The Portability and Other Required Transfers Impact Assessment (PORT-IA): Assessing Competition, Privacy, Cybersecurity, and Other Considerations

Peter Swire*

CITE AS: 6 GEO. L. TECH. REV. 57 (2022)

ABSTRACT

The goal of this article is to provide a framework for assessing issues of data portability and other required transfers of data. Greater portability and other required transfers of data can have pro-competitive effects – if more companies have access to commercially valuable data, then there can be less monopoly power and more innovation. On the other hand, making portability too easy can lead to serious privacy and cybersecurity effects, when the “wrong” people gain access to personal data. There is thus a tension between opening data flows, to promote competition and innovation, provide user

* Elizabeth and Tommy Holder Chair of Law and Ethics, School of Cybersecurity and Privacy and Scheller College of Business at the Georgia Institute of Technology; Senior Counsel, Alston & Bird LLP. Research support for this project has come from Alston & Bird LLP, Facebook, the Institute for Information Security and Privacy at Georgia Tech, the Georgia Tech Scheller College of Business, and Microsoft. During the period of research on this project, I received general funding from the Carnegie Corporation of New York and the Hewlett Foundation Cyber Project. My thanks for comments on earlier versions of this research presented at: Computers, Privacy & Data Protection ’21; Federal Trade Commission workshop “Data to Go: A Federal Trade Commission Workshop on Data Portability;” OECD Expert Discussion in Preparation for Data Portability Workshop; OECD Online Expert Workshop on Data Portability; Testimony before OECD Competition Committee on “Data Portability, Interoperability, and Competition;” the Privacy + Security Forum, and the Privacy Law Scholars Conference. For comments on earlier versions of this research, my thanks to Michael Barr, Kathleen Benway, Michael Froomkin, Inge Graef, DeBrac Kennedy-Mayo, Orin Kerr, Bijan Madhani, Aaron Massey, Wim Nauwelaerts, Gabriel Nicholas, and John Snyder. An earlier version of this paper was published on SSRN on September 8, 2020 and is available at https://peterswire.net/academic_publication. For the final publication, my thanks for research assistance to Simon Albert, Paul Greaves, Sara Guercio, and Duke Hatcher.
control, and for other reasons, and closing data flows, for reasons including protecting privacy and cybersecurity.

Part I explains that “portability” has become a technical legal term for transfers of an individual’s data. “Other Required Transfers” are mandated transfers for two or more people, so “PORT” is the general term for Portability or Other Required Transfers.

Part II examines three major trends causing increased importance for PORTability issues: (1) the individual right to data portability that took effect in the European Union (“EU”) in 2018 and in California in 2020; (2) the current, intense policy debates about whether and how to regulate the largest digital platforms; and (3) beyond digital platforms, important sectors of the economy increasingly have PORTability requirements.

Part III proposes a Portability and Other Required Transfers Impact Assessment (“PORT-IA.”). The approach is similar to Privacy or Data Protection Impact Assessments. The PORT-IA sets forth fourteen structured questions (“Structured Questions”) with detailed sub-parts.

Part IV and the appendices present seven case studies: (1) U.S. and EU phone number portability; (2) the new U.S. health care interoperability regulation; (3) EU portability requirements concerning health care data; (4) the EU Payment Services Directives; (5) U.S. financial services requirements under Section 1033 of the Dodd-Frank Act; (6) Open Data requirements for government agencies; and (7) lesser-known recent laws in Arizona and other states mandating portability for the data of automobile dealers.

Each case study maps the mandated data flows: where does the data originate; where does it go; what types of data are covered; and what precisely are the legal requirements. Each case study then examines the benefits of the PORT initiative, the risks and costs of the PORT initiative, and lessons learned.

Part V of the article “shows the work” for developing the Structured Questions for the PORT-IA. The Structured Questions evolved considerably during research on the case studies, and the current version of the Structured Questions has been validated by being tested against case studies across diverse sectors, data type, and geography.

The intent of the article is to create a coherent intellectual framework for assessing proposed PORTability initiatives. The PORT-IA, with its Structured Questions, can assist policymakers in deciding whether and how to mandate
PORTability. The PORT-IA can similarly assist companies in deciding whether and how to implement new PORTability features in their products and services. More broadly, the article shows the importance of multidisciplinary assessment of proposals for portability and other required transfers.

TABLE OF CONTENTS

Introduction .................................................................................................................. 60

I. Terminology: Defining PORTability ................................................................. 66

II. The New Importance of Data PORTability ................................................... 67

A. Digital Platforms and PORTability .............................................................. 68

B. PORTability and U.S. Antitrust Law ............................................................. 71

1. Why Digital Platforms Can Raise Antitrust Concerns ...................... 72

2. Why Data PORTability May Address These Antitrust Concerns 73

C. PORTability in Proposed and Enacted U.S. Privacy Laws, and Important Sectoral Requirements ................................................................. 76

1. Newly Enacted California Requirements and Other State Legislation......................................................................................................................... 76

2. Proposed Federal Legislation ...................................................................... 78

3. Sectoral PORTability Requirements .......................................................... 80

4. Summary on U.S. PORTability Requirements ........................................... 81

D. PORTability in EU Data Protection Law and Important Sectors .... 81

1. The GDPR Right to Data Portability .......................................................... 82

2. The Free Flow of Data Regulation ............................................................ 84

3. EU Sectoral PORTability Initiatives ............................................................. 85

4. Summary on EU PORTability Initiatives ....................................................... 86

E. PORTability and EU Competition Law .......................................................... 86

1. Article 102 Dominant Firm Analysis ............................................................ 87

2. The Possibility of Ex Ante Regulation of PORTability ..................... 89

III. The PORT-IA and Structured Questions ....................................................... 91

A. Overview of the PORT-IA ........................................................................... 91

B. Portability and Other Required Transfers Impact Assessments (PORT- IA): Structured Questions ................................................................. 93
INTRODUCTION

The goal of this article is to provide a framework for assessing issues of data portability and other required transfers of data. In the modern data economy, a crucial legal and policy question is when should data move from A to B, or be prevented from moving from A to B? This article addresses an emerging and important topic where there are often compelling and competing rationales both for mandating and for prohibiting the movement of data. The topic is data portability and interoperability – when a government should require data to move.¹

¹ For a companion article written specifically for an antitrust audience, see Peter Swire & John Snyder, Using the Portability and Other Required Transfers Impact Assessment ("PORT-IA") in Antitrust Law, CPI ANTITRUST CHRON. (Nov. 2020), https://peterswire.net/wp-content/uploads/CPI-Swire-Snyder.pdf.
Data portability presents both pros and cons. Often discussed in connection with the largest digital platforms, greater portability and other required transfers of data can have pro-competitive effects – if more companies can have access to commercially valuable data, then there can be less monopoly power and more innovation. On the other hand, making portability too easy can lead to serious privacy and cybersecurity effects, when the “wrong” people gain access to personal data. Thus, there is a tension between opening data flows, to promote competition and innovation, provide user control, and for other reasons, and closing data flows, for reasons including protecting privacy and cybersecurity.

Data portability is emerging as a crucial issue due to the confluence of at least three major trends: (1) the individual right to data portability (“RtDP”) that took effect in the European Union (“EU”) in 2018 and in California in 2020; (2) the current, intense policy debates about whether and how to regulate the largest digital platforms; and (3) beyond digital platforms, multiple sectors of the economy increasingly have data portability requirements.

First, under Article 20 of the General Data Protection Directive (“GDPR”), an individual RtDP came into effect in the EU in 2018. In essence, the RtDP provides individuals with the right to move “their” data back to themselves, or to a designated recipient. A similar individual right came into effect in early 2020 under the California Consumer Privacy Act (“CCPA”), affecting all companies that conduct significant business in that large state. We are thus in the early days of actual implementation of the RtDP, so numerous practical issues are arising for the first time.

A second major trend is the intense policy debate about whether and how to regulate the largest digital platforms, sometimes grouped as “GAFAM” (Google, Apple, Facebook, Amazon, and Microsoft). As a matter of U.S. antitrust law (or “competition law” as it is called in the EU) these platforms have come under intense scrutiny. For example, in the summer of 2020, the CEOs of Google, Apple, Facebook, and Amazon testified at a U.S. House Judiciary Antitrust Subcommittee hearing on the market power of online

---


platforms. In the EU, major cases have already advanced against Facebook and Google, and the EU Commission (the executive body for the EU) is preparing legislative proposals designed to increase competition in markets affected by the platforms.

Concerning the digital platforms, the debates about privacy (or “data protection” as it is generally called in the EU) have been similarly prominent. Innumerable companies have adjusted their information technology systems and data flows to come into compliance with the GDPR and CCPA, respectively. Many of the largest platforms have signed consent decrees with the Federal Trade Commission (“FTC”), and Facebook paid a record $5 billion fine in 2019 to settle FTC charges that it violated its consent decree. In addition, further proposals for additional privacy laws, including those affecting data portability, are proliferating.

With such enormous interest in both the antitrust and privacy issues related to the digital platforms, this article explains how data portability is the precise issue where these two policy areas systematically come into potential or actual conflict. Based on research for this article, very often the antitrust and privacy discussions of data portability occur separately. This article thus seeks to explain to privacy experts and others not focused on antitrust law the reasons that antitrust law often appears to push so strongly in favor of data portability. The article also seeks to explain to antitrust experts and others not focused on privacy and cybersecurity the reasons that the latter often appear to push so strongly against many possible forms of data portability.

The third major trend goes beyond digital platforms to multiple, important sectors of the economy that increasingly have data portability requirements. Public debates have often highlighted the early example of phone number portability – the longstanding legal requirement, in both the U.S. and EU, that a telephone carrier enables a consumer to shift the

---


consumer’s phone number to a different carrier. As discussed below, phone number portability has important features that create a stronger rationale for portability compared with other settings. This article presents seven case studies of such sectoral requirements, listed with the year of implementation, where applicable:

1. U.S. and EU phone number portability (2003 implementation for U.S.);⁷
2. U.S. health care interoperability regulation (2020);⁸
3. EU portability requirements concerning health care data (ongoing);⁹
4. The EU Payment Services Directives, requiring transfers among financial services organizations (due to delays, not yet fully implemented);¹⁰
5. Similar issues in the U.S. financial services sector, implementing Section 1033 of the Dodd-Frank Act of 2010 (with a notice of proposed rulemaking in 2020);¹¹
6. Open Data requirements for government agencies, especially in the US (ongoing);¹²
7. A lesser-known set of recent laws in Arizona and other states mandating portability for the data of automobile dealers (2019).¹³

---

¹³ See, e.g., ARIZ. REV. STAT. § 28-4651 to 28-4655 (LexisNexis 2021); see Appendix 7.
The article also discusses the EU Free Flow of Data regulation, implemented in 2019, which applies to cloud and software service providers. In summary, recent years have seen an unprecedented number of sectoral requirements related to the mobility of data.

In short, these three trends highlight the intense and increasing interest in data portability – the entry into force of the RTDP in the EU and California, the current antitrust and privacy debates concerning digital platforms, and the less-recognized flowering of multiple sectoral portability initiatives. To address these issues, Part I of the article defines terminology in order to clarify the difference between “portability” and “other required transfers.” By “portability,” this article means transfers about a single person. What this article calls “other required transfers” are transfers about more than one person, and often transfer of an entire database. Together, the article thus seeks to provide greater understanding concerning when “Portability and Other Required Transfers,” or the acronym “PORTs,” are likely to have the greatest benefits.

Part II provides context for the current PORTability debates about: digital platforms; U.S. antitrust and EU competition law issues; and the U.S. privacy law and EU data protection law issues.

In order to enable a consistent and disciplined evaluation of PORT initiatives, Part III proposes a Portability and Other Required Transfers Impact Assessment, or PORT-IA. This approach is similar to Privacy Impact Assessments required by U.S. laws such as the E-Government Act of 2002 or Data Protection Impact Assessments required by GDPR. Based on the seven case studies and overall research for this article, the PORT-IA sets forth fourteen “Structured Questions,” with sub-parts. For example, Question 2 examines the possible competition benefits from a PORT initiative, with sub-questions for topics such as network effects and barriers to entry. On the cost side, Question 8, with sub-questions, examines possible privacy risks from the

---

16 Commission Regulation 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), 2016 O.J. (L 119/1) (see art. 35) [hereinafter GDPR].
17 Part III defines these terms, as well as other critical terms for the PORT-IA.
PORT initiative, for both identified and de-identified data, and for the rights of third persons -- those other than the person making the portability request.

Part IV provides brief descriptions of the seven case studies. The descriptions emphasize a clear understanding of the mandated data flows: where does the data originate; where does it go; what types of data are covered; and what precisely are the legal requirements. For each of the seven case studies, there is an appendix examining the mandated data flows, the benefits of the PORT initiative, the risks and costs of the PORT initiative; and lessons learned.

Part V of the article “shows the work” for developing the Structured Questions for the PORT-IA. The methodology for this project began with drafting Structured Questions and then testing the draft against the seven detailed case studies. The Structured Questions evolved considerably from the initial draft to this final form. Based on this testing, I gave greater emphasis to how each case study and the Structured Questions address issues of authentication, secure transmission of data, and establishing technical standards for sharing data. I added sections on “onward transfer” and “fair, reasonable, and non-discriminatory terms” for protecting privacy and cybersecurity. On the antitrust side, I clarified the importance of lock-in effects to PORT proposals, and distinguished them more clearly from network effects. As currently drafted, the text of the Questions effectively incorporate the lessons from the case studies and other research to date.

The intent of the article is to create a coherent intellectual framework for assessing proposed PORTability initiatives. The PORT-IA, with its Structured Questions, can assist policymakers in deciding whether and how to mandate PORTability. The PORT-IA can similarly assist companies in deciding whether and how to implement new PORTability features in their products and services. My own research experience has assisted with this effort. As a professor, I have taught antitrust law as well as my regular privacy and cybersecurity courses, and I have written extensively about EU as well as U.S. law. More specifically, my writing on the intersection of antitrust and privacy dates back to 2007 testimony to the Federal Trade Commission, and

---

18 I have continued to write extensively about EU law since the 1998 book, PETER SWIRE & ROBERT LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, E-COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE (Editor’s Name, edition number, 1998). Relevant publications are at https://www.peterswire.net [https://perma.cc/Z7F2-WK7D].

19 Peter Swire, Protecting Consumers: Privacy Matters in Antitrust Analysis, CTR. FOR AM. PROGRESS (Oct. 19, 2007),
in 2013 I published a lengthy law review article, with a co-author, on the right to data portability.\textsuperscript{20}

Looking ahead, thoughtful design and implementation of PORTability initiatives will draw upon many different types of expertise. PORTability teams will benefit from having expertise in often-disparate intellectual discourses, including but not limited to antitrust, privacy, and cybersecurity. Multiple disciplines may be relevant to a PORTability initiative, such as policymakers, lawyers, and economists, along with engineers and other technical experts who actually build the systems for transferring data. To ensure that individual users actually want the proposed services, it will be helpful to learn from those knowledgeable about marketing and human/computer interaction. Privacy and consumer protection advocates, as well as other civil society stakeholders, may alert those designing a PORTability initiative to important, otherwise overlooked issues. As PORTability laws and proposals multiply, it makes sense to create a structured process for assessing portability and other required transfers. This Article presents a systematic way for all of these experts to work together on PORTability issues, based on lessons from seven detailed case studies.

I. TERMINOLOGY: DEFINING PORTABILITY

To date, even as the topic of data portability has become more prominent, there has been no systematic method to resolve the tension between opening data flows, especially for competition reasons, and closing data flows, especially for privacy and security reasons.

Part of the difficulty lies in terminology. The term “portability” has become a technical legal term -- Article 20 of the EU General Data Protection Regulation ("GDPR") mandates that individuals have a right to data portability,\textsuperscript{21} with a somewhat similar portability requirement in the California Consumer Privacy Act.\textsuperscript{22} In light of these laws, this article reserves the term “portability” to a required transfer when one person wishes to transfer the data.


\textsuperscript{21} GDPR art. 20.

\textsuperscript{22} California Consumer Privacy Act of 2018, \textit{supra} note 3, § 1798.100(d).
There are also increasingly broad proposals for mandatory transfers at a larger scale, such as opening an entire database for transfer in order to promote competition. In Europe, such proposals are often called “data sharing,” which is a vague term that can apply in other contexts. In the United States, such actions are sometimes called “inter-operability,” such as under a recently finalized regulation from the Department of Health and Human Services (“HHS”).

To promote clarity, this article limits the term “inter-operability” to the technical ability of two or more systems to exchange information. The article uses the term “other required transfers” for those transfers that are required and transfer the data of more than one person. Taken together, the article addresses Portability and Other Required Transfers, with the handy acronym of “PORT.” To clarify, a “portability” requirement applies only to transfers by one person, while a “PORTability” requirement or “PORT” initiative applies both to individual transfers and also mandated transfers applying to the data of more than one person.

II. THE NEW IMPORTANCE OF DATA PORTABILITY

Part II explains, for audiences from different backgrounds such as antitrust and privacy, why data PORTability has a significant and rising importance for numerous aspects of the law, with a focus on the United States and the European Union. In an era where data is often called “the new oil,”

| Part II first highlights the role of data PORTability in current policy and legal debates about the largest digital platforms. Second, it examines U.S. antitrust |

---


law, explaining in terms accessible to non-antitrust experts why PORTability has appeared as a promising approach for antitrust regulators and academics. Third, it examines the multiple laws and proposed laws that have emerged recently in the U.S. related to PORTability, including the RtDP in the California Consumer Privacy Act (“CCPA”), which went into effect in 2020. Fourth, it similarly examines the multiple laws and proposed laws in the EU for PORTability, beginning with the RtDP in the GDPR, but extending (as with the U.S.) to a number of important sectoral initiatives. Fifth, Part II returns to antitrust concerns, showing distinct ways that EU competition law may go further than U.S. antitrust law to address PORTability concerns.

A. Digital Platforms and PORTability

Policy and legal deliberations about PORTability have often focused on the largest digital platforms - GAFAM. The legislative history of the EU’s GDPR mentions social networks, in particular, as a cause for including the RtDP into the GDPR.26 A sizable fraction of the current literature about


26 Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free
PORTability, reviewed for this article, focuses on GAFAM. Despite the fact that there has been considerable legislative and policy activity on PORTability outside of these major platforms, such as for the health care and financial services sectors, the bulk of government, academic, and popular attention has concerned the large platforms.27

Increasingly, the power held by the largest digital platforms has raised concerns among government leaders. For instance, in the U.S., David Cicilline, the chair of the House subcommittee on antitrust said: “‘Because these companies are so central to our modern life, their business practices and decisions have an outsized effect on our economy and our democracy. Any single action by any one of these companies can affect hundreds of millions of us in profound and lasting ways.’”28 In the EU, Commissioner for Competition Margrethe Verstager has also highlighted concerns about the platforms’ dominance: “‘We may still find ourselves dealing with digital platforms that have become so dominant that they’re effectively private regulators, with the power to set the rules for markets that depend on those platforms.’”29

As policymakers and others consider how to act concerning the digital platforms, data PORTability has become an increasingly prominent theme. In 2019, the Stigler Center of the University of Chicago produced a major report on digital platforms, which repeatedly highlighted the importance of data PORTability.30 For instance, the report stated: (1) “An example of a regulation

Movement of Such Data (General Data Protection Regulation), art. 18, at 26, COM (2012) 11 final (Jan. 25, 2012).
27 This is discussed in detail below.
that would enhance competition is data portability.”

(2) “If the competitive environment is improved by data portability and the elimination of exclusionary conduct, the chance of success will rise and consumers will benefit from increased competition.”

(3) “In general, to maintain or improve their competitive advantage, incumbents have strong incentives to limit openness or interoperability and to be averse to data-portability policies.”

Similarly, a 2019 report by NYU School of Law’s Engelberg Center on Innovation Law & Policy stated: “A robust data portability system might allow regulators to contain the power of large platforms without having to take the drastic step of breaking them up.”

European leaders and enforcers have extensively highlighted the importance of PORTability. Margrethe Vestager, the European Commissioner for Competition, said in 2019:

The prominent position of data in digital markets may make it difficult for new entrants to compete on the market without access to a significant pool of data... In some settings, we can expect the foreclosure effects from a refusal to grant access to data to be high, in particular if a high degree of market concentration translates into a high degree of data concentration, and if that data yields an important competitive advantage in serving neighbouring markets. In such a setting, the need to ensure the possibility of entry may argue in favour of mandating access to data.”

---

platforms---committee-report---stigler center.pdf?la=en&hash=2D23583FF8BCC560B7FEF7A81E1F95C1DDC5225E&hash=2D23583FF8BCC560B7FEF7A81E1F95C1DDC5225E [https://perma.cc/256F-3FC7].

31 Id.
32 Id. at 113.
33 Id. at 41.
Cecilio Madero Villarego, another senior competition official in the EU, said in late 2019: “Among other things, we will continue to make sure that digital incumbents don’t make it too difficult for consumers to switch to competitors or use them in parallel.”\(^\text{36}\) As discussed further below, the United Kingdom Competition and Market Authority released a lengthy final report in 2020 called “Unlocking Digital Competition,” which examined competitive alternatives to incumbent digital platforms and suggested multiple ways to mandate greater PORTability.

In short, data PORTability has become an increasingly salient theme in debates about a critical global challenge for policymakers -- the future of digital platforms -- under U.S. antitrust and privacy law as well as EU competition and data protection law. The purpose of the PORT-IA is to create a tool for systematically assessing the multiple effects of mandating, or prohibiting, required transfers of data for digital platforms, as well as assessing more general effects of PORTability initiatives.

B. PORTability and U.S. Antitrust Law

Both U.S. academic experts and government officials have recently highlighted data PORTability as a potential remedy for antitrust problems, especially concerning the largest digital platforms. This section explains why digital platforms can raise antitrust concerns. It then highlights the growing attention to PORTability issues in recent years, and explains why PORTability requirements can appear to be an attractive remedy for antitrust concerns regarding digital platforms and elsewhere.

As a very brief introduction to U.S. antitrust law, three provisions are most relevant to claims against large digital platforms. Section 1 of the Sherman Antitrust Act prohibits combinations in restraint of trade, such as when two companies agree to act in an anti-competitive manner.\(^\text{37}\) Section 2 prohibits monopolization, or attempts to monopolize.\(^\text{38}\) A large market share alone is not enough to violate Section 2; monopolization concerns “the willful acquisition or maintenance of that power as distinguished from growth or development as a consequence of a superior product, business acumen, or


\(^\text{38}\) Id. § 2.
historic accident.” The Clayton Antitrust Act prohibits other, more specific conduct. Notably, Section 7 prohibits mergers and acquisitions where the effect may substantially lessen competition.

1. Why Digital Platforms Can Raise Antitrust Concerns

The Stigler Committee on Digital Platforms summarized the antitrust concerns in this way: “In particular, the platforms with which this report is most concerned demonstrate extremely strong network effects, very strong economies of scale, remarkable economies of scope due to the role of data, marginal costs close to zero, drastically lower distribution costs than brick and mortar firms, and a global reach.”

For readers less familiar with antitrust, here are succinct definitions to give an initial sense of the antitrust concerns: First, “network effects” means that the benefits to users increase as the number of people using a service increases. For instance, a telephone or text service with one user is not useful, but it becomes more useful as more people also use the telephone or text service. Second, “economies of scale” means that the cost per unit goes down with quantity sold. “Marginal cost” is the cost of adding one additional user. For instance, suppose it costs $1 million to write software for an online service, and it costs almost the same to serve 1,000 or 1 million users (“close to zero” marginal costs). In this example, economies of scale exist, because the average cost for 1,000 users is about $1,000, but the average cost for 1 million users is only about $1.00. Third, “economies of scope” means that costs are lower on average as the provider supplies additional services. For instance, an online platform with large amounts of users’ data may find that average costs decline as it adds a second, tenth, or twentieth service to its front page. For the additional services, the platform already can personalize a new service based on an existing user profile – the cost of adding a tenth or twentieth service will be lower, on average, than the first few services, which provided enough data for the platform to generate a user profile that enables targeted advertising. Fourth, distribution costs are lower online than in the physical world (“brick and mortar firms”), because adding an extra 1,000 users costs little online but requires a costly lease to sell in a physical store.

41 Stigler Committee on Digital Platforms, supra note 30, at 37. These terms, such as network effects, are discussed in greater detail in Part V, when explaining how the case studies provide the basis for the Structured Questions in the PORT-IA.
It is important to understand that many of the antitrust concerns about digital platforms focus on the role of data – the information about individuals that the platform accumulates. In terms used by Shoshanna Zuboff, this information includes both the “first text” and “second text.” In her usage, the “first text” is the actual words, transactions, or other information that a user experiences. For example, “first text” includes search terms, the words in a social network post, the map locations for a driver, or the list of purchases on a platform. The “second text” includes what the platform can infer or derive from the first text. For example, the second text may include statistical assessments of a person’s likely demographic groups, political views, propensity to buy certain types of goods, and so on. This inferred and derived data can provide powerful economic advantages to the companies that hold the largest and most nuanced databases about individuals.

Taken together, the Stigler Committee list of antitrust concerns, which is similar to other analyses of antitrust risk, highlights the possibility that it may be difficult to compete with large, established digital platforms. The platforms that gain scale can get more data about users than new entrants, resulting in network effects, economies of scale, and economies of scope. For a new competitor to compete with the incumbent platform, substantial investments could be required of the new competitor; in antitrust terms, there can be “barriers to entry” into the market. Once users are accustomed to multiple services from the same platform, it could be difficult or costly for those users to switch to different services. This means users may get “locked in” to the platform where their search history, friends list, map destinations, video preferences, shopping history, or other services are already personalized. These services work more seamlessly for the user than starting over with a new company that lacks that personalized knowledge.

2. Why Data PORTability May Address These Antitrust Concerns

To the extent that these large, nuanced databases provide a competitive advantage, a logical antitrust remedy would be to level the playing field. In the terminology of this article, one remedy would be the right to data portability, making it easier for the individual to transfer her or his data to a competing service. Another remedy would be to mandate “other required transfers” – transfers of data concerning multiple individuals, to enable stronger competition by new entrants against the incumbent platform. The vivid title for one recent law review article by Przemyslaw Palka is “The

---

42 SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 186 (Editor Name, Edition Number, 2019).
World of Fifty (Interoperable) Facebooks.” In Palka’s view, Facebook “should be obliged by the law to allow potential competitors to become interoperable with its platform and to grant them access to its network.” As discussed further below, there would be serious privacy and cybersecurity objections to opening up each user’s social media activity to multiple other companies without user consent. Nonetheless, Palka’s title illustrates the fundamental antitrust intuition – PORTability can increase competitors’ access to personal data, providing new entrants the opportunity to compete more effectively with the incumbent platforms.

Along with antitrust academics’ calls for PORTability, U.S. antitrust officials have expressed interest in this approach. In a speech in early 2020, FTC Director of the Bureau of Competition Ian Conner noted that the agency may consider a wide-range of remedies for anticompetitive mergers, including imposing a data portability remedy to ensure that entrants have access to data or other inputs controlled by a merged firm. Connor stated:

[We] may require the merged firm to affirmatively engage in behaviors, or enter into agreements to license assets and provide other competitive resources to new entrants…. The breadth of additional relief that may be considered include obligations to provide inputs, distribution, access or other rights, data, or supply of products and services to one or more entrants on specified terms or a non-discriminatory basis for some period of time.

In furtherance of such an approach, the FTC held its first data portability workshop on September 22, 2020. The workshop addressed topics including potential benefits to consumers and competition of data portability, risks to consumer privacy and strategies for mitigating those risks, corporate impact of mandatory data sharing and access, potential effects on innovation, data security best practices during data transmission, and what party should bear [81x195]43 Przemyslaw Palka, The World of Fifty (Interoperable) Facebooks, 51 SETON HALL L. REV. (forthcoming 2021), https://ssrn.com/abstract=3539792 [https://perma.cc/24EG-DLYT].

44 Id.

45 In the version of Palka’s article accessed in August 2020, Palka provides no discussion of the risks to privacy and cybersecurity that his proposal creates. There also is no discussion of the lack of users’ consent to having their personal data transferred to other companies.

the burden for ensuring interoperability." As the workshop description stated: "Data portability may also promote competition by allowing new entrants to access data they otherwise would not have, enabling the growth of competing platforms and services."48

State antitrust enforcers also appear to be considering data portability obligations to address competition concerns. In a 2020 American Bar Association panel discussing big data and competition, Texas Attorney General Ken Paxton noted that while data portability is not "a cure-all" for antitrust concerns, it “certainly is something that would be very helpful to consumers, giving them more control over the massive amount of data that companies are collecting from them."49

Notably, in U.S. discussions of PORTability, the remedy of required transfers of data is especially attractive because it is less drastic than possible alternatives. The Engelberg Center report in 2019 stated: “A robust data portability system might allow regulators to contain the power of large platforms without having to take the drastic step of breaking them up.”50 According to that report:

This theory is especially attractive in the context of services that rely on network effects, such as social networks. Users have years of conversations, shared photos, and connections with others on existing platforms. Being forced to leave that information behind would create a significant disincentive to jump to a competing platform, no matter how much better it is. Data portability allows users to bring their history somewhere new, even if they leave or delete their data from another platform.51

---


48 FED. TRADE COMM’N, supra note 47.


50 Nicholas & Weinberg, supra note 34.

51 Id.
In summary on U.S. antitrust law, policymakers and academics have recently given considerable attention to mandatory transfers of data to encourage competition. The writings to date have not, however, provided theoretical structure or practical guidance about how the antitrust analysis should fit with other effects of such mandatory transfers, including the privacy and cybersecurity risks.52

C. PORTability in Proposed and Enacted U.S. Privacy Laws, and Important Sectoral Requirements

At the same time that data PORTability has attracted intense interest in U.S. antitrust law, new PORTability obligations are being enacted or proposed in multiple ways in U.S. privacy laws both at the state and federal level. California has implemented its RtDP in its new comprehensive privacy law known as California Consumer Privacy Act (“CCPA”), and numerous other states have recently enacted or considered similar measures. The strongest candidates for national privacy legislation contain RtDP as well. In addition, there are newly enacted PORTability requirements in the health care and automobile industry sectors, joining long established requirements for telephone numbers and financial services. Taken together, these laws and proposals demonstrate considerably greater interest in PORTability than most have realized.

1. Newly Enacted California Requirements and Other State Legislation

In 2020, the CCPA applied the RtDP - for the first time - to numerous U.S. businesses doing business in California.53 Other states have recently enacted or considered similar laws.

52 One document that has addressed this set of issues is an OECD study released in 2021, which cites the 2020 version of this article and is broadly consistent with the analysis here. ORG. FOR ECON. COOPERATION AND DEV., DATA PORTABILITY, INTEROPERABILITY AND DIGITAL PLATFORM COMPETITION: BACKGROUND NOTE (Jun. 9, 2021), https://www.oecd.org/daf/competition/data-portability-interoperability-and-digital-platform-competition-2021.pdf [https://perma.cc/7X2B-9MYX].

53 Cal. Civ. Code § 1798.140(c) (West 2021) defines a covered business as a for-profit organization or entity that: collects consumers’ personal information or has consumers’ personal information collected on its behalf; determines the purposes and means of processing consumers’ personal information; does business in the State of California; and satisfies one or more of the following thresholds: (1) has annual gross revenues over $25 million, (2) annually buys, receives, sells or shares for commercial purposes, either alone or in combination, the personal information of 50,000 or more consumers, households, or (3) derives 50% or more of its annual revenues from selling consumers’ personal information.
The CCPA, which went into effect in January, 2020, guarantees consumers the right to access their data and to have their data provided to them in a “portable” and “readily useable format.” In this sense, a consumer’s “right to access” has been merged with the RtDP. Because the CCPA merges the RtDP with the right to access, there is no requirement for consumers to make a specific “portability” request under the CCPA. Rather, when a consumer requests access to the personal information that a business has collected, the business must produce the information in a “portable” format.

The CCPA is part of a flurry of other state-level proposed privacy legislation, often including the RtDP. In 2020 bills were introduced in at least Illinois, Maryland, Massachusetts, and New Hampshire with language identical to the CCPA, including its merger of the rights to access and portability, requiring that data provided to a consumer electronically “be in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance.” In 2021, both Colorado and Virginia enacted privacy laws containing the same portability language. Multiple other states have

54 Id. § 1798.140.
55 Id. § 1798.100(d).
56 This is unlike the approach in the EU. Under the GDPR, access is protected under Article 15 and data portability under Article 20. See Section D for additional explanation of these concepts in the GDPR. GDPR, supra note 16.
57 The regulations proposed by the California Attorney General impose some limits on these rights. The regulations would not require businesses to search for or provide archived data that (a) is not maintained in searchable or readily accessible form, (b) is maintained “solely for legal or compliance purposes;” and (c) is not sold or used for commercial purposes, provided the business describes to the consumer the categories of records that it did not search, because it meets the foregoing enumerated requirements in sections (a) through (c) of CAL. CODE REGS. tit. 20 § 999.313(c)(3), https://govt.westlaw.com/calregs/Document/1A57ACCFF5944430C841DDD8253FA66C8?viewType=FullText&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=(sc.Default) [https://perma.cc/Q4SP-UABW].
considered RtDP legislative proposals. Bills were introduced with stand-alone data portability provisions in the states of Washington and Minnesota, and other states with recent RtDP legislative proposals include Arizona, Hawaii, New Jersey, New Mexico, New York, Rhode Island, Texas, Virginia, and Wisconsin.

2. Proposed Federal Legislation

At the national level, PORTability has been the focus of one specific bipartisan proposal, and the RtDP has also become a standard feature of proposed comprehensive privacy laws. If a comprehensive federal privacy law does pass, it seems likely to include the RtDP.

