Improving Consumer Welfare with Data Portability

By Daniel Castro | November 29, 2021

Data protection laws and regulations can contain restrictive provisions, which limit data sharing and use, as well as permissive provisions, which increase it. Data portability is an example of a permissive provision that allows consumers to obtain a digital copy of their personal information from an online service and provide this information to other services. By carefully crafting data portability provisions, policymakers can enable consumers to obtain more value from their data, create new opportunities for businesses to innovate with data, and foster competition.

Data portability requirements should be carefully designed to avoid imposing unnecessary costs on organizations, exposing proprietary information, or undermining consumer privacy.

INTRODUCTION

There are many proposals under consideration for how to craft data protection laws and regulations that can protect consumer privacy while giving consumers more control over their personal information. One important provision that can be considered in data protection laws and regulations to improve consumer welfare is data portability. Unlike many restrictive provisions in data protection laws designed to limit how data is used and shared, data portability is a permissive provision intended to increase data use and sharing. As such, data portability is an important provision for policymakers interested in promoting data-driven innovation.

Data portability allows consumers to obtain a digital copy of their personal information from online services and provide this information to other services, allowing consumers to obtain more value from their data, creating new opportunities for businesses to innovate with data, and fostering competition. However, data portability requirements should be carefully designed to avoid imposing unnecessary costs on organizations, exposing proprietary information, or undermining consumer privacy.

This report offers several recommendations for how policymakers can support data portability. These are:

- Create data portability policies at the national level
- Prioritize high-impact opportunities for data portability
- Limit the scope of non-sector-specific data portability requirements
- Support industry-led data portability standards
- Encourage data portability APIs but allow data scraping
- Use data portability as a pathway to allow consumers to donate their data

WHAT IS DATA PORTABILITY?

Data portability refers to the ability of users to obtain and transfer a copy of their data from one data controller (e.g., an app or online service) to another. To enable data portability, data controllers must make user data available in a standardized, machine-readable format through either a direct download or an open application programming interface (API)—a set of functions a third party can use to access data directly from a service when users request their data be ported to that third party. Data portability also requires that data controllers make data available to consumers without any technical or legal restrictions on how it may be used.

Data portability laws and regulations may specify additional requirements, such as whether data controllers can charge for access to data, how often users may request and receive a copy of their data, or what type of structured format data controllers must use for the data they provide. They may also require data controllers to send data directly to third parties or establish specific technical provisions on how to authenticate users or securely transmit information. Data portability policies may also establish certain terms for third parties that receive user data, such as security standards or restrictions on how they use data they receive. They may also clarify liability for data breaches or data misuse. Finally, data portability policies often specify which data are subject to this requirement and which data, such as proprietary data, are exempt.

Data portability is similar to, but distinct from, data access provisions. Data access may also require data controllers to allow users to request a copy of their information. However, data access requirements may not specify that the data be provided in a machine-readable format and without hindrance to further reuse.

WHAT ARE THE BENEFITS DATA PORTABILITY?

There are three main benefits of data portability: increasing consumer control, unlocking more value from data, and fostering competition. Naturally, the potential value of data portability varies depending on the sector and data involved.

First, data portability can give users more control over their information. At a basic level, data portability ensures that consumers always have the option to gain full control over their data by obtaining a complete copy of their information. Data portability ensures that consumers can independently backup their data, without relying on a third party. For example, data portability allows consumers to archive a copy of personal photos that they may have created and shared using a mobile app, ensuring that even if they stop using the app, they still have a copy of their data. Data portability is especially useful in this context when a company ends a service, changes a free service to a paid one, modifies its terms of service, or goes out of business, as it ensures users do not lose their data.[1]

Second, data portability can allow users to unlock more value from their data. A prerequisite for data-driven innovation is the ability of organizations to access data. When data is tied to a single service, its value is limited to how that service can use the information. Data portability allows users to share their data with additional services, creating more opportunities for data-driven innovation because of greater efficiency, more data availability, and the ability to reuse data for secondary purposes. For example, consumers might use data portability to quickly transfer a digital copy of their credit card spending to an online budgeting app. Not only does this ability to transfer data create greater value for consumers, by giving them greater insights on their personal finances, but it also enables a whole new class of financial planning apps that would not otherwise exist without access to this data. Similarly, consumers without much of a credit history may struggle to get access to credit; data portability allows them to show their cash flow on prepaid card accounts, opening up new possibilities for underwriting.[2]

