PORTABILITY, NOT DOCTRINE, IS KEY TO UNLOCK USER AGENCY FOR DATA

BY CHRIS RILEY[1]

1 Director, Data Transfer Initiative.

CPI ANTITRUST CHRONICLE APRIL 2023

Visit www.competitionpolicyinternational.com for access to these articles and more!

PORTABILITY, NOT DOCTRINE, IS KEY TO UNLOCK USER AGENCY FOR DATA

By Chris Riley

Data is of central importance for users of digital services, and for many years has been the subject of significant attention in the realm of public policy. In the context of the historical common law doctrine of essential facilities, little wonder that many scholars have looked at data. But this is a poor choice of path. Digital data is both created and used within specific contexts, and its value derives from its use within contexts. Looking at personal data through the blunt lens of the essential facilities doctrine risks losing those contexts, and will struggle to reach an effective public policy balance, including taking into proper account privacy considerations. Meanwhile, there have been significant advancements in data portability for personal data, including both greater product offerings and more well-developed public policy principles and understandings. As public policy frameworks for data portability continue to develop, this article will offer some principles to guide those conversations to reinforce and strengthen the efficacy of data portability as a paradigm for governing personal data.

I. INTRODUCTION

Data is of central importance for users of digital services, and for many years has been the subject of significant attention in the realm of public policy. Some argue that the common law doctrine of essential facilities that has traditionally been applied to physical infrastructure in transportation, energy, and telecommunications, should now be applied to the realm of digital data flows. But this is a poor choice of path, and not only for the known distinction of data as non-rivalrous in nature. Digital data is both created and used within specific contexts, and its value derives from its use within contexts. Looking at personal data in particular through the blunt lens of the essential facilities doctrine risks losing those contexts and will struggle to reach an effective public policy balance, including taking into proper account privacy considerations.

The overarching public policy goal of strengthening the data economy is better served through existing data portability advancements happening all around the world, including both greater product offerings as well as more well-developed public policy principles and understandings. Among other benefits as compared to expanding court doctrine, data portability tools and policies explicitly consider privacy and data protection consideration and develop through consultative and multistakeholder processes that allow broad perspectives to influence output. In contrast, the blunt tool of court interpretation applying common law doctrine to specific instances of fact will inevitably fail to take diverse contexts and perspectives into account.

As public policy frameworks and tools for data portability continue to develop, this article offers three principles to reinforce and strengthen the efficacy of portability as a paradigm for governing personal data: empower users to transfer their data; protect privacy and security of data; and clarify liability for data transfers.

II. DATA CONTEXTS IN THE MODERN INTERNET ECOSYSTEM

Not all data is created equal. The scope of this article is personal data, transferred between businesses putting that data to functional, technical use. This is distinct from data issues arising in the context of researcher access, although that context also involves personal data; similarly, government access requests typically include personal data, but with very different policy tradeoffs. Personal data is defined in the European Union's General Data Protection Regulation (GDPR) Art. 4(1) as "related to an identified or identifiable natural person"; the category includes user communications, activity histories, and other data that can be associated with a person, but does not include data aggregated across many users where that identifiability is inherently and irretrievably lost, and also does not include data with no relation to natural persons such as business logistics data. Commercial exchanges of non-personal data are thus quite distinct.

Within the context of user-driven access to personal data, recent years have given rise to a rich ecosystem of Application Programming Interfaces paired with extensive documentation of digital platform operations, all aimed at developers building complementary tools. Mutually beneficial interconnections add value to the "host" service making data available as well as creating new markets for investment and innovation downstream, implementing the "standing on the shoulders of giants" model of technology development.

While some APIs offer access without requiring user authentication and execution to initiate transfer, such interfaces are limited to non-personal data to avoid violating well-established data protection laws in many jurisdictions, and powerful norms in others where the legal contours are less clear. The balance of data protection and portability has been of critical importance for many years, with the historical Cambridge Analytica incident long serving as a reminder that even user authentication is but a piece of the solution, incomplete by itself.

The modern API landscape is immense, the subject of conferences of developers such as the annual API Specifications Conference.[2] This richness creates a broad range of contexts in which data is originally contributed by a user to a system, or generated about the user based on activity, contexts which are described in developer documentation prepared alongside the APIs which make that data accessible to other organizations. This description of context is necessary because, as a consequence of continuous innovation, the use of the same data by two organizations is generally alike, but not exactly alike.

These slight variations are features, not bugs, of a technology ecosystem and competitive market. And they tie the value of digital data fundamentally to the contexts of its use. From that perspective, the common law doctrine of essential facilities has a blind spot, as it homogenizes the nature and use of inputs across different firms. Implementation through court systems creates a risk of extending, not remedying, that inherent myopia, by virtue of developing through a case-by-case basis tied to specific fact patterns.