The RtDP and interoperability are the primary focus of a proposed national law, the Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act introduced in 2019 by Democratic Senators Mark Warner of Virginia and Richard Blumenthal of Connecticut, and Republican Senator Josh Hawley of Missouri, and reintroduced in 2021 by

---


Democratic Representative Mary Gay Scanion. The bill applies to the largest online “covered platforms,” generally those with over 50 million users and a market capitalization of over $600 billion. The 2021 ACCESS Act would specifically impose a duty on large communications platform providers to “maintain transparent, third-party accessible interfaces” that would “enable the secure transfer of data to a user, or…to a business user”, including any competing business users, “at the direction of a user, in a structured, commonly used, and machine-readable format.”

Along with the stand-alone proposal in the ACCESS Act, the RtDP has become an increasingly standard feature in the proliferating number of Congressional proposals for comprehensive commercial privacy legislation. Cam Kerry has identified the bills introduced in the Senate Commerce Committee that “frame the issues for this discussion going into the next session of Congress.” Although the bills differ in other respects, such as federal preemption and a private right of action, the RtDP is included in the bills introduced in 2020 by both the Committee’s senior Republican, Senator Roger Wicker, and by the Committee’s senior Democrat, Senator Maria Cantwell. Bipartisan consensus on the RtDP is further indicated in other proposals by Democratic and Republican lawmakers.

65 ACCESS Act of 2021 § 5(6).
66 Id. at § 3.
68 U.S. Consumer Data Privacy Act of 2019, § 103.
3. Sectoral PORTability Requirements

Discussions about these U.S. state and federal legislative proposals have contained surprisingly little discussion of important U.S. sectoral PORTability initiatives. This article examines the following initiatives: (i) phone number portability; (ii) consumer financial services; (iii) automobile dealer software; and (iv) the health care system. Another case study examines analogous PORTability requirements in government Open Data initiatives.

The discussion below explains these mandates in greater detail, highlights the benefits and risks associated with each initiative, and reviews lessons learned. The principal point is to highlight the variety of ways that U.S. law is already creating PORT requirements. Two of these requirements have been in place for at least a decade, while the other two sectors recently enacted the requirements, as part of the broader interest in the topic.

Phone number portability - The most familiar of the existing requirements concerns phone number portability. For nearly twenty years, phone number portability has enabled consumers and businesses to transfer their phone number from one service to another (e.g. from Verizon to ATT or other services).\(^\text{72}\)

Consumer financial services - This sort of consumer mandate exists as well under Section 1033 of Dodd-Frank Act of 2010.\(^\text{73}\) That law includes a requirement that consumers be able to access their financial services records. It also specifies that the records, “shall be made available in an electronic form usable by consumers,” thereby enabling portability of those consumer records. In 2020, the Consumer Financial Protection Board issued an advance notice of proposed rulemaking, to further implement Section 1033.\(^\text{74}\)

Auto dealership software - In contrast to these consumer-focused requirements, Arizona and at least three other states in 2019 enacted protections for automobile dealers, enabling them transfer dealer-related data from one Dealer Management System (“DMS”) to another.\(^\text{75}\) The statute

\(^{72}\) See Appendix 4.
\(^{73}\) See Appendix 1.
\(^{74}\) Id.
specifically prohibits “cyber ransom,” defined as “encrypting, restricting or prohibiting or threatening or attempting to encrypt, restrict or prohibit a Dealer’s or a Dealer’s Authorized Integrator’s Access to Protected Dealer Data for monetary gain.”76 In other words, DMS providers must permit Protected Dealer Data to be ported to an Authorized Integrator or other party upon direction of the Dealer.

Health care databases – HHS issued a final regulation in March, 2020, which contains PORTability rights for individuals, similar to phone number portability and financial services.77 For instance, a company subject to the regulation cannot engage in “information blocking,” if individuals wish to transfer their health records to an app or other destination. The regulation also contains PORTability rights for companies, similar to the automobile dealer laws. Companies that use certified health information technology services gain new rights to PORT data to a different software provider, such as to avoid being locked-in to their current software system.

4. Summary on U.S. PORTability Requirements

The discussion here documents the sharp increase in PORTability proposals and enactments since California enacted the CCPA in 2018, containing the RtDP. Since that enactment, the RtDP has become an increasingly pervasive feature of privacy reform efforts at the state and federal level. Individuals have similarly received a RtDP for their health records under the 2020 regulation. Meanwhile, several states have enacted database-level PORTability for automobile dealers, and the Consumer Financial Protection Board is considering a regulation for the financial services sector. Taken together with the earlier RtDP rules for phone numbers, we are in an unprecedented period for considering PORTability requirements. This article, with its proposed PORT-IA, seeks to provide a rigorous analytical structure for assessing such PORTability requirements.

D. PORTability in EU Data Protection Law and Important Sectors

There are important similarities in the ways that the U.S. and EU have recently approached PORTability issues. With the implementation in California of portability requirements, many U.S. firms are required to provide individual portability that is broadly similar to the RtDP in the GDPR. On a

76 See Appendix 7.
77 See Appendix 2.
database level, the EU Free Flow of Data Regulation ("FFD Regulation") went into effect in 2019, with an approach similar to how the U.S. is requiring PORTability to enable companies in health care and the auto industry to switch to different cloud or software providers. The EU has also created a number of sectoral PORTability initiatives, including for health care and financial services, allowing this article’s direct EU/U.S. comparison in case studies about these sectors.

1. The GDPR Right to Data Portability

The EU Commission proposed the General Data Protection Regulation in 2012. As a co-author and I discussed in our 2013 law review article, to that point “no jurisdiction ha[d] experimented with anything resembling” the proposed RtDP. The GDPR entered into effect in 2018, with Article 20 defining individuals’ rights to transfer their personal data to themselves or to other services. Article 20 provides individuals, subject to certain conditions, “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.” Where technically feasible, the individual has “the right to have the personal data transmitted directly from one controller to another,” such as from one online service to another. Article 20 also states that the right “shall not adversely affect the rights and freedoms of others.” As discussed below, that provision is especially important in connection with social networks, because so much of the relevant data is about other people.

Because so much of this article discusses the direct and indirect effects of the EU enacting the RtDP, I highlight five points here. First, as I wrote in 2013, the GDPR’s RtDP was without precedent as a legal mandate. Actual experience with implementing the right began only in May 2018, when the GDPR went into effect. The European Data Protection Board has issued non-

---

80 GDPR, art. 20(1).
81 Id. at art. 20(2).
82 Id. at art. 20(4).
83 Swire & Lagos, supra note 79.
binding guidance on Article 20, but that guidance does not provide detailed analysis of how to meet possibly conflicting goals such as competition, privacy, and cybersecurity. Second, as mentioned in the introduction, the word “portability” has become a term of art for European lawyers, focused on implementing the requirements of Article 20 into practice. This article thus limits the term “portability” to transfers of an individual’s data. Third, some EU scholars have highlighted how portability exists at the intersection of data protection, competition, and consumer protection law. Different EU regulators typically enforce in these distinct areas of law, so there are intricate institutional questions about which actors are charged with enforcement, and the possibility exists that no one enforcement agency has legal competence to assess how best to meet the goals of data protection, competition, and consumer protection law. Fourth, EU scholars have also explained that the RtDP is designed to foster individual autonomy, i.e., individuals’ control over their own data. The RtDP applies not only to large platforms but also to small and medium enterprises, demonstrating that the right goes beyond prevention of monopoly market power. Fifth, possible amendment to the RtDP is under consideration. The EU issued a proposed Data Strategy in early 2020. As part of that strategy, the EU has put forward a proposed Data Act that could

84 GDPR, Art. 20; Guidelines on the Right to Data Portability Under Regulation 2016/679, WP242 rev.01, p. 3-4, [hereinafter WP242].


86 The EU separation of legal domains is different than in the U.S., where the FTC is a consumer protection agency, which brings enforcement actions to address privacy, cybersecurity, and antitrust concerns. See Inge Graef, supra note 85.; Graef et al., Data Portability and Data Control: Lessons for an Emerging Concept in EU Law, 19 GER. L.J. 1359 (2018); Orla Lynsky, Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability, 42 EUR. L. REV. (2017).

87 Graef et al., Data Portability and Data Control: Lessons for an Emerging Concept in EU Law, 19 GERMAN L.J. 1359 (2018) (“The RtDP of the GDPR is a first attempt to establish a general-purpose control mechanism of horizontal application that will mainly facilitate the sharing and reuse of data.”); Maria Tzanou, Data Protection as a Fundamental Right Next to Privacy? “Reconstructing” a Not So New Right, (2013) 3 INT’L. DATA PRIV. L. 88, 90 (“Data protection is not simply about informational privacy; it is about informational autonomy.”).

include, among other things, new rules to broaden the RtDP. According to the Data Act Inception Impact Assessment published by the EU, the Data Act aims to improve technical standards for portability, including for sectors such as smart home appliances, wearables, and home assistants.\textsuperscript{89} The EU’s proposal for a Digital Markets Act (which targets large online platforms designated as ‘gatekeepers’) would expand portability to require gatekeepers to include continuous and real-time access.\textsuperscript{90} Implementation of a PORT-IA, as proposed by this article, could be useful as the EU seeks to meet the multiple goals put forward in its Data Strategy.

2. The Free Flow of Data Regulation

The Article 20 RtDP applies to “personal data,” the EU data protection term that roughly corresponds to “personally identifiable information” in U.S. usage. In 2018, the EU issued the FFD Regulation, applying to non-personal data. One goal of the FFD Regulation was to enable easier porting of data of a company’s data from one service provider to another.\textsuperscript{91} By reducing legal, contractual, and technical obstacles to porting, the FFD Regulation sought to address vendor lock-in issues, including for cloud services.\textsuperscript{92} This concern about vendor lock-in is similarly a prominent theme for justifying the U.S. health care and automobile dealer PORTability requirements.

\textsuperscript{89} DATA ACT & AMENDED RULES ON THE LEGAL PROTECTION OF DATABASES, EUR. COMM’N (2020), https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-&-amended-rules-on-the-legal-protection-of-databases_en [https://perma.cc/95GX-Q4VU]. The approach reflects a recent report which supports shifting the RtDP from merely a one-time request (the personal data held about an individual at a moment in time) to the option of a continuous request (the individuals can submit standing requests to transfer data to themselves or a different service). Jan Krämer et al., Making Data Portability More Effective for the Digital Economy: Economic Implications and Regulatory Challenges, CTR. ON REGUL. IN EUR. (June 2020), https://www.cerre.eu/publications/report-making-data-portability-more-effective-digital-economy [https://perma.cc/RPW9-J7VE].


\textsuperscript{91} Recital 5 FFD Regulation (emphasis added); Recital 29 FFD Regulation (“The ability to port data without hindrance is a key factor in facilitating user choice and effective competition on markets for data processing services. The real or perceived difficulties in porting data cross-border also undermine the confidence of professional users when taking up cross-border offers, and thereby their confidence in the internal market. Whereas individual consumers benefit from existing Union law, the ability to switch between service providers is not facilitated for those users who act in the course of their business or professional activities.”).

\textsuperscript{92} Recital 6 FFD Regulation.
The FFD Regulation specifically addresses the lack of technical interoperability among service providers. Article 6 of the FFD Regulation requires the Commission to “encourage and facilitate the development of self-regulatory codes of conduct” to cover key aspects of porting non-personal data, such as: (i) the processes used for, and the location of, data back-ups; (ii) the available data formats and supports; (iii) the required IT configuration and minimum network bandwidth; (iv) the time required to complete the porting process; and (v) the guarantees for accessing data in the case of the bankruptcy of the service provider. Standards were issued in November, 2019 for Infrastructure as a Service (“IaaS”) and Software as a Service (“SaaS”).

3. EU Sectoral PORTability Initiatives

The RtDP and FFD Regulation are cross-sectoral, in the sense that individuals have the right to port data from services in any sector, and the FFD Regulation provides businesses from any sector the ability to switch to a different service provider. The EU has also promulgated important sectoral initiatives. The case studies, below, provide detailed information on EU PORTability initiatives for the substantial sectors of health care and financial services. The case studies more briefly compare the EU and U.S. experience with telephone number portability and government Open Data initiatives.

In addition, the EU has had sectoral initiatives in the automobile, energy, and digital content areas, further highlighting the variety of PORTability requirements as well as the growing number of sectors with these requirements. In the automobile sector, there has been tension between the interests of car manufacturers and providers of third-party aftersales services as regards data access. The latter have wished to access in-vehicle data in order to provide services. Car manufacturers had resisted such access, however, citing security and safety risks. Since 2007, an EU Regulation has required manufacturers to provide standardized access for vehicle repair and maintenance information to independent operators. Recently, two additional

---

93 Recital 31 FFD Regulation.
sectors added PORTability initiatives. In the energy sector, Member States must specify rules on access to customer data by eligible parties, such as data required for customer switching.  

Under the Digital Content Directive, consumers have a right, in the event of termination of the contract for the supply of digital content or a digital service, to retrieve content other than personal data which was provided or created by the consumer when using digital content or digital service.

4. Summary on EU PORTability Initiatives

The multiple EU and U.S. PORTability initiatives together provide a more extensive basis for comparison and analysis than previous scholarship has recognized. Along with these initiatives, other jurisdictions have been promulgating new PORTability requirements, including Australia and Singapore. Available time and limits of the author’s expertise are reasons why this article focuses on the EU and U.S. In addition, there have been enough PORTability examples in the EU and U.S. to provide a diverse sample of sectors and legal approaches, in order to develop and then stress test the Structured Questions of the PORT-IA.

E. PORTability and EU Competition Law

The discussion above of U.S. antitrust law highlighted the Stigler Committee’s competitive concerns regarding digital platforms, such as network effects, economies of scale, economies of scope, marginal costs close to zero, and global reach. These same concerns have been highlighted in Europe, as shown in Calvano and Polo’s helpful survey of the economic literature on market power, competition, and innovation in digital markets.

---

100 See Stigler, supra note 30.
The discussion here adds two topics that are not as prominent in U.S. discussions – the EU law concerning “dominant” firms, and the discussion of promulgating regulations for digital platforms to mandate PORTability in advance, rather than treating PORTability primarily as a possible remedy after an antitrust violation is shown.

1. Article 102 Dominant Firm Analysis

There are important similarities between U.S. antitrust law and EU competition law. For instance, Article 101 of the Treaty on the Functioning of the European Union (“TFEU”) prohibits agreements that restrict competition, similar to the Sherman Act’s prohibitions on agreements in restraint of trade.102

With that said, EU competition law goes beyond U.S. antitrust law in one important respect, potentially relevant to large digital platforms. Article 102 of the TFEU prohibits abuse “of a dominant position.”103 As Spencer Waller has recently documented, U.S. antitrust law differs from other nations because it lacks this prohibition on abuse of dominance, defined “as the ability to act independently from competition, consumers, or competitors.”104 Commissioner of Competition Vestager has stated: “dominant companies have a special responsibility not to misuse their power, to harm competition.” EU and member state cases have found a rebuttable presumption of dominance at a 50% market share.105 By contrast, market shares under current U.S. law would normally need to be significantly higher to trigger enforcement under Section 2 of the Sherman Antitrust Act.106

EU regulators have expressed concern about the possibility of a dominant firm extending market power into adjacent markets. In 2019, Cecilio Madero Villarejo, Acting Director-General for Competition said: “Because often in digital cases, we see there are smaller specialized companies or

103 Id.
106 Waller, supra note 104, at 5.
startups in adjacent markets that the dominant company is trying to monopolize. So our aim is to make sure that such companies can innovate and grow for the benefit of consumers. We need to preserve the opportunity for smaller rivals to break into the market by offering something different.”

A related concern is the possibility of the firm abusing its dominant position to advantage its own products and services. Villarejo has called “self-preferencing” a “recurring concern regarding big tech platforms.” Such concerns were a basis for the EU’s case concerning Google Search, based on claims of Google advantaging its own services in search results. Vestager has stated that the EU has investigated whether Amazon “has used its control of a platform to benefit its own services.” She said: “Millions of sellers use Amazon to connect with their customers. But Amazon also sells on the platform – competing with those sellers. And we’re investigating whether the company used data which it collected, as the operator of the platform, to deny other sellers a chance to compete on equal terms.” She added: “And this sort of thing can happen any time that a platform is both player and referee in this way.” The European Commission has since informed Amazon of its preliminary view that Amazon has breached EU antitrust rules by unfairly relying on non-public business data of independent sellers.

108 Id.
110 Id.
111 Id.
These concerns about dominant platforms reinforce the importance of data portability. Vestager states that large digital companies are often “active in a whole range of different areas,” and “it can be difficult for consumers to switch from one ecosystem to another.”\textsuperscript{113} Therefore, “there may be times when we also need to look at the way that these ecosystems can leave consumers locked in.”\textsuperscript{114} One response to “locked in” data is to find ways to unlock it, by porting the data to a different company. More broadly, failure of a dominant firm to act appropriately concerning data PORTability could be seen as an abuse of dominance and thus violative of Article 102.

2. The Possibility of Ex Ante Regulation of PORTability

In the U.S., much of the antitrust discussion has focused on data PORTability only after an antitrust violation is shown. By contrast, more of the discussion in the EU has been about the possibility of ex ante regulation – regulation before showing a violation, without the prior requirement of proving violation of the law.\textsuperscript{115}

For possible regulation, the most detailed discussion comes from the U.K. Competition and Markets Authority. In 2019, it published a report on “Unlocking Digital Competition,” led by U.S. economist Jason Furman.\textsuperscript{116} The CMA published an interim market study in 2019 on “Online platforms and digital advertising,”\textsuperscript{117} with its final report in July, 2020.\textsuperscript{118} All three of these documents stressed the importance of regulating to promote PORTability, in somewhat different ways. The Furman-led report emphasized the importance of new regulatory tools, stating on its first page: “The biggest gains, however, will come from going beyond these tools to focus on policies that actively promote competition, foster entry by new competitors, and

\textsuperscript{113} See Waller, supra note 104.
\textsuperscript{114} Id.
\textsuperscript{115} Some of the sectoral PORTability initiatives in the U.S. also constitute ex ante regulation. For instance, the automobile case study shows that there is ongoing antitrust litigation about the actions of the Dealer Management Services, seeking ex post remedies. In addition, the legislation in Arizona and other states are examples of ex ante regulation – the laws take effect without a judicial finding of antitrust violation.
\textsuperscript{118} Id.
benefit consumers. This will entail a code of conduct for the most significant digital platforms, measures to promote data mobility and systems with open standards, and expanding data openness.” 119 The interim market study concluded that there is “a strong argument for the development of an ex ante regulatory regime to govern the activities of large online platforms funded by digital advertising.” 120 The interim market study also included detailed appendices examining possible business structures that would PORT substantial flows of data from the largest platforms to other companies, in order to foster competition in online advertising and social media.121

The final market study also supported ex ante regulation, stating: “There is a compelling case for the development of a pro-competition ex ante regulatory regime, to oversee the activities of online platforms funded by digital advertising.” It proposes creation of a Digital Markets Unit, with powers to mandate both individual data portability and other required transfers:

- Increasing consumer control over data, which includes providing choices over the use of data and facilitating consumer-led data mobility;
- Mandating interoperability to overcome network effects and coordination failures;
- Mandating third-party access to data where data is valuable in overcoming barriers to entry and expansion and privacy concerns can be effectively managed; and
- Mandating data separation / data silos, in particular where the data has been collected by the platforms through the leveraging of market power.

In summary on EU competition law and PORTability, the economic analysis of risks to competition overlaps considerably with U.S. antitrust analysis. The EU notably goes beyond the U.S. approach in two respects. First, Article 102 TFEU provides a jurisprudence about abusive actions by a dominant firm, and failure to provide PORTability, depending on the facts, might be considered such an abuse. Second, the CMA reports show considerably greater attention to the possibility of ex ante regulation in order to foster data mobility, especially for digital platforms, whereas in the U.S. the discussion to date has been more focused on PORTability as an ex post remedy, after a showing of antitrust violation.

119 Furman, supra note 116 (emphasis added).
120 Interim Market Study, supra note 117, at 273.
121 Id. at Appendix K, L.
III. THE PORT-IA AND STRUCTURED QUESTIONS

Part II, above, documents the large and growing interest in PORT initiatives. Part III first gives a brief descriptive overview of the elements of the PORT-IA. It then sets forth the full proposed text for Structured Questions to implement such an impact assessment. The current version of the Structured Questions is based on lessons learned in applying a draft version of the Structured Questions to the seven case studies.

A. Overview of the PORT-IA

The PORT-IA begins with a description of the proposed data flows – the origination, the destination, what data is covered, and what is the applicable law or other requirement. As I tell my students in the first day of class, clear mapping of data flows is often essential for analyzing privacy and security risks. When the topic is portability - transfers of data – no accurate analysis can succeed without a data map and understanding of the law or other constraints that may affect the data transfer.

The PORT-IA next examines the benefits of the proposed PORT from multiple perspectives. For example, there are distinct theories of harm to competition, any of which might be addressed by a PORT initiative. These include: lock-in effects, when it is costly to switch to an alternative provider; network effects, where the benefits to users increase with the size of the service; dominant firm actions, where market leaders may create anti-competitive effects; and increased barriers to entry. There are also non-competition rationales for a PORT, including: user control/autonomy and other non-commercial benefits; innovation and other commercial benefits; and regulatory or other legal benefits of the initiatives. The benefits discussion also assesses whether the benefits contemplated by proponents of a PORT initiative can be achieved in practice; the PORT-IA examines technical or market obstacles to adoption, so that the ”gross” benefits (the benefits anticipated by proponents) are reduced to the “net” benefits (a realistic assessment of what is actually achievable).

The PORT-IA provides the equivalent analysis of likely costs and potential risks from the PORT initiative. Privacy risks can exist for the data subject (the person seeking portability), or third persons, such as when the data

---

subject seeks to transfer a photograph or other personal data of another person. Privacy risks can also exist for data that is supposed to be de-identified or anonymized; in practice, greater transfers of data may increase the risk that a person can be re-identified. For cybersecurity, a pervasive concern is authentication, how to determine that the person seeking to transfer data is authorized, rather than a hacker or other unauthorized person. Once authentication exists, it is important to transfer the data securely to the recipient, often through an encrypted Application Programming Interface (API). There can also be risks once the data is transferred to the receiving party, particularly where the data subject has not consented to onward transfers to additional parties. In addition, there may be competition risks from a PORT initiative, such as where incumbents create standards or compliance costs that can act as barriers to entry, restricting competition. Finally, there can be regulatory or legal costs from a PORT initiative, such as if existing consumer protection laws no longer apply once the data is transferred.

The purpose of the Structured Questions is to facilitate a consistent and rigorous analysis of the usefulness of any particular PORT initiative; the methodology is agnostic about whether an initiative, on balance, has net benefits or costs. As stated in my previous writing, “data portability is an attractive concept – we as consumers would like to be able to move ‘our’ stuff from one system to another.”123 With that said, implementing portability can have substantial cybersecurity and other risks, and may actually reduce consumer welfare.124 The agnostic approach in evaluating possible initiatives is consistent with the breadth of the issues under consideration – facts will vary considerably about when is it beneficial either to support data flows or reject them.

As another point, the structured questions include an assessment of the financial and other incentives of those presenting evidence of risks and benefits of a PORT initiative. Just because a party has an economic interest to support or oppose an initiative does not mean the facts it cites are incorrect; however, the PORT-IA should assess the evidence in light of possible bias. Where available, the PORT-IA should use evidence based on sources that are as objective as possible.

The next part of the article presents the actual Structured Questions to use in an impact assessment.

123 Swire & Lagos, supra note 20, at 379.
124 Id. at 380.
B. Portability and Other Required Transfers Impact Assessments (PORT-IA): Structured Questions

1. Define the challenge or opportunity that leads to a data portability or other required transfer initiative
   a. Describe the origination, where the data comes from (who is subject to a PORT)
   b. Describe the destination, where the data goes to (who can trigger a PORT)
   c. Describe the data that is subject to the PORT
   d. Describe the applicable law that governs the proposed PORT policy, regulation, product, or practice

Data PORTability Benefits:

2. Assess PORT rationales based on competition
   a. Does the PORT reduce lock-in effect and facilitate switching to competing providers? (Note: a lock-in effect can exist even in a market that is otherwise competitive, such as a low HHI.)
   b. Does the PORT reduce network effects that might exist even after users have the right/capacity to transfer their data?
   c. Does the PORT reduce any effect on competition from abuse by a dominant firm? For instance, does the PORT reduce the ability of a dominant firm to impose anti-competitive contract provisions or deny access to an essential facility?
   d. Does the PORT reduce barriers to entry in ways that made it easier for competitors to gain necessary scale?
   e. Are there any other competition rationales for the PORT?
   f. Note: for any competition analysis, define the market(s) where relevant.

3. Assess innovation and other commercial benefits due to the PORT
   a. Apart from any pro-competitive effects on existing markets, what commercial innovation may result due to the PORT?
   b. Are there any other significant commercial benefits?

4. Assess non-commercial benefits due to the PORT
   a. Apart from competition and commercial effects, does the PORT provide benefits for user autonomy, user control over information, or other individual benefits?
b. Apart from competition and commercial effects, does the PORT provide any public benefits, such as research for the benefit of the public?

5. Assess regulatory or legal benefits of the initiative
   a. As a result of the PORT, would consumers receive any legal benefits, such as expanded coverage of consumer protection laws?
   b. Would any other actors receive any legal benefits, such as enforceability of contracts?

6. Assess any reduced benefits due to lack of technical or market feasibility
   a. Are there technical obstacles to realizing the hoped-for benefits of the PORT? For instance, the data may be of poor quality or available in an incompatible format.
   b. Are there market obstacles to realizing the hoped-for benefits of the PORT? For instance, the demand for data may not fit well with the available supply of data from the PORT.
   c. Note: reserve discussion of privacy, cybersecurity or other specific risks for discussion below of Data PORTability Risks and Costs.

7. Assess incentives for those presenting evidence of benefits
   a. What parties have an economic or other incentive to support the PORT? Explain the incentives. Assess the asserted benefits in light of the incentives of some actors to support the initiative. Just because a party has an economic interest to support or oppose an initiative does not mean the facts it cites are incorrect; however, assess the evidence supporting the initiative in light of possible bias. Where available, identify evidence based on sources that are as objective as possible.

Data PORTability Risks and Costs:

8. Assess privacy risks from the PORT (alternatively, use existing privacy or data protection impact assessment)
   a. Privacy concerns related to personal data (personally identifiable information) of the data subject
      i. What are the risks to the data subject’s own identifiable data? What steps (technical, administrative, etc.) can be taken to mitigate these risks?
ii. Other than costs of compliance itself, to what extent do the steps taken to protect privacy impede the goals of the data portability initiative?

b. Privacy concerns related to personal data (PII) of third persons
   i. What are the risks from the PORT to third persons’ identifiable data (that is, data about persons other than the data subject whose data is PORTed)? What steps (technical, administrative, etc.) can be taken to mitigate these risks?
   ii. Other than costs of compliance itself, to what extent do the steps taken to protect privacy impede the goals of the data portability initiative?

c. Privacy concerns relating to de-identified data
   i. De-identified data is designed to be no longer linkable to a particular data subject. Some PORT initiatives contemplate sharing of de-identified data with other companies, for reasons including research and promotion of competition. The Federal Trade Commission test for proper handling of de-identified data is that there should be (1) reasonable technical controls, (2) no re-identification by the recipient; and (3) downstream controls on re-identification.
   ii. What are the risks from the PORT related to re-identification of data? What steps (technical, administrative, etc.) can be taken to mitigate these risks?
   iii. Other than costs of compliance itself, to what extent do the steps taken to protect the privacy of de-identified data impede the goals of the PORT initiative?

9. Assess security risks from portability
   a. Risks from unauthorized access
      i. What are the risks from a hacker or other unauthorized person taking advantage of the PORT?
         1. What authentication is appropriate to the risk?
         2. Besides authentication, are there any other steps (technical, administrative, etc.) that can be taken to mitigate these risks? To what extent are these steps consistent with the PORT’s possible requirements about “without hindrance”?
   b. Risks from insecure transmission of data. Once authentication is complete, what are the risks arising during transmission to the authorized recipient?
i. Is there effective encryption in transit, such as through a secure Application Programming Interface?

ii. Are there other security risks that can be better managed, arising from the method of transmission, such as the means for transferring credentials or other sensitive data?

c. Does the PORT reveal any information that assists hackers or other unauthorized access? For instance, are sources and methods of system security or surveillance compromised? Does the PORT make visible other data that was previously hidden or obscure, in ways that assist unauthorized access?

d. To what extent do the steps taken to prevent unauthorized access, such as stronger authentication requirements, impede the goals of the PORT initiative?

10. Assess risks from PORTability that may arise for either security and privacy

a. **Onward transfer: risks from access following authorized PORTing**
   
i. The concern is that once data is transferred from the controller to the recipient, there may be security or privacy risks arising after transfer to the recipient of the data.

   ii. To what extent is there notice about, and consent by, the data subject to explain privacy and security risks after transfer to the recipient? For instance, if the transfer is from a controller under stricter legal rules, to a recipient with less strict rules, is the data subject notified and does the data subject provide consent to any increased risk?

   iii. Would the goals of the PORT be met by transfer of pseudonymous or de-identified data? Are there other technical, administrative or other steps that can mitigate risk once data is transferred to the recipient?

   iv. To what extent are the goals of the PORT initiative impeded by steps taken to reduce risks from access following authorized porting?

b. Fair, reasonable, and non-discriminatory (FRAND) terms for security and privacy

   i. To what extent, if any, are security requirements different in their application to the controller initially holding the data than for the recipient of the PORT? Are
such differences justified on security grounds, or do they appear to unfairly discriminate against transfers to the recipient?

ii. To what extent, if any, are privacy requirements different in their application to the controller initially holding the data than for the recipient of the PORT? Are such differences justified on privacy grounds, or do they appear to unfairly discriminate against transfers to the recipient?

11. Assess risks to competition from the PORT
   a. Do the costs or burdens of compliance with the PORT’s requirements create a barrier to entry or competitive advantage for incumbents?
   b. Are there any competitive risks from established incumbents designing the standards for the PORT to favor incumbents? Are the PORT’s standards open and non-discriminatory?
   c. In practice does the PORT’s functionality discriminate in favor of affiliates of entrenched incumbents? For instance, is pricing data subject to the PORT, enabling incumbents to benefit from that pricing data? Have incumbents used porting to extend their dominance to related applications or properties?
   d. What steps can be taken to mitigate any such risks to competition?
   e. To what extent do such risks to competition impede the goals of the PORT initiative?

12. Assess regulatory or legal risks of the initiative
   a. As a result of the PORT, would consumers suffer any legal risks, such as reduced coverage of consumer protection laws?
   b. Would any other actors suffer any legal risks? Specifically, would the PORT affect the protection of trade secrets, copyright, or other intellectual property rights?

13. Assess any other significant costs or risks from portability, including obstacles to adoption
   a. Are there any other significant costs or risks from the PORT? For instance, one obstacle to adoption of a PORT can be the expense and time required to create standards for implementing the PORT.
   b. To what extent can such costs or risks be mitigated, such as by altering the design of the PORT initiative?
14. Assess incentives for those presenting evidence of risks
   a. What parties have an economic or other incentive to oppose the PORT? Explain the incentives. Assess the asserted risks in light of the incentives of some actors to oppose the initiative. Just because a party has an economic interest to support or oppose an initiative does not mean the facts it cites are incorrect; however, assess the evidence opposing the initiative in light of possible bias. Where available, identify evidence based on sources that are as objective as possible.

**Conclusion of PORT-IA:** Conduct a summary analysis of the benefits and risks of the PORT initiative, along with analysis of measures that might be taken to increase benefits or reduce risks.

**IV. SUMMARY OF THE CASE STUDIES**

Part IV provides a concise description of the data flows for each of the seven case studies, drawn from the seven appendices. Each case study begins with origination – where does the data come from. Next comes destination – where does the data go. It next defines the type of data subject to the PORT, and then sets forth the applicable law. Each full appendix also contains: benefits of the PORT; costs of the PORT; and lessons learned.

I emphasize two points about the case studies. First, phone number portability (the earliest implemented PORT initiatives) represents an uncharacteristically asymmetrical example of the potential benefits of PORT initiatives. To the extent observers or policymakers implicitly are relying on the phone number case study, they may have an unrealistically positive view about how easy and beneficial PORT initiatives will generally be. On the one side, phone number portability has significant pro-competitive benefits. Absent portability, individuals would be required to give up their cell phone numbers when switching to another carrier. The individual can suffer from “lock in” – losing the current cell phone number mean losing touch with friends and business contacts, with social and business costs. Incumbent providers thus may have the ability to gain monopoly profits from existing subscribers. On the cost side, there are low privacy risks with porting phone numbers – individuals actually want others to know the phone number so they can call them. In addition, there are manageable cybersecurity risks. Switching to a new cell carrier has often been done in person, in a way that involves effective authentication of the user. Overall, phone number portability thus has offered high benefits (consumer choice and avoiding lock-in) and low costs to
privacy and cybersecurity. My research shows that phone number portability is not representative of other PORT initiatives, which have a more complicated mix of costs and benefits.

The second point is that my examination of PORT initiatives intentionally omits detailed consideration of large online platforms. The ability to transfer data out of Facebook was a significant stated rationale for including the right to data portability in GDPR. However, focusing on PORT requirements for online platforms such as Facebook can actually stand in the way of dispassionate assessment of the benefits and costs of PORT initiatives. Some experts and actors already hold strong views about what PORT obligations to require of online platforms; in addition, focusing on Facebook or other major platforms is potentially confusing because there are so many different types of data that the platforms hold, with varying possible types of requirements. Attention to the seven current case studies thus may facilitate a more open-minded discussion of the strengths and weaknesses of various types of PORT initiatives.

