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

Peter Swire*

This article is prepared for the Privacy Law Scholars Conference 2020. The current version, as part of a larger research project, proposes a new framework for assessing issues of data portability and other required transfers of data. From a competition perspective, greater portability and other transfers of data can have pro-competitive effects, especially when one entity can otherwise gain market power by using data. 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, user control, and other values, and closing data flows, for reasons including protecting privacy and cybersecurity.

Part I of this PLSC version provides an introduction and overview for the project. Part II consists of the Structured Questions designed to enable a Portability and Other Required Transfer Impact Assessment ("PORT-IA"). Part III provides an example case study for phone number portability in the United States and European Union, as well as summaries of six other case studies, on: (1) EU financial services; (2) US financial services; (3) Open Data; (4) US health care; (5) EU health care; and (6) automobile dealer statutes passed in Arizona and other states. Part IV documents how the structured questions are consistent with the case studies and other research to date.

Part I: Introduction and Overview for the Project

A. Terminology.

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,[1] with a somewhat similar portability requirement in

* Elizabeth and Tommy Holder Chair of Law and Ethics, Georgia Tech Scheller College of Business; Senior Counsel, Alston & Bird LLP. Research support for this research project comes from Facebook, the Institute for Information Security and Privacy at Georgia Tech, and the Georgia Tech Scheller College of Business. The views expressed here are those of the author.

[1] 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, Art. 20 (hereinafter "GDPR").

the California Consumer Privacy Act, which entered into effect at the beginning of 2020.[2] In light of these laws, this article reserves the term "**portability**" to a required transfer when **one** person wishes to port (transfer) the data.

As discussed below, however, there are also increasingly broad proposals for mandatory transfers at a larger scale, such as opening up 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").[3] 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**" to 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 that apply to the data of more than one person.

B. <u>The PORT-IA</u>.

In order to enable a consistent and disciplined evaluation of PORT initiatives, this article proposes a Portability and Other Required Transfers Impact Assessment, or PORT-IA. The approach is similar to Privacy Impact Assessments required by U.S. laws such as the E-Government Act of 2002[4] or Data Protection Impact Assessments required by GDPR.[5]

Part II of the PLSC version of the research project includes a detailed set of structured questions to evaluate PORTability benefits and risks and costs. The PORT-IA begins with a description of the proposed data flows – what origination, what destination, what data is covered, and what applicable law or other requirements. The PORT-IA next examines the benefits of the proposed PORT from critical 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.[6] There are also non-competition rationales for a PORT, including: user control/autonomy and other non-

[2] California Consumer Privacy Act, Section 1798.100(d).
[3] https://www.hhs.gov/about/news/2020/03/09/hhs-finalizes-historic-rules-to-provide-patients-more-control-of-their-health-data.html.
[4] E-Government Act of 2002, Pub. L. 107-347, Sec. 208.
[5] GDPR, Article 35.
[6] For one detailed recent explanation of different theories of competitive harm, see Emilio Calvano & Michele Polo, "Market Power, Competition and Innovation in digital markets: A survey," (Dec. 1 2019), https://ssrn.com/abstract=3523611.

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 an 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 next 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.”[7] With that said, implementing portability can have substantial cybersecurity and other risks, and may actually reduce consumer welfare.[8] 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 overall 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.

[7] Peter Swire & Yianni Lagos, “Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique,” 72 Maryland Law Review 335, 379 (2013), https://ssrn.com/abstract=2159157.
[8] Id. at 380.

C. The Case Studies.

Part III of this version presents initial discussion of detailed case studies that explore and evaluate the benefits and costs of existing PORTability requirements in various sectors. The research and some writing is now complete for the following: (i) US and EU phone number portability;[9] (ii) the new US health care interoperability regulation;[10] (iii) EU portability requirements concerning health care data;[11] (iv) the EU Payment Services Directives, requiring transfers among financial services organizations;[12] (v) similar issues in the US financial services sector, implementing Section 1033 of the Dodd-Frank Act;[13] (vi) Open Data requirements for government agencies, especially in the US;[14] and (vii) a lesser-known set of recent laws in Arizona and other states mandating portability for the data of automobile dealers.[15]

This PLSC version of the research includes Part I of these seven case studies – a description of the origins of the data, its destination, what type of data is covered, and the applicable law. As discussed further below, an accurate description of the mandated data flow(s) is an essential first step to analyzing whether the mandate has net benefits or costs. The phone number portability is published in a relatively full version, to illustrate (at least in summary form) how the PORT-IA Structured Questions can assist in identifying major benefits and costs of an initiative.

