Fair Credit Reporting Act (FCRA): Regulates the collection of consumer credit information and credit report access.

Financial Data Exchange (FDX): A U.S. member-based organization across the financial ecosystem working toward enhanced consumer-controlled data through an API and shared technical standards.

Financial Data and Technology Associate (FDATA): A UK-based trade association with global chapters aiming to ensure consumer rights to access financial products.

General Data Protection Regulation (GDPR): An EU law passed in 2016 that aims to enhance data protection and privacy for all citizens of the EU and the European Economic Area.

Gramm-Leach-Bliley Act (GLBA): Requires financial institutions to explain their data sharing and protection methods and practices.

Habituation: A form of learning where people become less responsive to stimuli the more they are presented with that same stimuli. (e.g., disclosures).

Health Insurance Portability and Accountability Act (HIPPA): Protects the privacy and security of health information.

Homomorphic encryption: The ability to perform computations on encrypted information. Typically companies have to perform analysis on raw (unencrypted) data, which can leave it vulnerable to attack.

Multi-party computation: An analysis method that breaks apart the discrete tasks to be performed on information between multiple entities. The goal is for no single entity to have insight into the breadth of information being used.

National Automated Clearing House Association (NACHA): Oversees the ACH Network, the Quest Operating Rules for EBT, and Healthcare Electronic Funds Transfer.

Open Banking: A country-wide system for consumer-permissioned transfers of financial information between entities.

Prescriptive Regulation: A system of regulation that lays out detailed specifications and practices that business are expected to comply with.

Principal-based Regulation: A system of regulation that lays out broad but well-defined objectives that businesses are expected to comply with. Companies are responsible for the design and implementation of practices that meet the regulation.

Privacy-enhancing technologies: A set of technologies that seek to minimize the use of sensitive digital information without losing functionality.

Section 1033 of the Dodd-Frank Act: States that companies should make available to a consumer, upon request, information pertaining to their financial products and services in a usable electronic format.

Time/delay discounting: A behavioral economics term to describe the findings that people tend to value immediate rewards over future ones.

Unfair, Deceptive, or Abusive Acts and Practices (UDAAP): Practices that are defined as harmful to consumers financially and cannot be reasonably avoided.

References

[1] Mayo Clinic Networks. "What is contact tracing, and why is it important in fight against COVID-19?" MSN. April 28, 2019. https://www.msn.com/en-us/health/medical/what-is-contact-tracing-and-why-is-it-important-in-fight-against-covid-19/ar-BB13k54K

[2] "Privacy & Pandemics: The Role of Mobile Apps (Chart)." Future of Privacy Forum. April 2020. https://fpf.org/wp-content/uploads/2020/04/DP3T_The-Role-of-Mobile-Apps-Chart-10.pdf.

[3] "Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown." University of Oxford. April 16, 2020. https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown

[4] Timberg, Craig, Drew Harwell, and Alauna Safarpour. "Most Americans are not willing or able to use an app tracking coronavirus infections. That's a problem for Big Tech's plan to slow the pandemic." The Washington Post. April 29, 2020. https://www.washingtonpost.com/technology/2020/04/29/most-americans-are-not-willing-or-able-use-an-app-tracking-coronavirus-infections-thats-problem-big-techs-plan-slow-pandemic/

[5] Zetter, Kim. "Anonymized Phone Location Data Not So Anonymous, Researchers Find." Wired. March 27, 2013. https://www.wired.com/2013/03/anonymous-phone-location-data/

[6] Collins, Michael. "IRS' antiquated technology could delay delivery of $1,200 coronavirus stimulus checks, experts warn." USA Today. April 4, 2020.https://www.usatoday.com/story/news/politics/2020/04/04/coronavirus-stimulus-outdated-technology-could-delay-checks-experts-say/5112012002/

[7] Goldstein, Dana, Adam Popescu, and Nikole Hannah-Jones. "As School Moves Online, Many Students Stay Logged Out." New York Times. April 6, 2020. https://www.nytimes.com/2020/04/06/us/coronavirus-schools-attendance-absent.html?campaign_id=158&emc=edit_ot_20200505&instance_id=18236&nl=on-tech-with-shira-ovide&regi_id=92128841&segment_id=26646&te=1&user_id=c8211ba7a76400964e6e36c656c9497e

[8] Crocker, Andrew, Kurt Opsahl, and Bennett Cyphers. "The Challenge of Proximity Apps For COVID-19 Contact Tracing." Electronic Frontier Foundation. April 10, 2020. https://www.eff.org/deeplinks/2020/04/challenge-proximity-apps-covid-19-contact-tracing

[9] Brill, Julie and Peter Lee. "Preserving privacy while addressing COVID-19." Microsoft Corporation. April 20, 2020. https://blogs.microsoft.com/on-the-issues/2020/04/20/privacy-covid-19-data-collection/."

[10] Sonmez, Murat. "How personal data could help contribute to a COVID-19 solution." World Economic Forum. March 23, 2020. https://www.weforum.org/agenda/2020/03/covid-19-personal-data-new-commodity-market/

[11] Carlin, Bruce Ian, Arna Olafsson and Michaela Pagel. "FinTech and Consumer Financial Well-Being in the Information Age." (2019).

[12] Ceglowski, Maciej. "Statement of Maciej Cegłowski, Founder, Pinboard" United States Committee on Banking, Housing and Urban Affairs. United States Senate, May 7, 2019. https://www.banking.senate.gov/imo/media/doc/Ceglowski Testimony 5-7-19.pdf.

[13] Patrizio, Andy, and Andy Patrizio. "IDC: Expect 175 Zettabytes of Data Worldwide by 2025." Network World, December 3, 2018. https://www.networkworld.com/article/3325397/idc-expect-175-zettabytes-of-data-worldwide-by-2025.html.

[14] Various Authors. "The Privacy Project." The New York Times. Accessed March 2020. https://www.nytimes.com/series/new-york-times-privacy-project.

[15] "FTC Hearing 12: April 9 Session 1 Opening Remarks by FTC Chairman Joe Simons Followed by Panels on the Goals of Privacy Protection and the Data Risk Spectrum." Federal Trade Commission, September 26, 2019. https://www.ftc.gov/news-events/audio-video/video/ftc-hearing-12-april-9-session-1-opening-remarks-ftc-chairman-joe.

[16] Herrera, Tim. "You're Tracked Everywhere You Go Online. Use This Guide to Fight Back." The New York Times, November 24, 2019. https://www.nytimes.com/2019/11/24/smarter-living/privacy-online-how-to-stop-advertiser-tracking-opt-out.html?fallback=false&recId=412412904&locked=1&geoContinent=NA&geoRegion=CA&recAlloc=home&geoCountry=US&blockId=home-living&imp_id=444149970&action=click&module=Smarter%20Living&pgtype=Homepage.

[17] Hill, Kashmir. "I Cut Google Out Of My Life. It Screwed Up Everything." Gizmodo, January 29, 2019. https://gizmodo.com/i-cut-google-out-of-my-life-it-screwed-up-everything-1830565500.

[18] Auxier, Brooke, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information." Pew Research Center, December 31, 2019. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[19] Uberti, David. "Coronavirus Surveillance Highlights Need for Federal Privacy Law." Wall Street Journal, April 17, 2020. https://www.wsj.com/articles/coronavirus-surveillance-highlights-need-for-federal-privacy-law-11587115801?ns=prod/accounts-wsj.

[20] Bremmer, Ian. "The American International Order Is Over." Time Magazine, November 18, 2019. https://time.com/5730849/end-american-order-what-next/.

[21] "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation." Consumer Financial Protection Bureau, October 18, 2017. https://www.consumerfinance.gov/data-research/research-reports/consumer-protection-principles-consumer-authorized-financial-data-sharing-and-aggregation/.

[22] "Principles of the Law, Data Privacy." The American Law Institute. Accessed March 2020. https://www.ali.org/publications/show/data-privacy/#drafts.

[23] Asrow, Kaitlin, and Beth Brockland. "CFSI's Consumer Data Sharing Principles: A Framework for Industry-Wide Collaboration." Center for Financial Services Innovation, October 1, 2016. https://s3.amazonaws.com/cfsi-innovation-files-2018/wp-content/uploads/2016/10/31152340/2016_Data-Sharing-Principles1.pdf.

[24] Medine, David, and Gayatri Murthy. "Making Data Work for the Poor." CGAP, January 1, 2020. https://www.cgap.org/research/publication/making-data-work-poor.

[25] "The Appropriate Use of Customer Data in Financial Services." World Economic Forum, September 1, 2018. http://www3.weforum.org/docs/WP_Roadmap_Appropriate_Use_Customer_Data.pdf.

[26] The Digital Standard. Accessed March 2020. https://www.thedigitalstandard.org/.