Finally, data portability can enhance competition in four important ways. First, data portability fosters competition by reducing switching costs and avoiding vendor lock-in by making it possible for users to move their data from one service provider to another. Data portability reduces the opportunity for companies to artificially lock in customers by making it prohibitively expensive or cumbersome to move to another provider. Second, data portability can promote competition by creating more transparency about fees and alternatives. For example, consumers might use an app to analyze their home energy usage data to discover if they would pay less with an alternative energy provider, or review their bank fees to see if they would save money by switching to a different financial

institution. Third, data portability has pro-competitive effects by encouraging businesses to retain customers by offering better services. For example, when consumers can easily switch music streaming services, these services may invest in new ways to keep their users engaged on their platform, such as developing better recommendation algorithms.[3] Fourth, data portability allows new entrants to better compete with incumbents who may have collected data under less restrictive data protection laws and regulations. Without data portability and allowances for secondary uses of data, data protection rules can have anti-competitive effects, thus hurting consumer welfare and limiting innovation.

WHICH POLICIES ENABLE DATA PORTABILITY IN THE UNITED STATES?

A number of federal and state laws and regulations require data portability in the United States. This section provides an overview of some of the most prominent ones.

FEDERAL LAWS AND REGULATIONS

While the United States does not have a comprehensive federal data protection law, as shown in Table 1, it does have a number of sectoral data protection laws and some of these contain data portability requirements. In particular, federal privacy laws on health and financial data have created data portability rights for consumers.

Table 1: Federal laws requiring data portability

Law	Definition
HITECH Act	"The individual shall have a right to obtain from such covered entity a copy of such information in an electronic format and, if the individual chooses, to direct the covered entity to transmit such copy directly to an entity or person designated by the individual, provided that any such choice is clear, conspicuous, and specific."
Dodd-Frank Act	"Subject to rules prescribed by the Bureau, a covered person shall make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data. The information shall be made available in an electronic form usable by consumers."

Health Data

The Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act (ARRA) of 2009, updated the information disclosure requirements of the Health Insurance Portability and Accountability Act (HIPAA) of 1996.[4] HIPAA led to the creation of the HIPAA Privacy Rule in 2003, which established national standards for the protection of individuals' medical records and other personal health information. The HIPAA Privacy Rule specified that patients have a right to obtain a copy of their personal health information, and the HITECH expanded this requirement to specify that they had the right to obtain this information in an electronic format and that the data be sent to a designated third-party.[5]

Congress also passed the 21st Century Cures Act in 2016, which established additional requirements for data portability, including data exchange standards, secure application programming interfaces (APIs) for health information exchange, and stronger rules to prevent information blocking.[6] The legislation directed the Office of the National Coordinator for Health Information Technology to establish new rules for certified electronic health records systems. Under the new rules, certified EHR systems must have APIs that allow patients to easily access clinical and payment information through any third-party application they choose, including smartphone apps. Further, certified systems must be capable not only of exporting data for a single patient but also of exporting data for multiple patients for health care providers who want to change EHR systems.[7]

Parallel to these legislative and regulatory initiatives, there were a number of efforts beginning in 2010 to provide individuals access to an electronic copy of their personal health data through a voluntary "Blue Button" initiative. The Blue Button initiative initially reflected an effort to expedite patient access to their personal health data, even when industry data standards had not yet been fully developed. Prominent participants in the Blue Button initiative included the U.S. Department of Veterans Affairs, U.S. Department of Defense, and the Centers for Medicare and Medicaid Services.[8]

Financial Data

Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, gives consumers the right to access their financial information in an electronic format.[9] The Consumer Financial Protection Bureau (CFPB), responsible for implementing this law, has spent a number of years seeking feedback on how best to implement Section 1033, including by issuing a public request for information in 2016, releasing principles for financial data sharing and aggregation in 2017, and hosting a symposium on the topic in 2020.[10] More recently, in November 2020,

CFPB initiated a rulemaking process on Section 1033, and in July 2021, President Biden issued an executive order calling on the director of the CFPB to continue this process "to facilitate the portability of consumer financial transaction data so consumers can more easily switch financial institutions and use new, innovative financial products."[11]

STATE LAWS AND REGULATIONS

As of mid-2021, three states had passed comprehensive data protection laws: California, Colorado, and Virginia. As shown in Table 2, each of these states includes a data portability provision in the law. In general, each of these laws requires data controllers in the state to provide consumers an electronic copy of their data in a standardized format at no cost up to twice per year. They also all specify that consumers be allowed to transmit this data to a third party "without hindrance."