2 https://events.linuxfoundation.org/openapi-asc/.

In contrast, data portability as a paradigm well handles data in contexts that are not perfectly uniform, whether examined from the lens of privacy or promoting competition. In privacy, giving users agency to control the use of their data does not presume equivalence of uses, and in fact gives users the right to choose to use their data nowhere at all. Data portability gives users the ability to migrate their data to another service, even where the experience is different; that choice remains the user's.

III. ACCESS TO DATA IS CRITICAL; BUT THE AGENCY OF ACCESS MATTERS

The essential facilities doctrine, in a nutshell, holds that if a firm controls certain kinds of indispensable business inputs (facilities) and excludes competitors from access to those inputs, it can be in violation of antitrust under common law. In the United States, this doctrine has emerged as distinct from refusals to deal that arise from customers and supply chains, which do not depend on the input being essential; in the European Union, these, and other theories of illegal exclusionary conduct blur together a bit more, however in practice require a finding that the input is essential. (Graef, 157).[3] In lower American courts, one significant precedent also considers whether the input at hand could "practically be duplicated." (*Id.* 160) Thus, the essential facilities doctrine includes three factors: whether the input at hand is essential to the operation of a competing business, whether it is being denied to competitors, and if both of these are true, whether it is impractical to duplicate the input.

Digital data raises questions as to the applicability of these factors in many different contexts. The contextual necessity, non-duplicability, and accessibility of data are all legitimate subjects of debate in a broad range of scenarios. But this article does not propose to engage with these questions in depth. Rather, it emphasizes a factor entirely missing from the essential facilities framework: the lens of "who's asking."

There is a world of practical policy difference between a competing firm asking for access to data, and a user asking its service provider for access. These differences hold even if the outcome at the end of both asks is the same – i.e. even if the user subsequently provides the data to that competing firm.

The differences arising from "agency in the asking" begin with principles. Under the General Data Protection Regulation, data portability is a fundamental right in the European Union. That right inheres in individuals, not data controllers. A firm demanding access to personal data does not have any fundamental right to such access; only the data subject does. While the United States lacks a similar fundamental framework of digital rights, free market norms similarly do not extend to competitor rights of access, but do encompass the ability of individuals to "choose with their feet" and switch services within a market; and to make that freedom of choice real, some amount of necessary data may need to move with the user.

Agency also carries practical, strategic consequences as well. Protecting the privacy and security of user data in the context of data portability depends on authenticating the user before providing access and limiting the scope of data made available to that within the user's authorized access. Data transfers between firms, without the inherent limitations that come from individual user action and agency, pose a greater potential for privacy and security harm through the practical difficulties of managing necessary limitations on scope.

Even accepting the (debatable) premise that access to personal data is essential, not able to be duplicated, and not sufficiently accessible, forcing data transfer without centering on individual user agency introduces as much risk as remedy. Furthermore, it's unnecessary, given the rapid evolution of data portability.

IV. DATA PORTABILITY PRODUCTS AND PUBLIC POLICY ARE EVOLVING

A report by CERRE in 2020 expands in detail on the then-current state of public policy and products related to data portability.[4] It centers around the data portability rights established in the GDPR and the early stages of two products, Solid and the Data Transfer Project, along with the nascent ecosystem of Personal Information Management Systems. In the short time since then, both regulations and technologies have made substantial steps forward.

3 https://core.ac.uk/download/pdf/34662689.pdf.

4 https://cerre.eu/wp-content/uploads/2020/07/cerre_making_data_portability_more_effective_for_the_digital_economy_june2020.pdf.

Notably, the Data Transfer Project has continued to see growth in its open-source code base, as well as real world deployment.[5] The model of DTP works by identifying and building code to represent a central "data model" that articulates the core of a user experience to be migrated through portability tools, and then building adapters that translate from individual service APIs to and from that data model. In practice, this means that users can initiate data transfers through DTP that move data directly from one service to another, avoiding the technical challenge and bottleneck of downloading data over a local internet access service and storing it on a personal device, as well as translational issues that could arise between the exporting and importing services. Today, the DTP framework powers direct data transfer features within Google Takeout,[6] Facebook's Transfer your Information,[7] and Apple's Data and Privacy page,[8] collectively available to billions of internet users. DTP also includes software libraries that provide connections to over a dozen additional services. (Disclaimer: The author of this article is the inaugural executive director of the Data Transfer Initiative, a nonprofit organization established to invest dedicated resources in data portability, in principal part through supporting the Data Transfer Project.)