A. U.S. Financial Services


2. Destination. Consumers and their financial technology ("fintech") providers, such as Mint and Quicken.

3. Types of Data. Along with other use cases, consumers can use the fintech software to consolidate their multiple accounts into one place, for budgeting or other personal financial purposes.

4. Applicable Law. Section 1033 of the Dodd Frank Act requires consumer access to financial information, in an electronic form usable by consumers. “Covered persons” are those “offering or providing a consumer financial product or service.” A covered person shall make to a consumer available information concerning the financial product or service. Such

---

information shall include “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. The Consumer Financial Protection Bureau (“CFPB”) has the authority to issue rules for “standardized formats for data,” and announced in 2020 an advance notice of proposed rulemaking to do so.

B. U.S. Health Care

1. Overview of Three PORT Initiatives in the Proposed and Final Rule Implementing the 21st Century Cures Act

1.1. There are at least three, somewhat overlapping, PORT initiatives in the Proposed and Final Rule implementing the 21st Century Cures Act (“the Act”). The three initiatives, each of which are described below, relate to: Prohibitions on Information Blocking (Port Initiative A); Health IT Developer Certification Requirements (Port Initiative B); and Standardization of APIs (Port Initiative C).

1.2. The Proposed Rule for “Interoperability, Information Blocking, and the ONC Health IT Certification Program” was published on March 4, 2019, by the Office of the National Coordinator for Health Information Technology (“ONC”) of the U.S. Department of Health and Human Services (“HHS”). ONC’s stated purposes in implementing the Act are to: increase innovation and competition; reduce burden and advance interoperability; and promote patient access. The Final Rule was published on March 9, 2020, with regulatory text and accompanying material of over 1200 pages.

1.3. Note - the term “interoperability” is used in the Proposed Rule and the Final Rule to apply broadly, to: (1) technical interoperability (as I use...
the term generally in this article); (2) portability, or transfers involving one person; and (3) other required transfers, such as when a health care provider transfers all of its records from one information technology (“IT”) vendor to another.

2. PORT Initiative A: Information Blocking

2.1. Origination: Any (1) health care provider; (2) health IT developers of certified health IT; (3) health information exchanges; or (4) health information network.

2.2. Destination: An authorized recipient where there is patient consent, or for treatment, payment, or operations of an entity covered by the Health Information Portability and Accountability Act (“HIPAA”).

2.3. Types of Data: The scope of covered data is broad, covering “electronic health information” (“EHI”), which corresponds to the electronic Personal Health Information (“PHI”) covered by HIPAA.

2.4. Legal requirements. The Act prohibits “information blocking” as defined in section 171.103 of the Final Rule, subject to eight exceptions. Information blocking is any activity that “is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information.” ONC can impose significant penalties for information blocking, unless one of the exceptions applies. The eight exceptions are divided into two categories. The first category includes exceptions that allow for not fulfilling requests to access, exchange or use of EHI, including for (1) preventing harm; (2) promoting the privacy of EHI; (3) promoting the security of EHI; (4) responding to requests that are infeasible; and (5) maintaining and improving health IT performance. The second category of exceptions includes those that involve establishing procedures for fulfilling requests to access, exchange or use of EHI, including for: (6) recovering costs reasonably incurred; (7) licensing of interoperability elements on reasonable and non-discriminatory terms; and (8) limiting the content of responses to requests and establishing the manner for fulfilling requests.


135 21st Century Cures Act, supra note 8, at 1149 (“Electronic health information (EHI) is defined as it is in § 171.102.”).

136 Id. at § 171.103.

137 Id. at §§ 170, 170.200–05.

138 Id. at §§ 171.300–171.303.
3. PORT Initiative B: Health IT Developer Certification Requirements


3.2. Destination: (1) For an individual patient, to the patient or a third party chosen by the patient (portability for the individual patient); and (2) For all patients of a provider when the provider seeks to change health IT systems (transfer of data by the health provider from one IT provider to another).

3.3. Types of Data: Electronic health information. The export file must be computable and include documentation to allow for interpretation and use of EHI.

3.4. Legal requirements: Section 4002 of the Act requires HHS to establish “Conditions and Maintenance of Certifications Requirements for the ONC Health IT Certification Program.” ONC enforces any noncompliance. There are seven Conditions of Certification for health IT developers. Most relevant for purposes of this case study are: (1) information blocking (discussed above) and (2) Application Programming Interfaces (“APIs”), discussed below. Among the other requirements that apply to health IT developers is that the developer does not prohibit or restrict communications for specific subjects including: usability; interoperability; security; user experiences; business practices; and the manner in which a user of health IT has used such technology.139

4. PORT Initiative C: Standardized API

4.1. Origination: A health IT developer must “publish APIs and must allow health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs.”140 For instance, the API would enable export of the patient’s data from a health care provider to a smartphone app.141

140 21st Century Cures Act, supra note 8, at §§ 170, 170.404(a).
4.2. Destination: (1) For a single patient, to the patient or a third party chosen by the patient (portability for the individual patient); (2) For all patients of a provider when a provider seeks to change health IT systems (transfer of data by the health provider from one IT provider to another).

4.3. Types of data: A developer must provide access in the API to all data elements of a patient’s Electronic Health Record (EHR), to the extent permitted by privacy law. The Final Rule defines the “United States Core Data for Interoperability,” which sets forth the extensive required data elements, including clinical notes.\footnote{21st Century Cures Act, supra note 8, at §§ 170, 170.404(a).}

4.4. Legal requirements: The Rule sets forth detailed requirements, including that: (1) the API be usable “without special effort” by those using the API; (2) a developer publish business and technical documentation to enable the API to be used at scale; (3) the developer grants the health care providers “the sole authority and autonomy to permit API Users to interact with the API technology,”\footnote{Sweeney & Lipinski, supra note 132, at 20.} and (4) the API be licensed on reasonable and non-discriminatory terms, and include limits on fees.

C. U.S. Open Data

1. Open Data refers to public sector data published online by local, state, and federal agencies for free public access. With Open Data, government agencies are required or encouraged to transfer data into publicly-available websites. This case study focuses on the United States, and on data that is not intended to be personally identifiable.

2. Origination: The data comes from public agencies. Previously, this data was in printed form or otherwise not readily available online. Some of it, such as court records, was accessible in person but in a less convenient form than online access. Some of it was not available to the public or available only via a request under the Freedom of Information Act or similar state and local laws.\footnote{See Beth Simon Noveck, Forum: Is Open Data the Death of FOIA?, 126 YALE L. J. F. 273 (2016); Martin, Kristen et al., Privacy Interests in Public Records: An Empirical Investigation, 31 HARV. J. LAW & TECH. 111, 114-17 (2017).}

4. Types of Data: Public sector data that may be published includes, for example, National Oceanographic and Atmospheric Administration weather data, government procurement data, transportation data, public health data, agricultural data, and de-identified data regarding populations. In addition to Data.Gov, more than 260 cities and municipalities have launched their own open data initiatives. Each of the individual states have also made data publicly available and accessible online, to varying degrees.

5. Applicable law: The federal Data.Gov portal launched in 2009. The federal Data.Gov portal is now mandated by the OPEN Government Data Act, 44 U.S.C. § 3501 (Jan. 24, 2019). The OPEN Government Data Act requires “timely and equitable access to the agency’s public information.” However, each agency is left to interpret the meaning of “public information,” design its own Open Data policy, and decide which datasets to publish. The various state and local open data portals are each governed by state and municipal laws, regulations, policies, terms of use, and privacy policies.

D. U.S. and EU Phone Number Portability

1. This case study focuses primarily on the U.S. legal framework governing telephone number portability. It also includes, in Section 1.6, a summary

---


150 44 U.S.C.S. §3506(d)(1).

151 See id. at §3506(d)(5) (defining public information as “any information, regardless of form or format, that an agency discloses, disseminates, or makes available to the public”).
of the laws governing number portability in the E.U. The two regimes offer substantially similar rights to users with similar benefits, costs, and risks.

2. Origination. The Number Portability Administration Center, for the United States. NPAC serves as the authoritative database for routing and billing calls for telephone numbers no longer assigned to phone end users. NPAC facilitates phone number portability when an end user switches from one communications provider to another. Congress created and funded NPAC solely for the purpose of administering phone numbers.

3. Destination. Wireless and wireline phone service providers.

4. Types of Data. The information that is exchanged between new and old phone service providers consists of the following: (1) telephone number; (2) current assigned service provider ID; (3) the location routing number (LRN); (4) SS7 Destination Point Codes; (5) Service Type; (6) Alternative SPID (to identify a reseller); (7) billing ID; and (8) end user location and type.

5. Applicable Law. Phone number portability is mandated by the Telecommunications Act of 1996 and regulated by the Federal Communications Commission (FCC). The purpose of the Telecommunications Act is to establish a “procompetitive, deregulatory national policy framework” intended to “promote competition and reduce regulation, . . . to secure lower prices and higher quality services for American telecommunications consumers and encourage the rapid deployment of new telecommunications technologies.” In the 1996

153 Id.
154 Id. NPAC also operates in Canada where their phone numbers are administered and regulated by Neustar.
157 See 47 C.F.R. § 52.3 (2020) (“The Commission shall have exclusive authority over those portions of the North American Numbering Plan (NANP) that pertain to the United States.”). See also WIRELESS LOCAL NUMBER PORTABILITY, supra note 155.
Telecommunications Act, “Section 251(b)(2) requires LECs (local exchange carriers) ‘to provide, to the extent technically feasible, number portability in accordance with the requirements prescribed by the Commission.’” In 2003, the FCC issued an order that mandated number portability between wired to wireless and wireless to wireless phone service providers beginning in November 2003.

6. The European Union similarly mandated phone number portability via Article 30 of the Universal Services Directive (“USD”) of 2002. The USD mandated that consumers could change, in one working day, their fixed or mobile operator while keeping their old phone number. More specifically, Article 30 of the USD required telecoms operators to set a maximum time limit of one working day from the moment of concluding an operator change agreement to the moment of activating the number with another operator. The time limit shall not exceed one working day's loss of service during the process of changing operator and carry out the overall process within the shortest time possible.

E. EU Financial Services

1. This case study examines portability developments in the EU financial services sector. The primary focus is on the Payment Services Directive of November 2007 (“PSD1”) as updated and expanded in the Payment Services Directive of November 2015 (“PSD2”). In the UK, after study by the Open Banking Working Group, the Competition & Markets Authority (“CMA”) created the Open Banking Implementation Entity (“OBIE”) to set software standards and industry guidelines to implement PSD2. Notably, the OBIE issued specifications for Application

162 Id.
Programming Interfaces (“APIs”) to mandate secure connections between banks and other payment service providers (“PSPs”).

2. Origination. Consumer PSPs, including banks.

3. Destination. (1) Consumers and (2) PSPs, including “account servicing payment service providers,” “payment initiation service providers,” and “account information service providers,” as defined in PSD2.\(^{167}\)

4. Types of Data. The payments data in question relates to the various forms of payments information handled by payment processors of all types within the industry.\(^{168}\) The relevant product market is the retail payments market which includes card, internet, and mobile payments.

5. Applicable Law. Recital 16 and Article 28 of PSD1 granted access to payment systems for “authorised or registered payment service providers” on an “objective, non-discriminatory and proportionate” basis, which is similar to the term “fair, reasonable, and non-discriminatory” used in patent and other settings (“FRAND”).\(^{169}\) PSD2 notably widened the scope of PSD1 to cover third party “payment initiation services,” such as Sofort in Germany, IDeal in the Netherlands and Trustly in Sweden.\(^{170}\) Prior to PSD2, such new providers had not been regulated at the EU level, so PSD2 covered them, in order to address issues that may have arisen with respect to confidentiality, liability, or security of transactions with such providers.

F. EU Health Care


\(^{167}\) These terms are defined in Article 4 of PSD2. E.g., PSD2 art. 4. (“‘account servicing payment service provider’ means a payment service provider providing and maintaining a payment account for a payer”).

\(^{168}\) Pursuant to, respectively, Articles 45, 46, 47, 48, and 49 of PSD2.


which is designed to assist EU citizens travelling between Member States to have seamless access to healthcare services by giving Member States the possibility of exchanging health data electronically, in a secure and interoperable way. Despite the many efforts further described in the Appendix, there has been limited success implementing the exchange of such “eHealth” data. Exchanges of eHealth data are currently limited to (1) “ePrescription”/“eDispensation;” and (2) “Patient Summaries.” Only one Member State is currently exchanging both of these types of data, and only with a small number of other Member States. In short, the initiatives for greater interoperability and portability have produced much more limited results than proponents have wished.

2. Origination. The health care practitioner (HCP) or health care system in the Member State where the individual resides.

3. Destination. (1) With respect to ePrescription/eDispensation data, the data will be received by a pharmacy used by that individual in another Member State; and (2) with respect to Patient Summary data, the data will be received by an HCP who is consulted by the individual in another EU Member State.

4. Types of Data. (1) ePrescription/eDispensation data contains the data in a medical prescription which has been provided to the individual; and (2) the Patient Summary contains important health-related information about the individual such as an individual’s allergies, current medication, previous illness, and surgeries, as well as data for the administration of the patient, such as identifying data and contact information.

5. Applicable Law, Actions, and Initiatives. This PORT initiative is the output of a lengthy history of action and initiatives in the EU linked to eHealth interoperability and standardization. References to multiple resources are provided at the end of this Appendix.


G. U.S. Automobile Dealers

1. Automobile dealers typically contract with software companies for “Dealer Management System” (“DMS”) services to assist dealers with their business operations. The DMS is a software platform that provides a wide range of functions including accounting, vehicle inventory, financing and insurance, and managing service and parts operations. Historically, many or all of these functions have been performed by the DMS software. The two largest in the United States, CDK Global, LLC (“CDK”) and The Reynolds & Reynolds Company (“Reynolds”), have a large market share with their combined market share exceeding 90% of vehicles sold.174 Automobile dealers have also contracted with third-party systems integrators and application developers (“third-party software providers”) to provide some of these services, most typically when they charged less for a particular application than DMS providers or provided additional functionality or a better product.

2. CDK and Reynolds have changed their position over time concerning a dealer’s ability to authorize third-party software providers to access dealer data on the DMS on behalf of the dealer. Previously, both CDK and Reynolds permitted such authorization. First Reynolds and later CDK changed their practices to generally prohibit those dealers from allowing such authorization. In 2019, Arizona and at least three other states enacted statutes that require a PORT for the transfer of data from the DMS to recipients authorized by automobile dealers, including systems integrators or other third-party software providers. The laws are intended to give dealers more control over their data stored in the DMS.

3. CDK and Reynolds have challenged the Arizona statute in federal court, claiming that the statute is unlawful.175 Separately, third-party software providers, dealers, and others have brought lawsuits against CDK and Reynolds, alleging (among other things) that they entered into an agreement to exclude third-party software providers in violation of


antitrust laws. Peter Swire has served as an expert witness for the Arizona Automobile Dealers Association in the suit concerning the Arizona statute, and for Authenticom and other software providers in the antitrust suits against CDK and Reynolds.177

4. Origination. A “Dealer Data System.”178 “Dealer Data System” is a defined term under the Arizona law which refers to a DMS.179

5. Destination. A recipient authorized by the automobile dealer (“Dealer”). Notably, the statute provides that a Dealer can give consent to port data from the Dealer Data System to an “Authorized Integrator.” An Authorized Integrator is defined as a “third party with whom the Dealer enters into a contractual relationship to perform a specific function for a Dealer that allows the third party to access Protected Dealer Data or to write data to a Dealer Data System, or both, to carry out the specified function.”180 For example, a Dealer might contract with an Authorized Integrator to support third party applications for service appointments, inventory management, and customer relationship management.

6. Types of Data. The PORT statute applies to “Protected Dealer Data,” which it defines as: (i) “personal, financial, or other data relating to a consumer that a consumer provides to a dealer or that a dealer otherwise obtains and that is stored in the Dealer’s Dealer Data System;” and (ii) “other data that relates to a Dealer’s business operations in the Dealer’s Dealer Data System.”181 More colloquially, the statute applies to the data

---


177 Swire testified publicly in a preliminary injunction hearing in 2017 in federal court in Wisconsin. After that hearing, the district court enjoined CDK and Reynolds from continuing their activities that limited portability. Expert report/declaration of Peter Swire, Authenticom, Inc. v. CDK Global, LLC, No. 17-cv-318-jdp, 2017 U.S. Dist. LEXIS 109409 (W.D. Wis. July 14, 2017); Authenticom, Inc. v. CDK Glob., LLC, No. 17-cv-318-jdp, 2017 U.S. Dist. LEXIS 109409, at *1 (W.D. Wis. July 14, 2017), rev’d on other grounds, 874 F.3d 1019, 1020 (7th Cir. 2017). This case study makes no assertions about the validity of facts in the ongoing litigation; instead, the case study relies on publicly available documents, and presents facts in the form: “PORT proponents claim” or “PORT opponents claim.”

178 ARIZ. REV. STAT. § 28-4651 (2020).

179 Id. at 3(b).

180 Id. at 1.

181 Id. The definition of “Protected Dealer Data” also includes “motor vehicle diagnostic data that is stored in a Dealer Data System.” This case study addresses all Protected Dealer Data except requirements concerning motor vehicle diagnostic data.
in a DMS that pertains specifically to that dealer’s business operations – not to data about other dealers.

7. Applicable Law. Arizona Revised Statute (“A.R.S.”) Sections 28-4651 to 28-4655, and similar laws passed in other states. The law enables the Dealer to select and authorize third parties to receive Protected Dealer Data. The law prohibits what it defines as “cyber ransom,” which means “to encrypt, restrict or prohibit or threaten or attempt to encrypt, restrict or prohibit a Dealer’s or a Dealer’s Authorized Integrator’s Access to Protected Dealer Data for monetary gain.” In other words, under the statute, a DMS provider must permit Protected Dealer Data to be ported to an Authorized Integrator or other party, where the Dealer so directs. The law also makes it illegal to otherwise prohibit or restrict a Dealer’s ability to protect, store, copy, share, or use Protected Dealer Data, including charging fees for such access.

V. DOCUMENTING HOW THE STRUCTURED QUESTIONS ARE CONSISTENT WITH THE CASE STUDIES AND OTHER RESEARCH TO DATE

Part V “shows the work” for developing the Structured Questions for the Portability and Other Required Transfers Impact Assessment (“PORT-IA”). The methodology for this project began with draft Structured Questions and then tested the draft against the seven detailed case studies. The Structured Questions evolved considerably during the research phase of the case studies. Based on this testing, I gave greater emphasis to how each case study and the Structured Questions address issues of authentication, secure transmission of data, and establishing technical standards for sharing data. The sections on “onward transfer” and “fair, reasonable, and non-discriminatory terms” for protecting privacy and cybersecurity were added. On the antitrust side, the importance of lock-in effects to PORT proposals was clarified, and lock-in effects were distinguished more clearly from network effects. As currently drafted, the text of the Questions effectively incorporates the lessons from the case studies and other research to date.

184 Id. § 28-4653(A)(3).
The work to date provides validation for the Structured Questions as an effective tool for identifying and assessing the key issues for a PORTability initiative. The discussion here builds on background research on existing and proposed PORTability requirements, in both the United States and EU, including the “Free Flow of Data” Regulation in the EU for non-personal data.\(^{185}\) It also builds on background research on competition/antitrust issues for both the United States and EU.\(^{186}\) The text of the Structured Questions evolved through application to case studies in diverse sectors (financial, health care, phone, Open Data, and automobile), and under the differing EU and U.S. legal systems. As currently drafted, the text of the Questions effectively incorporates the lessons from the research performed to date. Policymakers and companies can thus use the discussion here to perform their own PORT-IAs of PORTability initiatives.

**Question 1: Define the challenge or opportunity that leads to a possible data portability or other required transfer initiative**

a) Describe the origination, where the data comes from (who is subject to a PORT)
b) Describe the destination, where the data goes to (who can trigger a PORT)
c) Describe the data that is subject to the PORT
d) Describe the applicable law that governs the proposed PORT policy, regulation, product, or practice

In order to analyze a PORTability requirement, the first step is to accurately map the relevant data flows. There is no way to understand the benefits and costs of a PORTability requirement unless one first clearly describes the data flow.

Question 1(a) asks for the origination — where the data comes from. This is the entity that is the subject of the PORT obligation and is required to make data available when the PORT applies. Next, for 1(b), there must be a clear definition of the destination of the PORT — to whom does the data flow? There may be multiple possible recipients. For instance, the GDPR’s RtDP has two major destinations — the individual data subject or, under certain circumstances, a different controller that receives the data on the individual’s behalf.\(^{187}\) Defining each recipient class is a useful exercise — the conditions that apply to the individual’s request may be different than those that apply to

---

\(^{185}\) *FFD Regulation, supra* note 14.

\(^{186}\) Thanks to John Snyder for assistance with U.S. antitrust law and Simon Albert, James Ashe-Taylor, and Lydia Rachionati for assistance with EU competition law.

\(^{187}\) *GDPR, supra* note 2, art. 6.
a service that competes with or supplements the original service. For instance, an individual likely authenticates himself or herself differently than would a large corporation that exchanges data regularly with the company subject to the PORT requirement.

Similarly, Question 1(c) indicates there must be a clear understanding about what data is subject to the PORT. Imagine you are an engineer tasked with implementing a PORT. Your team must precisely enable the data types and data fields for which compliance is required. As a policy matter, careful attention to the scope of data under the PORT is also important. Failure to approach this task with rigor can lead to confusion. For example, the GDPR RtDP has puzzling coverage—it applies to only two of the six legal bases for processing data provided by GDPR Article 6.\footnote{\textit{GDPR}, supra note 2, art. 20.} The right applies to data processed based on (i) consent or (ii) on a contract, but not to data processed under (iii) a legal obligation; (iv) to protect the vital interests of a person; (v) for a task in the public interest; or (vi) where necessary for legitimate interests.\footnote{\textit{GDPR}, supra note 2, art. 20(1); see also GDPR, supra note 187, recital 68.} The exception for processing based on legitimate interests is especially puzzling, given that that basis for processing is used widely by entities complying with GDPR.\footnote{See generally Richie Koch, \textit{Everything you need to know about GDPR compliance}, GDPR.EU, https://gdpr.eu/compliance/ (last visited July 20, 2020) (acting as a guide for GDPR compliance for small and medium-sized businesses) [https://perma.cc/U2HC-DHLT].} More generally, these complexities of GDPR Article 6 illustrate the practical importance of carefully defining what data is subject to the PORT.

Question 1(d) asks for a description of the law (or non-legal requirement) that governs the proposed PORT. Statutory or regulatory obligations, whether of general applicability or industry specific, provide a baseline for consideration of any PORTability policy, and must be matched in the implementation. As described below, some analysis may be required to confirm: (1) who must transfer data, (2) who can request the PORT, (3) what data is covered, and (4) what specific legal (or other) provisions apply to each of these.

Under any regulatory system, perhaps the single most important element is defining the scope of what entities are covered. It may take careful research to identify all of the parties subject to a regulatory system. For example, the Gramm-Leach-Bliley Act (“GLBA”), as described in the U.S. financial
services case study, covers “financial institutions.” Although it is straightforward to determine that a bank is a “financial institution,” there are some companies that require additional analysis. For instance, the FTC in 2019 issued a proposed rule to add the category of “finder” to those who must comply with the privacy and security requirements of GLBA.

Likewise, the lengthy HHS Rule relating to PORTability of health care information has separate provisions that apply the prohibition on information blocking to: (1) health care providers; (2) IT developers of certified health IT; (3) health information exchanges; and (4) health information networks. The scope of the rule’s requirements varies among these four categories.

In many instances, it is relatively straightforward to define who can request the PORT. As discussed further in the cybersecurity discussion, for requests from individuals, the main concern is to authenticate the individual and to exclude unauthorized persons. Authentication can be more complex for a company claiming to conduct a PORT on behalf of an authorized individual. The company requesting the data must both authenticate itself and also prove that it has the requisite consent from the individual.

With respect to what data is covered, the answer can vary greatly depending on a person’s role in the organization. Article 20 of GDPR says the RtDP applies “to the personal data concerning him or her”, and more specifically the personal data that person has “provided to a controller.” Also, the data must be transferred “without hindrance.” For an attorney, these words constitute the legal requirement. For a software engineer, however, those words are merely the starting point. Next, the engineer must “specify functional and nonfunctional requirements to support business processes, user interactions, data transforms and transfers, security and privacy requirements,

191 Gramm-Leach-Bliley Act, 16 C.F.R. § 313.3(k)(1) (2020) [hereinafter GLBA] (defining financial institution as “any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)). An institution that is significantly engaged in financial activities is a financial institution.”).
192 The proposed rule would extend the definition of “financial institution” to include “a finder in bringing together one or more buyers and sellers of any product or service for transactions that the parties themselves negotiate.” GLBA, supra note 191, at § 314.2(f)(2)(xiii); 84 Fed. Reg. 13158 (proposed Apr. 4, 2019). Such “finders” have not previously been listed as financial institutions.
193 See 21st Century Cures Act, § 201; see also The Final Rule, supra note 8.
194 GDPR, supra note 2, art. 20.
195 Id.
as well as corresponding system tests.”196 Similarly, while a lawyer may think the legal requirement is defined by what is “reasonable” or “proportionate,” an engineer may respond: “I can’t code for reasonable.” In preparing a PORT-IA, the analysis of benefits and costs should take account of the perspectives of different members of a team. The costs of building a new system for PORTability may vary enormously, for instance, depending on whether the requirement applies to a few data fields or a multitude.

Finally, for Question 1(d), the team performing the PORT-IA must know the full set of applicable requirements. Those requirements may come from a binding statute or regulation, such as GDPR or the mandates on a U.S. health IT developer. Other legal requirements may arise that are not from a statute or regulation. For instance, there may be an internal company policy that describes which data fields it will transfer. If that internal company policy is memorialized in a public policy or statement, violating that policy may be considered a deceptive trade practice, with enforcement by the FTC.197

In conclusion on Question 1, clear definition of the data flow(s) is essential to an accurate assessment of benefits and costs. Once a clear definition exists, it is far easier to conduct the PORT-IA. The analysis can focus on the defined data flows without being distracted by issues that are irrelevant to the data flows actually within scope.

Data PORTability Benefits:

Question 2: Assess PORT rationales based on competition

a) Does the PORT reduce lock-in effect and facilitate switching to competing providers? (Note: a lock-in effect can exist even in a market that is otherwise competitive, such as a low HHI.)

Question 2(a) addresses lock-in effects. The term “lock-in” is evocative—it is a big problem if someone is locked into a room and cannot get out. In the physical world, locking someone into a room is generally illegal, triggering the rules against false imprisonment.198 As a linguistic matter, considering the

---

198 See Restatement (Third) of Int’l Torts to Pers. § 7 (Am. Law Inst., Tentative Draft No.3-8, 1997) (explaining that “an actor is subject to liability to another for false imprisonment if: (a) the actor intends to confine the other within a limited area . . . ; (b) the
metaphor of a “lock-in” helps to illuminate why proponents use the term in justifying each PORT proposal. If the doors and windows are always unlocked or wide open, then there is little reason to pass a law requiring them to be open. That is, PORTability proposals exist where critics can claim that something is locked that should be open.

The case studies illustrate that portability initiatives have sought to address a wide-range of causes of lock-in, including technological, practical, contractual, and competitive restraints:

1. **Phone portability.** The mobile phone provider locks in the customer if the customer cannot switch to a competing service. Without portability, social and business contacts may not be able to call the customer. Historically, this lock-in effect reflected a combination of contractual and technological barriers to switching.\(^{199}\)

2. **Banks and competing financial services.** Both PSD2 in the EU and Dodd-Frank in the United States target the problem that a consumer may get locked in to one bank, without the ability to export transaction history to a competing bank or innovative fintech service. PSD2 expanded the scope of PSD1 to include “payment initiation services,” in hopes of reducing lock-in effects even further.\(^{200}\)

3. **Patient health records.** The HHS rule seeks to unlock the ability of a patient to transfer medical records to innovative apps.\(^{201}\) The EU health care case study addresses the problem of the resident of one Member State being geographically locked-in, unable to travel for work and vacation and have medical records readily available in other countries.

4. **Auto dealers.** It is expensive, in terms of time and money, for an auto dealer to switch from one Dealer Management System (“DMS”) to another, so dealers say they are locked in to their current DMS.

5. **Open Data.** The lock-in for Open Data is more metaphorical. Before an Open Data initiative, one can consider the government data to be

---

\(^{199}\) See Appendix 4, Phone Portability Case Study.

\(^{200}\) Council Directive 2015/2366, art. 4 of November 25, 2015, on Payment Services in the Internal Market, 2015 O.J. (L 337) (EU) [hereinafter PSD2] (“’Payment initiation service’ means a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider[.]”); Dodd-Frank Act § 5533(d).

“locked away,” inaccessible to the general public. With an Open Data requirement, the data is unlocked.

6. **The GDPR right to data portability.** One important motivation for the inclusion of the RtDP in GDPR was to address concerns that individuals would get locked-in to digital platforms, without a ready way to export their own data.\(^\text{202}\)

7. **The Free Flow of Data Regulation.** An important motivation for the FFD Regulation was to address “various lock-in issues.”\(^\text{203}\)

For competition purposes, it is relevant that lock-in problems can arise even in the absence of a concentrated market. Put another way, there need not be a monopoly or dominant firm in order for a lock-in effect to exist. For example, the U.S. banking market for domestic deposits lacks a dominant firm. The largest firm in the market is JP Morgan Chase, which has roughly a 10% market share for domestic deposits.\(^\text{204}\) Second, consumer lock-in for mobile phone numbers does not seem to depend on market concentration. Absent a regulatory obligation, even a small carrier would have rational incentives to make it difficult for subscribers to leave.\(^\text{205}\)

These two examples illustrate that lock-in may be due to high switching costs, rather than the existence of monopoly power at the moment the consumer chooses a mobile carrier or bank. For mobile phones, the switching costs are due to the hassle of telling everyone the new number, plus the calls the individual or company may not receive from social or business contacts. For banks, scholars have identified a variety of switching costs, including “transactional costs related to changing a bank account from one bank to another or to taxes related when closing financial securities earlier than contractually planned.”\(^\text{206}\) For consumers considering shifting to a new

\(^\text{202}\) See GDPR, supra note 2, at art. 20, recital 68.

\(^\text{203}\) FFD Regulation, supra note 14.


\(^\text{205}\) The carrier would have an incentive to make it difficult for the customer to leave if the value to the carrier of locking in the customer exceeds the value to the carrier of offering consumers an easy way to port the phone number to a different carrier. Suppose, for example, that a barrier to leaving gains the carrier $50 on average in customer retention, while customers would only pay $10 on average to have an easy mechanism for porting. Under those facts, it is rational, even in a competitive market, for the carrier to make it difficult to leave.

\(^\text{206}\) Damien Egarius & Laurent Weill, Switching costs and market power in the banking industry: The case of cooperative banks, 42 J. of INT’L FIN. MKT., INST. MONEY 155, 156 (2016).
fintech company, such as to consolidate all of a family’s financial records, a particularly high switching cost may be retrieving the transactional history and other historical records from the previous bank. Thus, even where financial markets have numerous competitors, a PORT requirement may facilitate consumers having the ability to move that historical record to a new firm.

In conclusion, the prominence of lock-in effects in all the case studies suggests the importance of identifying the cause of lock-in effects early in consideration of a PORT initiative. To determine the benefits of a PORT initiative, determine what data is actually locked-in, as well as the benefits that would result from unlocking. In the absence of a coherent story of lock-in, it may be hard to justify requiring a PORT.

b) Does the PORT reduce network effects that might exist even after users have the right/capacity to transfer their data?

Question 2(b) addresses network effects. There are two important types of networks effects. Direct network effects cause a customer to value a service, network, or platform more as the number of users increases. Indirect network effects can be generated where the growth of one side of a platform (such as user engagement) leads to increased demand on the other side of the platforms (such as advertising). Both types of network effects have been cited as barriers to entry that protect incumbent social networks and other digital platforms, and therefore are a central rationale for PORT initiatives related to platforms and other multi-sided markets.

Perhaps surprisingly, network effects have been much less prominent explanations for the PORT initiatives examined in the case studies:

1. Phone portability. This case study shows an important interaction of technical interoperability with PORT requirements. For phone calls, there is a long history of interoperability, in the sense that subscribers to one carrier, such as AT&T, can easily make a call to subscribers of another carrier, such as T-Mobile or a new start-up. In this respect,

---

207 See generally David S. Evans & Richard Schmalensee, Network Effects: March to the Evidence, Not to the Slogans, COMPETITION POLICY INT’L, INC. (2017), https://mitsloan.mit.edu/shared/ods/documents/?PublicationDocumentID=4243 (discussing indirect and direct network effects, and an economist’s perspective that the normalized “winner-take-all notion” has been disproven in some instances) [https://perma.cc/T9QF-BDBX].

208 Id.

209 See infra Appendix 4: U.S. and EU Phone Number Portability.
easy interoperability reduces or eliminates the network effect of a consumer choosing the largest carrier.\textsuperscript{210} The rationale for phone number portability thus appears to rely much more on high switching costs, as discussed above, rather than on network effects.

2. Financial services. A system for payment services can have strong network effects—the more places a credit card can be used, for instance, the greater value to consumers. The PSD2 and U.S. case studies, however, do not seem primarily to involve individual firms taking advantage of that sort of network effect. Instead, the focus of the PORT initiatives is more on opening the traditional banking industry to fintech competitors. European competition regulators brought an action against the banking industry’s European Payments Council, leading to the opening the payments system to non-banks on a fair, reasonable, and non-discriminatory basis.\textsuperscript{211} Similarly, a major theme in the United States has been to assure that non-banks can interoperate with the banking system.