Table 2: Data portability provisions in state privacy laws

Law	Definition
California ("California Consumer Privacy Act")*	"A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period."
Colorado ("Colorado Privacy Act")	"A consumer has the right to obtain the personal data in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another entity without hindrance. A consumer may exercise this right no more than two times per calendar year. Nothing in this subsection…requires a controller to provide the data to the consumer in a manner that would disclose the controller's trade secrets."
Virginia ("Virginia Consumer Data Protection Act")	"A controller shall comply with an authenticated consumer request to exercise the right…to obtain a copy of his personal data that he previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated

means… Information provided in response to a consumer request shall be provided by a controller free of charge, up to twice annually per consumer. If requests from a consumer are manifestly unfounded, excessive, or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive, or repetitive nature of the request."

*** The California Privacy Rights Act of 2020 modifies the CCPA, but will not go into effect until 2023.**

Some states have also implemented sectoral-based data portability requirements, most notably in utilities. The Obama administration launched the "Green Button" initiative in January 2012.[12] The goal was to create an industry-led effort to make energy usage information available to consumers in a digital format to help them better manage their energy use. Utilities had begun to collect significantly more energy information as they adopted advanced smart meters, and this information could potentially be used to build new smart home applications, optimize and compare building energy use, and investigate options such as rooftop solar panels. Over 50 utilities have signed on to the initiative, representing over 60 million potential homes and businesses that could eventually have access to their data. The Green Button Alliance, a non-profit organization, now manages the development of the technical standard for electricity, natural gas, and water usage data.[13]

In addition to these voluntary efforts, a handful of states have created regulations to require data portability for energy data.[14] For example, the California Public Utilities Commission established rules in 2013 requiring utilities to provide customer energy data to third parties upon request using the Green Button standard.[15] Similarly, the Colorado Public Utilities Commission requires utilities to provide data to the customer or a designated third party, without charge and in a machine-readable format using "nationally recognized open standards and best practices."[16] Other states with data portability requirements include Illinois, Maine, Oregon, and Texas, as well as the District of Columbia, but the specific requirements vary by location.[17]

WHICH POLICIES ENABLE DATA PORTABILITY OUTSIDE THE UNITED STATES?

A number of countries outside the United States have passed data protection laws with data portability requirements. Key examples are discussed below.

EUROPEAN UNION

GDPR

The most prominent example outside the United States is the data portability provision in the European Union's General Data Protection Regulation (GDPR), which went into effect in EU member states on May 25, 2018. The GDPR enumerates a number of consumer data rights with Article 20, shown below in Table 3, establishing the right to data portability. Specifically, the GDPR requires data controllers to make data available to individuals in a "structured, commonly used and machine-readable format" and specifies that individuals have "the right to transmit those data to another controller without hindrance."[18] Notably, the GDPR only requires data transfers when "technically feasible," which leaves significant ambiguity for when a data controller would have to allow a consumer to share their data with a competing service.

In addition to initiatives by individual organizations to comply with the GDPR's data portability requirements, some industries have gone further to coordinate their data portability efforts. For example, Google has long embraced the concept of data portability. In 2007, it formed an internal team named the "Data Liberation Front," which was tasked with making it easier for users to take their data, such as contacts, social media, and photos, out of Google products.[19] Similarly, Facebook has offered a "Download Your Information" option since 2010.[20] After the GDPR, Google worked with Apple, Facebook, Microsoft, Twitter, and SmugMug to form the Data Transfer Project, an open-source platform to help users move data seamlessly between different online services.[21] The project has produced data models to facilitate importing and exporting data between different systems, as well as company-specific adapters that translate data from one company's APIs into the common data models.[22] The Data Transfer Project also specifies technical details such as how to handle error and rate limits so as not to overload these systems.

Similarly, three European telecom operators, Deutsche Telekom, Orange, and Telefónica, created the Data Portability Cooperation initiative, facilitated by the GSMA, an industry association of mobile operators, to develop a set of specifications for secure data portability within the telecom sector.[23]

PSD2

The revised Payment Services Directive (PSD2) is an EU Directive, approved in 2015, to establish a more integrated market for payment services throughout the European Union.[24] In addition to establishing rules allowing online payment services to access a user's bank account (e.g., to initiate a payment from the bank), PSD2 established rules for allowing online services to access a user's bank information (e.g., to provide a

consolidated view of multiple bank accounts). Given the sensitivity of this information, PSD2 established a detailed set of criteria for how account information service providers could gain access this information, what security measures they must follow, and who bears liability for any data breaches.

Table 3: Data portability provision in the GDPR and PSD2

Law	Definition
GDPR	"The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided… In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible."
PSD2	"In relation to payment accounts, the account servicing payment service provider shall: (a) communicate securely with the account information service providers in accordance with point (d) of Article 98(1); and (b) treat data requests transmitted through the services of an account information service provider without any discrimination for other than objective reasons."