[27] "2019 Data Symposium: The Role of Consumers in the Data Ecosystem." Federal Reserve Bank of San Francisco, July 1, 2019. https://www.frbsf.org/banking/fintech/events/2019/november/role-of-consumers-in-data-ecosystem/.

[28] "CFPB Symposium: Consumer Access to Financial Records." Consumer Financial Protection Bureau, February 26, 2020. https://www.consumerfinance.gov/about-us/events/archive-past-events/cfpb-symposium-consumer-access-financial-records/; Lux, Marshall and Matthew Shackelford. "The New Frontier of Consumer Protection: Financial Data Privacy and Security." Harvard Kennedy School Mossavar-Rahmani Center for Business and Government, March 2020. https://www.hks.harvard.edu/centers/mrcbg/publications/awp/awp135

[29] Open Banking. Accessed March 2020. https://www.openbanking.org.uk/.

[30] Bennett, Tess. "How the Consumer Data Right Opens up Cross Industry Opportunities - Which-50." Which-50, March 9, 2020. https://which-50.com/how-the-consumer-data-right-opens-up-cross-industry-opportunities/.

[31] "Principles of the Law, Data Privacy." The American Law Institute. Accessed March 2020. https://www.ali.org/publications/show/data-privacy/#drafts.

[32] Samson, Renate, and Anna Scott. "For Stronger Data Rights, We Must Start with a Shared Language of Data." The Open Data Institute, June 13, 2019. https://theodi.org/article/for-stronger-data-rights-we-must-start-with-a-shared-language-of-data/.

[33] Marr, Bernard. "Where Can You Buy Big Data? Here Are The Biggest Consumer Data Brokers." Forbes Magazine, September 7, 2017. https://www.forbes.com/sites/bernardmarr/2017/09/07/where-can-you-buy-big-data-here-are-the-biggest-consumer-data-brokers/.

[34] "Personally Identifiable Information (PII)." Computer Security Resource Center. Accessed March 2020. https://csrc.nist.gov/glossary/term/personally-identifiable-information.

[35] Armerding, Taylor. "The 18 Biggest Data Breaches of the 21st Century." CSO Online, December 20, 2018. https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

[36] "Art. 4 GDPR – Definitions." General Data Protection Regulation (GDPR). Accessed March 2020. https://gdpr-info.eu/art-4-gdpr/.

[37] "Description and History of Common Law." Radford University. Accessed March 2020. https://www.radford.edu/~junnever/law/commonlaw.htm.

[38] Diggelmann, Oliver, and Maria Nicole Cleis. "How the Right to Privacy Became a Human Right." Human Rights Law Review. Oxford University Press, July 7, 2014. https://academic.oup.com/hrlr/article-abstract/14/3/441/644279?redirectedFrom=fulltext.

[39] "Right to Privacy." Constitution of United States of America 1789. Constitution Laws, December 22, 2019. https://constitution.laws.com/right-to-privacy.

[40] "Invasion of Privacy." USLegal. Accessed March 2020. https://torts.uslegal.com/intentional-torts/invasion-of-privacy/.

[41] "Roe v. Wade, 410 U.S. 113 (1973)." Justia US Supreme Court. Accessed March 2020. https://supreme.justia.com/cases/federal/us/410/113/.

[42] Carter, Ian. "Positive and Negative Liberty." Stanford Encyclopedia of Philosophy. Stanford University, August 2, 2016. https://plato.stanford.edu/entries/liberty-positive-negative/#TwoConLib.

[43] "Board of Governors of the Federal Reserve System." Federal Reserve Board. Accessed March 2020. https://www.federalreserve.gov/aboutthefed.htm.

[44] FinancialDataExchange. Accessed March 2020. https://financialdataexchange.org/.

[45] Schaus, Paul. "When Open Banking and Data Privacy Collide." American Banker, December 11, 2019. https://www.americanbanker.com/opinion/when-open-banking-and-data-privacy-collide.

[46] FinRegLab. Accessed March 2020. https://finreglab.org/.

[47] Reinsel, David, John Gantz, and John Rydning. "The Digitization of the World, From Edge to Core." Seagate. Accessed March 2020. https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf.

[48] *ibid*

[49] "A Brief History of the Digital Revolution." Science and Technology Facilities Council. Accessed March 2020. https://stfc.ukri.org/files/digital-revolution-infographic/.

[50] Buteau, Antoine. "Big Data for Big Business? A Taxonomy of Data-Driven Business Models Used by Startups." The PNR, July 11, 2017. https://medium.com/pnr/big-data-for-big-business-a-taxonomy-of-data-driven-business-models-used-by-startups-e256929f4ccf.

[51] Rooney, Kate. "Fintechs Help Boost US Personal Loan Surge to a Record $138 Billion." CNBC, February 24, 2019. https://www.cnbc.com/2019/02/21/personal-loans-surge-to-a-record-138-billion-in-us-as-fintechs-lead-new-lending-charge.html.

[52] "Demographics of Mobile Device Ownership and Adoption in the United States." Pew Research Center. Accessed March 2020. https://www.pewresearch.org/internet/fact-sheet/mobile/.

[53] Brown, Eileen. "Seven out of Ten Americans Are Comfortable with IoT Tech in the Home." ZDNet, March 29, 2019. https://www.zdnet.com/article/seven-out-of-ten-americans-are-comfortable-with-iot-tech-in-the-home/.

[54] Patrizio, Andy. "IDC: Expect 175 Zettabytes of Data Worldwide by 2025." Network World, December 3, 2018. https://www.networkworld.com/article/3325397/idc-expect-175-zettabytes-of-data-worldwide-by-2025.html.

[55] Duffin, Karen, Amanda Aronczyk, and Liza Yeager. "Episode 964: BILLBOARDS." NPR, January 16, 2020. https://www.npr.org/2020/01/15/796799769/episode-964-billboards.

[56] Hill, Kashmir. "I Got Access to My Secret Consumer Score. Now You Can Get Yours, Too." The New York Times, November 4, 2019. https://www.nytimes.com/2019/11/04/business/secret-consumer-score-access.html.

[57] Evans, Carol. "From Catalogs to Clicks, The Fair Lending Implications of Targeted, Internet Marketing." Consumer Compliance Outlook Third Issue 2019. Accessed March 2020. https://www.consumercomplianceoutlook.org/assets/2019/third-issue/ccoi32019.pdf?la=en.

[58] "CFPB Symposium: Consumer Access to Financial Records." Consumer Financial Protection Bureau. Accessed March 2020. https://www.consumerfinance.gov/about-us/events/cfpb-symposium-consumer-access-financial-records/.

[59] Dixon, Pam. "A Brief Introduction to Fair Information Practices." World Privacy Forum. Accessed March 2020. https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/.

[60] "Records, Computers and the Rights of Citizens." Office of the Assistant Secretary for Planning and Evaluation, June 16, 2016. https://aspe.hhs.gov/report/records-computers-and-rights-citizens.

[61] "A Summary of Your Rights Under the Fair Credit Reporting Act." Consumer Financial Protection Bureau. Accessed March 2020. https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

[62] "Privacy Act of 1974." The United States Department of Justice, January 15, 2020. https://www.justice.gov/opcl/privacy-act-1974.

[63] "The Health Insurance Portability and Accountability Act of 1996." U.S. Department of Health & Human Services, Accessed May 2020. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

[64] Solove, Daniel J., and Paul M. Schwartz. Information Privacy Law. New York: Wolters Kluwer Law & Business, 2018.

[65] "Privacy Online: A Report to Congress at 7-14." Federal Trade Commission, June 1, 1998. http://www.ftc.gov/reports/privacy3/index.htm; "Privacy Online: December 1996 Staff Report at 8-12." Federal Trade Commission. Accessed March 17, 2020. http://www.ftc.gov/reports/privacy/ privacy1.htm.

[66] Hartzog, Woodrow. "The Inadequate, Invaluable Fair Information Practices." Digital Commons@UM Carey Law, University of Maryland Francis King Carey Law School. Accessed March 2020. https://digitalcommons.law.umaryland.edu/mlr/vol76/iss4/4/.

[67] "A Brief Introduction to Fair Information Practices." World Privacy Forum. Accessed March 2020. https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/.

[68] "Consumer Data Right (CDR)." Australian Competition and Consumer Commission. Accessed March 2020. https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0.

[69] Panday, Jyoti. "India's Supreme Court Upholds Right to Privacy as a Fundamental Right-and It's About Time." Electronic Frontier Foundation, October 11, 2017. https://www.eff.org/deeplinks/2017/08/indias-supreme-court-upholds-right-privacy-fundamental-right-and-its-about-time.