3. Health care. The U.S. health case study offers some lessons concerning network effects. One way to view the recent HHS regulation is that it encourages “multi-homing”—where patients so choose, the patient data can port to new apps, as well as continuing to reside within the traditional healthcare providers and insurers.\textsuperscript{212} This porting has the potential to create network effects for apps that enter the market, where such apps could offer improved services to patients, such as better data analysis, if more patients use the app. A secondary theme for the HHS regulation may be to reduce the advantages of network effects on the largest existing databases of health data, but combatting incumbents’

\textsuperscript{210} There may be other network effects. For instance, a large network may find it more economical to invest in a large network of cell towers. A small competitor may lack the budget to build cell towers, and thus its subscribers may have to pay a higher price or receive a lower-quality service. The point in the text is that there is effective interoperability for the subscriber of one service to call subscribers of the other services—choosing a carrier therefore does not create network effects in the ability to call more people.


\textsuperscript{212} See 21st Century Cures Act, 114 Pub. L. No. 255, 114 H.R. 34 (enacted 2016); see also The Final Rule, supra note 8.
network effects has not been a primary theme in justifying the PORT.213

4. Auto dealers. Network effects are not a primary theme in the competition analysis of the U.S. state laws concerning auto dealers and dealer management software.

5. The Open Data case study concerns PORT requirements on government agencies and does not implicate antitrust law and network effects.

In contrast, the importance of network effects to social networks and other digital platforms becomes more apparent. By definition, social networks are likely to exhibit strong network effects: the ability to connect with many people is a prime attraction for users.

c) Does the PORT reduce any effect on competition from abuse by a dominant firm? For instance, does the PORT reduce the ability of a dominant firm to impose anti-competitive contract provisions or deny access to an essential facility?

Question 2(c) addresses how abuse by a dominant firm affects competition. The role of a dominant firm is important to PORT initiatives in at least two ways. First, a dominant firm may be able to exert market power in various ways, including raised prices and lower quality. Lack of portability can be an example of lower quality – the users may have preferences to transfer their data, and would benefit if they could (i.e., gain greater consumer surplus), but the dominant firm fails to provide portability. Second, mandatory PORTability is a potentially attractive remedy for abuse by a dominant firm. The ability to gain access to data can arguably facilitate and encourage nascent competitors and help create or restore competition to a market segment previously controlled by a dominant firm. This approach may be attractive because it is less drastic than other possible remedies, such as breaking up a dominant firm.

As discussed in Part II, EU competition law has broader theories of liability concerning dominant firms than U.S. antitrust law. Article 102 TFEU prohibits undertakings, which are dominant within a relevant European market or a substantial part of it, from abusing their market power.214 A firm is considered to be dominant when it is able to behave “independently of its

213 The EU case study primarily concerns overcoming barriers to expanding the geographic scope of health markets, and combating network effects has not been a major theme.
214 Consolidated Version of the Treaty on the Functioning of the European Union art. 102, May 9, 2008, 2008 O.J. (C 115) 89 (ex Article 82 TEC) [hereinafter TFEU].
competitors, its customers and ultimately of consumers.”

The Commission uses various tools to determine dominance; it has stated that dominance is not likely with market share below 40%, and that market shares above 50% may lead to a rebuttable presumption of dominance. European competition law places on dominant companies a special responsibility to act fairly on the market. For a firm considered ‘dominant,’ imposing certain contractual restrictions or acquiring certain contractual rights could be abusive, as well as refusing to deal with third parties seeking access to essential inputs or facilities. Competition authorities in Europe have also brought enforcement, including against Google, on the theory that the company was a dominant firm, discriminating in search results in favor of its own services.

By contrast, U.S. antitrust law lacks a comparable counterpart to Article 102. Generally, even dominant firms are encouraged to compete aggressively, and run afoul of U.S. antitrust law when they engage in “exclusionary conduct.” Historically, the closest doctrinal match to Europe’s special responsibility would attach in the narrow circumstances where a monopolist was found to control an “essential facility,” thereby reducing any plausible competition. Where such an essential facility exists,

216 Id. at para. 14.
219 See 15 U.S.C. § 2 (2018); see also Verizon Commc’ns., Inc. v. Law Offices of Curtis V. Trinko, LLP, 540 U.S. 398, 407 (2004); U.S. v. Grinnell Corp., 384 U.S. 563, 570-71 (1966) (holding that “[t]he offense of monopoly under § 2 of the Sherman Act has two elements: (1) the possession of monopoly power in the relevant market and (2) the willful acquisition or maintenance of that power”).
220 See e.g., Case 322/81, Nederlandsche Banden Industrie Michelin v. Comm’n 1983 E.C.R. 3461 (Michelin I), para. 57; Case T-83/91 Tetra Pak v. Comm’n (Tetra Pak II) 1993 E.C.R. II-755, para. 114; Case T-111/96 ITT Promedia v. Comm’n 1998 E.C.R. II-2937, para. 139; Case T-228/97 Irish Sugar v. Comm’n, 1999 E.C.R. II-2969, para. 112; and Case T-203/01, Michelin v. Comm’n, 2003 E.C.R. II-4071 (Michelin II), para. 97. See Opinion of Attorney General Jacobs on Case C-7/97, Oscar Bronner GmbH & Co. KG v. Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG and Others (May 28, 1998), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:61997CC0007&from=EN (“An essential facility can be a product such as a raw material or a service, including provision of access to a place such as a harbour or airport or to a distribution system such as a
a logical remedy is to require the facility to mandate access, such as through PORTability obligations. Today, the essential facilities doctrine is rarely successful.221 However, the FTC and other regulators are apparently contemplating imposing data PORTability as a remedy for a broader range of antitrust concerns, including, for example, as a remedy for prior acquisitions challenged under the antitrust laws.222

Concerns about dominant firm behavior have been prominent rationales for PORTability requirements applied to digital platforms. Facebook was specifically mentioned in the legislative history for the Article 20 RtDP. The ACCESS Act in the United States and the recommendations of the UK CMA illustrate the regulatory interest in spurring PORTability to address perceived risk to competition by incumbent digital platforms.223 Such initiatives can be based on legislators’ views about possibly dominant behavior, without the need for proof or adjudication of a violation of antitrust or competition laws.

Importantly, the case studies illustrate that PORT initiatives can be initiated even in the absence of a finding that market participants have undertaken conduct actionable under general EU competition or U.S. antitrust law. The auto dealer case study illustrates the possibility of ex ante regulation instead of ex post enforcement of general antitrust rules. Dealers and third-party software providers are currently pursuing an antitrust lawsuit against the two largest DMS providers, alleging among other things an illegal, contractual

telecommunications network. In many cases the relationship is vertical in the sense that the dominant undertaking reserves the product or service to, or discriminates in favour of, its own downstream operation at the expense of competitors on the downstream market. It may however also be horizontal in the sense of tying sales of related but distinct products or services.”) [https://perma.cc/BP53-9XQB].


222 See, e.g., Conner, supra note 46 (“[W]e may require the merged firm to affirmatively engage in behaviors, or enter into agreements to license assets and provide other competitive resources to new entrants…. The breadth of additional relief that may be considered include obligations to provide inputs, distribution, access or other rights, data, or supply of products and services to one or more entrants on specified terms or a non-discriminatory basis for some period of time.”).

223 See ACCESS Act of 2019, supra note 63; COMPETITION MARKETS & AUTHORITY Online platforms and digital advertising: Market study interim report, 1, 228 (2019), https://assets.publishing.service.gov.uk/media/5dfa0580ed915d0933009761/Interim_report.pdf [https://perma.cc/9367-QEZ8]; see also supra notes 116-21 (discussing CMA studies).
restraint of trade by two firms with high market power. At the same time, without waiting for a court determination of antitrust liability, Arizona and other states have already enacted legislation to allow Dealers to transfer Dealer Data to their authorized third-party software providers.

In conclusion, a PORT-IA should consider any claim about abuse of a dominant market position under the law applying in that jurisdiction and evaluate the extent to which the PORT initiative would remedy any such abuse. More than for other theories of harm, the legal doctrines currently vary considerably under EU competition and U.S. antitrust law. A strict finding of legal liability is not necessary, however, as a predicate for legislative action to address concerns about dominant firms.

d) Does the PORT reduce barriers to entry in ways that made it easier for competitors to gain necessary scale?

Reducing barriers to entry is one of the most commonly cited ways in which data portability has been advocated as a remedy for competition concerns. Incumbent firms, particularly digital platforms, have been viewed as the beneficiaries of network effects that result in a competitive tipping point, leading to a “winner take all” situation. Access to an incumbent’s data through PORT initiatives may facilitate a nascent competitor’s efforts to obtain necessary scale and to facilitate switching in sufficient numbers to overcome these barriers to entry.

The case studies illustrate ways in which data PORTability initiatives in a range of industries have been implemented with the goal of overcoming barriers to entry:

- In the EU, significant areas of the payments market had remained fragmented along national borders. The Payment Services Directives sought to address both (a) geographic barriers to entry, existing previously in national markets; and (b) product barriers to entry, to

---


225 See e.g. ARIZ. REV. STAT. §§ 28-4651 to 28-4655 (2019) (also known as the Dealer Data Security Law); see also David Muller, supra note 175.

allow entry by fintech and other competitors to provide consumers with new services, such as mobile payments.\textsuperscript{227}

- For U.S. health care, a significant goal of the HHS rule was to reduce barriers to entry for smartphone apps and other non-traditional participants in the health care system.\textsuperscript{228}

- Reducing barriers to entry appears to be a secondary goal for the EU health care initiative.\textsuperscript{229} The emphasis has been more on enabling a data subject to receive health care in a different Member State, rather than enabling new competitors to sell services in a different country.

- The Arizona statute sought to reduce barriers to entry in the market for software services used by automobile dealers.\textsuperscript{230} Under the statute, Dealers can choose to buy from Authorized Integrators, who were previously denied access to the two largest DMS Providers.\textsuperscript{231}

- Open Data proponents have discussed positive competitive effects for government procurement, such as by enabling new entrants to bid effectively.\textsuperscript{232} The magnitude of any such effect is unclear and appears to vary by program. Outside of the government procurement context, reduction of market power of dominant firms has been at most a secondary rationale for Open Data initiatives.

e) **Are there any other competition rationales for the PORT?**

Although there were not particular examples in the case studies, there may be other competition considerations in addition to the four theories discussed already – lock-in, network effects, dominant firm behavior, and reducing barriers to entry.

The Open Data discussion suggests a conceptual limit on the likely benefits to competition due to PORTability. Conceptually, Open Data in the


\textsuperscript{228} See 21\textsuperscript{st} Century Cures Act, 114 P.L. 255, 114 H.R. 34 (enacted 2016); see also The Final Rule, supra note 8.


\textsuperscript{231} Id.

public sector is equivalent to maximum PORTability in the private sector – the maximum amount of data is available to data recipients at zero or low cost. Nonetheless, even with easy and free access to data, often there are little or no innovation or other business impacts from a particular Open Data dataset. Similarly, modest benefits can easily exist in the private sector, even where there are extensive PORTability requirements, unless the data that is subject to the PORT is economically useful.

Question 3: Assess innovation and other commercial benefits due to the PORT

a) Apart from any pro-competitive effects on existing markets, what commercial innovation may result due to the PORT?

b) Are there any other significant commercial benefits?

1. **Open Data** proponents claim that the data enables innovative new market entrants. Positive examples may include apps, such as weather apps, traffic apps, restaurant health violation apps, and crime and safety apps. Open Data initiatives have also been promoted as spurring growth of new businesses in general. In practice, the innovation and commercial benefits are quite possibly smaller than some proponents have envisioned—the supply of data from an Open Data initiative is not necessarily matched with the demand for data by potential entrants.

2. **Large-scale PORTs at the enterprise level.** Conceptually, proposals for large-scale PORTs in the private sector are similar to Open Data mandates in the public sector: the mandate requires openness for a category of data. For both, the openness is subject to constraints, such as for privacy and security. In addition, the supply of data under the initiative may not prove a good match for the demand for data, creating less innovation and competition than proponents had hoped.

3. **U.S. financial services.** Proponents have emphasized how portability may lead to innovation, such as by facilitating entry of a broader range of fintech companies who can compete with traditional banks.

---


234 See id.

235 See id.

236 See U.S. DEPT. OF TREASURY, A FINANCIAL SYSTEM THAT CREATES ECONOMIC OPPORTUNITIES: NONBANK FINANCIALS, FINTECH, AND INNOVATION, 31-33 (Report on
Similarly, PSD2 stated: “the current degree of innovation in the field of payments might lead to the rapid emergence of new payment channels in the forthcoming years.”\footnote{237}

4. **U.S. and EU health care.** The U.S. prohibition on information blocking is designed to reduce the ability of incumbents to insist that local physicians adopt a particular electronic health record platform, opening the possibility of innovative services.\footnote{238} The mandatory APIs are designed to enable patients and others to take advantage of innovations such as smartphone apps.\footnote{239} By contrast, the focus of the EU health care PORTability initiative is on smoother data flows among incumbent health systems.\footnote{240} There is far less focus on moving patient data from traditional providers to innovations such as smartphone apps.

5. **U.S. automobile dealers.** Proponents of the PORT claim that CDK’s and Reynolds’ limits on transfers impair competition in the app market, reducing the possibility of new entrants and innovation in provisioning software services to Dealers.

**Question 4: Assess non-commercial benefits due to the PORT**

a) Apart from competition and commercial effects, does the PORT provide benefits for user autonomy, user control over information, or other individual benefits?

A major, repeatedly used rationale for PORTability is to provide users with greater control over “their” data. This idea of user control over data is often called “user autonomy” or “freedom of choice.”\footnote{241}

\footnote{237} PSD2, supra note 200, at recital 67
\footnote{239} Id. at 25924.
\footnote{240} See GDPR, supra note 2, at 45.

Executive Order 13772, 2018) (Professor Barr notes, “As a drafter of the provision that became §1033, I can state that the scope of the provision was intended to be broad – providing a framework for customer access that would encourage competition and innovation, including through the use of third-party providers and aggregators. The Treasury Department has taken a similar view.”); see also Plaid, *Plaid Unveils Investments by Citi Ventures and American Express Ventures*, PRNEWswire (Feb. 6, 2017), http://www.prnewswire.com/news-releases/plaid-unveils-investments-by-citi-ventures-and-american-express-ventures-300402531.html (Both Citi and American Express announced investments in data aggregator Plaid (joining Goldman Sachs), citing the goal of “better access to clean, high-quality financial data, enabling innovation and a secure infrastructure for the financial services ecosystem.”) [https://perma.cc/P8KE-85Z8].
• The GDPR RtDP illustrates the importance of user control over data. The portability requirement is not simply about enhancing competition—small companies face the same portability requirements under Article 20 as monopolists.242

• U.S. financial services. The Consumer Financial Protection Bureau published nonbinding principles in October 2017 that expressed a vision of consumers “enhanc[ing] their financial lives when they control information regarding their accounts or use of financial services.”243 Similarly, PSD2 emphasized freedom of choice. The goals of PSD2 are to provide individual bank customers a greater freedom of choice in selecting payment providers and accessing new entrants and innovative providers, in addition to any improved price and quality that results from greater competition.244
• **Phone number portability** provides consumers greater autonomy over their phone numbers because they can respond to price and service changes without having to change their telephone number. This is especially true for business customers whose costs could include revising marketing materials, keeping track of customers’ information once they change numbers, and the possibility of losing customers because a business changed its phone number.

• For both **U.S. and EU health care**, improved patient choice and control over information have been important rationales for the PORTability requirements.

• User control can refer to companies, and not only to individuals. User control is a rationale for several of the PORT initiatives, so that companies can control “their” data:
  
  o The **HHS regulation** requires a certified IT health software provider to enable transfer “without special effort” of a medical provider’s data to a competing IT software provider.  
  
  o The **Arizona auto dealer statute** requires Dealer Data Providers to follow directions of Dealers on the ability to access and transfer Dealer Data.

  o A principal goal of the **FFD Regulation** is to enable companies to port “their data from one service provider to another or back to their own information technology (IT) systems, not least upon termination of their contract with a service provider.”

  o **Phone number portability** benefits business customers, so that they can change their phone number(s). Otherwise, shifting to new phone numbers could include costs such as revising marketing materials, keeping track of customers’ information and to ensure that consumers, merchants and companies enjoy choice and transparency of payment services to benefit fully from the internal market.”); see also id. (“This should generate efficiencies in the payment system as a whole and lead to more choice and more transparency of payment services while strengthening the trust of consumers in a harmonized payments market.”); see also id. at 43 (“This Directive should specify the obligations on payment service providers as regards the provision of information to the payment service users who should receive the same high level of clear information about payment services in order to make well-informed choices and be able to choose freely within the Union.”); see also id. at 46 (“The issuing of a card-based payment instrument by a payment service provider, whether a credit institution or a payment institution, other than that servicing the account of the customer, would provide increased competition in the market and thus more choice and a better offer for consumers.”).

245 21st Century Cures Act, supra note 8, at §§ 170, 170.404(a).

246 See **ARIZ. REV. STAT. § 28-4651** (LexisNexis 2019).

247 **FFD Regulation**, supra note 14, at 60.
once they change numbers, and the possibility of losing customers because a business changed its phone number.

- Many or most Open Data initiatives occur without an opt-in or opt-out by the individual person in the dataset. Because individuals have little control in determining the data that is published, they have little means of mitigating their own individual privacy concerns and are ultimately reliant on the government agency to erect adequate privacy protections around the data that is released.

**b) Apart from competition and commercial effects, does the PORT provide any public benefits, such as research for the benefit of the public?**

- HHS hopes that the interoperability rule’s information transfers will benefit medical research.\(^{248}\)

- Proponents of Open Data have emphasized how it contributes to scientific research, for areas including, but not limited to, medicine, environmental science, social sciences, computer science, and agricultural and biological sciences.\(^{249}\) National open data portals are cited in scientific research more frequently than local portals, likely because national portals tend to include more data sets.\(^{250}\) Beyond scientific research,

- Proponents of Open Data have identified a range of possible public benefits, beyond scientific research. For example: (1) Open Data can be relevant for legal proceedings.\(^{251}\) (2) NOAA weather data has “significantly lowered the economic and human costs of weather-related damage through forecasts.”\(^{252}\) (3) Opening Global Positioning System data has “improved safety, emergency response times and


\(^{250}\) *Id.* at 5.

\(^{251}\) See Stefaan Verhulst & Andrew Young, *When Demand and Supply Meet*, OPEN DATA IMPACT, 13 (Mar. 2016), https://www.thegovlab.org/static/files/publications/open-data-impact-key-findings.pdf (discussing how, in a lawsuit, Ohio residents used a map derived from open data to prove that the distribution of clean water in their town was racially inequitable) [https://perma.cc/H5D8-YRDL].

\(^{252}\) *Id.*
environmental quality.”\(^{253}\) (4) The Opioid Mapping Initiative created a comprehensive map to address the opioid crisis.\(^{254}\)

**Question 5: Assess regulatory or legal benefits of the initiative**

a) As a result of the PORT, would consumers receive any legal benefits, such as expanded coverage of consumer protection laws?

b) Would any other actors receive any legal benefits, such as enforceability of contracts?

Beyond possible use of Open Data information in a lawsuit, the case studies did not provide any significant illustrations of such legal benefits. This question is included for symmetry with Question 12, which discusses legal harms from a PORT requirement, such as loss of consumer protection or intellectual property rights.

**Question 6: Assess any reduced benefits due to lack of technical or market feasibility**

a) Are there technical obstacles to realizing the hoped-for benefits of the PORT? For instance, the data may be of poor quality or available in an incompatible format.

- Phone number portability for the United States did not become generally operative until seven years after passage of the Telecommunications Act of 1996.\(^{255}\) One important reason for the delay was the lack of technical means to ensure successful transfer of the phone number from one carrier to another.
- For EU financial services, despite mandates and deadlines for achieving interoperability, there have been repeated delays in meeting requirements for APIs and other components needed for effective implementation.
- For EU health care, the exchange of ePrescription/eDispensation and Patient Summaries data relies on the voluntary cooperation of health authorities connecting to the eHealth digital service infrastructure (eHDSI).\(^{256}\) It appears that this voluntary approach to technical standards has led to even more delays than the mandatory approaches

\(^{253}\) *Id.*

\(^{254}\) *Id.*

\(^{255}\) See Kessing, *supra* note 160.

under the Open Banking program in the UK. There are continued, serious problems of incompatible health IT systems across the Member States.257

b) Are there market obstacles to realizing the hoped-for benefits of the PORT? For instance, the demand for data may not fit well with the available supply of data from the PORT.

- For Open Data, data sets are often published in a manner that can be accessed and analyzed manually but cannot be readily used by software programs.258
- Once Open Data is published (and businesses may begin to rely upon that data), data may not be updated in a complete and timely manner.
- For Open Data, there has been a disconnect between the supply of public sector data and the demand for that data. Agencies appear to tend to publish data without proof whether it is the type of data that is useful to businesses and individuals.
- For EU health care, the technical problems described above are compounded by the fact that each Member State retains the competency to govern its own health policy, and national markets for health care are mostly separate. In the absence of any regulatory requirements at the EU level, progress on interoperability and PORTability has remained very slow, despite numerous policy statements supporting such initiatives.259

257 See Directive 2011/24, of the European Parliament and of the Council of 9 March 2011 on the Application of Patients’ Rights in Cross-Border Healthcare, 2011 O.J. (L 88) 45, 52 (stating that “widely different and incompatible formats and standards are used for provision of healthcare using ICTs throughout the Union, creating both obstacles to this mode of cross-border healthcare provision and possible risks to health protection”).


c) Note – reserve discussion of privacy, cybersecurity or other specific risks for discussion below of Data PORTability Risks and Costs.

**Question 7:** Assess incentives for those presenting evidence of benefits.

a) What parties have an economic or other incentive to support the PORT? Explain the incentives. Assess the asserted benefits in light of the incentives of some actors to support the initiative. Just because a party has an economic interest to support or oppose an initiative does not mean the facts it cites are incorrect; however, assess the evidence supporting the initiative in light of possible bias. Where available, identify evidence based on sources that are as objective as possible.

- **EU and U.S. financial services.** An important rationale for the benefits of PSD and U.S. financial services portability has been to enable non-banks to compete with banks.\(^{260}\) Non-banks have often favored the PORT initiatives while banks have sometimes opposed.

- **U.S. automobile dealers.** Automobile dealers and software providers have filed lawsuits against CDK and Reynolds, alleging that those providers’ contracts, and the limits on PORTability, violate the antitrust laws.\(^{261}\)

**Data PORTability Risks and Costs:**

---


Question 8: Assess privacy risks from the PORT (alternatively, use existing privacy or data protection impact assessment)

a) Privacy concerns related to personal data (personally identifiable information) of the data subject
   
   i. What are the risks to the data subject’s own identifiable data? What steps (technical, administrative, etc.) can be taken to mitigate these risks?
   
   ii. Other than costs of compliance itself, to what extent do the steps taken to protect privacy impede the goals of the data portability initiative?

1. Privacy risks for phone number portability are generally very low—people usually want their personal and business contacts to be able to continue to call them. Phone number portability thus contrasts greatly with other case studies: users generally want dissemination of the phone number, but often have privacy concerns about other categories of personal data, such as financial and medical data.

2. Financial services. Privacy issues exist, to reveal personal financial data generally, and especially because unauthorized access to personal financial data can be used for identity theft. Greater security issues exist in addition when the portability mechanism enables transfer of funds.

3. For EU financial services, European data protection regulators made it a priority to include concrete data protection rules in PSD2 itself, rather than accepting vague assertions of compliance with applicable data protection laws. This precedent may suggest that other PORTability initiatives in the EU will have specific data protection rules in the text, going beyond the text of GDPR.

4. For Open Data, one type of privacy risk comes from public records about individuals that have historically been open to the public, but relatively difficult to access. For instance, the U.S. National Center for State Courts has held multiple conferences on issues of privacy and

---

online access to court records.\textsuperscript{263} Due to privacy concerns, courts have amended various rules, such as requiring redaction of Social Security numbers and other sensitive information.\textsuperscript{264}

5. For Open Data identifiable records, there are sometimes privacy concerns about sub-categories of records or populations. For instance, government employees have expressed privacy concerns because their employment data may technically be “public information” and could be published unless excluded from publication by the applicable Open Data policy. There may similarly be reasons to exclude data about other populations, such as the address and other information of first responders or victims of crime and domestic violence.

6. U.S. health care illustrates complexity that can exist for individual consent to processing. As transfers of EHI occur to more recipients, there are risks to user trust. It is not clear how well patients will understand where their patient data is going. How to manage patient consent may therefore be a challenging task. If patients lose trust in how their data is protected, there may be patient reluctance to disclose fully to their medical providers.

7. U.S. automobile dealer data. Personal data of the customers of automobile dealers, such as lending data, is often covered by the GLBA. Entities processing data on behalf of auto dealers, such as software providers, thus are often service providers that must similarly comply with GLBA requirements.\textsuperscript{265}

\textbf{b) Privacy concerns related to personal data (PII) of third persons}

i. What are the risks from the PORT to third persons’ identifiable data (that is, data about persons other than the data subject whose data is PORTed)? What steps (technical, administrative, etc.) can be taken to mitigate these risks?

ii. Other than costs of compliance itself, to what extent do the steps taken to protect privacy impede the goals of the data portability initiative?


\textsuperscript{264} Id.

For the case studies, privacy concerns about third persons – persons other than the data subject – were not a significant issue. The case studies thus sharply contrast with social networks, where personal data pervasively applies to more than one person. Outside of the realm of social networks, the research has not identified any successful PORTability initiative that has substantially included data implicating the rights of third persons.

c) Privacy concerns relating to de-identified data
   i. De-identified data is designed to be no longer linkable to a particular data subject. Some PORT initiatives contemplate sharing of de-identified data with other companies, for reasons including research and promotion of competition. The Federal Trade Commission test for proper handling of de-identified data is that there should be (1) reasonable technical controls, (2) no re-identification by the recipient; and (3) downstream controls on re-identification.
   ii. What are the risks from the PORT related to re-identification of data? What steps (technical, administrative, etc.) can be taken to mitigate these risks?
   iii. Other than costs of compliance itself, to what extent do the steps taken to protect the privacy of de-identified data impede the goals of the PORT initiative?

1. U.S. financial services. There have been press accounts of fintech companies, such as Yodlee, allegedly making de-identified data available to its business customers.\footnote{See Joseph Cox, \textit{Leaked Document Shows How Big Companies Buy Credit Card Data on Millions of Americans}, \textit{VICE} (Feb. 19, 2020), https://www.vice.com/en_us/article/jged4x/envestnet-yodlee-credit-card-bank-data-not-anonymous [https://perma.cc/Y9HK-8S3U]; see also Bradley Hope, \textit{Provider of Personal Finance Tools Tracks Bank Cards, Sells Data to Investors}, \textit{DEMOCRATIC UNDERGROUND} (Aug. 6, 2015), https://www.democraticunderground.com/10141169602 (explaining that Yodlee, an FSP that provides personal financial management tools by aggregating and processing consumer data from a number of different accounts, sells scrubbed and anonymized transactional data) [https://perma.cc/A45G-ESJ2].} This sort of database may be subject to re-identification by the business customers. It is also an example of an onward transfer problem, discussed below: the business customers may be able to violate a data subject’s privacy when they receive supposedly de-identified data from the data recipient (Yodlee).
2. A major constraint on the usefulness of Open Data is the risk of re-identifying individuals in a data set. For example, GPS data for commuters may be de-identified before being published in an open database. Individual users, however, may repeatedly drive between home and work. Assisted by these important data points, an analyst may find it relatively easy to re-identify individuals in the database, such as by consulting publicly available information about people’s home addresses and jobs.

3. The European experience with Open Data is consistent with privacy being a significant limiting factor. The Open Sector and Public Sector Information Directive entered into force in 2019, replacing earlier European Union Directives. The new Directive “focuses on the economic aspects of the re-use of information rather than on access to information by citizens.” Notably, its “high-value datasets” apply predominantly to non-personal data: (1) geospatial; (2) earth observation and environment; (3) meteorological; (4) statistics; and (5) mobility. The only exception appears to be a “companies and company ownership” dataset, which would reveal personal data for individuals who own companies of public record.

4. The research to date has not included a case study about Smart Cities. Initiatives for Smart Cities, however, have repeatedly encountered concerns about re-identification of supposedly anonymized databases. In this respect, the risks of re-identification show an important overlap between Open Data and Smart Cities initiatives.

---


268 Id.

269 Id.

270 See id.

271 See Teena Maddox, Smart Cities: A Fact Sheet, TECHREPUBLIC (July 16, 2018), https://www.techrepublic.com/article/smart-cities-the-smart-persons-guide/ (“A smart city uses [Internet of Things] sensors and technology to connect components across a city to derive data and improve the lives of citizens and visitors. . . .Oftentimes, a mobile app is provided to give immediate access to data, communication channels, and more so that people can do everything from avoiding traffic jams, to finding a parking spot, and reporting a pothole or an overflowing dumpster.”) [https://perma.cc/9GVM-CKH5].

272 See, e.g., Nick Summers, Google’s smart city dream is turning into a privacy nightmare, ENGADGET (Oct. 26, 2018), https://www.engadget.com/2018-10-26-sidewalk-labs-ann-cavoukian-smart-city.html (discussing privacy issues with Google’s smart city attempts, as well as a Google expert consultant’s decision to leave her position after discovering the data collected would not be de-identified) [https://perma.cc/X4RP-K3YZ].
Question 9: Assess security risks from the PORT

a) Risks from unauthorized access

i. What are the risks from a hacker or other unauthorized person taking advantage of the PORT?

1. What authentication is appropriate to the risk?
2. Besides authentication, are there any other steps (technical, administrative, etc.) that can be taken to mitigate these risks? To what extent are these steps consistent with the PORT’s possible requirements about “without hindrance”?

Authentication is an important feature in each case study.

1. Effective authentication is vital for financial services portability, in both the EU and United States, given the risk of an unauthorized person using a portability mechanism to steal from an account. Read-only access may be a technique to reduce unauthorized access from a PORT initiative. By providing a read-only access code to data aggregators, financial institutions may limit third parties to viewing account balances and histories, rather than being able to initiate funds transfers or modify important financial account information.

2. EU financial services. PSD2 explicitly requires “strong customer authentication” (“SCA”). The European Banking Association produced technical regulatory standards, and Member States were required to apply the resulting SCA measures within 18 months.

3. EU health care. The Cross-Border Healthcare Directive states that the eHealth Network’s objectives are to “support Member States in developing common identification and authentication measures to

---

273 See Strong Customer Authentication Requirement of PSD2 Comes Into Force, EUR. COMM’N (Sept. 13, 2019), https://ec.europa.eu/info/publications/190913-safer-payment-services_en [https://perma.cc/97A5-NUQQ]; see also PSD2, supra note 10, at art. 4 (“[S]trong customer authentication’ means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data[.]”).
274 See PSD2, supra note 10, at art. 115(4) (“By way of derogation from paragraph 2, Member States shall ensure the application of the security measures referred to in Articles 65, 66, 67 and 97 from 18 months after the date of entry into force of the regulatory technical standards referred to in Article 98.”).
facilitate transferability of data in cross-border healthcare.” It appears that standardized authentication has been difficult to develop.

4. For **U.S. health care**, the certification requirements under the rule require the authentication protections of SMART Health IT, including regular re-authorization required through the use of “refresh tokens.”

5. For **phone number portability**, new phone service has often occurred in the United States by in-person visits to retail stores, often involving contracts that require a driver’s license or other effective identification. These practices have likely reduced the authentication/security risks from phone number portability.

6. **U.S. automobile dealers.** Authentication has been a significant area of disagreement in this case study. DMS providers have instituted policies that allow Dealers to issue credentials to their employees, but not to certain software providers. DMS providers have claimed cybersecurity risks from software providers selected by the Dealers, who could access the DMS with dealer-provided credentials. PORT proponents have responded that Dealers should be able to authorize access to Dealer Data for both employees and software providers, and that authorizing software providers does not increase cybersecurity risk. The Arizona statute requires a DMS provider to grant access to a software provider authorized by the Dealer, if the provider meets the requirements of an automobile industry cybersecurity standard.

**b) Risks from insecure transmission of data.** Once authentication is complete, what are the risks arising during transmission to the authorized recipient?

---

276 *Best Practices in Authorization for SMART on FHIR EHRs, SMART Health IT*, https://docs.smarthealthit.org/authorization/best-practices/ [https://perma.cc/L5AY-MU6L] (last visited Mar. 10, 2020); see *Overview: What is a Refresh Token, OKTA* https://developer.okta.com/docs/guides/refresh-tokens/overview/ (“A refresh token is a special token that is used to generate additional access tokens. This allows you to have short-lived access tokens without having to collect credentials every time one expires. You request this token alongside the access and/or ID tokens as part of a user's initial authentication flow.”) [https://perma.cc/85XD-FWJK] (last visited July 7, 2020).
278 See id.
279 See id.
280 *ARIZ. REV. STAT.* § 28-4653(B) (2019). The requirement is for the entity accessing the data be “compliant with the Star Standards or other generally accepted standards that are at least as comprehensive as the Star Standards.” *Id.*
i. Is there effective encryption in transit, such as through a secure Application Programming Interface?

ii. Are there other security risks that can be better managed, arising from the method of transmission, such as the means for transferring credentials or other sensitive data?