UK

In 2017, the UK's Competition and Markets Authority (CMA) ordered the nine largest banks in Great Britain and Northern Ireland to adopt data portability provisions to address a lack of competition in retail banking. The order called for the creation of an independent organization to establish and maintain at no charge an open API standard and data format standards for accessing financial data.[25] This organization, the Open Banking Implementation Entity (OBIE), has since developed not only robust technical standards for secure data exchange and customer authentication in line with the CMA's order and PSD2's technical requirements, but it has also nurtured a growing ecosystem of hundreds of participants from financial institutions to fintech services.[26]

AUSTRALIA

The Australian government introduced the Consumer Data Right (CDR) in 2017.[27] The law establishes a right to data portability for consumers in designated sectors of the Australian economy, requiring businesses to disclose information on consumers to themselves or to accredited third parties in accordance with data standards.[28] The first designated sector for the CDR was banking, and Australian government has begun drafting rules for the energy and telecommunications sectors.[29]

CHINA

Article 45 of the Personal Information Protection Law gives individuals the right to request a copy of their personal data and transfer their personal data to a third party, so long as the parties meet the government's cybersecurity requirements.[30] The law came into force on November 1, 2021.

THE PHILIPPINES

The Data Privacy Act of 2012 established a right to data portability. Individuals in the Philippines may request a copy of their personal data for further use by a data controller if the data is held in an electronic and commonly used format. The National Privacy Commission is authorized to set technical standards and procedures for data transfers.[31]

SINGAPORE

In November 2020, Singapore passed an amendment to the Personal Data Protection Act 2012 that included new regulations for data portability.[32] The law directs data controllers to directly transmit data to third parties with a presence in Singapore upon request from users. Data controllers must deny requests if the data transfer would threaten the safety or physical or mental health of the user or a third party, or if the transfer would be contrary to the national interest. Unlike under other data portability laws, users do not directly receive a copy of their personal data.

THAILAND

Thailand's Personal Data Protection Law gives data subjects the right to request that data controllers send their data to other data controllers if the data can be read by automated tools and the transfer can be done by automatic means. Data controllers are exempt from data portability requests in certain cases, such as when the transfer is against the public interest or will violate the rights and freedoms of others.

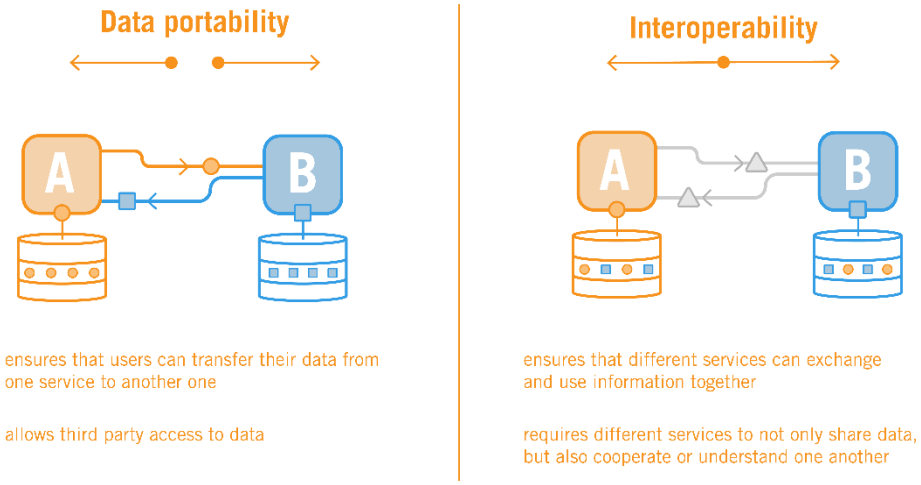
The Cabinet of Parliament of the Kingdom of Thailand has twice approved a Royal Decree postponing enforcement of several provisions of the Personal Data Protection Law, including those dealing with data portability, for certain organizations, such as those in the financial, transportation, and

telecommunications sectors. The law is currently set to take effect for exempt entities on May 31, 2022.[33]

HOW DOES DATA PORTABILITY DIFFER FROM INTEROPERABILITY?