[70] Greenberg, Pam. "Security Breach Notification Laws." National Conference of State Legislatures. Accessed March 2020. https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[71] "Dodd-Frank Wall Street Reform and Consumer Protection Act." United States Congress. Accessed March 2020. https://legcounsel.house.gov/Comps/Dodd-Frank%20Wall%20Street%20Reform%20and%20Consumer%20Protection%20Act.pdf.

[72] "We Can't Wait: Obama Administration Unveils Blueprint for a 'Privacy Bill of Rights' to Protect Consumers Online." National Archives and Records Administration, February 23, 2012. https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.

[73] Bard, Yoni, and Scott Bloomberg. "CCPA: The (Qualified) Right to Deletion." Security, Privacy and the Law, July 24, 2019. https://www.securityprivacyandthelaw.com/2019/07/ccpa-the-qualified-right-to-deletion/.

[74] "Florida's Legislature to Consider Consumer Data Privacy Bill Akin to California's CCPA." The National Law Review, January 14, 2020. https://www.natlawreview.com/article/florida-s-legislature-to-consider-consumer-data-privacy-bill-akin-to-california-s

[75] O'Connor, Nuala. "Reforming the U.S. Approach to Data Protection and Privacy." Council on Foreign Relations, January 30, 2018. https://www.cfr.org/report/reforming-us-approach-data-protection.

[76] Branson, Katie. "Federal Consumer Data Privacy Legislation in the 116th Congress." Educause Review, May 13, 2019. https://er.educause.edu/blogs/2019/5/federal-consumer-data-privacy-legislation-in-the-116th-congress.; "All Info - S.583 - 116th Congress (2019-2020): Data Privacy Act." United States Congress, February 27, 2019. https://www.congress.gov/bill/116th-congress/senate-bill/583/all-info.

[77] "The Time Is Now: A Framework for Comprehensive Privacy Protection and Digital Rights in the United States." Public Citizen. Accessed March 18, 2020. https://www.citizen.org/wp-content/uploads/migration/privacy-and-digital-rights-for-all-framework.pdf

[78] FinancialDataExchange. Accessed March 2020. https://financialdataexchange.org/.

[79] Kelion, Leo. "Amazon: How Bezos Built His Data Machine." BBC News. Accessed March 2020. https://www.bbc.co.uk/news/extra/CLQYZENMBI/amazon-data?mc_cid=c445d0c887&mc_eid=e526eabd50.

[80] Swant, Marty. "Andrew Yang Proposes Digital Data Should Be Treated Like A Property Right." Forbes Magazine, October 1, 2019. https://www.forbes.com/sites/martyswant/2019/10/01/andrew-yang-proposes-digital-data-should-be-treated-like-a-property-right/#62cf50243ab7.

[81] Akred, John, and Anjali Samani. "Your Data Is Worth More Than You Think." MIT Sloan Management Review, January 18, 2018. https://sloanreview.mit.edu/article/your-data-is-worth-more-than-you-think/.

[82] Barratt, Jane. "Data as Currency: A View to the Future." Knowledge at Wharton on SiriusXM. August 27, 2019

[83] Sinha, G. Alex, A Real-Property Model of Privacy (August 26, 2018). G. Alex Sinha, A Real-Property Model of Privacy, 68 DePaul L. Rev. 567 (2019). https://ssrn.com/abstract=3238974

[84] Jeffrey Ritter & Anna Mayer, Regulating Data as Property: A New Construct for Moving Forward, 16 Duke Law & Technology Review 220-277 (2018)

[85] "Non-Rivalrous Goods - Definition and Characteristics." Corporate Finance Institute. Accessed March 2020. https://corporatefinanceinstitute.com/resources/knowledge/economics/non-rivalrous-goods/.

[86] "Public Goods." Lumen. Accessed March 2020. https://courses.lumenlearning.com/boundless-economics/chapter/public-goods/.

[87] "United States v. Miller." Oyez. Accessed March 2020. https://www.oyez.org/cases/1975/74-1179.

[88] "Carpenter v. United States." Oyez. Accessed March 2020. https://www.oyez.org/cases/2017/16-402.

[89] Fusselll, Sydney. "What Amazon Thinks You're Worth." The Atlantic, July 18, 2019. https://www.theatlantic.com/technology/archive/2019/07/amazon-pays-users-access-browser-data/594199/.

[90] Lanier, Jaron. "Jaron Lanier Fixes the Internet." The New York Times, September 23, 2019. https://www.nytimes.com/interactive/2019/09/23/opinion/data-privacy-jaron-lanier.html.

[91] Thomas, Owen. "Gov. Gavin Newsom Wants to Give You a 'Data Dividend.' Good Luck with That." San Francisco Chronicle, February 16, 2019. https://www.sfchronicle.com/business/article/Gov-Gavin-Newsom-wants-to-give-you-a-data-13621447.php.

[92] Groves, Theodore, and John Ledyard. "Optimal Allocation of Public Goods: A Solution to the 'Free Rider' Problem." Econometrica 45, no. 4 (1977): 783. https://doi.org/10.2307/1912672.

[93] Fairfield, Joshua, and Christoph Engel. "Privacy as a Public Good." Privacy and Power, n.d., 95–128. https://doi.org/10.1017/cbo9781316658888.004.

[94] Doffman, Zak. "China Is Using Facial Recognition To Track Ethnic Minorities, Even In Beijing." Forbes Magazine, August 4, 2019. https://www.forbes.com/sites/zakdoffman/2019/05/03/china-new-data-breach-exposes-facial-recognition-and-ethnicity-tracking-in-beijing/#fc5fcf34a757.

[95] Ben-Shahar, Omri. "Data Pollution." University of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 854; U of Chicago, Public Law Working Paper No. 679 (2017). https://ssrn.com/abstract=3191231.

[96] Jeong, Sarah. "Selling Your Private Information Is a Terrible Idea." The New York Times, July 5, 2019. https://www.nytimes.com/2019/07/05/opinion/health-data-property-privacy.html.

[97] Jones, Charles and Christopher Tonetti . "Nonrivalry and the Economics of Data." Stanford Graduate School of Business and NBER, March 2020. https://christophertonetti.com/files/papers/JonesTonetti_DataNonrivalry.pdf

[98] brave.com. Accessed March 2020. https://brave.com/.

[99] "Web History Timeline." Pew Research Center, December 31, 2019. https://www.pewresearch.org/internet/2014/03/11/world-wide-web-timeline/.

[100] "Public Workshop on Consumer Privacy on the Global Information Infrastructure." Official Transcript Proceedings Before the Federal Trade Commission. Federal Trade Commission, June 4, 1996. https://www.ftc.gov/sites/default/files/documents/public_events/consumer-privacy-global-information-infrastructure/pw960604.pdf.

[101] "Federal Trade Commission Act." Federal Trade Commission, December 14, 2018. https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act.

[102] "Privacy Online: A Report to Congress." Federal Trade Commission, June 1998. https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

[103] "Children's Online Privacy Protection Act of 1998." 15 U.S.C. 6501–6505 (2018). https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule.

[104] "FTC Recommends Congressional Action to Protect Consumer Privacy Online." Federal Trade Commission. May 22, 2000. https://www.ftc.gov/news-events/press-releases/2000/05/ftc-recommends-congressional-action-protect-consumer-privacy.

[105] Barr, Michael S., Abigail Dehart, and Andrew Kang. "Consumer Autonomy and Pathways to Portability in Banking and Financial Services." Center on Finance, Law and Policy, November 3, 2019. http://financelawpolicy.umich.edu/files/umich-cflp-working-paper-consumer-autonomy-and-data-portability-pathways-Nov-3.pdf.

[106] Hill, Kashmir. "I Got Access to My Secret Consumer Score. Now You Can Get Yours, Too." The New York Times, November 4, 2019. https://www.nytimes.com/2019/11/04/business/secret-consumer-score-access.html?smid=nytcore-ios-share.

[107] "Consumer Survey: Financial Apps and Data Privacy." The Clearing House, November 2019. https://www.theclearinghouse.org/-/media/New/TCH/Documents/Data-Privacy/2019-TCH-ConsumerSurveyReport.pdf.

[108] Madrigal, Alexis C. "Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days." Atlantic Media Company, March 1, 2012. https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.

[109] Budington, Bill. "Ring Doorbell App Packed with Third-Party Trackers." Electronic Frontier Foundation, January 31, 2020. https://www.eff.org/deeplinks/2020/01/ring-doorbell-app-packed-third-party-trackers.

[110] Litman-navarro, Kevin. "We Read 150 Privacy Policies. They Were an Incomprehensible Disaster." The New York Times, June 12, 2019. https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.

[111] "Adhesion Contract (Contract of Adhesion)." Legal Information Institute. Accessed March 2020. https://www.law.cornell.edu/wex/adhesion_contract_(contract_of_adhesion).