Every PORT initiative has to address the issues of how, at a technical level, to transfer data from the data controller to the data recipient. For each initiative, there will need to be a technical mechanism for transfer, an assessment of its costs, and the question of how secure the transfer is. For data in transit, effective encryption reduces the possibility of unauthorized parties gaining access to the data. To implement encryption effectively, there may be other security risks to manage, including how credentials or other sensitive data are distributed. Security and cost are important considerations in crafting interoperability standards or other mechanisms for transfers.

My research to date has focused on portability (transfers of data about one person) and other required transfers (transfers about more than one person), rather than interoperability, which is defined as “the ability of two or more systems or components to exchange information and to use the information that has been exchanged.”

Defining the conditions for when technical interoperability efforts will be successful has largely been beyond the scope of the research to date. Some interoperability issues, such as for APIs, are discussed in detail in the case studies; additional factors would need to be considered, however, to generalize about when efforts to craft technical standards for PORTability are likely to succeed.

1. U.S. health care. HHS extensively seeks to define standards to improve interoperability for electronic health information. The creation of such standards in the EU health care sector has been far slower than proponents have wished.

---


2. **U.S. financial services.** The CFPB has not issued regulations, authorized under Dodd-Frank, for “standardized formats for data,”\(^{283}\) although in 2020 it released an advanced notice of proposed rulemaking.

3. **EU financial services.** Implementation of APIs has been a major issue in the implementation of PSD2.
   a. The text of PSD2 has only one passing reference in a recital to “online interfaces” which “provide the payment service user with aggregated online information on one or more payment accounts held with one or more other payment service providers.”\(^{284}\) PSD2 itself does not provide detailed requirements for the APIs to achieve the collaboration and resulting market entry which it foresees.
   b. By contrast, when the UK implemented PSD2, its Open Banking requirements mandated specific standards for APIs, for the nine leading banking institutions, as well as licensing by the Financial Conduct Authority for third parties using the APIs.\(^{285}\)
   c. The trade press has reported: “Many European banks have continued to drag their heels on their PSD2 implementation, causing huge frustration across the fintech community which has been holding its breath for the quality APIs they need for their cutting-edge open banking innovations to work.”\(^{286}\)

4. **U.S. health care.** Under the HHS Rule, a health IT developer “must publish APIs and must allow health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs.”\(^{287}\)

5. **U.S. automobile dealer data.** The Arizona statute requires a DMS provider to “adopt and make a standardized framework for the exchange” of Dealer

---

\(^{283}\) Dodd-Frank Act, 12 U.S.C. § 5533(d) (2020) (“The Bureau, by rule, shall prescribe standards applicable to covered persons to promote the development and use of standardized formats for information, including through the use of machine readable files, to be made available to consumers under this section.”).

\(^{284}\) See PSD2, supra note 10, at recital 28.

\(^{285}\) In the UK, the Open Banking API standard from the CMA Open Banking Implementation Entity (“OBIE”) has been adopted by most banks. See API Specifications, OPEN BANKING, https://standards.openbanking.org.uk/api-specifications/ [https://perma.cc/7EJG-3Z7Y] (last visited July 20, 2020).


\(^{287}\) 21st Century Cures Act, § 170.404 (2020).
Data, and to “provide access to open Application Programming Interfaces to authorized integrators.”

6. **Phone portability.** In contrast to EU financial services, the HHS Rule, and the Arizona statute, U.S. phone portability has a different model for transfer of the data. Portability exists through a centralized entity, the Number Portability Administration Center.

   a. Each participating carrier thus has the relatively simple task of connecting securely to one entity.
   b. The other PORTability initiatives, by contrast, rely on an open API approach, where each entity is supposed to be able to interact with each other entity.
   c. The NPAC approach is simpler to scale – the number of connections goes up arithmetically (add one for each new entity). The open API approach can be much harder to scale, because the number of possible combinations of sending/receiving entities goes up geometrically (the number of connections for each new entity rises rapidly).
   d. The open API approach can succeed, however, if the interoperability standards operate effectively, so that each new entity can successfully interoperate at low cost with each of the entities already in the system.

c) **Does the PORT reveal any information that assists hackers or other unauthorized access?** For instance, are sources and methods of system security or surveillance compromised? Does the PORT make visible other data that was previously hidden or obscure, in ways that assist unauthorized access?

PORT initiatives, fundamentally, open up data flows. There are multiple ways in which greater disclosure and opening up of data flows can increase cybersecurity risk. The existence and significance of these risks will vary in each case.

1. **Financial services** initiatives can provide bad actors with an increased number of attack points, especially because traditional banks often have relatively strict cybersecurity and regulatory programs. Some express the concern that, when non-banks are data recipients, attackers can use phishing, social engineering or other attacks against the non-

---

288 ARIZ. REV. STAT. § 28-4654(A)(1)-(2).
bank, which may be a smaller company than the bank, and may lack the same cybersecurity protections.\textsuperscript{290} Similarly, attackers may be able to target devices such as laptops, tablets and phones that store consumers’ credentials for non-banks, which may result in privacy invasions or theft from an account.

2. \textbf{Open Data} initiatives, or other PORTability initiatives, may reveal vulnerabilities that malicious actors could exploit. There are complex arguments about when and whether there can be “security through obscurity.”\textsuperscript{291} Opening up databases can, however, lead to a greater likelihood of attack on the databases. Opening up databases can also reveal non-cyber vulnerabilities, as illustrated by the limits on information disclosure under the Environmental Protection Agency’s “Worst-Case Scenario” database.\textsuperscript{292}

3. In \textbf{Open Data} projects, there has been concern that the databases may increase the attack surface of the government agency hosting the database, including the possibility of running executable code when interacting with the database.

Mandatory openness can also pose risks to sources and methods of system security or surveillance. Public disclosure about government intelligence activities, for instance, has historically been strictly limited, to protect sources and methods and for other reasons.\textsuperscript{293}

\begin{footnotesize}


\textsuperscript{292} \textit{EPA Issues Worst Case Scenario Regulations}, \textit{COMPETITIVE ENTER. INST.} (Apr. 26, 2000), https://cei.org/content/epa-issues-worst-case-scenario-regulations [https://perma.cc/3CFL-T2RY]. The database at issue under those regulations revealed where dangerous chemicals were stored or used, potentially enabling “terrorist or other criminals to conduct attacks that would cause the largest number of deaths.” \textit{Id.}

\end{footnotesize}
d) To what extent do the steps taken to prevent unauthorized access, such as stronger authentication requirements, impede the goals of the PORT initiative?

1. For U.S. financial services, the Consumer Financial Protection Bureau has not issued regulations, permitted under the statute, for “standardized formats for data, to facilitate interoperability.” Critics have cited the lack of regulations for slow adoption of effective portability in practice. On the other hand, the case study on EU financial services has shown slow adoption, including extensions of deadlines for adoption, even where regulations are in place.

2. For U.S. automobile dealers, the DMS providers have stated that cybersecurity reasons justify blocking authentication and use of APIs by software providers.

Question 10: Assess risks from the PORT that may arise for either security and privacy

a) Onward transfer: risks from access following authorized PORTing
   i. The concern is that once data is transferred from the controller to the recipient, there may be security or privacy risks arising after transfer to the recipient of the data.
   ii. To what extent is there notice about, and consent by, the data subject for privacy and security risks after transfer to the recipient? For instance, if the transfer is from a controller under stricter legal rules, to a recipient with less strict rules, is the data subject notified and does the data subject provide consent to any increased risk?
   iii. Would the goals of the PORT be met by transfer of pseudonymous or de-identified data? Are there other technical, administrative or other steps that can mitigate risk once data is transferred to the recipient?

---

iv. To what extent are the goals of the PORT initiative impeded by steps taken to reduce risks from access following authorized porting?

The risks of “onward transfer” are well known under EU data protection and other privacy-related regimes. For instance, Standard Contractual Clauses and the EU/U.S. Privacy Shield both require protections in the event of onward transfers.

Onward transfer commonly requires cybersecurity protections. For instance, under the HIPAA Security Rule a contractor must appropriately safeguard the data. The rule also requires that any sub-contractor similarly must safeguard the data, and so on for sub-sub-contractors. This sort of cybersecurity requirement of protection, in the event of onward transfer, is very common across sectors.

1. For U.S. health care, there is an important onward transfer issue because data often goes from a highly regulated entity (covered by

---

297 An “onward transfer” is “[a] transfer of personal data to a fourth party or beyond. For instance, the first party is the data subject, the second party is the controller, the third party is the processor, and the fourth party is a sub-contractor of the processor.” Onward transfer includes transfers to the fourth or subsequent party. Onward Transfer, IAPP, https://iapp.org/resources/article/onward-transfer/ (last visited July 20, 2020).


301 See, e.g., GLBA, 12 C.F.R. § 216.1; GDPR art. 26.
HIPAA) to a less-regulated entity (not covered by HIPAA).\textsuperscript{302} The new HHS rule does not require a change to the notice provided to patients under HIPAA, despite the new onward transfers authorized by, and encouraged by, the new HHS rule.\textsuperscript{303} This lack of notice to individuals has been the subject of criticism about the new HHS rule, and the alleged lack of strict privacy protections when personal data goes to smartphone apps and other recipients of data has also been criticized.\textsuperscript{304}

2. U.S. financial services. There have been press accounts of fintech companies, such as Yodlee, allegedly making de-identified data available to its business customers.\textsuperscript{305} This sort of database is subject to possible re-identification by the business customers, which is a privacy risk, as discussed above. It is also an example of an onward transfer problem: business customers may be able to violate a data subject’s privacy when they receive supposedly de-identified data from the original data recipient (Yodlee).

3. U.S. automobile dealer data. In contrast, under the Arizona statute, a software provider cannot authorize onward transfer without prior written consent of the Dealer.\textsuperscript{306}

4. Similarly, under GDPR, when a data subject authorizes portability to a data recipient, that recipient cannot generally make an onward transfer except with a data subject’s consent.\textsuperscript{307}

\textsuperscript{302}U.S. DEP’T HEALTH AND HUMAN SERVS., EXAMINING OVERSIGHT OF THE PRIVACY & SECURITY OF HEALTH DATA COLLECTED BY ENTITIES NOT REGULATED BY HIPAA 1, 6 (June 17, 2016), https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf [https://perma.cc/7KWA-BF9L]. The U.S. Health Care case study illustrates the privacy and security risks when data is transferred from a highly regulated entity (under HIPAA) to less-regulated entities (under the vague “unfair and deceptive practices” protections of the FTC Act).

\textsuperscript{303}See Final Rule, supra note 8, §§ 170, 171.

\textsuperscript{304}U.S. DEP’T HEALTH AND HUMAN SERVS., supra note 302, at 20–30.


\textsuperscript{306}ARIZ. REV. STAT. § 28-4654 (2019).

b) Fair, reasonable, and non-discriminatory (FRAND) terms for security and privacy

i. To what extent, if any, are security requirements different in their application to the controller initially holding the data than for the recipient of the PORT? Are such differences justified on security grounds, or do they appear to unfairly discriminate against transfers to the recipient?

ii. To what extent, if any, are privacy requirements different in their application to the controller initially holding the data than for the recipient of the PORT? Are such differences justified on privacy grounds, or do they appear to unfairly discriminate against transfers to the recipient?

This question addresses the tension between two goals: (i) ensuring that privacy and security are protected; and (ii) protecting against the possibility that privacy or cybersecurity may be used as a pretext for failing to provide PORTability.

To address the risk of pretext, several case studies have implemented some version of FRAND, the requirement that provisions that block PORTability be “fair, reasonable, and non-discriminatory.” The term “FRAND” emerges from patent licensing, where there is (1) a standard setting organization; (2) the standards apply to Standard Essential Patents; and (3) the terms must be FRAND. Applied to a PORT initiative, the principle of FRAND can apply (1) to the controller (the origin of the PORT), for (2) data covered by the PORT requirement, where (3) the terms would be FRAND. There is no general requirement in the law that all PORTability initiatives include a FRAND requirement, but the concept has been prominent in multiple PORT initiatives.

1. EU financial services. Concerns about discriminatory and possibly pretextual arguments about cybersecurity have been prominent in development of PSD2.³⁰⁹

³⁰⁹ See PSD2, art. 35(1) (“Member States shall ensure that the rules on access of authorised or registered payment service providers that are legal persons to payment systems are objective, non-discriminatory and proportionate and that they do not inhibit access more than is necessary to safeguard against specific risks such as settlement risk, operational risk
o PSD1 granted access to payment systems for authorized or registered payment service providers on an “objective, non-discriminatory and proportionate” basis, which is similar to the terms “fair, reasonable, and non-discriminatory” used in patent and other settings.\footnote{310}{See\ Ménière, supra note 308.}


\footnote{312}{Id.}

Allegations included that the EPC had justified its standardization process for secure online transactions on cybersecurity grounds, but that the standards in fact discriminated against players that were not controlled by a bank.\footnote{312}{See Press Release, Eur. Comm’n, Antitrust: Commission closes investigation of EPC but continues monitoring online payments market (June 13, 2013), https://europa.eu/rapid/press-release_MEMO-13-553_en.htm [https://perma.cc/LPA7-ADDZ].}

o The European Commission closed its investigation after the EPC stopped developing its project in such a way as to exclude new entrants not linked to a bank.\footnote{313}{See Final Rule, supra note 8, §§ 170, 171.}

2. The HHS rule contains a FRAND requirement as part of a broader set of rules that encourage PORTability and seek to prohibit the controller from creating barriers to information sharing. The rule: (1) requires software licenses by health IT providers to be offered on “reasonable and non-discriminatory terms”; (2) prohibits a health IT developer from charging customers a fee that exceeds the developer’s actual costs to provide interfaces or other technical interoperability services; and (3) prohibits a health IT developer from restricting communications about its products, including criticisms of the products, for topics such as usability, security, and user experiences.\footnote{314}{See Final Rule, supra note 8, §§ 170, 171.}

and business risk and to protect the financial and operational stability of the payment system. Payment systems shall not impose on payment service providers, on payment service users or on other payment systems any of the following requirements: (a) restrictive rule on effective participation in other payment systems; (b) rule which discriminates between authorised payment service providers or between registered payment service providers in relation to the rights, obligations and entitlements of participants; (c) restriction on the basis of institutional status.”).
3. For U.S. health care, in addition to prohibiting discrimination, the information blocking prohibitions have exceptions for security and privacy, but the exceptions are limited fairly carefully.\(^{315}\)
   a. For security, an entity can block the flow of Electronic Health Information ("EHI") in defined circumstances, if the practice is directly related to safeguarding the confidentiality, integrity or availability of EHI.\(^{316}\) The block, to be lawful, must be performed in a consistent, non-discriminatory manner, and undertaken pursuant to an organization policy or principled case-by-case determination.\(^{317}\)
   b. For privacy, in response to criticisms of the proposed rule, HHS somewhat expanded the privacy exception to the prohibition on information blocking. For privacy protections that go beyond the exception, HHS enforcement is still possible on the grounds that the alleged privacy protection constitutes prohibited information blocking.\(^{318}\)

4. The Arizona auto dealer law exhibits a similar concern that the DMS provider, as controller, may use security as an excuse not to share Dealer Data.
   a. Section 28-4652 broadly states that a Dealer can transfer data to its chosen software providers “through any widely acceptable electronic file format or protocol that complies with [the auto industry] Star Standards or other generally accepted standards that are at least as comprehensive as the Star Standards.”\(^{319}\)
   b. In addition, the statute prohibits a DMS provider from placing an “unreasonable limitation” on access by the chosen software providers.\(^{320}\)
   c. Similar to the HHS rule, the Arizona statute limits the fees that the controller can charge for transfer, roughly to actual costs.

5. The FFD Regulation addressed barriers to users switching from one service provider to another, “not least upon termination of their contract with a services provider.”\(^{321}\)
   a. The principles document issued with the first two codes stated: “Stakeholders have the right to reuse data under fair,
reasonably and non-discriminatory terms, with well-defined and duly justified restrictions.\textsuperscript{322}

In conclusion, this Article emphasizes that FRAND has been a prominent feature of recent PORT initiatives, and perhaps could be characterized as an emerging “norm” for PORT initiatives. To the extent that a controller does discriminate in favor of its own activities, concerning security and privacy requirements, there may be criticism for the failure to observe the norm of FRAND.

**Question 11: Assess risks to competition from the PORT**

a) Do the costs or burdens of compliance with the PORT’s requirements create a barrier to entry or competitive advantage for incumbents?

b) Are there any competitive risks from established incumbents designing the standards for the PORT to favor incumbents? Are the PORT’s standards open and non-discriminatory?

c) In practice does the PORT’s functionality discriminate in favor of affiliates of entrenched incumbents? For instance, is pricing data subject to the PORT, enabling incumbents to benefit from that pricing data? Have incumbents used porting to extend their dominance to related applications or properties?

d) What steps can be taken to mitigate any such risks to competition?

e) To what extent do such risks to competition impede the goals of the PORT initiative?

The general point of Question 11 is simple. Question 1 highlighted the possible benefits to competition from a PORTability initiative. Question 11 notes there can be possible risks to competition as well.

The case studies in general did not highlight risks to competition from PORT initiatives. The main exception was that the HHS proposed rule mandated the disclosure of pricing information. The FTC and commenters noted the potential anticompetitive effects of this requirement.\textsuperscript{323} The final

\textsuperscript{322} Finland’s Presidency of the Council of the European Union, Principles for a Human-Centric, Thriving and Balanced Data Economy 3 (2019), https://api.hankeikkuna.fi/asiakirjat/2d0f4123-e651-4874-960d-5cc3fac319b6/1f6b3855-fe1d-4ea6-8636-0b8d4a1d6519/RAPORTTI_20191123084411.pdf [https://perma.cc/M32C-NBK7]; see Switching & Porting, SWIPO (SWIPO stands for “Switching Cloud Providers and Porting Data”), https://swipo.eu/ (setting standards for switching cloud providers) (last visited July 20, 2020) [https://perma.cc/Q4XF-NETC].

\textsuperscript{323} See Final Rule, supra note 8, §§ 170, 171. The FTC’s comments to the Proposed Rule called for clarification of “when market pricing is not deemed information blocking” and for leniency when applying exceptions to market pricing information. FTC, Comment Letter
HHS rule changed, and “does not expressly include or exclude price information.”

The possible risks to competition arise especially when one established incumbent, or a group of established incumbents, creates the mechanisms for data transfer. One classic example is if a monopolist favors its own product in an official standards process. Any such risks to competition would also need to be managed in a PORTability initiative such as the Data Transfer Project.

**Question 12: Assess regulatory or legal risks of the initiative**

a) As a result of the PORT, would consumers suffer any legal risks, such as reduced coverage of consumer protection laws?

- For U.S. financial services, Regulation E, which implements the Electronic Funds Transfer Act, provides that consumers generally are not liable for unauthorized electronic fund transfers. Regulation E applies to banks but appears not to generally apply to fintech software providers. It appears that consumers lose the protections of Regulation E when the unauthorized person gains access to the bank account via fintech software.
• For U.S. health care, the portability requirements may shift patient data from an entity covered by the HIPAA privacy rule to other entities that are outside of HIPAA.329

• For EU financial services, the case study illustrates the possibility of non-uniform implementation of PORT requirements. Although all Member States were required to transpose PSD2 into national law,330 in some Member States, there may be a distinction in practice between the theoretical legal position and reality on the ground.331 In other words, PSD2 may aim to expand the relevant geographic market to a single European payments area, but the risk in doing so may be exposure in more strictly-protected jurisdictions to less well-regulated EU Member States or those subject to ongoing proceedings about the application of the rule of law.332

that transfers by that person are no longer authorized. *Id.* § 1005.2(m) cmt. 2. The aggregator might be liable under Regulation E, but only if it allows consumers to transfer funds through the aggregator. *Id.*


331 The European Commission has published all of the national transposition measures for PSD2 by each EU Member State, including the UK, which had to be in place by January 13, 2018. *See Document 32015L2366, EUR-LEX, https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32015L2366 [https://perma.cc/W64L-BNMM] (last visited July 22, 2020). The European Commission then verifies the “completeness and correctness of the transposition of EU law into national law as formally notified to it by the member states.” *Id.*

For EU health care, Article 9(4) of the GDPR specifically permits individual Member States to introduce further conditions and limitations with regard to health data. 333 Although there are potential privacy benefits due to such additional protections, differing national laws can be an obstacle to the goals of PORTability, including the ability of citizens in one Member State to readily receive health care when in a different Member State.

b) Would any other actors suffer any legal risks? Specifically, would the PORT affect the protection of trade secrets, copyright, or other intellectual property rights?

• For U.S. healthcare, the large incumbent Epic Systems Corporation supported the overall objective of the rule, but commented that the rule “eliminat[ed] standard intellectual property protections.” 334
• For the Arizona auto dealer statute, DMS providers CDK and Reynolds have objected to what they assert is a loss of their intellectual property protections due to the mandatory PORT requirements. 335
• Professor Inge Graef has written about the intersection of EU intellectual property law and data portability. 336

Question 13: Assess any other significant costs or risks from portability, including obstacles to adoption

a) Are there any other significant costs or risks from the PORT? For instance, one obstacle to adoption of a PORT can be the expense and time required to create standards for implementing the PORT.

b) To what extent can such costs or risks be mitigated, such as by altering the design of the PORT initiative?


333 GDPR, art. 9(4).


Question 13 states that the PORT-IA should assess the costs of creating a proposed PORT, to the extent such costs or risks have not been explicitly considered in response to other questions.

**Question 14: Assess incentives for those presenting evidence of risks or costs**

a) What parties have an economic or other incentive to oppose the PORT? Explain the incentives. Assess the asserted risks in light of the incentives of some actors to oppose the initiative. Just because a party has an economic interest to support or oppose an initiative does not mean the facts it cites are incorrect; however, assess the evidence opposing the initiative in light of possible bias. Where available, identify evidence based on sources that are as objective as possible.

- For **EU financial services**, the public comments on PSD2 split depending on industry sector. Banks and card networks often argued that the PORT should be left to the market rather than regulation, whereas merchants supported the regulation of the card networks’ multi-lateral interchange fees. Consumer groups also supported regulation. These comments illustrate the importance of taking the financial interests of the commenter into account when assessing the evidence for and against a PORT initiative.
- **U.S. automobile dealer data.** CDK and Reynolds face significant damages in the automobile antitrust lawsuits, and therefore have an incentive to claim that security and privacy risks from the PORT are high.

**VI. CONCLUSION**

---


338 Id.

This article seeks to reduce the intellectual confusion about initiatives that have previously been lumped together under terms including “portability,” “inter-operability,” and “data sharing.” Along with providing new terminology, this article provides an intellectual framework for assessing PORTability that is agnostic—due to the wide range of possible factual settings, there is no prior assumption about whether a PORTability initiative will have net benefits. As shown in Part V, the case studies have shaped the Structured Questions in the PORT-IA, and the current version of the Structured Questions have been validated by being tested against case studies across diverse sectors, data type, and geography.

One result of the research project may be to assist single-issue regulators, such as competition or privacy authorities, to recognize the legal and policy considerations that may arise from other disciplines.\(^\text{340}\) For instance, an antitrust enforcer may become more aware of cybersecurity risks from insecure log-ins; even though the right to data portability is intended to be “without hindrance,” there should be enough hindrance to ensure that the person requesting the data is who they say they are. Privacy regulators may also benefit from considering the multiple effects of a PORT initiative, some of which may provide substantial benefits to consumers (“data subjects” in privacy terms). For example, the GDPR requires consent to be “freely given, specific, informed and unambiguous.”\(^\text{341}\) In some settings, such as consent by employees, regulators presume that consent is not valid due to concern about employer power.\(^\text{342}\) By contrast, where a PORT-IA shows strong benefits to individuals, and an individual has agreed to the transfer, then the presumption in favor of valid consent could be stronger. More generally, overall policy prescriptions or enforcement actions should be based on the multiple legal rules and policy goals at stake. As another example, before a court issues an order requiring PORTability in an antitrust case, there should be consideration of possible security, privacy, or other harms from such an order.

In conclusion, my hope is that this research project will promote a more informed discussion of PORT initiatives, including in public policy and by companies considering a PORTability service. Such initiatives implicate multiple disciplines including competition, privacy, and cybersecurity. The assessment of such initiatives should be similarly multi-disciplinary.


\(^\text{341}\) GDPR, Art. 4(11).

\(^\text{342}\) Art. 29 Data Protection Working Party, Guidelines on Consent under Regulation 2016/679 at 8, (Nov. 28, 2017) (“Given the imbalance of power between an employer and its staff members, employees can only give free consent in exceptional circumstances.”).
APPENDIX 1: U.S. FINANCIAL SERVICES: PORT – IA

1. DESCRIPTION OF PORTABILITY OR OTHER REQUIRED TRANSFER (PORT) INITIATIVE

1.1. Origination. Consumer financial services providers, notably banks.

1.2. Destination. Consumers and their financial technology (“fintech”) providers, such as Mint and Quicken.344

1.3. Types of Data. Along with other use cases, consumers can use the fintech software to consolidate their multiple accounts into one place, for budgeting or other personal financial purposes.

1.4. Applicable Law. Section 1033 of the Dodd Frank Act requires consumer access to financial information, in an electronic form usable by consumers. “Covered persons” are those “offering or providing a consumer financial product or service.”345 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.”346 The Consumer Financial Protection Bureau (“CFPB”) has the authority to issue rules for “standardized formats for information,”347 and announced in October, 2020 an Advance Notice of Proposed Rulemaking on Consumer Access to Financial Records. This notice outlined various use cases for consumer-authorized financial data such as “personal financial management, making and receiving payments, assisting consumers with improving savings outcomes, underwriting credit, and many other services.” 348

343 Thanks to Deona Kalala for research assistance on this case study.
346 Id. § 5533(a).
347 Id. § 5533(d).
2. BENEFITS OF PORT INITIATIVE

2.1. User autonomy and control over information. User control has been an important rationale for requiring financial services firms to provide users with access to their financial information, including in “an electronic form usable by consumers.” Indeed, the CFPB published nonbinding principles in October 2017 that expressed a vision of consumers “enhance[ing] their financial lives when they control information regarding their accounts or use of financial services.” Treasury shared the goal of ensuring consumers have access to clear disclosures that allow users to easily “weigh the risks and benefits of using a fintech application” and determine whether to enable or revoke a right to access their financial data.

2.2. Competition. Proponents have emphasized the possible benefits to competition from the PORT requirements. The initiative in

352 CONSUMER FIN. PROT. BUREAU, CONSUMER-AUTHORIZED FINANCIAL DATA SHARING AND AGGREGATION 4 (Oct. 18, 2017),
particular may reduce lock-in effects. There are often high perceived or actual costs for consumers to switch financial institutions, and the PORT requirement would make such switching easier. The PORT requirement may reduce barriers to entry. By contrast, network effects and high market share have not been important competition-based rationales for the PORT requirements.

Competitive realities in the marketplace indicate substantial competition in the financial services industry within the United States. For example, JPMorgan Chase Bank, which is the largest


354 Reduced information barriers enable customers to more easily move from one financial services provider to another and access custom financial products and services. It also eases the path for new market entrants that seek to provide innovative financial services products. See, e.g., COMPETITION & MKTS. AUTHORITY (CMA), MAKING BANKS WORK HARDER FOR YOU (2016), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/544942/overview-of-the-banking-retail-market.pdf (“Ensuring that consumers can provide third parties with access to information about the services and products provided to them would help to remedy the regulatory and structural barriers that prevent many consumer financial services markets from responding to consumer demand.”)

U.S. provider of consumer services, has roughly a 10% market share for domestic deposits.356

2.3. **Innovation.** Proponents have emphasized how portability may lead to innovation, such as by facilitating entry of a broader range of fintech companies who can compete with traditional banks.357 Proponents also note that increased access to financial data flows can improve access to lending products.358

2.4. **Technical obstacles to portability.** In the absence of regulations from the CFPB for “standardized formats for data,” there have been technical and market obstacles to efficient sharing of consumer data, reducing the possible benefits from the PORT initiative.359 For instance, PNC Bank in 2019 announced it would not allow access to

---


357 Professor Barr notes, “As a drafter of the provision that became §1033, I can state that the scope of the provision was intended to be broad – providing a framework for customer access that would encourage competition and innovation, including through the use of third-party providers and aggregators. The Treasury Department has taken a similar view.” See U.S. DEPT. OF TREASURY, supra note 7. Both Citi and American Express announced investments in data aggregator Plaid (joining Goldman Sachs), citing the goal of “better access to clean, high-quality financial data, enabling innovation and a secure infrastructure for the financial services ecosystem.” *Plaid Unveils Investments by Citi Ventures and American Express Ventures*, PLAID (Feb. 6, 2017), http://www.prnewswire.com/news-releases/plaid-unveils-investments-by-citi-ventures-and-american-express-ventures-300402531.html [https://perma.cc/AC6S-V9ZA].


consumer accounts by third-party software providers, citing security concerns.\textsuperscript{360}

3. RISKS AND COSTS OF PORT INITIATIVE

3.1. Security. Providing effective security has been a major obstacle to adoption of ready portability between financial services providers: (1) The risks of unauthorized access are high, including access to highly sensitive financial information and also the possibility of actually stealing funds from the account.\textsuperscript{361} (2) In the absence of “standardized formats for data,” there are cybersecurity risks from the most common mechanism for data sharing, which is screen-scraping.\textsuperscript{362} Strong authentication is vital to preventing unauthorized persons from gaining access to consumer financial accounts.\textsuperscript{363}

3.2. Privacy. (1) There are high risks to privacy if an unauthorized person can gain access to personal data in a financial account. Among other privacy risks, the individual may face a higher risk of identity fraud when an unauthorized person learns the Social Security number and other financial details that help enable such fraud. (2) There have been publicized concerns that transfers of de-identified data can create privacy risks, due to the risk of re-identification.\textsuperscript{364}


\textsuperscript{364} See Bradley Hope, \textit{Provider of Personal Finance Tools Tracks Bank Cards, Sells Data to Investors}, \textit{DEMOCRATIC UNDERGROUND} (Aug. 6, 2015, 10:30 PM), https://www.democraticunderground.com/10141169602 (explaining that Yodlee, an FSP that provides personal financial management tools by aggregating and processing consumer data from a number of different accounts, sells scrubbed and anonymized transactional data).
3.3. **Regulatory effects.** Regulation E, which implements the Electronic Funds Transfer Act, provides that consumers generally are not liable for unauthorized electronic fund transfers.\(^{365}\) Regulation E applies to banks but not generally to fintech software providers.\(^{366}\) The protections of Regulation E generally do not apply to transfers “by a person who was furnished the access device to the account by the consumer.”\(^{367}\) Consumers may thus lose the protections of Regulation E when the unauthorized person gains access to the bank account via fintech software.\(^{368}\) This regulation has grown in

[https://perma.cc/J7ZA-V7AL]. Such insights can be used to “re-identify” individuals; researchers from the Massachusetts Institute of Technology have said that they could unmask roughly 90% of people in a database of anonymous credit-card transactions with four pieces of information that included date and transaction location from a private database provided to them by an unidentified company. Yves-Alexandre de Montjoye, Laura Radaelli, Vivek Kumar Singh & Alex Pentland, *Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata*, 347 SCI. MAG. 536 (Jan. 30, 2015), https://science.sciencemag.org/content/347/6221/536 [https://perma.cc/T5TM-4HTJ]; see also Solon Barocas & Andrew Selbst, *Big Data’s Disparate Impact*, 104 CAL. L. REV. 671, 671 (2016) (“Errors…may befall historically disadvantaged groups at higher rates because they are less involved in the formal economy and its data-generating activities, have unequal access to and relatively less fluency in the technology necessary to engage online, or are less profitable customers or important constituents and therefore less interesting as targets of observation.”).

\(^{365}\) 12 C.F.R § 1005.6 (2020).


\(^{367}\) 12 C.F.R. §1005.2(m)(1).

\(^{368}\) An unauthorized electronic fund transfer is a transfer by someone other than the consumer without actual authority to make the transfer and from which the consumer receives no benefit. 12 C.F.R. § 1005.2(m). The term does not include transfers “by a person who was furnished the access device to the account by the consumer, unless the consumer has notified the financial institution that transfers by that person are no longer authorized.” *Id.* § 1005.2(m)(1). The Official Staff Commentary further explains that if the consumer furnishes an access device and grants authority to a person who exceeds that authority, the consumer is liable unless the consumer has notified the financial institution that transfers by that person are no longer authorized. *Id.* § 1005.2(m)(1). The aggregator might be liable under Regulation E, but only if it allows consumers to transfer funds through the aggregator. *Id.*
importance as data aggregators now hold data on over twenty million consumers accounts.369

3.4. Incentives of those presenting evidence. Incumbents, such as traditional banks, have a financial incentive to emphasize the risks to security and privacy if fintech software has access to bank account information.370

4. LESSONS LEARNED

4.1. This case study shows that the US has issued a general requirement of consumer access, along with a mandate that the information “shall be made available in an electronic form usable by consumers.” This approach contrasts with the much more detailed regulations under the Payment Services Directive in the EU.

4.2. This case study illustrates the reason for the PORT to include an assessment of regulatory effects. Regulation E applies to traditional banks but may not provide protection to the consumer if the loss occurs due to unauthorized transfers through use of a third-party fintech software provider.

4.3. This case study illustrates high security risks in the absence of strong authentication. Unauthorized access can result in disclosure of sensitive data, a large privacy risk. It can also result in theft of funds, potentially even including entire balances in multiple financial accounts.