Data portability is different from interoperability, although the concepts are sometimes conflated. As shown in Figure 1, the purpose of data portability is to ensure users can transfer their data from one service to another, whereas the purpose of interoperability is to ensure that different services can exchange and use information together. In some cases, data portability may enable a degree of interoperability, such as if two services allow users to share their data back and forth so that user data is fully synced in both services. But interoperability requires different services not only to share data, but also to understand and cooperate with one another. For example, data portability allows users to switch from one email service provider to another—such as from Gmail to Outlook.com—and move all their messages with them, but interoperability is what allows users with one email service provider to send messages to users of different email service providers.

Figure 1: Data portability versus interoperability



The distinction can be seen in policies such as PSD2, which contains both data portability and interoperability requirements. The data portability requirements allow users to authorize third-party services, such as mobile apps, to access their data from their bank accounts, whereas the interoperability requirements allow users to authorize these third-party services to make payments directly from their bank accounts. In some cases, the difference between data portability and interoperability can be thought of as analogous to the difference between "read" access to a system's data versus "read and write" access.

HOW DO REGULATORS ENFORCE DATA PORTABILITY?

Many provisions in data protection laws and regulations are created as legal rights or obligations: Positive rights (entitlements) require others to act a certain way whereas negative rights (liberties) limit others from interfering with an individual's ability to do something. Examples of positive data rights include an obligation for data controllers to obtain user consent before collecting personal data; an obligation for data controllers to notify consumers in the event of a data breach; or an obligation for data controllers to provide consumers notice about their data collection policies. Examples of negative data rights include the freedom for employees not to disclose health conditions to their employer, or the freedom of individuals to refuse to share their data with law enforcement without a warrant.

Data portability encompasses both a positive and a negative data right: an obligation for data controllers to make user data available for electronic access, and the freedom for users to share their data with third parties without interference. This distinction is important because enforcement of positive data rights differs from that of negative data rights. Regulators can more easily verify compliance with positive data rights because they can confirm the presence of a specific practice—such as by checking whether a data controller has obtained consent to process data or whether it has notified consumers in the event of a data breach—either directly or by relying on a third-party validator. In contrast, regulators cannot verify negative rights directly because doing so would require proving something does not exist. Instead, regulators enforce negative rights through investigating claims providing evidence of violations, such as a complaint by an employee that their employer has demanded private health information.

Regulators face similar challenges when enforcing data portability requirements. While it is fairly straightforward for regulators to verify that a data controller provides its users the ability to download a copy of their data, it must actively monitor complaints to understand if data controllers put in place functional barriers that hinder data portability in practice. For example, the Department of Health and Human Services (HHS) created a standardized process to allow the public to report claims of information blocking among health care providers and health IT vendors, and authorized the Office of the Inspector General Office to investigate these claims.[34] The Department of Justice eventually forced one vendor to pay $155 million to settle a claim that it did not meet HHS's requirements, including that it "failed to satisfy data portability requirements intended to permit healthcare providers to transfer patient data from [its] software to the software of other vendors."[35]

Enforcement of data portability may be necessary when data controllers block access to user data in ways that thwart competition. In October

2020, SongShift, an app that lets users transfer music playlists between different streaming platforms, announced that Spotify had notified the company that it was revoking its access to Spotify's API—effectively preventing Spotify users from transferring their playlists to other services, an apparent violation, at least in spirit, to its commitment to data portability under GDPR.[36] In response to complaints, Spotify reversed course later that month.

Without mandatory data portability obligations, voluntary data sharing agreements can fall apart when they are not in the interest of the data controller.[37] For example, despite previously allowing it, PNC Bank made security updates in 2019 that prevented customers from accessing their bank data through certain third-party apps. While the bank stated that the changes were made to improve security, they also had the effect of cutting off access to competing peer-to-peer payment services like Venmo, while still allowing access to Zelle, a platform backed by the bank.[38]

HOW DOES DATA PORTABILITY IMPACT PRIVACY AND SECURITY?

Data portability raises important privacy and security issues that if not addressed can expose consumer data to new vulnerabilities. Unfortunately, many data portability laws do not address these issues, leaving it to the private sector to find appropriate solutions. These issues generally fall into one of three categories.

First, since data portability enables the transfer of personal information, it is important for the data controller to ensure that it only shares data when the user has authorized the transfer. In one experiment, a researcher made a series of unauthorized data requests for the personal information of someone else from more than 150 businesses, large and small, subject to the GDPR. They found that 24 percent of these businesses turned over the personal information without any verification and another 16 percent provided the information with only weak verification of their identity, such as a falsified scan of a postmarked envelop).[39] Data controllers should always verify data portability requests to prevent unauthorized data sharing.