[112] Pogue, David. "10 Tips to Avoid Leaving Tracks Around the Internet." The New York Times, October 4, 2019. https://www.nytimes.com/2019/10/04/smarter-living/10-tips-internet-privacy-crowdwise.html.

[113] Cakebread, Caroline. "You're Not Alone, No One Reads Terms of Service Agreements." Business Insider, November 15, 2017. https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11.

[114] "Studies Show Consumers Express Privacy Concerns, but Actions Say Otherwise." International Association of Privacy Professionals, April 2, 2019. https://iapp.org/news/a/studies-show-consumers-express-privacy-concerns-but-actions-say-otherwise/.

[115] Spiekermann, Sarah and Berendt, Bettina and Grossklags, Jens, "E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior." February 20, 2009. https://ssrn.com/abstract=761107; Athey, Susan, Christian Catalini, and Catherine Tucker. "The Digital Privacy Paradox: Small Money, Small Costs, Small Talk." The Federal Trade Commission, September 27, 2017. https://www.ftc.gov/system/files/documents/public_comments/2017/09/00010-141392.pdf.

[116] John, Leslie K. "We Say We Want Privacy Online, But Our Actions Say Otherwise." Harvard Business Review, May 8, 2017. https://hbr.org/2015/10/we-say-we-want-privacy-online-but-our-actions-say-otherwise.

[117] Schwartz, Barry. "The Paradox of Choice: Why More Is Less." Harper Perennial, January 18, 2005.

[118] Habib, Hana, Yixin Zou, Aditi Jannu, Neha Sridhar, Chelse Swoopes, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. "An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites." USENIX, January 1, 1970. https://www.usenix.org/conference/soups2019/presentation/habib.

[119] John, Leslie K, Alessandro Acquisti, and George Lowenstein. "Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information." Journal of Consumer Research. Carnegie Mellon University, February 2011 https://www.cmu.edu/dietrich/sds/docs/loewenstein/StrangersPlane.pdf.

[120] Utz, Christine, Degeling, Martin, Fahl, Sascha, Schaub, Florian, Holz, Thorsten. "(Un)informed Consent: Studying GDPR Consent Notices in the Field." Cornell University. October 22, 2019. https://arxiv.org/abs/1909.02638.

[121] Svirsky, Dan. "Why Are Privacy Preferences Inconsistent?" Harvard Law School. John M. Olin Center for Law, Economics, and Business Fellows' Discussion Paper Series. June 2018. http://www.law.harvard.edu/programs/olin_center/fellows_papers/pdf/Svirsky_81.pdf.

[122] Madden, G. J., & Bickel, W. K. "Impulsivity: The behavioral and neurological science of discounting," American Psychological Association, 2010, https://doi.org/10.1037/12069-000.; Frederick, Shane, George Loewenstein, and Ted O'Donoghue. "Time Discounting and Time Preference:" Advances in Behavioral Economics, June 2002, 162–222. https://www.aeaweb.org/articles?id=10.1257/002205102320161311.

[123] Sharot, Tali. "The Optimism Bias." Current Biology 21, no. 23, December 5, 2011. https://doi.org/10.1016/j.cub.2011.10.030.; Evans, Dylan. "Your Judgment of Risk Is Compromised." Harvard Business Review, July 23, 2014. https://hbr.org/2012/06/recognize-the-limits-of-judgme.

[124] Cranor, Lorrie Faith, Pedro Giovanni Leon, and Blase Ur. "A Large-Scale Evaluation of U.S. Financial Institutions' Standardized Privacy Notices." Carnegie Mellon University. Accessed March 2020. https://dl.acm.org/doi/pdf/10.1145/2911988?download=true.

[125] Bank Privacy Demonstration Website. Carnegie Mellon University. Accessed March 2020. https://cups.cs.cmu.edu/bankprivacy/

[126] Norton, Michael. "Trust and transparency in service provision," YouTube. July 28, 2015. https://www.youtube.com/watch?v=6WCChCXZH5w.

[127] "European Data Protection Board Issues Guidance on PSD2 and GDPR." Ashurst, January 16, 2018. https://www.ashurst.com/en/news-and-insights/legal-updates/european-data-protection-board-issues-guidance-on-psd2-and-gdpr/.

[128] "Lawful Basis for Processing." ICO. Accessed March 2020. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/.

[129] "Legitimate Interest." GDPREU.org. Accessed March 2020. https://www.gdpreu.org/the-regulation/key-concepts/legitimate-interest/.

[130] "Lawful Basis for Processing." Information Commissioner's Office. Accessed March 2020. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/.

[131] "Our Response to the White Paper on a Data Protection Framework for India." Dvara Research, February 7, 2018. https://www.dvara.com/blog/2018/02/07/our-response-to-the-white-paper-on-a-data-protection-framework-for-india/.

[132] "Click to Consent? Not Good Enough Anymore." Office of the Privacy Commissioner, September 2, 2019. https://privacy.org.nz/blog/click-to-consent-not-good-enough-anymore/.

[133] Medine, David, and Gayatri Murthy. "Making Data Work for the Poor." CGAP, January 2020. https://www.cgap.org/research/publication/making-data-work-poor.

[134] Shaub, Florian, Rebecca Balebako, and Lorrie Faith Cranor. "Designing Effective Privacy Notices and Controls." CSDL | IEEE Computer Society, June 2017. https://www.computer.org/csdl/magazine/ic/2017/03/mic2017030070/13rRUwgQpnc.

[135] "Consumer Experience Guidelines." Consumer Data Standards, November 12, 2019. https://consumerdatastandards.org.au/wp-content/uploads/2019/11/CX-Guidelines-v1.0.1.pdf.

[136] Joseph, Seb. "WTF Is the Data Transparency Label?" Digiday, December 3, 2019. https://digiday.com/marketing/wtf-data-transparency-label/?mc_cid=7b6844c431&mc_eid=e526eabd50.

[137] ISO 9000 Family Quality Management. ISO. Access March 2020. https://www.iso.org/iso-9001-quality-management.html

[138] "Trans Union LLC v. Federal Trade Commission." Legal Information Institute, June 10, 2002. https://www.law.cornell.edu/supremecourt/text/536/915/USSC_PRO_536_915_01-1080.

[139] "ACA Connects – America's Communications Association. Et Al v. Aaron Frey, Et Al." Accessed March 2020. https://acaconnects.org/wp-content/uploads/2020/02/200214-Complaint-404pm-R2226412xAB81A.pdf.

[140] "Principles of the Law, Data Privacy." The American Law Institute. Accessed March 2020. https://www.ali.org/publications/show/data-privacy/#drafts.

[141] "Federal Regulators Issue Joint Statement on the Use of Alternative Data in Credit Underwriting." Consumer Financial Protection Bureau, December 3, 2019. https://www.consumerfinance.gov/about-us/newsroom/federal-regulators-issue-joint-statement-use-alternative-data-credit-underwriting/.

[142] Vidal, Maria Fernandez, and David Medine. "Is Data Privacy Good for Business?" CGAP, December 2019. https://www.cgap.org/research/publication/data-privacy-good-business.

[143] Dranoff, Sarah. "Identity Theft: A Low–Income Issue." American Bar Association, December 15, 2014. https://www.americanbar.org/groups/legal_services/publications/dialogue/volume/17/winter-2014/identity-theft--a-lowincome-issue/.

[144] Li, Xiaoqian, Wenhong Chen, and Joseph D. Straubhaar. "Privacy at the Margins: Concerns, Skills, and Activities: Multilayered Privacy Issues in Disadvantaged Urban Communities." Semantic Scholar, January 1, 1970. https://www.semanticscholar.org/paper/Privacy-at-the-Margins|-Concerns,-Skills,-and-in-Li-Chen/439c56d493b41d101bcb46ec9c4d278015ba7bd9.

[145] Cottrill, Caitlin, and Piyushimita (Vonu) Thakuriah. "Privacy and Gender: Reviewing Women's Attitudes Toward Privacy in the Context of Intelligent Transportation Systems and Location-Based Services." 2011. https://www.nap.edu/read/22887/chapter/13.

[146] Guberek, Tamy, Allison McDonald, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama, and Florian Schaub. "Keeping a Low Profile?: Technology, Risk and Privacy among Undocumented Immigrants." ACM Digital Library, April 1, 2018. https://dl.acm.org/doi/10.1145/3173574.3173688.

[147] Fussell, Sidney. "Why Can't This Soap Dispenser Identify Dark Skin?" Gizmodo, August 17, 2017. https://gizmodo.com/why-cant-this-soap-dispenser-identify-dark-skin-1797931773.