4.4. The financial services PORT initiative provides bad actors with a number of attack points.371 For instance, they can obtain individuals’

371 “FinCEN has . . . seen a high amount of fraud, including automated clearing house (ACH) fraud, credit card fraud, and wire fraud, enabled through the use of synthetic
log-in credentials by posing as a financial services provider through phishing or social engineering attacks.\footnote{372} They also can target devices, such as laptops, tablets, and phones, that store consumers’ credentials.\footnote{373}

4.5. The CFPB has not issued regulations, as permitted under the statute, for “standardized formats for data.” Critics have cited this lack of regulations for slow adoption of effective portability in practice.\footnote{374} In October 2020, the CFPB issued an advanced notice of proposed rulemaking on consumer-authorized access to financial records.\footnote{375} In contrast, the case study on EU financial services has shown slow adoption, including extensions of deadlines for adoption, even where regulations are in place.

4.6. Better security mechanisms than screen scraping may be available. Many banks and fintech providers have created application programming interfaces (‘‘APIs’’) that no longer require consumers to provide actual log-in credentials to third-party software providers. Another option is increased use of two-factor authentication.

identities and through account takeovers via fintech platforms. In some cases, cybercriminals appear to be using fintech data aggregators and integrators to facilitate account takeovers and fraudulent wires. By using stolen data to create fraudulent accounts on fintech platforms, cybercriminals are able to exploit the platforms’ integration with various financial services to initiate seemingly legitimate financial activity while creating a degree of separation from traditional fraud detection efforts. Some criminals are also monetizing stolen credit card information through fraudulent merchant accounts to charge victims’ cards or are simply creating fraudulent user accounts on fintech platforms as part of identity theft or synthetic identity fraud.” Kenneth A. Blanco, Director, FinCEN, Identity: Attack Surface and a Key to Countering Illicit Finance, Address at the Federal Identity (FedID) Forum and Exposition (Sept. 24, 2019), in FIN. CRIMES ENFORCEMENT NETWORK, https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-federal-identity-fedid [https://perma.cc/W2PC-78H5].

\footnote{372} “Many customers value the convenience of financial data aggregation and appreciate having a single snapshot of multiple accounts. But sharing security credentials for financial account information can come with some risks. Foremost, you can potentially expose yourself to privacy and security risks. These include potential vulnerability to cyber fraud, unauthorized transactions and identity theft. A key risk is that the aggregators could be storing all consumer financial information or security credentials in one place, creating a new and heightened security risk for consumers.” Know Before You Share: Be Mindful of Data Aggregation Risks, Investor Alert, FINRA (Mar. 29, 2018), https://www.finra.org/investors/alerts/be-mindful-data-aggregation-risks [https://perma.cc/PG58-TFXS].

\footnote{374} Id.

\footnote{375} Barr et. al., supra note 359.

\footnote{376} CONSUMER FIN. PROT. BUREAU, supra note 130.
4.7. Privacy risks can occur due to fintech vendors’ practices. The FTC has sued peer-to-peer payment service provider Venmo under the FTC Act and the GLBA for misrepresentations regarding the steps necessary to keep financial transactions private. Additionally, there have been public complaints about fintech companies’ datasets that were supposedly de-identified but actually remained re-identifiable.

4.8. Providing read-only access to code may reduce risk from the PORT initiative. By providing read-only access to data aggregators, financial institutions could ensure third parties only view account balances and histories, rather than being able to initiate funds transfers or modify important financial account information.

---


377 See Swire & Lagos, supra note 20.
APPENDIX 2: U.S. HEALTH CARE: PORT–IA

1. DESCRIPTION OF PORTABILITY OR OTHER REQUIRED TRANSFER (PORT) INITIATIVES

Overview of Three PORT Initiatives in the 21st Century Cures Act Rulemaking Process

There are at least three, somewhat overlapping, PORT initiatives in the proposed and final rule implementing the 21st Century Cures Act (“the Act”). The three initiatives relate to: (a) prohibitions on information blocking; (b) health IT developer certification requirements; and (c) standardization of APIs.

The U.S. Department of Health and Human Services’ (HHS) Office of the National Coordinator for Health Information Technology (ONC) published its proposed rule for “Interoperability, Information Blocking, and the ONC Health IT Certification Program” on March 4, 2019. ONC’s stated purposes in implementing the Act are to: advance interoperability; support the access, exchange, and use of electronic health information (EHI); and address occurrences of information blocking. The final rule was first published by HHS on March 9, 2020, with over 1,200 pages of regulatory text and accompanying material.

---

378 Thanks to Deona Kalala and Sara Guercio for research assistance on this case study.
certification requirements will be fully effective by December 31, 2023. 383

The term “interoperability” is used broadly in the final rule to apply to: (1) technical interoperability (as I use the term generally in this overall PORT project); (2) portability, or transfers involving one person; and (3) other required transfers, such as when a health care provider transfers all of its records from one information technology (IT) vendor to another.

1.1. PORT Initiative A: Information Blocking

1.1.1. Origination: Any (1) health care provider; (2) health IT developers of certified health IT; (3) health information exchanges; or (4) health information network.

1.1.2. Destination: An authorized recipient where there is either (1) patient consent or (2) for treatment, payment, or operations of an entity covered by the Health Information Portability and Accountability Act (“HIPAA”). 384

1.1.3. Types of Data: The scope of covered data is broad, covering “electronic health information” (EHI), which corresponds to the electronic personal health information (PHI) covered by HIPAA. 385

1.1.4. Legal requirements: The Act prohibits information blocking as defined in section 171.103 of the Final Rule, subject to eight exceptions. Information blocking is any activity that “is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information.” 386 ONC can impose significant penalties for information blocking, unless one of the exceptions applies. The eight exceptions are divided into two categories. First are exceptions that enable not fulfilling requests

---


385 45 C.F.R. § 171.102 (“Electronic health information (EHI) is defined as it is in 45 CFR 160.103.”).

to access, exchange or use of EHI, including for (1) preventing harm; (2) promoting the privacy of EHI; (3) promoting the security of EHI; (4) responding to requests that are infeasible; and (5) maintaining and improving health IT performance.\textsuperscript{387} Second are exceptions for establishing procedures to fulfill requests to access, exchange or use of EHI, including for: (6) recovering costs reasonably incurred; (7) licensing of interoperability elements on reasonable and non-discriminatory terms; and (8) limiting the content of responses to requests and establishing the manner for fulfilling requests.\textsuperscript{388}

1.2. PORT Initiative B: Health IT Developer Certification Requirements

1.2.1. Origination: Software of a covered health IT developer.

1.2.2. Destination: (1) For an individual patient, to the patient or a patient’s chosen third party (portability for the individual patient); and (2) for all patients of a provider when the provider seeks to change health IT systems (transfer of data by the health provider from one IT provider to another).

1.2.3. Types of Data: Electronic health information. The export file must be computable and include documentation to allow for interpretation and use of EHI.

1.2.4. Legal requirements: Section 4002 of the Act requires HHS to establish “Conditions and Maintenance of Certifications Requirements for the ONC Health IT Certification Program.” ONC enforces any noncompliance. There are seven Conditions of Certification for health IT developers. Most relevant for purposes of this case study are: (1) information blocking and (2) application programming interfaces (APIs). Among the other requirements that apply to health IT developers is that the developer does not prohibit or restrict communications for specific subjects including: usability; interoperability; security; user experiences; business practices; and the manner in which a user of health IT has used such technology.\textsuperscript{389}

\textsuperscript{387} Id.
\textsuperscript{388} Id.
\textsuperscript{389} Anthony & Lipinski, supra note 132; 45 C.F.R. § 170.402.
1.3. PORT Initiative C: Standardized APIs

1.3.1. Origination: A health IT developer must “publish APIs that allow health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs.” For example, the API should enable export of the patient’s data from a health care provider to a smartphone app.

1.3.2. Destination: (1) For an individual patient, to the patient or a patient’s chosen third party (portability for the individual patient); and (2) for all patients of a provider when the provider seeks to change health IT systems (transfer of data by the health provider from one IT provider to another).

1.3.3. Types of data: A developer must provide access in the API to all data elements of a patient’s electronic health record (EHR), to the extent permitted by privacy law. The final rule defines the “United States Core Data for Interoperability,” which sets forth the extensive data elements required, including clinical notes.

1.3.4. Legal requirements: The Rule sets forth detailed requirements, including that: (1) the API be usable “without special effort” by users of the API; (2) a developer publish business and technical documentation to enable the API to be used at scale; (3) the developer grants the health care providers “the sole authority and autonomy to permit API Users to interact with the API technology,” and (4) the API be licensed on reasonable and non-discriminatory term with limits on fees.

2. BENEFITS OF PORT INITIATIVE

2.1. User autonomy and control over information. User autonomy and control apply both to individual patients and to companies in the health care system (e.g., health care providers). Patients have a broad right of access under Section 406 of the Act. The mandatory use of APIs is intended to enable a patient to port data where the patient wishes, including smartphone apps. The Act reinforces the HIPAA requirement that a patient must provide explicit authorization (opt-in consent) for many transfers of health information.

390 Final Rule, supra note 8, at 25,647.
391 Id. at 25,816.
392 Id. at 25,644.
393 Id. at 25,647.
2.2. Health care providers also gain new rights over the data they hold. Notably, a certified health IT software provider must enable transfer of a provider’s data “without special effort” to a competing IT software provider.\footnote{Id. at 25,644.}

2.3. \textbf{Competition}. The strict rules prohibiting information blocking are designed to enhance competition. Incumbent companies holding patient data must open up their systems to enable transfer “without special effort,” even to competitors. From HHS’s perspective, entities frequently exercised their control over EHI in ways that created barriers to entry for developers and other health care providers, limiting the availability and use of EHI.\footnote{Id.} Such practices can weaken competition among health care providers and health IT developers by limiting patient mobility, encouraging consolidation, and creating barriers to entry for developers of new and innovative applications and technologies that enable more effective uses of clinical data to improve population health and the patient experience.\footnote{Id.} The information blocking prohibition creates penalties and enforcement mechanisms to deter these harmful practices.

2.4. The final rule also seeks to prohibit rent-seeking and other opportunistic pricing practices, including by any dominant firm. For example, this includes: (1) requiring software licenses to be provided on “reasonable and non-discriminatory terms”;\footnote{Id. at 25,814.} (2) prohibiting a health IT developer from charging customers a fee that exceeds the developer’s actual costs to provide interfaces or other technical interoperability services;\footnote{Id. at 25,753.} and (3) prohibiting a health IT developer from restricting communications about its products, including criticisms of the products, for topics such as usability, security, and user experiences.\footnote{Id. at 25,732.}

2.5. \textbf{Innovation and research}. The information blocking requirements seek to encourage innovation and advancement in the access, exchange, and use of health IT-enabled care delivery. The prohibition on information blocking is designed to reduce the ability of incumbents to insist that local physicians adopt a particular EHR
platform.\textsuperscript{400} The mandatory APIs were designed to enable patients and others to take advantage of innovations like smartphone apps.\textsuperscript{401} HHS also believes that information transfers will benefit medical research.\textsuperscript{402}

2.6. Technical obstacles to portability. Because the final rule has not yet gone into effect, there is limited evidence about the extent to which there will be technical or market obstacles to the benefits sought under the new PORT initiatives. For instance, the European Union mandated open APIs under its Payment Services Directive, but there have been significant delays in adoption.\textsuperscript{403} The rule may impose administrative compliance burdens on health IT developers, EHR management, and other affected actors.

3. RISKS AND COSTS OF THE PORT INITIATIVE

3.1. Privacy. EHI often includes patients’ clinical data, in contrast to the claims-related data that were most important when HIPAA went into effect two decades ago. The broader range of patient data can lead to increased privacy risks. Patient data could be transferred beyond the scope of a patient’s consent or preferences. Patients also face privacy risks when data moves from entities covered by HIPAA (providers and insurers) to smartphone apps or other systems that are outside of the scope of HIPAA. Privacy advocates have expressed concern that the latter are covered only by the general protections of the Federal Trade Commission Act, rather than the more detailed and protective HIPAA requirements.\textsuperscript{404} There are also privacy concerns when large databases of patient data are transferred, including mandatory

\textsuperscript{400} Id. at 25,820.
\textsuperscript{401} Don Rucker, ONC’s Proposed Rule Will Connect People to their Care, HEALTH IT BUZZ (Feb. 11, 2019), https://www.healthit.gov/buzz-blog/interoperability/oncs-proposed-rule-will-connect-people-to-their-care [https://perma.cc/FX2G-Z2BT].
\textsuperscript{402} Final Rule, supra note 8 at 25,722-3; Kathy Kenyon, Overcoming Contractual Barriers to EHR Research, HEALTH AFF. BLOG (Oct.14, 2015), http://healthaffairs.org/blog/2015/10/14/overcoming-contractual-barriers-to-ehr-research/ [https://perma.cc/Q498-YCSF].
transfers expected under the information blocking requirements. Such databases face significant risk of re-identifying patient data.

3.2. To avoid penalties for information blocking, an actor can invoke the privacy exception if one of four sub-exceptions applies: (1) practices that satisfy preconditions prescribed by privacy laws; (2) certain practices not regulated by HIPAA but still implement privacy choice; (3) denial of access requests where specifically permitted by HIPAA; or (4) practices that give effect to an individual’s privacy preferences. Comments on the proposed rule criticized the privacy protection as inadequate.

3.3. The final rule did expand the privacy exception. For instance, the final rule states that actors may establish processes to notify a patient—before the patient transfers data to an app—whether the third-party app developer has attested to meeting certain “best practices” for privacy policies and practices. The final rule recommends that these best practices include terms such as: (1) making the privacy policy accessible at all times, including updated version; (2) sharing the privacy policy prior to the technology’s receipt of EHI; and (3) including a requirement for express consent before an individual’s EHI is accessed, exchanged, or used, as well as receiving the individual’s express consent before the individual’s EHI is sold.

3.4. Security. The Security of EHI exception allows Covered Health Care Providers to block the flow of EHI in defined circumstances if the practice is directly related to safeguarding the confidentiality, integrity or availability of EHI. To be lawful, the block must be performed in a consistent, non-discriminatory manner, and it must be undertaken pursuant to an organizational policy or principled case-by-case determination.

405 Anthony & Lipinski, supra note 132, at 32.


3.5. Unauthorized access is a risk for most PORT initiatives, including healthcare. The certification requirements under the Proposed Rule require the authentication protections of SMART Health IT,\(^{409}\) including regular re-authorization required through the use of refresh tokens.\(^{410}\)

3.6. As with privacy protections, patients may lose HIPAA legal protections when the PORT is made to an entity that operates outside of HIPAA coverage.\(^{411}\)

3.7. Competitive Effects. The proposed rule mandated the disclosure of pricing information.\(^{412}\) The FTC and over 1,000 other commenters noted potential anticompetitive effects associated with the open disclosure of pricing information.\(^{413}\) In a comparable proposal, the FTC identified two main anticompetitive effects associated with this type of information sharing.\(^{414}\) First, the disclosure of price and cost information “may chill competition by facilitating or increasing the


\(^{411}\) Rebecca Pifer, Industry Cheers Spirit But Not Fine Print In HHS Interoperability Rules, HEALTHCARE DIVE (June 5, 2019), https://www.healthcaredive.com/news/industry-cheers-spirit-but-not-fine-print-in-hhs-interoperability-rules/556099/ (last visited Nov. 12, 2021) (“Patients may be unaware that once they authorize a covered entity to push their health information to a third-party app and such an entity is a HIPAA non-covered entity, the rights afforded under HIPAA no longer apply.”) [https://perma.cc/6JLF-7FXF].

\(^{412}\) Final Rule, supra note 8, at 25,727.


likelihood of unlawful collusion.”415 Second, it may “undermine the effectiveness of selective contracting” that reduces health care costs.416 The definition of EHI under the final rule “does not expressly include or exclude price information.” 417 Instead, it generally provides that “to the extent that ePHI includes price information and is included in a designated record set, it would be considered EHI.”418

3.8. Incentives of interested parties. Due to their proprietary databases, private health care software companies, such as Epic Systems Corporation, have an incentive to object to the information blocking rule. Consistent with that incentive, Epic’s comments supported the rule’s overall objective, but complained that it “eliminated standard intellectual property protections” and “creates real risks that patients will actually lose control of their data.”419

4. LESSONS LEARNED

4.1. In addition to the patient portability rights, this case study illustrates a requirement that a software vendor make it easy for the vendor’s customer to switch to a different software vendor. These requirements are similar to the Arizona auto dealers case study and the Free Flow of Data Regulation in the EU. In these instances, incumbent software vendors may claim that the transfer requirements undermine intellectual property rights and threaten cybersecurity.

4.2. The Proposed Rule sets limits on how cybersecurity (or privacy) can be used as a basis for blocking information flows. The Proposed Rule requires relating an information blocking practice to specific means for safeguarding confidentiality, integrity, and availability of EHI. A purported security measure is illegal “information blocking” unless it is tailored to specific security risks and implemented in a consistent


416 Id.

417 21st Century Cures Act, supra note 413, at 631.

418 Id. at 631.

and non-discriminatory manner. Similar themes about the possibility of cybersecurity being used a pretext to block information flows arise in the Arizona auto dealers case study.

4.3. This case study illustrates the privacy and security risks when data is transferred from a highly-regulated entity (under HIPAA) to less-regulated entities (under the vaguer “unfair and deceptive practices” protections of the FTC Act).

4.4. As transfers of EHI occur to more recipients, there are risks to user trust. It is not clear how well patients understand where their patient data is going. How to manage patient consent may be a challenging task. If patients lose trust in how their data is protected, they may be reluctant to disclose fully to their medical providers. In addition, reduction in user trust can reduce consumer control over their data and reduce their autonomy; where users perceive risk in how their data will be used, they experience less control over their data.

4.5. This possible lack of consumer understanding and risk to trust can also arise in other case studies, such as consumer financial data flows to new categories of recipients.

4.6. This case study illustrates how transfer of pricing data may lead to anti-competitive effects and illustrates the difficulty of eliminating price information from the data contained in a PORT. The FTC’s concerns about transfer of pricing data and confidential terms of service show the importance of considering both the pro- and anti-competitive effects of a PORT initiative.
APPENDIX 3: U.S. OPEN DATA: PORT–IA

1. DESCRIPTION OF PORTABILITY OR OTHER REQUIRED TRANSFER (PORT) INITIATIVE

1.1. Open data refers to public sector data published online by local, state, and federal agencies for free public access. With open data, government agencies are required or encouraged to transfer data into publicly-available websites. This case study focuses specifically on the United States and on data that is not intended to be personally identifiable.

1.2. Origination: The data comes from public agencies. Previously, this data was in printed form or otherwise not readily available online. Some, such as court records, were accessible in person, but in a less convenient form than online access. Some were not available to the public or available only via a request under the Freedom of Information Act or similar state and local laws.

1.3. Destination: Publicly available websites.

1.4. Types of Data: Public sector data that may be published includes, for example, National Oceanographic and Atmospheric Administration weather data, government procurement data, transportation data, public health data, agricultural data, and de-identified population data. In addition to Data.Gov, more than 260 cities and municipalities have launched their own open data initiatives. Each individual U.S. state has also made data publicly available and accessible online to varying degrees.

420 Thanks to Raechel Bimmerle for research assistance on this case study.
422 See Whittington, supra note 145; Frederick Borgesius, Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework, 30 BERKELEY TECH. L.J. 2073, 2081 (2015); see also, e.g., STATE OF ILLINOIS DATA PORTAL, https://data.illinois.gov/ (last visited Nov. 12, 2021) [https://perma.cc/WS98-YMEF].
1.5. **Applicable law:** The federal Data.Gov portal launched in 2009, and it is governed by the OPEN Government Data Act, 44 U.S.C. § 3501. The OPEN Government Data Act requires “timely and equitable access to the agency’s public information.” However, each agency is left to interpret the meaning of “public information,” to design its own open data policy, and to decide which datasets to publish. These various state and local open data portals are governed by individual state and municipal laws, regulations, policies, terms of use, and privacy policies.

2. **BENEFITS OF PORT INITIATIVE**

2.1. **Commercial Innovation.** Open data proponents claim that the data enables innovative new market entrants, such as weather apps, traffic apps, restaurant health violation apps, and crime and safety apps. The availability of open data has spurred the creation of new financial industries including the weather derivative financial industry. Similarly, open GPS data has “led to a proliferation of commercial applications across industries and sectors, including agriculture, construction, transportation, aerospace and . . . everyday life.”

2.2. Open data initiatives have been promoted as spurring growth of new businesses in general. For example, New York’s Business Atlas is an open data project that provides neighborhood-level data to potential

---

428 44 U.S.C. § 3506(d)(1) (containing examples of statutory provisions concerning agency dissemination of public information).
430 See id.
431 Verhulst & Young, supra note 429.
432 Id.
small business owners. This data helps an entrepreneur determine where to open a new business location. The breadth of commercial applications making use of open data is documented in the Open Data Impact Map developed by the Center for Open Data Enterprise.

2.3. **Competition.** New entry, as described above, may spur increased competition. Proponents have discussed positive competitive effects for government procurement; one example is enabling new entrants to bid effectively. However, the magnitude of any such effect is unclear and appears to vary by program. Outside of the government procurement context, reduction of dominant firms’ market power has been at most a secondary rationale for open data initiatives.

2.4. **Research.** Open data contributes to scientific research areas including, but not limited to, medicine, environmental science, social sciences, computer science, and agricultural and biological sciences. National open data portals are cited in scientific research more frequently than local portals—likely because national portals tend to include more data sets. Beyond scientific research, open data has many other uses, such as for legal proceedings. For example, African-
American residents of Zanesville, Ohio successfully used a map derived from open data in a lawsuit to prove that the distribution of clean water in their town was racially inequitable.\textsuperscript{439}

2.5. \textbf{Other Possible Public Benefits}. Open data proponents have identified a range of public benefits. For example: (1) “opening up weather data through NOAA has significantly lowered the economic and human costs of weather-related damage through forecasts;”\textsuperscript{440} (2) opening Global Positioning System (GPS) data has “improved safety, emergency response times and environmental quality;”\textsuperscript{441} (3) the Opioid Mapping Initiative created a comprehensive map to address the opioid crisis, using police data, hospitalization data, and mortality reports, in addition to reports of revival using Naloxone and information about treatment facilities.\textsuperscript{442} Local governments use this map to inform the deployment of police and EMS responses. Another claimed benefit of open data is improved public trust, transparency, and accountability in government. Any such results, however, are difficult to measure.\textsuperscript{443}

2.6. \textbf{Market and Technical Obstacles to Realization of Open Data Benefits}. The purported benefits of open data are tempered by technical and practical barriers to adoption. First, there has been a disconnect between the supply of public sector data and the demand for that data. Agencies tend to publish data without regard to whether it is the type of data that is useful to businesses and individuals.\textsuperscript{444} Second, data sets are often published in a manner that can be accessed and analyzed manually but cannot be readily used by software

\textsuperscript{439} Verhulst & Young, supra note 429.
\textsuperscript{440} Id.
\textsuperscript{441} Id.
\textsuperscript{443} Julia Keseru, \textit{A new approach to measuring the impact of open data}, SUNLIGHT FOUND. (May 5, 2015), https://sunlightfoundation.com/2015/05/05/a-new-approach-to-measuring-the-impact-of-open-data/ [https://perma.cc/75M7-MU6Q].
programs. Fourth, open data initiatives require buy-in from internal stakeholders to be successful, and buy-in varies by the agency, department, and interest (or lack thereof) of management-level employees. Finally, once data is published, (and businesses begin to rely upon that data), data may not be updated in a complete and timely manner.

3. RISKS AND COSTS OF PORT INITIATIVE

3.1. Privacy. Privacy can be a significant factor in limiting the scope of open data initiatives. First, there is a privacy risk from public records about individuals that have historically been open to the public, but relatively difficult to access. For instance, the National Center for State Courts has held multiple conferences on issues of privacy and online access to court records. Due to privacy concerns, courts have amended their rules, such as requiring redaction of Social Security numbers and other sensitive information. Second, for identifiable records, there are sometimes privacy concerns about sub-categories of records. For instance, government employees have expressed privacy concerns because their employment data is technically “public information” and could be published unless excluded from publication by the applicable open data policy. Third, there may also be reasons to exempt certain populations from an open data initiative, such as address and other information about first responders or victims of crime and domestic violence.

3.2. A different type of privacy risk comes from datasets that are designed to be de-identified. For instance, GPS data may be de-identified before

---

446 Ruijer, supra note 444, at 15; see also Stephen Larrick, Why should cities have an open data policy?, SUNLIGHT FOUND., (Oct. 1, 2015), https://sunlightfoundation.com/2015/10/01/why-should-cities-have-an-open-data-policy/ [https://perma.cc/X7HJ-7URZ]; see also Kitchin, supra note 444.
449 Id.
450 Id. at 1915–17.
451 Id. at 1916.
it is published. An individual user, however, may repeatedly drive between home and work, making it relatively easy to re-identify location data. Faced with this risk, an open data initiative faces a trade-off between utility of the data (detail can make the data more useful) and privacy risk (detail can increase the likelihood of re-identification).

3.3. **Autonomy.** Many open data initiatives occur without an opt-in or opt-out by the individual person in the dataset. Because individuals have little autonomy in determining the data that is published, they have little means of mitigating their own individual privacy concerns and are ultimately reliant on the government agency to erect adequate privacy protections around the data that is released.

3.4. **Security.** Open data projects raise at least three cybersecurity concerns. First, malicious actors might use open data to disrupt municipal, state, or federal activities by studying and disrupting public services, including utilities and public transportation routes during peak usage times or along high-traffic routes. Seattle’s servers, for instance, “are regularly targeted by Chinese hackers and other international actors.” Next, if not implemented well, open data initiatives may expose the government web sites to greater risk of attack, such as when non-government users can run executable code on the government side to take advantage of open data. Third, open data initiatives may pose risks to data integrity. For instance, malicious actors can alter or remove data sets after publication or hack the open data portal and publish their own fraudulent data sets.

4. **LESSONS LEARNED**

4.1. Open data initiatives provide potentially important insights concerning mandatory data sharing in the private sector. For example, in the United Kingdom, as discussed above in connection with EU competition law, the Competition and Markets Authority has

---

452 Id. at 1956; see also Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA L. REV. 1701, 1705 (2010) (noting that for 87 percent of the American population no two people share the combination of zip code, birth date with year, and sex, heightening the risk of re-identification of seemingly innocuous de-identified data).

453 See Whittington, supra note 2 at 1917.

454 Id. at 1913.

455 Andrew Wong, Vicky Liu, William Caelli, & Tony Sahama, An Architecture for Trustworthy Open Data Services, 454 IFIP ADVANCES IN INFO. AND COMM’N TECH. (Apr. 30, 2015), https://doi.org/10.1007/978-3-319-18491-3_1.
proposed a range of possible mandates on data sharing by platforms.\textsuperscript{456} These mandates can be thought of as equivalent to open data requirements for government agencies. To the extent that open data initiatives have succeeded, they can show possible benefits of mandatory data sharing. In contrast, to the extent that open data initiatives have been narrowed or shown few results, they could inform reasons to expect more limited benefits from private-sector PORT initiatives.

4.2. The principal benefits from open data initiatives appear to be for research and commercial innovation. In contrast to other case studies that involve dominant firms, open data initiatives are not generally tailored to reducing market power in a defined market.

4.3. Privacy is a significant limiting factor on the scope of open data initiatives. For the U.S. government Data.Gov portal, interviews with persons involved showed that the original hoped-for scope was narrowed considerably due to privacy considerations. In particular, this case study illustrates the importance of considering the risk that de-identified data may be subject to re-identification attacks.

4.4. The European experience is consistent with privacy being a significant limiting factor. The Open Sector and Public Sector Information Directive entered into force in 2019, replacing earlier European Union Directives.\textsuperscript{457} The 2019 Directive “focuses on the economic aspects of the re-use of information rather than on access to information by citizens.”\textsuperscript{458} Notably, its “high-value datasets” apply predominantly to non-personal data: (1) geospatial; (2) earth observation and environment; (3) meteorological; (4) statistics; and (5) mobility. The only exception appears to be when “companies and company ownership” dataset would reveal personal data, for individuals who own companies of public record.

\textsuperscript{456} COMPETITION \& MKTS. AUTH., Online platforms and digital advertising: Market study interim report (2019), https://assets.publishing.service.gov.uk/media/5dfa0580ed915d0933009761/Interim_report.pdf [https://perma.cc/C56F-7FGK].
\textsuperscript{458} Id.
4.5. Some open data initiatives fail to match the supply and demand for particular data. To be useful, open data requires a critical mass of timely, accurate, machine-readable, and standardized data sets on topics actually of interest to users.

4.6. Once data is open to the public, it is generally open to bad actors as well. Open data initiatives may reveal vulnerabilities, such as the precise location of chemical plants, which can be physically attacked.\(^{459}\) Open data websites may open locales to targeted hacking and public service disruption attacks. Where such security risks exist, one response can be implementation of additional authentication measures to seek to prevent access by malicious actors.\(^{460}\) Another response is to simply withhold particular high-risk data sets from publication or to limit publication to certain constituencies.\(^{461}\)

---

\(^{459}\) Accidental Release Prevention Requirements; Risk Management Programs Under the Clean Air Act Section 112(r)(7); Distribution of Off-Site Consequence Analysis Information, 65 Fed. Reg. 48, 108, 111–48, 112 (Aug. 4, 2000) (discussing the risks of the EPA publishing “offsite consequences analysis” on the internet, including the risk that “terrorists or other criminals will attempt to cause an industrial chemical release in the United States.”).

\(^{460}\) See Wong, supra note 34, at 152.

\(^{461}\) See, e.g., supra note 459, at 127–48, 128.
APPENDIX 4: U.S. AND EU PHONE NUMBER PORTABILITY: PORT – IA

1. DESCRIPTION OF PORTABILITY OR OTHER REQUIRED TRANSFER (PORT) INITIATIVE

1.1. This case study focuses primarily on the U.S. legal framework governing telephone number portability. Section 1.6 includes a brief summary of the laws governing number portability in the E.U. The two regimes offer substantially similar rights to users, with similar benefits, costs, and risks.

1.2. Origination. In the United States, the Number Portability Administration Center (NPAC) serves as “the telecom industry’s common, authoritative database used for routing, rating and billing calls for telephone numbers that are no longer assigned” to phone end users. NPAC facilitates phone number portability when an end user switches from one communications provider to another. Congress created and funded NPAC solely for the purpose of administering phone numbers.

1.3. Destination. Wireless and wireline phone service providers.

1.4. Types of Data. The information that is exchanged between new and old phone service providers consists of: (1) telephone number; (2) current assigned service provider ID; (3) the location routing number (LRN); (4) SS7 Destination Point Codes; (5) service type; (6) alternative SPID (to identify a reseller); (7) billing ID; and (8) end user location and type.

1.5. Applicable Law. Phone number portability is mandated by the Telecommunications Act of 1996 and regulated by the Federal

---

462 Thanks to Kaelyne Yumul Wietelman for research assistance on this case study.
464 Id. (NPAC also operates in Canada where their phone numbers are administered and regulated by Neustar).
Communications Commission (FCC). The purpose of the Telecommunications Act is to establish a “procompetitive, deregulatory national policy framework” intended to “promote competition and reduce regulation. . . to secure lower prices and higher quality services for American telecommunications consumers and encourage the rapid deployment of new telecommunications technologies.” In the 1996 Telecommunications Act, “Section 251(b)(2) requires LECs (local exchange carriers) ‘to provide, to the extent technically feasible, number portability in accordance with the requirements prescribed by the Commission.’” In 2003, the FCC issued an order that mandated number portability between wired to wireless and wireless to wireless phone service providers beginning in November 2003.

1.6. The European Union similarly mandated phone number portability via Article 30 of the Universal Services Directive (USD) of 2002. The USD mandated that consumers could change, in one working day, their fixed or mobile operator while keeping their old phone number. More specifically, Article 30 of the USD required telecoms operators to: (1) set a maximum time limit of one working day from the moment of concluding an operator change agreement to the moment when the number is activated with another operator, (2) not exceed one working day’s loss of service during the process of changing operator, and (3) carry out the overall process within the shortest time possible.

2. BENEFITS OF PORT INITIATIVE

2.1. User Autonomy and Control Over Information. Consumers enjoy greater autonomy over their phone numbers because they can respond to price and service changes without having to change their telephone number and no longer have to “incur the . . . costs associated with changing telephone numbers” This is especially true for business

467 See 47 C.F.R. § 52.3 (2020) (“The Commission shall have exclusive authority over those portions of the North American Numbering Plan (NANP) that pertain to the United States.”); see also Wireless Local Number Portability, supra note 465.


472 Id. at art. 30.

customers whose costs could include revising marketing materials, keeping track of customers’ information once they change numbers, and losing customers because of the change in phone number.\textsuperscript{474}

2.2. Competition. The phone number PORT benefits competition by reducing barriers to entry and switching costs. Without the phone number PORT, new phone providers would have to incentivize potential customers significantly to convince customers to leave their current phone service and change their phone number.\textsuperscript{475} Instead, the NPAC assumed the majority of the administrative burden associated with changing the information connected with the phone number if the consumer wants to change service providers.\textsuperscript{476} Moreover, with phone number portability, consumers do not have the burden of switching their phone numbers and informing their family friends and business contacts of the number change. Therefore, retaining a phone number reduces the network effects that a dominant phone carrier may have because a consumer need not worry about the significant number of contacts that will have to be informed about a new phone number.\textsuperscript{477} Additionally, when there is an increase in willingness of a “consumer to change to another service provider,” there is an increase in competition.\textsuperscript{478} Thus, consumers have “more choices and reduce[d]}

\textsuperscript{474} Id.