Second, data portability can involve personal data that is also associated with someone other than the user making the data portability request. For example, a user's social media interactions, lists of contacts, and photos, videos, and other media, may involve the personal information of others. Indeed, allowing users to authorize the transfer of not just their own data but the data they can access about their friends on a social network is what led to the Cambridge Analytica scandal.[40] Some users may not want their personal data downloaded by a user or shared with other entities. At the same time, limiting the transfer of this information, could limit the

utility of data portability for the users making these requests, especially when there are important linkages between different users, such as on social media. There are various possibilities for addressing these concerns, such as using hashed identifiers in lieu of personally identifiable contact information, or using unique identifiers for individual relationship pairs to allow another service to reconstruct these connections and relationships if both parties transfer their data.[41]

Third, data portability raises questions about the liability of the data controller for misuse of data by the recipient. Generally, the responsibility for the user's data should end at the point at which the data controller has securely transferred the user's data to the correct party, whether it be the user or another designated service. However, policymakers have not always provided clear guidance on this issue, raising questions about the liability and responsibility for a data controller if, for example, it suspects that the account may have been compromised, or that the recipient is not processing data in accordance with applicable laws. To address these concerns, policymakers may require certain minimum security requirements for data controllers to be eligible to receive data directly from data controllers.

HOW SHOULD POLICYMAKERS SUPPORT DATA PORTABILITY?

There are various ways that policymakers can support data portability.

CREATE DATA PORTABILITY POLICIES AT THE NATIONAL LEVEL

Data portability is an important provision in many data privacy laws. However, these policies should be created at the national level, not the state level, to avoid a patchwork of laws that create unnecessary uncertainty for consumers and complexity for organizations. For example, legislation such as the "Access to Consumer Energy Information Act," or E-Access Act, would direct the Energy Secretary to establish model data-sharing standards and policies for state regulators to use to ensure that consumers can gain access to information about their residential electric and natural gas usage.[42] Federal data portability policies should address issues such as privacy and security to prevent unauthorized disclosures.

PRIORITIZE HIGH-IMPACT OPPORTUNITIES FOR DATA PORTABILITY

As discussed in this report, data portability creates significant consumer benefit in certain sectors, such as health care, financial services, and energy. And while there are likely many other instances where data portability may create value to consumers, the cost to businesses of providing data portability may not always outweigh these benefits. Therefore, policymakers should prioritize enacting sector-specific rules for data portability where there are clear benefits to consumers, rather than implementing a broad data portability requirement that would apply to all

consumer data. Focusing on sector-specific rules will also enable policymakers to create more detailed requirements to address concerns about privacy and competition as they apply to individual sectors.

LIMIT THE SCOPE OF NON-SECTOR-SPECIFIC DATA PORTABILITY REQUIREMENTS

If policymakers decide to create a broad data portability requirement that applies to consumer data in all sectors, they should limit the scope of this requirement to data directly provided by consumers. Excluding data that service providers might observe about users or infer about users from a data portability requirement will help protect both user privacy and proprietary data. For example, a user's pattern of engagement with content on an online service might allow a competitor to reverse-engineer the recommendation algorithms used on that platform and reveal sensitive proprietary information.

SUPPORT INDUSTRY-LED DATA PORTABILITY STANDARDS

While the public sector has an important role to play in ensuring that data controllers adhere to their data portability obligations, it should allow the private sector to lead on the development of data portability standards. Industry-led data portability standards, such as the Green Button Initiative, the Open Banking Implementation Entity (OBIE), the Financial Data Exchange (FDX), and others, show that industry stakeholders are often best positioned to address the technical details of interoperability, such as the data models, APIs, and security standards, especially to address the complexities involved in transferring data between services.

ENCOURAGE DATA PORTABILITY APIS BUT ALLOW DATA SCRAPING

In general, APIs provide the most direct and secure way to allow users to transfer data between different services in a standardized electronic format. However, data controllers may not always choose to make user data available through APIs, or they may impose constraints on those APIs that make them insufficient for certain applications. While policymakers should generally encourage the development of industry-standard APIs, when these are not available or are insufficient to meet consumer needs, they should not prevent users from exercising their data portability rights by using web-scraping technology, which allows users to capture the data that they would get through a web browser.

USE DATA PORTABILITY AS A PATHWAY TO ALLOW CONSUMERS TO DONATE THEIR DATA

Many individuals have expressed interest in sharing their data for altruistic purposes, such as to advance medical research or improve understanding of how students learn. Unfortunately, consumers often cannot easily share their data. Data portability can offer a pathway to allow individuals to share their data that is collected for one purpose to be used for additional

purposes that benefit others. Policymakers should therefore ensure that data portability laws and regulations do not preclude any types of secondary uses of their data. In addition, some individuals may prefer to share their data only after they are no longer alive, similar to other types of donations. Therefore, policymakers should consider whether consumers can elect to exercise their data portability rights posthumously.