[148] Vincent, James. "Google 'Fixed' Its Racist Algorithm by Removing Gorillas from Its Image-Labeling Tech." The Verge, January 12, 2018. https://www.theverge.com/2018/1/12/16882408/google-racist-gorillas-photo-recognition-algorithm-ai.

[149] Dastin, Jeffrey. "Amazon Scraps Secret AI Recruiting Tool That Showed Bias against Women." Thomson Reuters, October 10, 2018. https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

[150] Madden, Mary. "Privacy, Security, and Digital Inequality." Data & Society Research Institute, September 27, 2017. https://datasociety.net/library/privacy-security-and-digital-inequality/.

[151] Vogels, Emily A., and Monica Anderson. "Americans and Digital Knowledge." Pew Research Center, December 31, 2019. https://www.pewresearch.org/internet/2019/10/09/americans-and-digital-knowledge/.

[152] Anderson, Monica, and Madhumitha Kumar. "Digital Divide Persists Even as Lower-Income Americans Make Gains in Tech Adoption." Pew Research Center, May 7, 2019. https://www.pewresearch.org/fact-tank/2019/05/07/digital-divide-persists-even-as-lower-income-americans-make-gains-in-tech-adoption/.

[153] Auxier, Brooke, and Lee Rainie. "Key Takeaways on Americans' Views about Privacy, Surveillance and Data-Sharing." Pew Research Center, November 15, 2019. https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/.

[154] Schwartz, Adam, and Cindy Cohn. "'Information Fiduciaries' Must Protect Your Data Privacy." Electronic Frontier Foundation, October 25, 2018. https://www.eff.org/deeplinks/2018/10/information-fiduciaries-must-protect-your-data-privacy.

[155] Medine, David, and Gayatri Murthy. "Making Data Work for the Poor." CGAP, January 2020. https://www.cgap.org/research/publication/making-data-work-poor.

[156] Khan, Lina, and David E. Pozen. "A Skeptical View of Information Fiduciaries." Scholarship Archive. Columbia Law School, 2019. https://scholarship.law.columbia.edu/faculty_scholarship/2451/.

[157] "Conflicts of Interest and Medical Practice." Institute of Medicine (US) Committee on Conflict of Interest in Medical Research, Education, and Practice. National Academies Press; 2009. https://www.ncbi.nlm.nih.gov/books/NBK22944/.

[158] O'hara, Kieron. "Data Trusts: Ethics, Architecture and Governance for Trustworthy Data Stewardship." Semantic Scholar, February 2019. https://www.researchgate.net/publication/331275252_Data_Trusts_Ethics_Architecture_and_Governance_for_Trustworthy_Data_Stewardship.

[159] Hardjono, Thomas, and Alex Pentland. "Data Cooperatives: Towards a Foundation for Decentralized Personal Data Management." Cornell University, May 21, 2019. https://arxiv.org/abs/1905.08819.

[160] Institute For The Future. Accessed March 2020. http://www.iftf.org/home/.

[161] DigiLocker. Accessed March 2020. https://digilocker.gov.in/.

[162] "A European Strategy for Data." European Commission. Accessed March 2020. https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy.

[163] Dodds, Leigh, and Olivier Thereaux. "How do we create trustworthy and sustainable data institutions?" The Open Data Institute, February 18, 2020. https://theodi.org/article/how-do-we-create-trustworthy-and-sustainable-data-institutions/?mc_cid=c445d0c887&mc_eid=e526eabd50.

[164] Hartzog, Woodrow. "The Inadequate, Invaluable Fair Information Practices." Accessed March 2020. https://digitalcommons.law.umaryland.edu/mlr/vol76/iss4/4/.

[165] Elliott, Douglas J. "Data Rights in Finance: Key Public Policy Questions and Answers." Oliver Wyman. Accessed March 2020. https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2019/may/Data%20Rights%20in%20Finance_POV_web_20190403.pdf.

[166] Acquisti, Alessandro. "Privacy, Economics, and Regulation: A Note." The Federal Reserve Bank of Atlanta, May 2019. https://www.frbatlanta.org/-/media/documents/news/conferences/2019/0519-financial-markets-conference/papers/acquisti_policy-session-two_privacy-economics-and-regulation-a-note.pdf.

[167] "Competition and Data." Privacy International, September 26, 2020. https://privacyinternational.org/explainer/2293/competition-and-data.

[168] "Data Sharing and Open Data for Banks." Government of the United Kingdom, December 3, 2014. https://www.gov.uk/government/publications/data-sharing-and-open-data-for-banks.

[169] Reynolds, Faith, and Mark Chidley. "Consumer Priorities for Open Banking." United Kingdom Open Banking Implementation Entity. Manifesto Growth Architects, Accessed March 2020. https://www.openbanking.org.uk/wp-content/uploads/Consumer-Priorities-for-Open-Banking-report-June-2019.pdf.

[170] Nicholas, Gabriel and Michael Weinberg. "Data Portability and Platform Competition" New York University School of Law. Nov 2019. https://www.law.nyu.edu/sites/default/files/Data%20Portability%20and%20Platform%20Competition%20-

%20Is%20User%20Data%20Exported%20From%20Facebook%20Actually%20Useful%20to%20Competitors.pdf.

[171] King, Noel, and Jacob Goldstein. "Episode 908: I Am Not A Robot." NPR, April 24, 2019. https://www.npr.org/sections/money/2019/04/24/716854013/episode-908-i-am-not-a-robot.

[172] "GDPR: Data Hygiene Enables Business Growth." PrivSec Report, January 8, 2018. https://gdpr.report/news/2018/01/05/gdpr-data-hygiene-enables-business-growth/.

[173] Barr, Michael S., Abigail Dehart, and Andrew Kang. "Consumer Autonomy and Pathways to Portability in Banking and Financial Services." Center on Finance, Law and Policy, November 3, 2019. http://financelawpolicy.umich.edu/files/umich-cflp-working-paper-consumer-autonomy-and-data-portability-pathways-Nov-3.pdf.

[174] Huge, Francois Kim, Patrick Laurent, Simon Ramos, and Laurent Berliner. "RegTech Universe 2020." Deloitte Luxembourg, February 10, 2020. https://www2.deloitte.com/lu/en/pages/technology/articles/regtech-companies-compliance.html.

[175] "Leveraging Digital Finance for Gender Equality and Women's Empowerment." UN Women. Accessed March 2020. https://www.unwomen.org/en/digital-library/publications/2019/09/discussion-paper-leveraging-digital-finance-for-gender-equality-and-womens-empowerment.

[176] Katz, Lauren. "'I Sold My Face to Google for $5': Why Google's Attempt to Make Facial Recognition Tech More Inclusive Failed." Vox, October 17, 2019. https://www.vox.com/recode/2019/10/17/20917285/google-pixel-4-facial-recognition-tech-black-people-reset-podcast.

[177] Moon, Angela. "State-Sponsored Cyberattacks on Banks on the Rise: Report." Reuters, March 22, 2019. https://www.reuters.com/article/us-cyber-banks/state-sponsored-cyberattacks-on-banks-on-the-rise-report-idUSKCN1R32NJ.

[178] Davies, Tom. "Cybersecurity in Europe Is Improving: Thank You GDPR?" PrivSec Report, December 20, 2018. https://gdpr.report/news/2018/12/27/cybersecurity-in-europe-is-improving-thank-you-gdpr/.

[179] Khurana, Amandeep. "Council Post: Meeting The Data Privacy Challenge: An Industry Call To Action." Forbes, April 23, 2019. https://www.forbes.com/sites/forbestechcouncil/2019/04/23/meeting-the-data-privacy-challenge-an-industry-call-to-action/#5bba8c392d8c.

[180] Alcott, Hunt, Matthew Gentzkow, and Chuan Yu. "Trends in the Diffusion of Misinformation on Social Media." Stanford University, October 2018. https://web.stanford.edu/~gentzkow/research/fake-news-trends.pdf.

[181] Ben-Shahar, Omri. "Data Pollution." University of Chicago Coase-Sandor Institute for Law & Economics, June 12, 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3191231.

[182] "Update Report into Adtech and Real Time Bidding." United Kingdom Information Commissioner's Office, June 20, 2019. https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf.

[183] Johnson, Garrett, and Scott Shriver. "Privacy & Market Concentration: Intended & Unintended Consequences of the GDPR." SSRN, November 15, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3477686.

[184] The 1996 Reform Act amendments imposed certain dispute obligations on furnishers. The 2003 FACT Act amendments allowed consumers to obtain credit scores and free annual reports. The 2003 amendments also gave consumers the right to dispute errors directly with furnishers.

[185] "Key Dimensions and Processes in the U.S. Credit Reporting System: A Review of How the Nation's Largest Credit Bureaus Manage Consumer Data." Consumer Financial Protection Bureau, December 2012. https://files.consumerfinance.gov/f/201212_cfpb_credit-reporting-white-paper.pdf.