\textsuperscript{475} First Report and Order, Implementation of the Local Competition Provisions in the Telecommunications Act of 1996 and Interconnection between Local Exchange Carriers and Commercial Mobile Radio Service Providers, F.C.C. 96-325, 12 (1996), https://transition.fcc.gov/Bureaus/Common_Carrier/Orders/1996/fcc96325.pdf (“The statute also directs us to remove the existing operational barriers to entering the local market. Vigorous competition would be impeded by technical disadvantages and other handicaps that prevent a new entrant from offering services that consumers perceive to be equal in quality to the offerings of incumbent LECs. Our recently-issued number portability Report and Order addressed one of the most significant operational barriers to competition by permitting customers to retain their phone numbers when they change local carriers.”) [https://perma.cc/LP2S-SFUR]; see also Tel. No. Portability, 11 FCC Rcd. 8352, 8489 (1996) (“[A] lack of number portability likely would deter entry by competitive providers of local service because of the value customers place on retaining their telephone numbers.”).

\textsuperscript{476} See NO. PORTABILITY ADMIN. CTR., What is LNP?, https://www.npac.com/number-portability/what-is-lnp (last visited Mar. 11, 2020) (“Prior to the introduction of LNP, changing service providers meant having to get a new telephone number. Number porting changed that, making it possible for consumers to retain the same telephone number.”) [ https://perma.cc/APJ9-8TR9].

\textsuperscript{477} Minjung Park, The Economic Impact of Wireless Number Portability, 59 J. INDUS. ECON. 714, 716 (2011) (“[T]he inability of end users to retain their phone numbers when changing service providers forces them to inform their family, friends and business contacts of their new phone numbers.”).

\textsuperscript{478} See What is LNP?, supra note 476.
prices.” Indeed, prices for wireless services decreased after number portability was mandated for wireless service providers.

2.3. Technical obstacles to portability. The lack of technology was initially the greatest challenge for implementing data portability with phone numbers. Long-term service portability was not an option when number portability became required. LECs were required to use current available number portability measures. These portability requirements took place over a long period of time, and the FCC has continuing legal authority to update these requirements.

3. RISKS AND COSTS OF PORT INITIATIVE

3.1. Security. At the time that wired and wireless phone number PORTs were implemented, few potential or anticipated security risks existed. Enrollment for a new phone service was often done in person, so there was opportunity for relatively strong end-user authentication.

3.2. Recently, however, mobile number portability hacking has been on the rise. Hackers have convinced phone carriers to port numbers, after which the hacker can reset passwords on every online account that uses that phone number for account authentication. In order to

---

479 Id.
480 See Park, supra note 477, at 715.
482 Id.
483 Separate Statement of Chairman Michael J. Copps, Tel. Number Portability, CTIA Petitions for Declaratory Ruling on Wireline-Wireless Porting Issues, CC No. 95-116, FCC 03-284 (2003) (“It was some seven years ago, in the 1996 Act, when Congress recognized that the ability of consumers to retain their phone numbers when switching providers would facilitate the development of competition. Congress instructed us to get this job done and to use ‘technical feasibility’ as our guide in making sure the vision became reality. This we have labored mightily to do so. As a result, American consumers will be able to take their digits with them, unimpeded by the hassle, loss of identity and attendant expenses that until now have accompanied switching between service providers and technologies.”).
484 See Alix Langone, My Cell Phone Number Was Stolen. It Nearly Ruined My Life, MONEY (Jun. 8, 2018), https://money.com/cell-phone-porting-scamb-t-mobile/ (“A T-Mobile spokesperson said these are industry-wide issues, but did acknowledge a recent ‘uptick’ in cell phone hijacking.”) [https://perma.cc/U9E2-JXHP].
485 See Lorrie Cranor, Your mobile phone account could be hijacked by an identity thief, FTC (Jun. 7, 2016), https://www.ftc.gov/news-events/blogs/techftc/2016/06/your-mobile-phone-account-could-be-hijacked-identity-thief (“In January 2013, there were 1,038 incidents of these types of identity theft reported, representing 3.2% of all identity theft incidents reported to the FTC that month. By January 2016, that number had increased to 2,658 such incidents, representing 6.3% of all identity thefts reported to the FTC that month. Such thefts involved all four of the major mobile carriers.”) [https://perma.cc/M8BT-X8SU].
carry out a “port-out scam,” all a hacker generally needs to know is a person’s phone number, name, address, last four digits of a social security number, and the person’s account login information.\(^\text{486}\) A hacker can obtain this information through theft or phishing. Particularly with authentication through one-time passwords sent through SMS text, phone numbers are increasingly important because a hacker can change the user’s account passwords and easily steal money, information, or identification.\(^\text{487}\) Phone users can mitigate the risk from phone number portability by making security questions more difficult to guess, as well as by getting a virtual phone number or VoIP plan and using that number publicly rather than the assigned 10-digit phone number.\(^\text{488}\) This would make it more difficult for hackers to connect the VoIP number to any identifying information about a person because the VoIP plan or the virtual phone number would not be connected to personal identifying information on other accounts.\(^\text{488}\)

### 3.3. Privacy

The privacy risks associated with the phone number PORT are low, as were the security risks at the time portability was mandated. Consumers and businesses typically want their phone number to be known to others, so there are low privacy concerns when the number is transferred to a new carrier. When consumers wish to have a private or unlisted number, they can easily decide not to port a previous phone number to a new carrier. In addition, transfer of a phone number to a new carrier generally is done without the transfer of significant personal data from the old to the new carrier.\(^\text{489}\)

---


\(^\text{489}\) See Memorandum Opinion and Order and Further Notice of Proposed Rulemaking, Telephone Number Portability, CTIA Petitions for Declaratory Ruling on Wireline-Wireless Porting Issues, CC No. 95-116, FCC 03-284 n. 62 (2003), https://www.fcc.gov/general/wireless-local-number-portability-wlnp#recent, (“We anticipate that a minimal amount of identifying information will be transmitted from the wireless carrier to the LEC when a customer seeks to port. For example, carriers may choose to verify the zip code of the porting-out wireline customer in their validation procedures.”) [https://perma.cc/W6KY-ZJWA].
4. LESSONS LEARNED

4.1. This case study shows that the U.S. and EU have mandated number portability to give consumers more control over their phone number and the information linked to the phone number.

4.2. This case study illustrates how portability can be significantly easier to manage when the data is stored and managed through one entity like the Number Portability Administration Center.

4.3. Number portability was effective because it occurred over an extended period of time and the requirements depended on what was technologically feasible. As technology became more sophisticated, so did the number portability possibilities between wireless and wireline providers.

4.4. Phone number portability has a combination of large benefits and low costs that has made it a prime example for proponents of other PORT initiatives. The benefits are high due primarily to the reduced lock-in effect for all phone users. The privacy and security risks were very low at the time the PORT was enacted (although security risks have become greater recently). The other case studies have not generally shown this pattern of clearly large benefits and low costs, so the phone number portability case study is less representative of the range of PORT initiatives than supporters of PORTability may have assumed.

4.5. There are security issues that now occur with mobile number porting that were not possible twenty years ago. For example, there are security risks with one-time passwords and two-factor authentications using SMS text because hackers can utilize social engineering and trick phone companies to port a customer’s phone information into a new phone. Afterwards, the hacker steals information and accounts associated with the phone number.

4.6. Consumers have utilized the benefits of phone number portability; millions of customers a year have taken advantage of it since the PORT went into effect.490

---

APPENDIX 5: EU FINANCIAL SERVICES: PORT-IA

1. SUMMARY OF THE PORTABILITY OR OTHER REQUIRED TRANSFER (PORT) INITIATIVE

1.1. This case study examines portability developments in the EU financial services sector. The primary focus is on the Payment Services Directive of November 2007 (“PSD1”) as updated and expanded in the Payment Services Directive of November 2015 (“PSD2”). In the UK, after study by the Open Banking Working Group, the Competition & Markets Authority (“CMA”) created the Open Banking Implementation Entity (“OBIE”) to set software standards.

491 Thanks to Simon Albert for research assistance on this case study.
493 PSD2, supra note 227, pmbl. § 6 (stating “New rules should be established to close the regulatory gaps while at the same time providing more legal clarity and ensuring consistent application of the legislative framework across the Union. Equivalent operating conditions should be guaranteed, to existing and new players on the market, enabling new means of payment to reach a broader market, and ensuring a high level of consumer protection in the use of those payment services across the Union as a whole. This should generate efficiencies in the payment system as a whole and lead to more choice and more transparency of payment services while strengthening the trust of consumers in a harmonised payments market.”). PSD2, supra note 227, pmbl. § 109 (referring to “the objective of this Directive, namely the further integration of an internal market in payment services”).
and industry guidelines to implement PSD2. Notably, the OBIE issued specifications for Application Programming Interfaces ("APIs") to mandate secure connections between banks and other payment service providers ("PSPs").

1.2. **Origination.** Consumer PSPs, including banks.

1.3. **Destination.** (1) Consumers; and (2) PSPs, including “account servicing payment service providers,” “payment initiation service providers,” and “account information service providers,” as defined in PSD2.

1.4. **Types of Data.** The payments data in question relates to the various forms of payments information handled by payment processors of all types within the industry. The relevant product market is the retail payments market which includes card, internet, and mobile payments.

---


496 These terms are defined in Article 4 of PSD2. See, e.g., PSD2, supra note 227, art. 4 (“‘account servicing payment service provider’ means a payment service provider providing and maintaining a payment account for a payer.’”).

497 See PSD2, supra note 227, art. 45 (“A PSP must provide to the payment service user a specification of the information or unique identifier to be provided by the payment service user in order for a payment order to be properly initiated or executed.”); see PSD2, supra note 227, art. 46 (“Where a payment order is initiated through a payment initiation service provider, the payment initiation service provider shall, immediately after initiation, provide the payer and, where applicable, the payee with a reference enabling the payer and the payee to identify the payment transaction and, where appropriate, the payee to identify the payer, and any information transferred with the payment transaction.”); see PSD2, supra note 227, art. 47 (“Where a payment order is initiated through a payment initiation service provider, it shall make available to the payer’s account servicing PSP the reference of the payment transaction.”); see PSD2, supra note 227, art. 48 (“Immediately after receipt of the payment order, the payer’s PSP shall provide the payer with a reference enabling the payer to identify the payment transaction and, where appropriate, information relating to the payee.”); see PSD2, supra note 227, art. 49 (“Immediately after the execution of the payment transaction, the payee’s PSP shall provide the payee with a reference enabling the payee to identify the payment transaction and, where appropriate, the payer and any information transferred with the payment transaction.”). See also PSD2, supra note 227, art. 4 §§ 32-33 ("‘sensitive payment data’ means data, including personalised security credentials which can be used to
1.5. **Applicable Law.** Recital 16 and Article 28 of PSD1 granted access to payment systems for “authorised or registered payment service providers” on an “objective, non-discriminatory and proportionate” basis, which is similar to the term “fair, reasonable, and non-discriminatory” used in patent and other settings (“FRAND”).\(^\text{498}\) PSD2 notably widened the scope of PSD1 to cover third party “payment initiation services,” such as Sofort in Germany, IDEAL in the Netherlands, and Trustly in Sweden.\(^\text{499}\) Prior to PSD2, such new providers had not been regulated at the EU level, so PSD2 covered them, addressing issues which may have arisen with respect to confidentiality, liability, or security of transactions with such providers.

1.6. This case study also looks at official policy documents issued by the European institutions for discussion purposes as part of the wider legislative process prior to the enactment of PSD2. One of those was a “Green Paper,” published by the European Commission in January 2012.\(^\text{500}\)

---

carry out fraud. For the activities of payment initiation service providers and account information service providers, the name of the account owner and the account number do not constitute sensitive payment data; ... ‘unique identifier’ means a combination of letters, numbers or symbols specified to the payment service user by the payment service provider and to be provided by the payment service user to identify unambiguously another payment service user and/or the payment account of that other payment service user for a payment transaction.”)


\(^{499}\) *e Payment Services Directive FAQ* (“During the past years, new players have emerged in the area of internet payments offering consumers the possibility to pay instantly for their internet bookings or online shopping without the need for a credit card (around 60% of the EU population does not have a credit card). These services establish a payment link between the payer and the online merchant via the payer’s online banking module. These innovative and low cost payment solutions are called ‘payment initiation services’ and are already offered in a number of Member States (e.g. Sofort in Germany, Ideal in the Netherlands, Trustly in Sweden). Until now, these new providers were not regulated at EU level. The new Directive will cover these new payment providers (‘payment initiation services’), addressing issues which may arise with respect to confidentiality, liability or security of such transactions.”)

2. BENEFITS OF PORT INITIATIVE

2.1. Competition. The stated objective of PSD2 was the further integration of the European internal market in payment services including by breaking down the pre-existing fragmentation in the market along national borders and creating a single market across the entire European Union.\(^{501}\) PSD2 was concerned (see recital 4) that “significant areas of the payments market, in particular card, internet and mobile payments, remain fragmented along national borders.” The risk within those fragmented national markets was that they may have featured high degrees of market concentration, which may have benefited existing incumbents but not consumers obliged to use those incumbents’ (costly) services. PSD2’s move from those fragmented national markets to EU-wide markets was intended to reduce those incumbents’ overall market power and make them more responsive to consumers.

2.2. A principal aim of PSD2 was to reduce lock-in effects. One specific aim was to reduce the pre-existing fragmentation of the market, so that consumers had other options and could switch to competing providers and new entrants.\(^{502}\) PSD2 provided for the wider range of

---

\(^{501}\) See PSD2, supra note 227, pmbl. § 5 (“[T]he continued development of an integrated internal market for safe electronic payments is crucial in order to support the growth of the Union economy and to ensure that consumers, merchants and companies enjoy choice and transparency of payment services to benefit fully from the internal market.”).

\(^{502}\) See Proposal for a directive of the European Parliament and of the Council on Payment Services in the Internal Market and amending Directives 2002/65/EC, 2013/36/UE and 2009/110/EC and repealing Directive 2007/64/EC and Proposal for a Regulation of the European Parliament and of the Council on Interchange Fees for Card-Based Payment Transactions, at 163-164, COM (2013) 547 final (July 24, 2013), https://eur-lex.europa.eu/resource.html?uri=cellar:906ed6d3-f509-11e2-a22e-01aa75ed71a1.0001.04/DOC_2&format=PDF [https://perma.cc/X63Z-SK89] (“Market fragmentation currently hinders the emergence of potential pan-European payment innovations in the areas of e- and m-payments and consumers can only benefit from these services in their own domestic market. Technical differences between national payment formats and infrastructures also represent a major hurdle for the supply side. New market entrants or existing payment providers who would like to start offering innovative services see their business case restricted to the national market which limits the scalability of the potential revenues and therefore discourages start-up investments. Similarly, market fragmentation reduces potential economies of scale on the cost side of these new initiatives and makes it difficult for existing schemes, interested in establishing interoperability, to justify this with a viable business case. More importantly, as innovative services mostly emerge at national level only, there is a risk that market fragmentation is increased and
third party providers than those covered under Article 28 of PSD1, so that consumers can more easily switch from the existing incumbent banks to the new forms of payment providers entering the market based on new technology. In particular, the application of the “objective, non-discriminatory and proportionate” requirements to these new forms of payment providers was designed to reduce lock-in effects.\(^{503}\)

2.3. One of the key aims of the legislative process was to remove barriers to entry so that competitors could enter, expand, and grow by providing consumers with new services, such as mobile payments. It was not designed to entrench the dominance of major platforms or incumbents, such as banks or card networks such as Visa and Mastercard. PSD2 also has a broader geographic scope than PSD1: PSD2 is designed to strengthen the EU’s digital single market and covers payments to and from third countries outside of the EU, where one of the PSPs is located in the EU. By contrast, PSD1 only applied to intra-EU payments. As regards the further removal of barriers to entry, the European Commission has continued to take antitrust enforcement action against those card networks as regards their high multi-lateral interchange fees for point-of-sale retail transactions,\(^{504}\)

\(^{503}\) See also PSD1, supra note 227, pmbl. § 29 and PSD2, supra note 227, pmbl. § 62 (both referring to “facilitat[ing] customer mobility” specifically as regards to terminating framework contracts). In the UK, this initiative is known as “open banking,” giving customers the option to share information about how they operate their bank account with third party organizations. See What is Open Banking?, OPEN BANKING, https://www.openbanking.org.uk/customers/what-is-open-banking/ [https://perma.cc/77BU-TEWC].

contributing to several follow-on damages actions in the English courts. The European Commission has explicitly linked those interchange fees with barriers to entry. It fined Mastercard €570 million in 2019 for obstructing merchants' access to cross-border card payment services. The Commission found that “Mastercard's cross-border acquiring rules acted as an additional barrier to cross-border trade in a market where interpenetration between Contracting Parties to the EEA Agreement was difficult because of other barriers to cross-border acquiring.”

2.4. Innovation. As PSD2 noted in recital 67, “the current degree of innovation in the field of payments might lead to the rapid emergence of new payment channels in the forthcoming years.” PSD2 was therefore designed to expedite and accommodate those innovations.

2.5. User Autonomy and Control. As regards user “autonomy,” in EU parlance, this appears as “freedom of choice.” The European Commission’s Green Paper included “freedom of choice” at the heart


506 PSD2, supra note 227, pmbl. § 67.
of its vision, as part of the anticipated gains from PSD2. The goals of PSD2 are to provide individual bank customers a greater freedom of choice in selecting payment providers and accessing new entrants and innovative providers, in addition to any improved price and quality that may result from greater competition.

3. RISKS AND COSTS OF PORT INITIATIVE

3.1. Privacy and Data Protection. Privacy and data protection are fundamental European rights which are similarly prioritized by PSD2. Since the provision of payment services by PSPs often results in the processing of personal data, PSD2 applied European data protection rules to the sector. PSD2 is clearly drafted to require that all data controllers within its ambit are governed by strict privacy and security rules. This aims to avoid data transfers from a controller under stricter legal rules, to a recipient with less strict rules, to ensure a level playing field amongst market participants.

3.2. This meant that any national implementing measures had to: (i) specify the precise purpose of any data processing; (ii) refer to the relevant legal basis; (iii) comply with the relevant security requirements; and (iv) respect the principles of necessity, proportionality, purpose limitation, and a proportionate data retention

---

507 Green Paper, supra note 50, at 15 (“European payment users (companies, consumers, merchants) will fully benefit from competition, freedom of choice and more efficient payment operations if cross-border interoperability is achieved.”).

508 See PSD2, supra note 227, pmbl. § 5 (“The continued development of an integrated internal market for safe electronic payments is crucial in order to support the growth of the Union economy and to ensure that consumers, merchants and companies enjoy choice and transparency of payment services to benefit fully from the internal market.”). See PSD2, supra note 227, pmbl. § 6 (“This should generate efficiencies in the payment system as a whole and lead to more choice and more transparency of payment services while strengthening the trust of consumers in a harmonized payments market.”). See PSD2, supra note 227, pmbl. § 54 (“This Directive should specify the obligations on payment service providers as regards the provision of information to the payment service users who should receive the same high level of clear information about payment services in order to make well-informed choices and be able to choose freely within the Union.”). See PSD2, supra note 227, pmbl. § 67 (“The issuing of a card-based payment instrument by a payment service provider, whether a credit institution or a payment institution, other than that servicing the account of the customer, would provide increased competition in the market and thus more choice and a better offer for consumers.”).

509 See e.g., PSD2, supra note 227, pmbl. §§ 6, 10, 33, 47, 50, 69, 93–95; see also PSD2, art 35. Note also that data subjects have rights of data access independent of PSD2, which refers to the importance of such “fundamental rights” in recitals 46 and 90, and refers to other, pre-existing data protection directives in Article 94. PSD2, supra note 227, pmbl. §§ 46, 90; see also PSD2, supra note 227, art. 94.
period. PSD2 also required data protection “by design” and “by default” within all data processing systems resulting from PSD2.\(^5\)

3.3. The European Data Protection Supervisor (“EDPS”) was dissatisfied with early drafts of PSD2 and made important submissions during the PSD2 legislative process, insisting on concrete data protection safeguards, rather than mere assertions of compliance with applicable data protection laws.\(^6\) The EDPS may make similar interventions as regards potential PORTs in the digital or other sectors.

3.4. **Security – Authentication and Unauthorized Access.** Major security issues face the payment industry. PSD2 recognized the security risks when designing the PORT and sought to address them

---

\(^5\) See PSD2, supra note 227, pmbl. §§ 21, 46, 89–90, 93, 111; see also PSD2, supra note 227, art. 94.

\(^6\) Officials from the European Data Protection Supervisor (“EDPS”) made several interventions on this subject. One official stated at a conference that the European Commission had failed to make online and electronic operators, i.e. “third-party providers,” (TPPs) subject to sufficient duties to protect clients’ data. The EDPS’ concerns were to be addressed in a formal EDPS Opinion. The main worries related to access to personal information, data retention and the proportionality and necessity of the processing of personal data. The resulting Opinion welcomed the introduction of a substantive provision stating that any processing of personal data taking place in the frame of the proposed Directive should be done in full respect of the national laws governing data protection. The EDPS stated, however, that this assertion was essential but not sufficient. The EDPS requested concrete safeguards that would apply to any situation in which personal data processing was envisaged. The EDPS therefore made a significant number of very detailed and specific recommendations for changes to the document. EDPS Supervisor Giovanni Buttarelli addressed a European Parliament hearing, warning that the draft legislation to open up the payments market to new operators lacked clear wording on who would have access to sensitive banking information. The hearing covered both the draft PSD2 and IFR. Buttarelli stated that “everything which is needed is missing.” Buttarelli said that one of the concerns related to the “increasing significant amount of personal data” processed by payments companies, including names, account numbers and the contents of contracts. He encouraged EU legislators to introduce more precise definitions on the processing of data. Given Buttarelli’s stature in the field, this warning may show the importance of privacy to this regulatory initiative. These warnings appear to have been heeded, in that the final text of PSD2, as enacted, contains frequent references to the need for relevant privacy and data protection requirements. See Opinion of the European Data Protection Supervisor on a Proposal for a Directive of the European Parliament and of the Council on Payment Services in the Internal Market Amending Directives 2002/65/EC, 2006/48/EC and 2009/110/EC and repealing Directive 2007/64/EC, and for a Regulation of the European Parliament and of the Council on Interchange Fees for Card-Based Payment Transactions, EUROPEAN DATA PROTECTION SUPERVISOR (Dec. 5, 2013), https://edps.europa.eu/sites/edp/files/publication/13-12-05_opinion_payments_en.pdf [https://perma.cc/3YZH-PLBM].
in its final text. The key risks turn on fraud and unauthorized access to the payment account. PSD2 stated that security was “fundamental,” requiring “strong customer authentication” to address such risks.\footnote{See PSD2, supra note 227, pmbl. §§ 7, 69, 95–96.}

3.5. The need for security and, by extension, for data privacy, has delayed the full achievement of the PORT in PSD2.\footnote{See Tim Bradshaw & Nicholas Megaw, Ecommerce Groups Sound Alarm Over EU Security Rules, FIN. TIMES (June 4, 2019), https://www.ft.com/content/cbf37fe4-8615-11e9-a028-86cea8523dc2; see also Nick Megaw, Be Careful What You Wish for: The battle Over EU’s Wide-Ranging Open Banking Legislation, PSD2 is Far From Over, FIN. TIMES (Sept. 23, 2019), https://www.ft.com/content/9c3fe37a-de35-11e9-9743-db5a370481bc.} PSD2 explicitly requires “strong customer authentication” (“SCA”).\footnote{See PSD2, supra note 227, pmbl. §107; PSD2, arts. 4 § 30, 97–98.} Although most of PSD2’s provisions applied from January 13, 2018, as regards SCA, PSD2 required the European Banking Association (“EBA”) to produce regulatory technical standards. EU Member States were then required to apply the resulting SCA measures from 18 months after the date of entry into force of those regulatory technical standards.\footnote{See PSD2, supra note 227, art. 115 § 4 (“By way of derogation from paragraph 2, Member States shall ensure the application of the security measures referred to in Articles 65, 66, 67 and 97 from 18 months after the date of entry into force of the regulatory technical standards referred to in Article 98.”).}

In theory, the SCA requirement of PSD2 came into force in September, 2019.\footnote{For the new rules, see Strong Customer Authentication Requirement of PSD2 Comes into Force, EUR. COMM’N (Sept. 13, 2019), https://ec.europa.eu/info/publications/190913-safer-payment-services_en [https://perma.cc/PZ9Q-UQ3A].} However, in October 2019, the EBA published an opinion stating that the deadline for the migration to SCA under PSD2 would be pushed back to December 31, 2020.\footnote{For the extended transition period, see EBA Publishes Opinion on the Deadline and Process for Completing the Migration to Strong Customer Authentication (SCA) for E-Commerce Card-Based Payment Transactions, EUR. BANKING AUTH. (Oct. 16, 2019), https://eba.europa.eu/eba-publishes-opinion-on-the-deadline-and-process-for-completing-the-migration-to-strong-customer-authentication-sca-for-e-commerce-card-based-payment [https://perma.cc/9HL5-5VXP].} In mid-2021, the EBA ultimately reported “significant progress” in industry compliance with the new SCA requirements.\footnote{In June 2021, the EBA published a report on the data provided by payment service providers (PSPs) on their readiness to apply strong customer authentication for e-commerce card-based payment transactions. The report found that the industry had reported significant progress over the previous 9 months in complying with the requirements for SCA for e-commerce card-based payment transactions. See EBA Publishes Report on the Data Provided by PSPs on their Readiness to Apply Strong Customer Authentication for E-Commerce Card-Based Payment Transactions, EUR. BANKING AUTH. (June 11, 2021), [https://perma.cc/9HL5-5VXP].} The standards required multi-factor
authentication, entailing substantial changes to processes and technology at retailers, banks and payment groups, as well as cooperation from consumers. The new rules mean that if customers do not approve a transaction – e.g. by entering a code received in a text message from their bank or scanning their fingerprint on their smartphone - they may not be allowed to complete a purchase. These rules are currently imposing on potentially unprepared relevant companies a significant compliance effort, so that the transition period was extended to give the industry extra time to comply.

3.6. Security – Application Programming Interfaces (“APIs”). Adoption of APIs has been an important issue under PSD2, for a mix of security and competition reasons. As explained here, the mandatory transition to the use of APIs and “open banking,” as prompted by PSD2, has been repeatedly delayed, due to complaints from industry participants and concerns that third-party providers would be unable to continue providing their existing services.519

3.7. Introduction to APIs. APIs are seen as the most reliable and tested technology to facilitate secure and reliable access to customers’ accounts, such as to send payment messages and account information between banks and third-party service providers. In layman’s terms, APIs may be seen as “electrical sockets that have predictable patterns of openings” into which other applications that match those patterns can “plug in.”520 Previously, third-party PSPs most generally gained access to a consumer’s account using the less secure method of “screen scraping.”521 To enable screen scraping, a consumer typically


provides passwords and other credentials, to enable the third-party provider to log in on the consumer’s behalf. The shift to APIs means that consumers no longer need to share their credentials with the third-party provider, thereby increasing security.

3.8. Firms can use APIs internally, to integrate their own internal operations. Of greater relevance to “open banking,” firms may use APIs externally, to create a secure connection for data to flow to and from an outside entity. APIs can therefore be key to the functioning of a PORT via interoperability and standardization. A public or open API may be accessible by almost anyone with little or no contractual arrangements. Such APIs can lead to new ways of working and competing on the market. This is particularly the case in the banking and payments sector, where for security and competitive reasons, banks have often developed their own closed in-house solutions that were not readily compatible with other financial institutions, especially non-banks. When APIs are in place with third parties, banks may then transform themselves from “walled gardens” into platform businesses, able to collaborate with other firms via the use of effective APIs to give consumers high-tech and lower cost payment solutions. Widespread use of APIs can help “unbundle” or “separate” services to create a more level playing field and increase competition.522

the current practice of third party access without identification that a few respondents referred to as ‘screen scraping’, or mistakenly as ‘direct access’, will no longer be allowed once the transition period under the PSD2 has elapsed and the RTS applies.”). See Strong Customer Authentication, FIN. CONDUCT AUTH. (June 18, 2020), https://www.fca.org.uk/firms/strong-customer-authentication [https://perma.cc/78XZ-62L7] (explaining that in the UK, in September 2019, the Financial Conduct Authority (“FCA”) gave businesses scope to continue to rely on “screen scraping” to provide payment services for six months longer than previously anticipated, stating: “where an ASPSP is providing access to TPPs through APIs, and did not have all payment accounts accessible by APIs on or before 14 June 2019, it should keep existing screen-scraping channels available during the adjustment period. This means not applying SCA to access accounts online during this period [. . .] Where relevant, during the adjustment period, TPPs should be able to continue using existing screen-scraping methods to access payment accounts online [. . .] During the adjustment period, TPPs should use an eIDAs or an equivalent certificate to identify themselves. Where it is not possible to do so, for instance when accessing accounts via existing screen-scraping channels, they should continue to be transparent and open about their identities.”).

522 A recent academic article on APIs, PSD2 and open banking has outlined the circumstances when remedies such as these may be required to resolve competition concerns: “Examples from energy and telecommunications sectors show that this kind of regulatory intervention aims to infuse competition at industries where incumbents retain a dominant position and market power that leads to monopolistic behaviour at the expense of
3.9. APIs in PSD2 and “Open Banking.” The text of PSD2 has only one reference in a recital to “online interfaces” which “provide the payment service user with aggregated online information on one or more payment accounts held with one or more other payment service providers.” PSD2 itself does not provide detailed requirements for the APIs needed to achieve the collaboration and resulting market entry which it foresees. By contrast, when the UK implemented PSD2, its Open Banking requirements mandated specific standards for APIs, for the nine leading banking institutions, as well as licensing by the Financial Conduct Authority for third parties using the APIs.

3.10. Practical issues with installing APIs. There have been numerous practical obstacles to installing APIs, including challenges for incumbent banks to connect their legacy IT systems with outside third parties. Such obstacles exist in the UK, even pursuant to the relatively specific API standards issued by the OBIE. PSD2’s lack of similar standards has led to additional variation in how Member States and individual banks have adopted technology to provide the required access to payments information by third-party PSPs, acting on behalf of consumers.

the end customer. By allowing third party access to the existing transmission and distribution network of incumbents, regulators help ‘unbundle’ or ‘separate’ services to create a more level playing field. Regulators can use such regulatory approaches along with advanced technology to tackle issues such as price discrimination, cross subsidies, and high barriers to entry that are often present when incumbents hold high market power with limited competition.” See Zachariadis & Ozcan, supra note 520, at 5.

523 See PSD2, supra note 227, pmbl.§ 28.

524 The UK transposed PSD2 into national law via the following pieces of secondary legislation: The Payment Services Regulations 2017, c. 752; The Payment Services and Systems and Electronic Money (Miscellaneous Amendments) Regulations 2017, c. 1173; and The Financial Services (Payment Services) Regulations 2018, c. 06 (repealed by The Financial Services (Payment Services) Regulations 2020, c. 030).


3.11. Resulting delays and extensions to API timelines. Given the complexities set out above, a trade press article provides a succinct summary, that “many European banks have continued to drag their heels on their PSD2 implementation, causing huge frustration across the fintech community which has been holding its breath for the quality APIs they need for their cutting-edge open banking innovations to work.”527

3.12. Incumbents’ Opposition to the PORT and Potential Misuse of Security Concerns. The European Commission has previously taken antitrust enforcement action against incumbent banks, including based on concerns that standards that were supposedly based on security were in fact being used to discriminate against non-banks. In September 2011, the European Commission started antitrust proceedings against the European Payments Council (“EPC”), the organization behind the self-regulatory implementation of the Single European Payments Area. Allegations included that the EPC had justified its standardization process for secure online transactions on cybersecurity grounds, but that the standards in fact discriminated against players that were not controlled by a bank. In June 2013, the European Commission closed its investigation after the EPC stopped developing its project in such a way as to exclude new entrants not linked to a bank.528

4. LESSONS LEARNED

4.1. When the European Commission published its “Green Paper” proposing new legislation, the public comments split depending on industry sector. The European Commission received hundreds of submissions to their consultation. Banks and card networks often argued that the PORT should be left to the market rather than regulation, whereas merchants supported the regulation of the card


527 See e.g., A Year of Yet More Delays, supra note 519; see, e.g., Sobering September Preview, supra note 519.

networks’ multi-lateral interchange fees. Consumer groups also supported regulation.\textsuperscript{529} These comments illustrate the importance of taking the financial interests of the commenter into account when assessing the evidence for and against a PORT initiative.

4.2. The history suggests that certain actors, especially banks, could have posed a threat to the PORT’s benefits, such as by using security requirements to try to exclude new entrants. The European Commission intervened to remove that threat, by bringing the competition case against the banking industry’s EPC.\textsuperscript{530} This European Commission action illustrates the risks that an incumbent can face unless its security policies operate in a reasonable and non-discriminatory manner. Subsequently, some banks complained about how hard it was to balance the PORT’s interoperability requirements with competition law compliance.\textsuperscript{531} Hence the far stronger and wider-ranging FRAND requirements in PSD2, in contrast to PSD1, to create the level playing field sought by policy makers.\textsuperscript{532}


\textsuperscript{530} The European Payments Council (“EPC”) is the organization behind the self-regulatory implementation of the Single European Payments Area, which was also the banking industry’s standardization body for payments. In September 2011, the European Commission started antitrust proceedings against the EPC in response to a complaint regarding certain standards that they were developing for electronic payments. These standards were needed for secure online transactions; they allowed different e-payment schemes to talk to each other and were based on services familiar to all, such as home-banking. The complaint alleged that these standards discriminated against players that were not controlled by a bank. Ultimately in June 2013, the European Commission closed its investigation after the EPC stopped developing its project in such a way as to exclude new entrants not linked to a bank. Therefore, the complainant withdrew its complaint. See AT.39876 EPC Online Payments, COMPETITION POLICY (July 28, 2020), https://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_39876 [https://perma.cc/3Z53-8T3X]. See European Commission Press Release, Antitrust: Commission Closes Investigation of EPC But Continues Monitoring Online Payments Market (June 13, 2013), https://europa.eu/rapid/press-release_MEMO-13-553_en.htm [https://perma.cc/2B5F-WX5E].