REFERENCES

1. James Fallows, "A Problem Google Has Created for Itself," *The Atlantic*, March 21, 2013, https://www.theatlantic.com/technology/archive/2013/03/a-problem-google-has-created-for-itself/274232/.
2. Chi Chi Wu, "Preserving the Right of Consumers to Access Personal Financial Data," Testimony before the U.S. House of Representatives Committee on Financial Services, Task Force on Financial Technology, September 21, 2021, https://financialservices.house.gov/uploadedfiles/hhrg-117-ba00-wstate-wuc-20210921.pdf.
3. Esmeralda Florez Ramos and Knut Blind, "Data portability effects on data-driven innovation of online platforms: Analyzing Spotify," *Telecommunications Policy*, Volume 44, Issue 9, 2020, https://www.sciencedirect.com/science/article/abs/pii/S030859612030118X.
4. "Health IT Legislation," HealthIT.gov, June 8, 2021, https://www.healthit.gov/topic/laws-regulation-and-policy/health-it-legislation.
5. "Health Information Technology for Economic and Clinical Health Act," Pub. L. No. 111-5, 123 Stat. 226 (2009), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf.
6. 21st Century Cures Act, H.R. 34, 114th Cong. (2015), https://www.congress.gov/bill/114th-congress/house-bill/34/text.
7. "Information Blocking and the ONC Health IT Certification Program: Extension of Compliance Dates and Timeframes in Response to the COVID-19 Public Health Emergency," Federal Register, November 4, 2020, https://www.federalregister.gov/documents/2020/11/04/2020-24376/information-blocking-and-the-onc-health-it-certification-program-extension-of-compliance-dates-and.
8. "Blue Button," HealthIT.gov, April 8, 2019, https://www.healthit.gov/topic/health-it-initiatives/blue-button; "Blue Button," U.S. Department of Veterans Affairs, September 30, 2021, https://www.va.gov/bluebutton/; "CMS Blue Button 2.0," CMS Blue Button 2.0, n.d., https://bluebutton.cms.gov/.
9. "Open Banking, Data Sharing, and the CFPB's 1033 Rulemaking," Congressional Research Service, September 9, 2021, https://crsreports.congress.gov/product/pdf/IN/IN11745.
10. "Request for Information Regarding Consumer Access to Financial Records," Federal Register, November 22, 2012, https://www.federalregister.gov/documents/2016/11/22/2016-28086/request-for-information-regarding-consumer-access-to-financial-records; "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation, " Consumer Financial Protection Bureau, October 18, 2017, https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf; "Bureau Symposium: Consumer Access to Financial Records," Consumer Financial Protection Bureau, July 2020,

https://files.consumerfinance.gov/f/documents/cfpb_bureau-symposium-consumer-access-financial-records_report.pdf.

11. "Executive Order on Promoting Competition in the American Economy," The White House, July 9, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/.
12. "Green Button," Energy.gov, n.d., https://www.energy.gov/data/green-button.
13. "About Green Button and the Alliance," Green Button Alliance, n.d., https://www.greenbuttonalliance.org/about.
14. "Energy Data Portability," Mission:data, January 2019, http://www.missiondata.io/s/Energy-Data-Portability.pdf.
15. "Data Access," ACEEE, August 2020, https://database.aceee.org/state/data-access.
16. Ibid.
17. Ibid.
18. "Art. 20 GDPR: Right to Data Portability," in EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.
19. "The Data Liberation Front Delivers Google Takeout," Data Liberation Blog, Google, June 28, 2011, http://dataliberation.blogspot.com/2011/06/data-liberation-front-delivers-google.html.
20. Erin Egan, "Data Portability and Privacy," Facebook, September 2019, https://about.fb.com/wp-content/uploads/2020/02/data-portability-privacy-white-paper.pdf.
21. "About Us," Data Transfer Project, n.d., https://datatransferproject.dev/.
22. "Technical Overview," Data Transfer Project, n.d., https://datatransferproject.dev/documentation.
23. "Telecoms as the 'Secured Data Hub' for the digital society," GSMA, n.d., https://www.dataportabilitycooperation.org/assets/Telecoms_Secured_Data_Hub.pdf.
24. EU Directive 2015/2366: Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366.
25. "Retail Banking Market Investigation: The Retail Banking Market Investigation Order 2017," Competition & Markets Authority, February 2, 2017, https://assets.publishing.service.gov.uk/media/5893063bed915d06e1000000/retail-banking-market-investigation-order-2017.pdf.
26. "Annual Report: 2020," Open Banking, 2020, https://insights.openbanking.org.uk/annual-report-2020/home/.