[186] "Survey Shows An Increasing Number of Consumers Have Obtained Their Credit Scores and Know Much More About Credit Scores · Consumer Federation of America." Consumer Federation of America, June 18, 2018. https://consumerfed.org/press_release/survey-shows-an-increasing-number-of-consumers-have-obtained-their-credit-scores-and-know-much-more-about-credit-scores/.

[187] "Report to Congress - Federal Trade Commission." Federal Trade Commission, January 2015. https://www.ftc.gov/sites/default/files/documents/reports/under-section-318-and-319-fair-and-accurate-credit-transaction-act-2003/041209factarpt.pdf.

[188] Cranor, Lorrie Faith, Pedro Giovanni Leon, and Blase Ur. "A Large-Scale Evaluation of U.S. Financial Institutions' Standardized Privacy Notices." Carnegie Mellon University. Accessed March 2020. https://dl.acm.org/doi/pdf/10.1145/2911988?download=true.

[189] Sovern, Jeff. "Can Cost-Benefit Analysis Help Consumer Protection Laws? Or at Least Benefit Analysis?" University of Irvine School of Law. Accessed March 2020. https://www.law.uci.edu/lawreview/vol4/no4/Sovern.pdf.

[190] "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation." Consumer Financial Protection Bureau, October 18, 2017. https://www.consumerfinance.gov/data-research/research-reports/consumer-protection-principles-consumer-authorized-financial-data-sharing-and-aggregation/.

[191] Asrow, Kaitlin. "The 2018 California Consumer Privacy Act: Understanding Its Implications and Ambiguities." Federal Reserve Bank of San Francisco, April 25, 2019. https://www.frbsf.org/banking/publications/fintech-edge/2019/april/2018-california-consumer-privacy-act/.

[192] "California Consumer Privacy Act of 2018 (1798.150(a)(1))." California Legislative Information, California Civil Code. Accessed March 2020. https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV§ionNum.

[193] "California Consumer Privacy Act of 2018 (1798. 130(a)(5))." California Legislative Information, California Civil Code. Accessed March 2020. https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV§ionNum.

[194] "CCPA Financial Incentives for Personal Information." Clarip. Accessed March 2020. https://www.clarip.com/data-privacy/ccpa-financial-incentives/.

[195] Mnuchin, Steve, and Craig S Phillips. "A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation." United States Department of the Treasury, July 2018. https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation.pdf.

[196] "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29." Office of the Comptroller of the Currency. March 5, 2020. https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html

[197] "Electronic Fund Transfer Act." Board of Governors of the Federal Reserve System. Accessed March 2020. https://www.federalreserve.gov/boarddocs/caletters/2008/0807/08-07_attachment.pdf.

[198] "Fair Debt Collection Practices Act." Federal Trade Commission, March 23, 2016. https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-debt-collection-practices-act-text.

[199] "Children's Online Privacy Protection Rule." Federal Trade Commission. Accessed March 2020. https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule.

[200] "The Equal Credit Opportunity Act." The United States Department of Justice, November 8, 2017. https://www.justice.gov/crt/equal-credit-opportunity-act-3.

[201] "The Fair Housing Act." The United States Department of Justice, December 21, 2017. https://www.justice.gov/crt/fair-housing-act-1.

[202] "Unfair, Deceptive, or Abusive Acts or Practices (UDAAPs) Examination Procedures." Consumer Financial Protection Bureau, October 1, 2012. https://www.consumerfinance.gov/policy-compliance/guidance/supervision-examinations/unfair-deceptive-or-abusive-acts-or-practices-udaaps-examination-procedures/.

[203] Greenberg, Pam. "Security Breach Notification Laws." March 8, 2020. https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[204] Lux, Marshall and Matthew Shackelford. "The New Frontier of Consumer Protection: Financial Data Privacy and Security." Harvard Kennedy School Mossavar-Rahmani Center for Business and Government, March 2020. https://www.hks.harvard.edu/centers/mrcbg/publications/awp/awp135

[205] Koh, Yoree. "New Mexico Sues Google Over Children's Data Privacy." The Wall Street Journal, February 20, 2020. https://www.wsj.com/articles/new-mexico-sues-google-over-childrens-data-privacy-11582240443?mc_cid=52ea36b51e&mc_eid=e526eabd50.

[206] Charles, Dan. "An Airbnb For Farmland Hits A Snag, As Farmers Raise Data Privacy Concerns." NPR, February 24, 2020. https://www.npr.org/sections/thesalt/2020/02/24/808764422/data-privacy-concerns-are-raised-after-startup-tries-to-rent-farmland?te=1&nl=the-privacy.

[207] "Energy Data Portability." Mission Data, October 2019. https://static1.squarespace.com/static/52d5c817e4b062861277ea97/t/5c3a849b562fa75d70fd7953/1547338949271/Energy+Data+Portability.pdf

[208] Bari, Lisa, and Daniel P. O'Neill. "Rethinking Patient Data Privacy In The Era Of Digital Health." Health Affairs, December 12, 2019. https://www.healthaffairs.org/do/10.1377/hblog20191210.216658/full/.

[209] *ibid*

[210] "OCR Issues Request for Information on Potential Updates to HIPAA Rules to Improve Data Sharing." HIPAA Journal, December 13, 2018. https://www.hipaajournal.com/ocr-issues-request-for-information-on-potential-updates-to-hipaa-rules-to-improve-data-sharing/.

[211] Heath, Sara. "Patient Data Access Prep Lacking Ahead of 21st Century Cures Act." PatientEngagementHIT, October 15, 2019. https://patientengagementhit.com/news/patient-data-access-prep-lacking-ahead-of-21st-century-cures-act.

[212] Nahra, Kirk. "Privacy and Security Impacts of the 21st Century Cures Legislation." International Association of Privacy Professionals, January 12, 2017. https://iapp.org/news/a/privacy-and-security-impacts-of-the-21st-century-cures-legislation/.; Jason, Christopher. "Key Reminders of New Data Regulations for 21st Century Cures Act." Health Care Media, October 24, 2019. https://ehrintelligence.com/news/key-reminders-of-new-data-regulations-for-21st-century-cures-act.

[213] "What Is FERPA?" Protecting Student Privacy. US Department of Education. Accessed March 2020. https://studentprivacy.ed.gov/faq/what-ferpa.

[214] "Family Educational Rights and Privacy Act (FERPA)." US Department of Education, March 1, 2018. https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

[215] "General Data Protection Regulation (GDPR)." Intersoft Consulting. Accessed March 2020. https://gdpr-info.eu/.

[216] "The Personal Data Protection Bill, 2018." Ministry of Electronics and Information Technology. Government of India. Accessed March 27, 2020. https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.

[217] "What Is Aadhaar - Unique Identification Authority of India: Government of India." Unique Identification Authority of India. Government of India. Accessed March 30, 2020. https://uidai.gov.in/what-is-aadhaar.html.

[218] "Digital Locker: Ministry of Electronics and Information Technology, Government of India." Ministry of Electronics and Information Technology. Government of India. Accessed March 27, 2020. https://meity.gov.in/digital-locker.

[219] "Open Banking, Preparing for Lift Off." United Kingdom Open Banking Implementation Entity, July 15, 2019. https://www.openbanking.org.uk/wp-content/uploads/open-banking-report-150719.pdf.

[220] "Consumer Data Right (CDR)." Australian Competition and Consumer Commission, December 20, 2019. https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0.

[221] Monteiro, Renato Leite. "The new Brazilian General Data Protection Law — a detailed analysis." IAPP. Accessed March 202. https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/

[222] "Consumer-directed finance: the future of financial services." Government of Canada. Accessed March 2020. https://www.canada.ca/en/department-finance/programs/consultations/2019/open-banking/report.html

[223] "Canada's Digital Charter: Trust in a digital world." Government of Canada. Accessed March 2020. https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html

[224] McGowan, Kathleen, Priya Vora, Matthew Homer, and Jonathan Dolan. "Personal Data Empowerment: Restoring Power to the People in a Digital Age." Pathways for Prosperity Commission, Technology & Inclusion Development, September 2018. https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2018-11/personal_data_empowerment.pdf.

[225] "About Us." Digital Identity New Zealand. Accessed March 2020. https://digitalidentity.nz/about/#:~:text=Digital%20Identity%20NZ%20is%20a,future%20for%20all%20New%20Zealanders

[226] "Digital ID and e-KYC." Monetary Authority of Singapore. Accessed March 2020. https://www.mas.gov.sg/development/fintech/technologies---digital-id-and-e-kyc.

[227] "Report of Review Committee on Open APIs: Promoting Open Innovation." Japan Banking Association. Accessed March 2020. https://www.zenginkyo.or.jp/fileadmin/res/en/news/news170713.pdf.