\textsuperscript{531} See Feedback Statement, supra note 529, at 23 (“Several banks emphasised the difficult balance between achieving interoperability and complying with competition law, specifically referring to the investigation opened by the commission on the e-payment standardisation work by the EPC.”).

\textsuperscript{532} The FRAND requirements in PSD2 were stricter than those in PSD1, in that, although PSD2’s Article 35 on non-discrimination as regards PSPs’ access to payment systems corresponded to PSD1’s existing Article 28, PSD’s Article 36 on access to accounts
4.3. This case study illustrates how a stronger PORT requirement can result in greater competition. Restricting competition, as the EPC attempted to do with its standards, can jeopardize a PORT. The case study also illustrates how strict security, privacy, and customer consent requirements can be met while implementing a strong PORT requirement. The European Commission, in drafting PSD2, explicitly recognized the need to accommodate the multiple relevant regulatory regimes. 533

4.4. The payments industry also offers valuable lessons as regards the trade-offs between a PORT and data privacy. In particular, the EDPS was not satisfied with general statements in the draft Directive that data protection laws should be observed, and instead insisted on substantive data protection guarantees in the final text of PSD2. Any future PORT initiatives in the EU may similarly face expert scrutiny by data protection officials, and their support for including substantive privacy protections in final legislation.

4.5. This case study illustrates delay in implementation of the PORT initiative. Notably, the implementation of PSD2 has seen repeated delays as regards the mandatory transition to APIs and SCA, as set out above.

maintained with a credit institution had no corresponding article in PSD1. Therefore, Article 36 of PSD2 was a new requirement. Recital 39 of PSD2 explained the reasoning behind this new requirement: “When engaging in the provision of one or more of the payment services covered by this Directive, payment service providers should always hold payment accounts used exclusively for payment transactions. In order to enable payment service providers to provide payment services, it is indispensable that they have the possibility to open and maintain accounts with credit institutions. Member States should ensure that access to such accounts be provided in a manner that is not discriminatory and that is proportionate to the legitimate aim it intends to achieve. While access can be basic, it should always be sufficiently extensive for the payment institution to be able to provide its services in an unobstructed and efficient way.” PSD2, supra note 227, art. 36. The European Commission further explained that “For payment institutions, access to a payment account maintained by a credit institution is vital for the operation of their business. PSD2 provides specifically that Member States will have to ensure that credit institutions do not block or hinder access to payment accounts and that payment institutions have access to credit institutions’ payment accounts services in an objective, non-discriminatory and proportionate manner. This aspect is very relevant for money remittance services as many of them have lost access to the banking system in the recent years.” See Payment Services Directive FAQ, supra note 492. 533 See e.g., PSD2, supra note 227, pmbl. § 29. “This raises a series of legal issues, such as consumer protection, security and liability as well as competition and data protection issues, in particular regarding protection of the payment service users’ data in accordance with Union data protection rules. The new rules should therefore respond to those issues.”
4.6. When meeting the multiple regulatory goals, including competition and security, there may be practical difficulties in achieving the desired inter-operability. Such difficulties suggest the importance of a strategy to achieve actual implementation, such as by engaging industry in a timely manner prior to required implementation. Another risk is that without the effective and timely implementation of the relevant SCA and API requirements, then fraud by bad actors exploiting certain of PSD2’s provisions might become so high that the very aims of the PORT could be jeopardized. In other words, legislators can mandate PORTs, but in reality, any such PORT is contingent on effective authentication processes actually being commercially available to ensure the requisite security levels are in place to protect consumers and combat fraud.

4.7. Along with delays, the case study illustrates the possibility of non-uniform implementation of PORT requirements. Although all EU Member States were required to transpose PSD2 into national law, in some Member States effective safeguards may not be in place in practice. In other words, PSD2 may aim to expand the relevant geographic market to a single European payments area, but the risk in doing so may be exposure to less well-regulated EU Member States or those subject to ongoing proceedings about the application of the rule of law.


APPENDIX 6: EU HEALTH DATA: PORT-IA

1. DESCRIPTION OF PORTABILITY OR OTHER REQUIRED TRANSFER (PORT) INITIATIVE

1.1. In 2011, the European Parliament and the Council of the European Union adopted Directive 2011/24/EU (the Cross-Border Healthcare Directive). That Directive is designed to assist EU citizens travelling between Member States to have seamless access to healthcare services. It does so by giving Member States the possibility of exchanging health data electronically, in a secure and interoperable way. Despite the many efforts further described below, there has been limited success implementing the exchange of such “eHealth” data. Exchanges of eHealth data are currently limited to (1) “ePrescription”/“eDispensation;” and (2) “Patient Summaries.” As of 2020, only one Member State was exchanging both of these types of data, and only with a small number of other Member States. In short, the initiatives for greater interoperability and portability have produced much more limited results than proponents have wished.

1.2. Origination. The health care practitioner (HCP) or health care system in the Member State where the individual resides.

1.3. Destination. (1) With respect to ePrescription/eDispensation data, the data will be received by a pharmacy used by that individual in another

---

537 Thanks to Paul Greaves and Laura Song for research assistance on this case study.
Member State; and (2) with respect to Patient Summary data, the data will be received by an HCP who is consulted by the individual in another EU Member State.

1.4. **Types of Data.** (1) ePrescription/eDispensation data contains the data in a medical prescription which has been provided to the individual; and (2) the Patient Summary contains important health-related information about the individual such as an individual’s “allergies, current medication, previous illness, and surgeries,” as well as data for the administration of the patient, such as identifying data and contact information.

1.5. **Applicable Law, Actions and Initiatives.** This PORT initiative is the output of a lengthy history of action and initiatives in the EU linked to eHealth interoperability and standardization. References to multiple resources are provided at the end of this Appendix.

1.6. The key piece of EU legislation with respect to this PORT initiative is the 2011 Cross-Border Healthcare Directive, which set up the “eHealth Network,” a voluntary network connecting national authorities responsible for eHealth designated by the Member States. Among the objectives of the eHealth Network are to “work towards delivering sustainable economic and social benefits of European eHealth systems and services and interoperable applications,” and to draw up guidelines, such as the “data that are to be included in patients’ summaries and that can be shared between health professionals to enable continuity of care and patient safety across borders.”

1.7. The exchange of ePrescription/eDispensation and Patient Summaries data relies on the voluntary cooperation of health authorities connecting to the eHealth digital service infrastructure (eHDSI). Through “core services,” the European Commission is providing a common information technology infrastructure and crosscutting

---


services (such as with respect to terminology and interoperability). The eHDSI is supported by the Connecting Europe Facility and uses the guidelines agreed by the eHealth Network.

2. BENEFITS OF PORT INITIATIVE

2.1. **User autonomy and control over information.** Individual patients are provided with control over their health data by enabling them, when travelling over borders within the EU, to have HCPs and pharmacists access such data. This reinforces the goals under the GDPR and EU law generally of removing the obstacles to flows of personal data within the Union, and providing individuals with access to, and control over their own personal data. It also supports the “free movement of people” rights which apply to EU citizens.

2.2. **Innovation.** The PORT initiative is designed to enable EU citizens to continue to benefit from healthcare under similar conditions as if they were in their home Member State, when travelling in other Member States. It means that individuals can obtain medication without needing to bring a printed prescription and without the difficulties associated with language barriers. It also allows HCPs in the Member State of travel to access basic and essential medical data through the Patient Summary, in the HCP’s own language, which may save lives.

---


543 Id. (explaining that the Connecting Europe Facility supports trans-European networks and infrastructure in the sectors of transport, telecommunications and energy. It finances projects that address common challenges through the provision of technical and organizational expertise).

544 The “right to data portability” under Article 20 of the GDPR could in theory permit individuals to transfer their prescription or other health data between healthcare providers or pharmacies in different Member States, however the right would not necessarily provide all of the benefits outlined below. For example, under the right to data portability under the GDPR, the personal data transferred would not necessarily be in the correct language in the Member State to which the individual has traveled. Directive 2016/679 of 25 May 2018, General Data Protection Regulation art. 20, 2016 O.J. (L 119) 1, 19 [hereinafter GDPR].

in critical cases.\textsuperscript{546} It leads to enhanced safety of treatments received.\textsuperscript{547} The PORT initiative could result in new patterns of delivery of healthcare. Individuals may be able to take advantage of the portability of their health data to obtain more specialized treatment, or better treatment in a Member State other than their home Member State.\textsuperscript{548}

2.3. \textbf{Technical obstacles to portability}. The slow adoption of the PORT initiative appears to be linked to the complicated technical obstacles to interoperability. The recitals to the Cross-Border Healthcare Directive state that “widely different and incompatible formats and standards are used for provision of healthcare using ICTs throughout the Union, creating both obstacles to this mode of cross-border healthcare provision and possible risks to health protection.”\textsuperscript{549} Many other publications and initiatives highlight the issue of lack of interoperability. For example, the EU Commission’s 2012 eHealth Action Plan recognizes the “lack of interoperability between eHealth solutions” as a barrier to deployment of eHealth, and recognized the need for an eHealth interoperability framework.\textsuperscript{550} The EU Commission’s 2019 \textit{Recommendation on a European Electronic Health Record Exchange Format} indicates that obstacles still remain with respect to EHRs, given its statement that “many of the formats and standards in electronic health record systems – that are information systems for recording, retrieving and managing electronic health records – used across the Union are incompatible.”\textsuperscript{551}


\textsuperscript{549} \textit{Id.} at 52-53.


2.4. **Legal obstacles to portability.** The technical problems described above are compounded by the fact that responsibility for health protection, and in particular, the development and deployment of eHealth systems, fall to each individual Member State, rather than to the EU.\(^{552}\) This is recognized by the recitals to the Cross-Border Healthcare Directive, which state that “[t]his Directive therefore should . . . respect the division of competences [i.e., each Member State’s power to define their own health policy] by providing for the Commission and Member States to work together on developing measures which are not legally binding but provide additional tools that are available to Member States to facilitate greater interoperability of ICT systems in the healthcare field and to support patient access to eHealth applications, whenever Member States decide to introduce them.”\(^{553}\) The limited ability of the EU to bind Member States appears to explain in part the limited adoption of the PORT initiative.

3. **RISKS AND COSTS OF PORT INITIATIVE**

3.1. **Security.** Unauthorized access is a risk for most PORT initiatives, including health care. The obligation contained in the GDPR to implement “appropriate technical and organizational measures” for the security of processing is designed to scale according to, amongst other things, the risks that could be posed by a personal data breach.\(^{554}\) Such risks are higher with respect to health data than many other types of personal data. Security concerns could partially explain the reluctance to adopt this PORT initiative. With respect to authentication, the Cross-Border Healthcare Directive states that the eHealth Network’s objectives are to “support Member States in

\(^{552}\) See EU Cooperation, supra note 542 (demonstrating that The EU only has the competences conferred on it by the relevant EU treaties). For example, under the Treaty on European Union, the EU’s actions in the field of human health protection “shall complement national policies” and shall “respect the responsibilities of the Member States for the definition of their health policy.” Consolidated Version of the Treaty on European Union art. 3, June 7, 2016, 2016 O.J. (C 202) 13 [hereinafter **TEU**]. The EU’s actions “shall in particular encourage cooperation between the Member States to improve the complementarity of their health services in cross-border areas.” Consolidated Version of the Treaty on the Functioning of the European Union art. 168, Dec. 26, 2012, 2012 O.J. (C 326) 1 [hereinafter **TFEU**].


\(^{554}\) **GDPR**, supra note 21, art. 32; see also **GDPR**, supra note 21, art. 4(12) (defining a personal data breach as a “breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”).
developing common identification and authentication measures to facilitate transferability of data in cross-border healthcare.”

The eHealth Network in 2018 adopted, for example, a Recommendation Paper on Policies Regarding eIDAS eID and Health Professional Registries which described problems and open questions with respect to the eIDAS Regulation in the context of eHDSI. That paper highlighted in particular the variation in interpretation amongst Member States with respect to the existence (or non-existence) of a legal obligation to implement electronic identification for patients under the eIDAS Regulation.

3.2. Privacy. The GDPR recognizes health data as a “special category of personal data,” which is “particularly sensitive,” and the processing of which “could create significant risks to the fundamental rights and freedoms” of individuals. Organizations processing health data must therefore apply a higher standard of protection to such personal data.

3.3. Differences between Member States’ data protection rules with respect to health data also form a legal obstacle to portability. To a certain degree, the GDPR harmonizes Member States’ data protection rules, however Article 9(4) of the GDPR specifically permits individual Member States to introduce further conditions and limitations with regard to health data. Some of the exemptions in the GDPR which permit the processing of health data are also linked to Member State law. To the extent that a Member State may have

---

558 GDPR, supra note 21, art. 9.
559 GDPR, supra note 21, art. 51.
560 GDPR, supra note 21, art. 9 § 4; For example, under Article 9 of the Belgian Data Protection Law of 30 July 2018, controllers processing personal data concerning health must implement additional measures not prescribed by the GDPR, including keeping a register of the categories of individuals who have access to health data together with a description of their capacity with respect to the data.
561 For example, the exemptions under Article 9(h) apply to processing for the purposes of “preventive or occupational medicine . . . , medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.”
introduced additional rules restricting the processing of health data, healthcare providers may face additional challenges in connection with the interoperability and portability with respect to such data. Differing regulatory interpretations and priorities across each Member States’ data protection authorities may also lead to different approaches.

3.4. **Competition risks.** The objective of this PORT initiative is to provide seamless access to healthcare for individuals travelling in the EU, and so it does not impact competition in the same way as a PORT initiative designed to enable new entrants to compete or to offer new services. Nevertheless, to the extent that incumbents protect against new entrants, incumbents may have an incentive to make health data less rather than more useful (e.g., by creating standards which prevent new operators from using the data to provide a service). Competition could, for example, arise in situations where individuals live next to a border with a neighboring Member State and choose to obtain healthcare or prescriptions in that neighboring Member State rather than their own.

4. **LESSONS LEARNED**

4.1. There has been a failure to create effective standards, despite heavy investment by the EU. Some of the many actions and initiatives are listed in the Appendix, and together these provide an indication of the amount of accumulated effort which has been put into the exchange of eHealth data – with limited results. To take one example, epSOS ran over six years and had a project budget of over 38 million euros, but only covered sharing of Patient Summary and ePrescription/eDispensation data \(^562\) – it did not cover broader Electronic Health Records.

4.2. Years of dedicated effort has failed to achieve widespread adoption of cross-border health data sharing. As of 2020,\(^563\) only three Member States had started to share or access ePrescription/eDispensation data

---

The exemptions under Article 9(i) apply to processing for reasons of “public interest in the area of public health.” Both require a basis in “Union or Member State Law.” GDPR, supra note 21, arts. 9(h)-9(i).


\(^{563}\) Research for this Appendix was last comprehensively updated May 2020. Since that time, it appears that Portugal does exchange ePrescription data. See Electronic Cross-Border Health Services, supra note 172.
and only five Member States had started to share or access Patient Summary data. Only one Member State (Croatia) had adopted both. However, even amongst countries which have adopted exchange of data, the possible exchanges are limited. For example, with respect to Croatia, it appears that:

1) Medicines could be retrieved in Croatian pharmacies with an ePrescription from Finland, but the inverse is not true: a patient from Croatia could not obtain medication using an ePrescription when in Finland; and

2) HCPs in Croatia could access Patient Summaries of citizens coming from the Czechia and Malta, but HCPs from the Czechia and Malta could not access Patient Summaries of citizens coming from Croatia.

As of 2020, it also appears that there was only one pair of countries that were mutually exchanging data: HCPs in Malta and Portugal could mutually access one another’s Patient Summaries. Neither Malta nor Portugal at that time were exchanging ePrescription/eDispensation data with any Member State.\textsuperscript{564}

4.3. This PORT initiative appears focused on incumbent health systems operating more effectively, in contrast to the U.S. healthcare PORT initiative, which focuses on creating new entrants to the healthcare market. The recitals to the Cross-Border Healthcare Directive do not suggest a focus on increasing competition by permitting new entrants to access health data in order to provide health services. Although, for example, the Commission’s 2019 Recommendation on a European Electronic Health Record Exchange Format does mention “digital solutions linked to health apps, or wearable devices” (Recital 5), and “new technologies for health” (Recital 9), research for this Article found no suggestion that increasing competition in the private sector is a significant objective of the recommendation.

4.4. Lack of essential legal authority may be an important barrier to effective PORT requirements. As highlighted above, the EU lacks authority to require Member States to adopt certain measures with respect to this PORT initiative, and the exchange of

\textsuperscript{564} Id. (demonstrating that Portugal began sharing ePrescription data with some countries starting in 2020).
ePrescription/eDispensation and Patient Summaries data relies to an extent on voluntary cooperation among the Member States. This seems likely to have limited the successful adoption of the initiative, when compared with the EU financial services case, which is more heavily based upon mandatory requirements imposed on Member States.

4.5. Where there are numerous standards in a complex system, it appears that successful portability becomes more difficult. As highlighted above, various initiatives have recognized the lack of interoperability for eHealth data,\(^5\) which appears to have contributed to the slow adoption of this PORT initiative.

**Additional Resources**

This PORT initiative is the output of a lengthy history of action and initiatives in the EU linked to eHealth interoperability and standardization. Examples of actions and initiatives are:

1) the European Commission's 2008 *Recommendation on Cross-Border Interoperability of Electronic Health Record Systems*, which provides a set of guidelines for the implementation of interoperable Electronic Health Records (EHRs) – this is a wider set of data which includes Patient Summaries and ePrescription/eDispensation;\(^6\)

2) the Council’s 2009 *Council Conclusions on Safe and Efficient Healthcare Through eHealth* which amongst other things calls upon the Member States to ensure that interoperability of eHealth services across organizational and national boundaries is taken into account in their health strategies and investment plans;\(^7\)

---


3) the European Commission's 2010 communication on interoperability for public services, which introduces the European Interoperability Framework (EIF). The EIF promotes and supports the delivery of European public services by fostering cross-border and cross-sector interoperability; 568

4) the “eHealth Governance Initiative” (eHGI), which was set up in 2011 as a high-level working group comprising of representatives from the Member States to drive forward eHealth in Europe; 569

5) the “CEN Technical Committee 251,” which is a technical decision-making body set up to focus on eHealth standardization within the EU;

6) epSOS, which ended in 2014. This was large-scale project which tested cross border sharing of ePrescription and Patient Summary, and covered, amongst other things, semantics, specifications and architecture; 570

7) the 2014 EXPAND (Expanding Health Data Interoperability Services) project which was aimed at filling the gap between “piloting” to “deployment,” and supported the epSOS to pave the way for the roll out of the eHDSI; 571

8) the Antilope project ran between 2013 and 2015, and was focused on the dissemination and adoption of the EIF. Antilope developed guidelines and recommendations that support the EIF; 572

---


570 See Project epSOS, supra note 563.


9) the Commission’s 2019 Recommendation on a European Electronic Health Record Exchange Format,\(^573\) which seeks to facilitate the cross-border interoperability of EHRs in the EU by supporting Members States in their efforts to ensure that citizens can securely access and exchange their health data wherever they are in the EU. It recommends that interoperability be further extended (beyond ePrescription/eDispensation and Patient Summary) to laboratory results, medical images and hospital discharge reports and puts forward recommended technical specifications for the exchange of this data;\(^574\) and

10) the renewed eHealth Stakeholder Group (ESG), composed of representatives of umbrella organizations/associations with a European outreach, representing the health tech industry, patients, healthcare professionals and the research community. It supports the Commission in the development of actions for the digital transformation of health and care in the EU. The renewed members were announced on 7 February 2020, with a mandate until 2022.\(^575\)

\(^{573}\) See European Health Record Exchange Format, supra note 551.


APPENDIX 7: US AUTOMOBILE DEALER DATA: PORT-IA 576

1. DESCRIPTION OF PORTABILITY OR OTHER REQUIRED TRANSFER (PORT) INITIATIVE

1.1. Automobile dealers typically contract with software companies for “Dealer Management System” (“DMS”) services, to assist dealers with their business operations. The DMS is a software platform that provides a wide range of functions including accounting, vehicle inventory, financing and insurance, and managing service and parts operations. Historically, many or all of these functions have been performed by the DMS software. The two largest in the United States, CDK Global, LLC (“CDK”) and The Reynolds & Reynolds Company (“Reynolds”), have a large market share, with their combined market share approximately 90% of vehicles sold.577 Automobile dealers have also contracted with third-party systems integrators and application developers (“third-party software providers”) to provide some of these services, most typically when they charged less for a particular application than DMS providers or provided additional functionality or a better product.

1.2. CDK and Reynolds have changed their position over time concerning a dealer’s ability to authorize third-party software providers to access dealer data on the DMS on behalf of the dealer. Previously, both CDK and Reynolds permitted such authorization. First Reynolds and later CDK changed their practices to generally prohibit those dealers from allowing such authorization. In 2019, Arizona and at least three other states enacted statutes that require a PORT for the transfer of data from the DMS to recipients authorized by automobile dealers, including systems integrators or other third-party software providers. The laws are intended to give dealers more control over their data stored in the DMS.

1.3. CDK and Reynolds have challenged the Arizona statute in federal court, claiming that the statute is unlawful.578 Separately, third-party

576 Thanks to Deona Kalala for research assistance on this case study in the U.S. automobile industry, which focuses on PORTability statutes passed in Arizona and at least three other states in 2019.
578 See e.g., David Muller, CDK, Reynolds Challenge Ariz. Dealer Data Law, 93 AUTO. NEWS 34 (Aug. 26, 2019), https://www.autonews.com/dealers/cdk-reynolds-challenge-ariz-
software providers, dealers, and others have brought lawsuits against CDK and Reynolds, alleging (among other things) that they entered into an agreement to exclude third-party software providers in violation of antitrust laws. The author has served as an expert witness for the Arizona Automobile Dealers Association in the suit concerning the Arizona statute, and for Authenticom and other software providers in the antitrust suits against CDK and Reynolds.

1.4. **Origination.** A “Dealer Data System” is a defined term under the Arizona law which refers to a DMS.

1.5. **Destination.** A recipient authorized by the automobile dealer (“Dealer”). Notably, the statute provides that a Dealer can give consent to port data from the Dealer Data System to an “Authorized Integrator.” An Authorized Integrator is defined as a “third party with whom the Dealer enters into a contractual relationship to perform a specific function for a Dealer that allows the third party to access Protected Dealer Data or to write data to a Dealer Data System, or both, to carry out the specified function.” For example, a Dealer might contract with an Authorized Integrator to support third party applications for service appointments, inventory management, and customer relationship management.

1.6. **Types of Data.** The PORT statute applies to “Protected Dealer Data,” which it defines as: (i) “personal, financial, or other data relating to a consumer that a consumer provides to a dealer or that a dealer

---


579 The author has submitted expert declarations on behalf of Authenticom in *Authenticom, Inc. v. CDK Global, LLC*, No. 17-cv-318 (W.D. Wis. 2017).

580 The author testified publicly in a preliminary injunction hearing in 2017 in federal court in Wisconsin. After that hearing, the district court enjoined CDK and Reynolds from continuing their activities that limited portability. *Authenticom, Inc. v. CDK Global, LLC*, No. 17-cv-318 (W.D. Wis. 2017), Dkt No. 58 (expert report/declaration of Peter Swire); *Authenticom, Inc. v. CDK Glob., LLC*, No. 17-cv-318-jdp, 2017 U.S. Dist. LEXIS 109409, at *1 (W.D. Wis. July 14, 2017), rev’d on other grounds 874 F.3d 1019, 1020 (7th Cir. 2017). This case study makes no assertions about the validity of facts in the ongoing litigation; instead, this case study relies on publicly-available documents, and presents facts in the form: “PORT proponents claim” or “PORT opponents claim.”


582 *Id.* § 3(b).

583 *Id.* § 1.
otherwise obtains and that is stored in the Dealer’s Dealer Data System;” and (ii) “other data that relates to a Dealer’s business operations in the Dealer’s Dealer Data System.” More colloquially, the statute applies to the data in a DMS that pertains specifically to that dealer’s business operations – not to data about other dealers.

1.7. **Applicable Law.** Arizona Revised Statute (“A.R.S.”) Sections 28-4651 to 28-4655, and similar laws passed in other states. The law enables the automobile dealer (“Dealer”) to select and authorize third parties to receive Protected Dealer Data. The law prohibits what it defines as “cyber ransom.” That term means “to encrypt, restrict or prohibit or threaten or attempt to encrypt, restrict or prohibit a Dealer’s or a Dealer’s Authorized Integrator’s Access to Protected Dealer Data for monetary gain.” In other words, under the statute, a DMS provider must permit Protected Dealer Data to be ported to an Authorized Integrator or other party, where the Dealer so directs. The law also makes it illegal to otherwise prohibit or restrict a Dealer’s ability to protect, store, copy, share, or use Protected Dealer Data, including charging fees for such access.

2. **BENEFITS OF PORT INITIATIVE**

2.1. **User autonomy and control over information.** PORT proponents assert that the Arizona statute assures that Dealers will retain autonomy and control over their Protected Dealer Data. PORT opponents, by contrast, argue that the PORT requirements impinge their ability to provide security for Dealer Data.

2.2. **Competition.** Proponents of the PORT initiative emphasize benefits to competition. Proponents of the PORT initiative contend that CDK and Reynolds reached an agreement in approximately 2015 to close their DMS to competing third-party software services, leading to a

---

584 *Id.* The definition of “Protected Dealer Data” also includes “motor vehicle diagnostic data that is stored in a Dealer Data System.” This case study addresses all Protected Dealer Data except requirements concerning motor vehicle diagnostic data.


587 *Id.* § 28-4653(A)(3).
large price increase for the services previously supplied by third-party software providers. The requirements in the Arizona law are designed to enable Authorized Integrators to compete with DMS providers in accessing Protected Dealer Data.

2.3. **Lock-in effect.** The high cost of switching DMS providers creates a lock-in effect, in the view of PORT proponents. They claim that switching DMS service providers is time-consuming, expensive, and disruptive to business operations.

2.4. **Innovation and barriers to entry.** One effect of monopoly pricing and the limitations imposed on third-party software providers would be to reduce innovation in the market for the software services available to Dealers. Proponents of the PORT claim that the methods that CDK and Reynolds make available for transferring data to app providers are expensive and make it difficult for other app providers to stay in business, thus reducing the possibility of new entrants and innovation in provisioning software services to Dealers.

2.5. **Incentives of those presenting evidence of benefits.** Dealers and third-party software providers have filed lawsuits against CDK and Reynolds, alleging that their agreements, and the limits on PORTability, violate the antitrust laws.

3. **RISKS AND COSTS OF PORT INITIATIVE**

3.1. **Security.** The DMS providers claim that their limits on access to their systems have been primarily motivated by good-faith cybersecurity concerns. PORT proponents claim that cybersecurity is being used as
a pretext for limiting access to Dealer data on the DMS, and that the primary motivation for limiting access has been to limit competition and raise prices rather than to protect cybersecurity.

One area of disagreement between the parties to the litigation has been about authentication. DMS providers have instituted policies that allow Dealers to issue credentials to their employees, but not to third parties, such as third-party software providers. DMS providers have claimed cybersecurity risks from third parties selected by the Dealers, who could access the DMS with dealer-provided credentials. PORT proponents have responded that Dealers should be able to authorize access to dealer data for both employees and third parties, and that authorizing third parties does not increase cybersecurity risk. The Arizona statute requires a DMS provider to provide access to a third-party software provider authorized by the Dealer, if the provider meets the requirements of an automobile industry cybersecurity standard.590

Another area of disagreement has been the extent to which there are secure mechanisms for third-party software providers to exchange information with the DMS. The Arizona statute in general prohibits “placing an unreasonable restriction on an authorized integrator.”591 More specifically, the statute requires a DMS provider to “adopt and make a standardized framework for the exchange” of Dealer Data, and to “provide access to open Application Programming Interfaces to authorized integrators.” 592 Historically, third-party software companies often relied on “screen scraping” to extract data from the DMS. Under this approach, the Dealer would issue credentials to a third party, who then would use software scripts to access data in the DMS. The DMS providers have made cybersecurity objections to such use of screen scraping. The Arizona statute allows DMS providers to comply with the statute by providing access to Application Programming Interfaces (“APIs”), rather than setting rules about screen scraping.

3.2. Privacy. Auto dealers collect personal data from their customers for the provision of services, such as for auto purchases and auto loans. Automobile loans and other financial services are covered by the

590 Id. § 28-4653(B). The requirement is for the entity accessing the data be “compliant with the Star Standards or other generally accepted standards that are at least as comprehensive as the Star Standards.” Id.
591 Id. § 28-4653(B).
592 Id. §§ 28-4654(A)(1), 28-4654(A)(2).
privacy and security requirements of the Gramm-Leach-Bliley Act ("GLBA"). Many dealers thus are covered by GLBA, and in such instances DMS providers and other third-party software providers who receive personal data are service providers, also covered by GLBA.

PORT opponents have claimed that personal data, such as for automobile loan borrowers, might not be adequately safeguarded by third-party software providers. However, the Arizona statute addresses “Protected Dealer Data,” which includes “personal, financial, or other data relating to a consumer that a consumer provides to a Dealer.” In addition to GLBA protections, measures in the Arizona statute to reduce that risk include: meeting an automobile industry cybersecurity standard; prohibiting the use of Protected Dealer Data without express consent of the Dealer; prohibiting third parties from using Protected Dealer Data in ways that are contrary to those third parties’ agreements with Dealers, and providing Dealers with rights to audit how third parties are using such data.

3.3. Other legal effects, including intellectual property. PORT opponents CDK and Reynolds have claimed that their intellectual property rights, for trade secrets and copyright, protect against access by third-party software providers. Proponents contend that the statute does not implicate any intellectual property rights.

Incentives of those presenting evidence of costs and risks. CDK and Reynolds face significant damages in the antitrust lawsuits, and

594 Id. § 28-4651(7)(a) (1999).
595 Id. § 28-4653(B). The requirement is for the entity accessing the data be “compliant with the Star Standards or other generally accepted standards that are at least as comprehensive as the Star Standards.” Id.
596 Id. §§ 28-4653(A)(1), 28-4653(B).
597 Id. § 28-4654(B).
598 Id.
therefore have an incentive to claim that security and privacy risks from the PORT are high.

4. LESSONS LEARNED

4.1. This case study is an example of a competition-based rationale for a mandatory PORT under state law. Proponents describe a market with two dominant firms, with over 90% market share in the market for DMS service providers, who are alleged to have agreed to limit access to Protected Dealer Data held in a DMS. To address the harms to competition, the Arizona law requires access, based on Dealer authorization, to Protected Dealer Data.

4.2. The case study illustrates the inter-connection of autonomy and competition arguments supporting the PORT. For dealers, the autonomy argument is based on an understanding of the underlying property right – the dealers “own their data,” and therefore should have control over who has access to that data. By contrast, for DMS providers, the autonomy argument is based on a contract – the DMS contract sets conditions for when dealers can transfer data to third parties or allow access to the DMS – the dealers argue that their contracts permit third party access; the DMS providers argue it does not. In a competitive market, the contract between the Dealer and DMS provider generally governs (although the meaning of the contracts are disputed here). By contrast, where the software is supplied by a dominant firm, or by two dominant firms acting pursuant to an agreement, then contractual limitations on access may violate antitrust law.

4.3. The case study illustrates a two-sided market for a non-consumer facing market. One side of the market is the DMS provider selling DMS software services to the automotive Dealers. Another side of the market is the Dealer seeking software services (apps) from either the DMS supplier or a third party. The antitrust concern, for proponents of the PORT, is that the dominant DMS providers have used their market power in the DMS market to extend their market power into the other side of the market – the market for apps (by extracting monopoly profits and by disadvantaging competing app providers).

4.4. The litigants have strong incentives to describe differently the costs and benefits of the PORT. The DMS suppliers have claimed cybersecurity risks and threats to what they assert is their intellectual property. The PORT proponents, by contrast, state that the
cybersecurity risks are essentially a pretext for blocking Dealer access to Protected Dealer Data. Proponents also question the broad claims to intellectual property protection.

4.5. The PORT requirements on automobile software providers under state legislation have significant similarities with requirements under the Inter-operability rule issued by the U.S. Department of Health and Human Services (“HHS”), and discussed in a separate case study.\(^{599}\) For instance, both PORT initiatives require creation of a standardized framework for the exchange of information. Both require use of an open API. For cybersecurity requirements, the HHS rule requires “fair and non-discriminatory” terms, while the Arizona statute prohibits placing an “unreasonable” limitation on an authorized third-party software company.

4.6. One general theme, across the case studies, is that there should be effective authentication before authorizing a PORT. The auto case study illustrates the difference between centralized and distributed authentication. DMS providers have sought to exercise centralized power over authentication, by prohibiting the Dealers from authorizing access by third parties such as an Authorized Integrator. Distributed authentication exists, by contrast, if the auto dealer establishes who is authorized to access the system on behalf of the auto dealer, including for employees and third parties authorized by the Dealer. The relative advantages of centralized vs. distributed authentication is an empirical question. Distributed authentication, however, is widely used, such as for eduroam, the “secure, world-wide roaming service developed for the international research and education community.”\(^{600}\) For instance, a university can issue (and revoke) credentials for authorized users, rather than having eduroam itself establish a global system for individual authorization of users.