27. "Consumer Data Right," Australian Competition & Consumer Commission, October 29, 2021, https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0.

28. "Competition and Consumer (Consumer Data Right) Rules 2020," Federal Register of Legislation, December 23, 2020, https://www.legislation.gov.au/Details/F2021C00076.

29. "Consumer Data Right," Australian Competition & Consumer Commission, October 29, 2021, https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0.

30. Personal Information Protection Law of the People's Republic of China, China (2021). http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml.

31. Republic Act 10173 - Data Privacy Act 2012 Chapter IV, The Philippines (2012). https://www.privacy.gov.ph/data-privacy-act/.

32. Personal Data Protection (Amendment) Act, Singapore (2020). https://www.parliament.gov.sg/docs/default-source/default-document-library/personal-data-protection-(amendment)-bill-37-2020.pdf.

33. Royal Decree on the Organizations and Businesses of which Personal Data Controllers are exempted from the Applicability of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2564 (2021), Thailand (2021). http://www.ratchakitcha.soc.go.th/DATA/PDF/2564/A/032/T_0001.PDF.

34. "Information Blocking," HealthIT.gov, March 19, 2021, https://www.healthit.gov/topic/information-blocking.

35. "Electronic Health Records Vendor to Pay $155 Million to Settle False Claims Act Allegations," U.S. Department of Justice, May 31, 2017, https://www.justice.gov/opa/pr/electronic-health-records-vendor-pay-155-million-settle-false-claims-act-allegations.

36. "A Note About Spotify Transfers," SongShift, October 21, 2020, https://songshift.com/blog/spotify_transfers.

37. Daniel Castro, "Blocked: Why Some Companies Restrict Data Access to Reduce Competition and How Open APIs Can Help," Center for Data Innovation, November 6, 2017, https://datainnovation.org/2017/11/blocked-why-some-companies-restrict-data-access-to-reduce-competition-and-how-open-apis-can-help/.

38. Yuka Hayashi, "Venmo Glitch Opens Window on War Between Banks, Fintech Firms," *The Wall Street Journal*, December 14, 2019, https://www.wsj.com/articles/venmo-glitch-opens-window-on-war-between-banks-fintech-firms-11576319402.

39. James Pavur and Casey Knerr, "GDPArrrrr: Using Privacy Laws to Steal Identities," Blackhat USA 2019, 2019, https://i.blackhat.com/USA-19/Thursday/us-19-Pavur-GDPArrrrr-Using-Privacy-Laws-To-Steal-Identities-wp.pdf.

40. Paul Przemyslaw Polanski, "Some thoughts on data portability in the aftermath of the Cambridge Analytica scandal," (2018), 7, *Journal of European Consumer and Market Law*, Issue 4, pp. 141-146, https://kluwerlawonline.com/journalarticle/Journal+of+European+Consumer+and+Market+Law/7.4/EuCML2018030.

41. Erin Egan, “Data Portability and Privacy,” Facebook, September 2019, https://about.fb.com/wp-content/uploads/2020/02/data-portability-privacy-white-paper.pdf.

42. E-Access Act, H.R. 5796, 116th Congress (2020), https://www.congress.gov/bill/116th-congress/house-bill/5796/text.

ACKNOWLEDGEMENTS

This report was made possible in part by the generous support of Plaid. The Center maintains complete editorial independence for all of its work. All opinions, findings, and recommendations are those of the Center and do not necessarily reflect the views of its supporters. Any errors and omissions are the author's alone.

ABOUT THE AUTHOR

Daniel Castro is the director of the Center for Data Innovation and vice president of the Information Technology and Innovation Foundation. He has a B.S. in foreign service from Georgetown University and an M.S. in information security technology and management from Carnegie Mellon University.

ABOUT THE CENTER FOR DATA INNOVATION

The Center for Data Innovation is the leading global think tank studying the intersection of data, technology, and public policy. With staff in Washington, D.C., and Brussels, the Center formulates and promotes pragmatic public policies designed to maximize the benefits of data-driven innovation in the public and private sectors. It educates policymakers and the public about the opportunities and challenges associated with data, as well as technology trends such as open data, artificial intelligence, and the Internet of Things. The Center is part of the nonprofit, nonpartisan Information Technology and Innovation Foundation (ITIF).

contact: info@datainnovation.org

datainnovation.org