[228] Digital Clearinghouse. Accessed March 2020. https://www.digitalclearinghouse.org/.

[229] Cyphers, Bennett. "Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance." Electronic Frontier Foundation, December 2, 2019. https://www.eff.org/wp/behind-the-one-way-mirror?te=1&nl=the-privacy project&emc=edit_priv_20200107?campaign_id=122&instance_id=15012&segment_id=20121&user_id=c8211ba7a76400964e6e36c656c9497e®i_id=9212884120200107.

[230] Hartzog, Woodrow. "The Inadequate, Invaluable Fair Information Practices." Digital Commons@UM Carey Law, University of Maryland Francis King Carey Law School. Accessed March 2020. https://digitalcommons.law.umaryland.edu/mlr/vol76/iss4/4/.

[231] "Privacy Online: A Report to Congress at 7-14." Federal Trade Commission, June 1, 1998. http://www.ftc.gov/reports/privacy3/index.htm.

[232] Solove, Daniel, and Paul M Schwartz. "ALI Data Privacy: Overview and Black Letter Text." GW Law, September 2019. https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2722&context=faculty_publications.

[233] Federal Trade Commission 2019 Privacy and Data Security Update." Federal Trade Commission, September 20, 2019. https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2019/2019-privacy-data-security-report-508.pdf.

[234] "FDATA North America Highlights Benefits of Open Banking for U.S. Consumers." Financial Data and Technology Association, April 2, 2019. https://fdata.global/north-america/2019/04/02/fdata-north-america-highlights-benefits-of-open-banking-for-u-s-consumers/.

[235] Barr, Michael S., Abigail Dehart, and Andrew Kang. "Consumer Autonomy and Pathways to Portability in Banking and Financial Services." Center on Finance, Law and Policy, November 3, 2019. http://financelawpolicy.umich.edu/files/umich-cflp-working-paper-consumer-autonomy-and-data-portability-pathways-Nov-3.pdf.

[236] Asrow, Kaitlin, and Beth Brockland. "Liability, Transparency and Consumer Control in Data Sharing, A Call to Action for Financial Services Providers and Regulators." Center for Financial Services Innovation, September 2017. https://s3.amazonaws.com/cfsi-innovation-files-2018/wp-content/uploads/2017/09/27001532/2017_Liability-Transparency-Control-in-Data-Sharing_Full.pdf.

[237] Acquisti, Alessandro. "Privacy, Economics, and Regulation: A Note." The Federal Reserve Bank of Atlanta, May 2019. https://www.frbatlanta.org/-/media/documents/news/conferences/2019/0519-financial-markets-conference/papers/acquisti_policy-session-two_privacy-economics-and-regulation-a-note.pdf.

[238] "FTC Obtains Record $191 Million Settlement from University of Phoenix to Resolve FTC Charges It Used Deceptive Advertising to Attract Prospective Students." Federal Trade Commission, January 30, 2020. https://www.ftc.gov/news-events/press-releases/2019/12/ftc-obtains-record-191-million-settlement-university-phoenix.

[239] Waddell, Kaveh. "Casinos Are Using AI for Even Greater Advantage." Axios, June 28, 2019. https://www.axios.com/casinos-gambling-ai-marketing-addiction-0f01b612-7384-4875-a61e-f35684804239.html.

[240] MacCarthy, Mark. "Fairness in Algorithmic Decision-Making." Brookings, December 6, 2019. https://www.brookings.edu/research/fairness-in-algorithmic-decision-making/.

[241] Hamilton, Alex. "New Study by Identity Theft Resource Center® Explores the Non-Economic Negative Impacts Caused by Identity Theft." Identity Theft Resource Center, July 4, 2019. https://www.idtheftcenter.org/new-study-by-identity-theft-resource-center-explores-the-non-economic-negative-impacts-caused-by-identity-theft/.

[242] Park, Andrea. "Data Privacy Is Most Important Factor in Building Consumer Trust." Becker's Hospital Review, January 14, 2020. https://www.beckershospitalreview.com/consumerism/data-privacy-is-most-important-factor-in-building-consumer-trust-report.html.

[243] Schwartz, Mathew J., and Ron Ross. "Equifax Breach 'Entirely Preventable,' House Report Finds." Bank Information Security, December 11, 2018. https://www.bankinfosecurity.com/equifax-breach-entirely-preventable-house-report-finds-a-11832.

[244] "What is Cybersecurity." Cisco. Accessed March 2020. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html.

[245] Temperton, James. "AVG Can Sell Your Browsing and Search History to Advertisers." WIRED, October 4, 2017. https://www.wired.co.uk/article/avg-privacy-policy-browser-search-data.

[246] "Cybersecurity Framework." NIST, March 20, 2020. https://www.nist.gov/cyberframework.

[247] "Financial Services Sector Cybersecurity Coordinating Council." Financial Sector Cybersecurity Profile. Accessed March 2020. https://fsscc.org/Financial-Sector-Cybersecurity-Profile.

[248] "Safeguards Rule." Federal Trade Commission, March 6, 2020. https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/safeguards-rule.

[249] PCI Security Standards Council Site. Accessed March 2020. https://www.pcisecuritystandards.org/.

[250] "Privacy Framework." NIST, March 2, 2020. https://www.nist.gov/privacy-framework.

[251] "Principles of the Law, Data Privacy." The American Law Institute. Accessed March 2020. https://www.ali.org/publications/show/data-privacy/#drafts.

[252] "Examples of Processing 'Likely to Result in High Risk'." United Kingdom Information Commissioner's Office. Accessed March 2020. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/.

[253] "Special Category Data." United Kingdom Information Commissioner's Office. Accessed March 2020. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/.

[254] "Analytics: The Real-World Use of Big Data in Financial Services." IBM. Said Business School at the University of Oxford, Accessed March 30, 2020. https://www.ibm.com/downloads/cas/E4BWZ1PY.

[255] "Global Financial Services Third-Party Risk Management Survey, Is It Time to Shift Your Perspective of Third-Party Risk?" Ernst & Young. Accessed March 2020. https://www.ey.com/Publication/vwLUAssets/ey-global-financial-services-third-party-risk-management-survey/$File/ey-global-financial-services-third-party-risk-management-survey.pdf.

[256] Auxier, Brooke, and Lee Rainie. "Key Takeaways on Americans' Views about Privacy, Surveillance and Data-Sharing." Pew Research Center, November 15, 2019. https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/.

[257] Kosoff, Jacob. "Europe's New API Rules Lay Groundwork for Regulating Open Banking." American Banker, January 21, 2020. https://www.americanbanker.com/opinion/europes-new-api-rules-lay-groundwork-for-regulating-open-banking.

[258] "Update Report into Adtech and Real Time Bidding." United Kingdom Information Commissioner's Office, June 20, 2019. https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf.

[259] "Most Cookie Banners Are Annoying and Deceptive. This Is Not Consent." Privacy International, March 21, 2020. https://privacyinternational.org/explainer/2975/most-cookie-banners-are-annoying-and-deceptive-not-consent.

[260] "Banking on Your Data: the Role of Big Data in Financial Services." Financial Services Committee, November 21, 2019. https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=404653.

[261] "Guidance on Vermont's Act 171 of 2018 Data Broker Regulation." Vermont Office of the Attorney General, Dec 2018. https://ago.vermont.gov/wp-content/uploads/2018/12/2018-12-11-VT-Data-Broker-Regulation-Guidance.pdf.

[262] "Principles of the Law, Data Privacy." The American Law Institute. Accessed March 2020. https://www.ali.org/publications/show/data-privacy/#drafts.

[263] Ohm, Paul. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." UCLA Law Review. UCLA School of Law. Accessed March 2020. https://www.uclalawreview.org/pdf/57-6-3.pdf.

[264] Sweeney, Latanya. "Simple Demographics Often Identify People Uniquely." Data Privacy Lab, January 1, 2000. https://dataprivacylab.org/projects/identifiability/index.html.

[265] Mayer, Jonathan, Patrick Mutchler, and John C. Mitchell. "Evaluating the Privacy Properties of Telephone Metadata." PNAS. National Academy of Sciences, May 17, 2016. https://www.pnas.org/content/113/20/5536.

[266] Acquisti, Alessandro, and Ralph Gross. “Predicting Social Security Numbers from Public Data.” PNAS. National Academy of Sciences, July 7, 2009. https://www.pnas.org/content/106/27/10975.

[267] Thompson, Stuart A., and Charlie Warzel. “Twelve Million Phones, One Dataset, Zero Privacy.” The New York Times, December 19, 2019. https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

[268] “Sharing Medical Data.” Data Privacy Lab, May 1997. https://dataprivacylab.org/dataprivacy/projects/law/law1.html.