These case studies, which will be published in more detail, have provided the basis for developing the structured questions for the PORT-IA. The goal has been generalizability – identifying and testing whether the PORT-IA provides the right set of questions to assess PORT initiatives that are diverse across sectors, data type, and geography. Part IV, discussed below, seeks to "show my work" – explain how details of the structured questions grew out of specific takeaways from the case studies. This PLSC version highlights two points about the case studies.

First, the earliest implemented PORT initiatives, for phone number portability, represent uncharacteristically asymmetrical examples of the potential benefits of PORT initiatives. To the

[9] Federal Communications Commission, "Wireless Local Number Portability," https://www.fcc.gov/general/wireless-local-number-portability-wlnp; European Commission, "Number Portability," https://ec.europa.eu/digital-single-market/en/number-portability.

[10] https://www.hhs.gov/about/news/2020/03/09/hhs-finalizes-historic-rules-to-provide-patients-more-control-of-their-health-data.html.

[11] *E.g.,* https://ec.europa.eu/health/ehealth/electronic_crossborder_healthservices_en.

[12] The Payment Services Directive-2 is Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366.

[13] 12 U.S.C. Sec. 5481(6). For discussion, see Michael Barr et al., "Consumer Autonomy and Pathways to Portability in Banking and Financial Services (November 2019). University of Michigan Center on Finance, Law & Policy Working Paper, https://ssrn.com/abstract=3483757.

[14] *E.g*., OPEN Government Data Act, 44 U.S.C. § 3501.

[15] *E.g.*, Arizona Revised Statute Section 28-4651 to 4655.

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 means that friends and business contacts may lose touch, 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 is often done in person, in a way that involves effective authentication of the user. Overall, phone number portability thus offers 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 port data out of Facebook was a significant stated rationale for including the right to data portability in GDPR.[16] 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.

D. Validation of the Structured Questions.

Part IV of the PLSC version is entitled "Documenting How the Structured Questions Are Consistent with the Case Studies and Other Research To Date." Part IV reprints each of the Structured Questions and then adds discussion to assist those who wish to perform a PORT-IA of a PORT initiative. Part IV discusses how the case studies and other research to date fit with the language of each of the Structured Questions.

Over the course of the research to date, the Structured Questions have evolved quite a bit, especially in response to specific results from the case studies. For instance, Regulation E, which implements the U.S. Electronic Funds Transfer Act, provides that consumers generally are not liable for unauthorized electronic fund transfers. Regulation E applies to banks but not

[16] *See* Peter Swire & Yianni Lagos, "Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique," 72 Maryland Law Review 335, 335-36 (2013), https://ssrn.com/abstract=2159157, citing *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 Movement of Such Data (General Data Protection Regulation)*, art. 18, at 26, COM (2012) 11 final (Jan. 25, 2012).

generally to non-banks such as fintech software providers. Based on this example, I learned to include Question 12(a): "As a result of the PORT, would consumers suffer any legal risks, such as reduced coverage of consumer protection laws?" Going forward, a person performing a PORT-IA would thus be alerted to look for changes in legal protections that may result when data shifts from the transferring entity to the recipient entity.

As currently drafted, the Structured Questions reflect the case studies and other research across the diverse sectors, data type, and geography. My belief is that 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.

E. The research project and next steps. The larger research project thus seeks to reduce the intellectual confusion about initiatives that have been lumped together under terms such as "portability," "inter-operability," and "data sharing." This PLSC version proposes clearer terminology, with "portability' as transfers involving one person's data (as in the right to data portability), and "other required transfers" for transfers involving more than one person's data. The seven case studies provide a basis for drafting the structured questions in the PORT impact assessment, or PORT-IA.

The longer research project includes a careful literature review. My own work on relevant issues dates back to 2007 testimony to the Federal Trade Commission on antitrust and privacy,[17] and a lengthy law review article in 2013 on the right to data portability.[18] Even more recently, there has been surprisingly little written comparing PORT initiatives across sectors, or analyzing when PORT initiatives are likely to be more or less beneficial.[19] The most similar research project has been led by Professor Inge Graef of Tilburg University.[20] That project includes references to additional potentially useful case studies; for instance, the EU requires PORTability to maintain competition in the aftermarket for repair and maintenance services for automobiles.[21] The literature review will include the burgeoning number of reports and

[17] Peter Swire, "Protecting Consumers: Privacy Matters in Antitrust Analysis," (Oct. 19, 2007), https://www.americanprogress.org/issues/economy/news/2007/10/19/3564/protecting-consumers-privacy-matters-in-antitrust-analysis.