The EU has taken the lead again on regulation, with the completion of its Digital Markets Act legislative process. The DMA, which will begin to take legal effect in 2023, includes a new, digital platform directed mandate to provide data portability, distinct from the rights of data subjects under the GDPR. Specifically, Article 6(9) of the DMA imposes the following obligation on designated gatekeepers:

> The gatekeeper shall provide end users and third parties authorised by an end user, at their request and free of charge, with effective portability of data provided by the end user or generated through the activity of the end user in the context of the use of the relevant core platform service, including by providing, free of charge, tools to facilitate the effective exercise of such data portability, and including by the provision of continuous and real-time access to such data.

Incorporating data portability with an objective not derived from privacy and data protection goes immediately to address a shortcoming of prior data portability policies, as articulated in (among other sources) a 2021 report by the OECD: "Further, it is clear that the objective of data portability and interoperability measures matters. Portability and interoperability measures implemented with objectives other than competition (such as data protection) may not have procompetitive impacts unless designed with market dynamics in mind." (OECD 2021, 49).[9]

Substantively, the language of the DMA expands on the GDPR in two fundamental ways. First, it specifies that portability must include data "generated through the activity of the end user" – data about, not from, a user. Second, data portability must include "the provision of continuous and real-time access to such data." While neither of these concepts has yet been defined, they will undoubtedly expand the horizon for users' ability to migrate their data to services of their choice.

V. THREE PRINCIPLES CAN SHAPE A USER-CENTRIC FUTURE FOR DATA PORTABILITY

Given this growth, the path ahead for data portability is bright, but remains uncertain. As the OECD's report made clear, design and implementation of data portability matter. This article thus offers three principles as guidance for policymakers and product builders to realize the benefits of data portability, particularly for technology users: empower users to transfer their data; protect privacy and security of data; and clarify liability for data transfers.

A. Empower Users to Transfer Their Data

The foundation for balancing public policy in data portability is ensuring that users are in control of transfers of their data. This is necessary to comport with both fundamental rights frameworks and free market principles. In practice, providing users with control has several ramifications for product and policy design. Users should be the sole initiator of data transfers, not businesses operating other than at the direct delegation of a user; furthermore, data portability should not become a lever for government access, which should continue to go through separate lawful access frameworks. The scope of data transfers initiated by a user should center around that user's data and not encompass data beyond that, particularly where broader scope of a transfer would harm another's privacy. Next, reciprocity should be offered - users risk being worse off if they choose to transfer data to a service, and later are unable to transfer it back, should the destination service not offer portability as effectively

5 https://dtinit.org/.

6 https://takeout.google.com/takeout/transfer/custom/photos.

7 https://www.facebook.com/tyi.

8 https://privacy.apple.com/.

9 https://www.oecd.org/daf/competition/data-portability-interoperability-and-digital-platform-competition-2021.pdf.

as the origin. And finally, once data has been transferred at a user's direction to a new service, that new service provider should have the same abilities and permissions for data collection and use as if the user had provided the data through existing means.

B. Protect Privacy and Security of Data

Conversations around public policy and data portability have long tangled with the risks that can arise if data transfers are not subject to sufficiently rigorous privacy and security practices. Yet, no clear framework or guidance exists. Legislation or regulation in one or more relevant jurisdictions could add significant value by setting minimum standards for privacy and security practices before permitting data transfer, as a dual means of ensuring baseline sufficiency and of insulating providers who are behaving responsibility from some legal risk. At the same time, such a standard should be a clear minimum, not a maximum. Providers may set higher standards for privacy and security, reflecting their inherent understanding of the risks associated with transfer of data they control, in contexts they shape. Should these higher standards not be met, providers should not be required to transfer data.

C. Clarify Liability for Data Transfers

The global advancement of data protection regulations poses some implementation complexity for data portability obligations. In particular, data transfer mechanisms offering practical benefits for data portability interfaces cannot be effective unless the recipients of data through these mechanisms can take advantage of the same benefits of legitimacy of data collection and use, conferred to the service provider by the user's intentional decision to transfer the data, building on the foundational principal of empowering users. Legislative and regulatory frameworks for data portability should not hold a service provider responsible either for transmitting or receiving data through a data transfer mechanism lawfully executed by a data user. However, once receiving the data, the recipient service provider should then accept and hold any potential liability associated with holding the data, such as obligations to respond to notice and takedown requests.

VI. CONCLUSION

Conversations of the efficacy of existing competition doctrine for tech are occurring worldwide, and there are contexts and circumstances in which these offer significant potential. However, the essential facilities doctrine is a hammer, and very few problems are nails. Access to personal data is a nuanced challenge, and any remedy must balance the considerations of user centricity, privacy and security, and service provider liability, all of which require a deft intervention. Fortunately, data portability public policy and tools have advanced substantially in recent years and provide a strong foundation for continued development.

CPI COMPETITION POLICY® INTERNATIONAL

CPI Subscriptions

CPI reaches more than 35,000 readers in over 150 countries every day. Our online library houses over 23,000 papers, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.