[269] LatanyaSweeney.com. Accessed March 2020. http://www.latanyasweeney.org/work/identifiability.html.

[270] “Annual Report to Congress 2018.” The National Academies of Sciences, Engineering and Medicine. Accessed March 2020. https://www.nationalacademies.org/annualreport/Report_to_Congress_2018.pdf.

[271] Dickinson, David, and Andy Zavoina. “Reg E and 'Contributory Negligence'.” BankersOnline. Accessed March 2020. https://www.bankersonline.com/qa/reg-e-and-contributory-negligence.

[272] “The Time Is Now: A Framework for Comprehensive Privacy Protection and Digital Rights in the United States.” Public Citizen. Accessed March 2020. https://www.citizen.org/wp-content/uploads/migration/privacy-and-digital-rights-for-all-framework.pdf.

[273] Dayen, David. “Tech Companies' Big Reveal: Hardly Anyone Files Arbitration Claims.” The American Prospect, November 26, 2019. https://prospect.org/power/tech-companies-hardly-anyone-files-arbitration-claims/.

[274] Pitsker, Kaitlin. “6 Things You Must Know About Class-Action Lawsuits.” Kiplingers Personal Finance, July 6, 2015. https://www.kiplinger.com/article/spending/T037-C000-S002-6-things-you-must-know-about-class-action-lawsuits.html.

[275] NYT Editorial Board. “A $5 Billion Fine for Facebook Won't Fix Privacy.” The New York Times, July 25, 2019. https://www.nytimes.com/2019/07/25/opinion/facebook-fine-5-billion.html.

[276] “Principles of the Law, Data Privacy.” The American Law Institute. Accessed March 2020. https://www.ali.org/publications/show/data-privacy/#drafts.

[277] “Data Protection Impact Assessments.” United Kingdom Information Commissioner's Office. Accessed March 2020. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/.

[278] “Bill of Rights, United States Constitution.” Encyclopedia Britannica. Accessed March 2020. https://www.britannica.com/topic/Bill-of-Rights-United-States-Constitution.

[279] McIntyre, Alan. “Top 10 Trends for Banks in 2020.” Accenture Banking Blog, January 28, 2020. https://bankingblog.accenture.com/top-10-trends-banks-2020.

[280] Mcleod, Saul. “Maslow's Hierarchy of Needs.” Simply Psychology. Accessed March 2020. https://www.simplypsychology.org/maslow.html.

[281] Stupp, Catherine. "Companies Scramble to Respond to Spam GDPR Requests." The Wall Street Journal, November 25, 2019. https://www.wsj.com/articles/companies-scramble-to-respond-to-spam-gdpr-requests-11574677802.

[282] Waters, Maxine. "Proposed Amendment to the Fair Credit Reporting Act." U.S. House Committee on Financial Services. U.S. House of Representatives, February 21, 2019. https://financialservices.house.gov/uploadedfiles/comprehensive_consumer_credit_reporting_reform_act_02262019.pdf

[283] "Principles of the Law, Data Privacy." The American Law Institute. Accessed March 2020. https://www.ali.org/publications/show/data-privacy/#drafts.

[284] "Machine Learning Basics with the K-Nearest Neighbors Algorithm." Towards Data Science, September 2018. https://towardsdatascience.com/machine-learning-basics-with-the-k-nearest-neighbors-algorithm-6a6e71d01761.

[285] Kroft, Steve. "The Data Brokers: Selling your personal information." 60 Minutes, March 2019. https://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/.

[286] Auxier, Brooke, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information." Pew Research Center, December 31, 2019. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[287] "Update Report into Adtech and Real Time Bidding." United Kingdom Information Commissioner's Office, June 20, 2019. https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf.

[288] Hartzog, Woodrow. "The Inadequate, Invaluable Fair Information Practices." Digital Commons@UM Carey Law, University of Maryland Francis King Carey Law School. Accessed March 2020. https://digitalcommons.law.umaryland.edu/mlr/vol76/iss4/4/.

[289] Kenny, Steve. "An Introduction to Privacy Enhancing Technologies." International Association of Privacy Professionals, January 29, 2010. https://iapp.org/news/a/2008-05-introduction-to-privacy-enhancing-technologies/.

[290] Shen, Yun, and Siani Pearson. "Privacy Enhancing Technologies: A Review." Hewlett Packard, August 6, 2011. https://www.hpl.hp.com/techreports/2011/HPL-2011-113.pdf.

[291] "Differential Privacy." Harvard University Privacy Tools Project. Accessed March 2020. https://privacytools.seas.harvard.edu/differential-privacy.

[292] Bebensee, Bjorn. "Local Differential Privacy: a tutorial." Seoul National University. July 27, 2019. https://deepai.org/publication/local-differential-privacy-a-tutorial.

[293] Perlroth, Nicole. "What Is End-to-End Encryption? Another Bull's-Eye on Big Tech." The New York Times, November 19, 2019. https://www.nytimes.com/2019/11/19/technology/end-to-end-encryption.html.

[294] Pagter, Jakob Illeborg. "A Short Introduction to Multiparty Computation (MPC)." Sepior, April 27, 2017. https://sepior.com/blog/2017/4/27/a-short-introduction-to-multiparty-computation-mpc.

[295] Wågström, Göran. "Council Post: A 2020 Vision Of Data Privacy." Forbes Magazine, February 3, 2020. https://www.forbes.com/sites/forbestechcouncil/2020/02/03/a-2020-vision-of-data-privacy/#4f4169d2634b.

[296] Crosman, Penny. "JPMorgan Chase Moves to Block Fintechs from Screen Scraping." American Banker, January 3, 2020. https://www.americanbanker.com/news/jpmorgan-chase-moves-to-block-fintechs-from-screen-scraping.; "Control TowerSM." Wells Fargo. Accessed March 30, 2020. https://www.wellsfargo.com/online-banking/manage-accounts/control-tower/.

[297] Myplaid. Plaid. Accessed March 2020. https://my.plaid.com/.

[298] "Prepared Remarks of FinCEN Director Kenneth A. Blanco, Delivered at the Federal Identity (FedID) Forum and Exposition." Financial Crimes Enforcement Network, September 24, 2019. https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-federal-identity-fedid.

[299] "What Is Aadhaar - Unique Identification Authority of India: Government of India." Unique Identification Authority of India. Government of India. Accessed March 30, 2020. https://uidai.gov.in/what-is-aadhaar.html.

[300] Whitney, Lance. "The Driver's License of the Future Is Coming to Your Smartphone." CNET, March 21, 2015. https://www.cnet.com/news/your-future-drivers-license-could-go-digital/.

[301] The Editorial Team, "MAS to Roll out National KYC Utility for Singapore." Finextra, March 24, 2017. https://www.finextra.com/newsarticle/30332/mas-to-roll-out-national-kyc-utility-for-singapore.

[302] Page, Rosalyn. "Mastercard to Pilot New Digital ID System." CMO Australia, December 17, 2019. https://www.cmo.com.au/article/669722/mastercard-pilot-new-digital-id-system/.

[303] Spring Labs. Accessed March 2020. https://www.springlabs.com/.

[304] Sovrin. Accessed March 2020. https://sovrin.org/.

[305] "Race to the Top: A New Business Paradigm for Identity Data." Omidyar Network, March 26, 2019. https://www.omidyar.com/blog/race-top-new-business-paradigm-identity-data.

[306] Cegłowski,, Maciej. "Statement of Maciej Cegłowski, Founder, Pinboard Before the U.S. Senate Committee on Banking, Housing, and Urban Development On the Topic of 'Privacy Rights and Data Collection in a Digital Economy.'" United States Senate Committee on Banking, Housing and Urban Affairs. United States Senate, March 7, 2019. https://www.banking.senate.gov/imo/media/doc/Ceglowski Testimony 5-7-19.pdf.

[307] Zuboff, Shoshana. "You Are Now Remotely Controlled." The New York Times, January 24, 2020. https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html.

[308] "Principles of the Law, Data Privacy." The American Law Institute. Accessed March 16, 2020. https://www.ali.org/publications/show/data-privacy/#drafts.

[309] Berners-lee, Tim. "I Invented the World Wide Web. Here's How We Can Fix It." The New York Times, November 25, 2019. https://www.nytimes.com/2019/11/24/opinion/world-wide-web.html.; "Big Tech Firms

Call For Industry Regulations." PYMNTS, January 27, 2020. https://www.pymnts.com/news/regulation/2020/big-tech-firms-call-for-industry-regulations/.

[310] Whittaker, Zack. "A Senate Bill Would Create a New US Data Protection Agency." TechCrunch, February 13, 2020. https://techcrunch.com/2020/02/13/gilliband-law-data-agency/.