[18] Peter Swire & Yianni Lagos, "Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique," 72 Maryland Law Review 335 (2013), https://ssrn.com/abstract=2159157.

[19] For one short assessment of the benefits and limits of portability, see Gabriel Nicholas & Michael Weinberg, "Silicon Valley's Favorite Idea for Encouraging Competition -- Data portability sounds promising, but it might not be the regulatory golden goose the private and public sectors hope it is," Slate, Nov. 14, 2019, https://slate.com/technology/2019/11/data-portability-facebook-competition-antitrust.html.

[20] Inge Graef et al., "Spillovers in Data Governance : the relationship between the GDPR's right to data portability and EU sector-specific data access regimes," TILEC Discussion Paper (April, 2019), http://ssrn.com/abstract=3369509; Inge Graef et al. "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law," 19 German L.J. 1359 (2018); Inge Graef, "Mandating portability and interoperability in online social networks: Regulatory and competition law issues in the European Union," 39 Telecommunications Policy 502 (2015). *See also* Orla Lynskey, "Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability," 42 European Law Review 793 (2017).

[21] Wolfgang Kerber & Jonas Severin Frank, "Data Governance Regimes in the Digital Economy: The Example of Connected Cars," (2017), https://ssrn.com/abstract=3064794.

initiatives from government, including: guidance on the right to data portability by European data protection regulators;[22] a December, 2019 report by the United Kingdom's Competition and Marketing Authority on "Online platforms and digital advertising," setting forth a number of possible ambitious PORT initiatives,[23] and the Augmenting Compatibility and Competition by Enabling Service Switching Act ("ACCESS Act"), a bipartisan bill introduced in the U.S. Senate in October, 2019 to require portability and interoperability.[24]

Building on the literature review and the case studies, the research project will examine in further depth each of the relevant aspects of the PORT-IA, including competition, autonomy/user control, privacy, cybersecurity, and other legal or regulatory considerations. The project will draw on my experience as a professor of privacy, cybersecurity, and antitrust law, and as a scholar who was written extensively about both EU and US law. The goal is to identify conditions where the benefits or costs of a PORT initiative are likely to be particularly great.

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. 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. For example, the GDPR requires consent to be "freely given, specific, informed and unambiguous."[25] In some settings, such as consent by employees, regulators presume that consent is not valid: "Given the imbalance of power between an employer and its staff members, employees can only give free consent in exceptional circumstances."[26] By contrast, where a PORT-IA shows strong benefits to individuals, then the presumptive validity of consent may be easier to establish.

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

===

[22] Guidelines on the right to data portability under Regulation 2016/679, WP242 rev.01, p. 3-4, available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.
[23] Competition and Markets Authority, "Online platforms and digital advertising market study," (Interim report; Dec. 2019), https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study.
[24] S. 2658, 116th Cong., https://www.congress.gov/bill/116th-congress/senate-bill/2658?q=%7B%22search%22%3A%5B%22Augmenting+Compatibility+and+Competition+by+Enabling+Service+Switching+%28ACCESS%29+Act%22%5D%7D&s=3&r=1
[25] GDPR, Art. 4(11).
[26] Article 29 Data Protection Working Party, "Guidelines on Consent under Regulation 2016/679," (Nov. 28, 2017), at 8.

Part II: 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 relevant 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 arising from the method of transmission, such as transfer of a user's passwords or other sensitive data to the recipient of the transfer?

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: 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.

===

Part III: Case Studies

III.A. Phone Number Portability

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. We also include, in Section 1.6, a brief summary of the laws governing number portability in the E.U. The two regimes offer substantially similar rights to users, and benefits and costs and risks of their PORT initiatives.

1.2. **Origination.** The Number Portability Administration Center, for the United States.[27] 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.[28] 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.[29]

1.3. **Destination.** Wireless and wireline phone service providers.[30]

1.4. **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)

[27] *The NPAC, Neustar & LNP*, NUMBER PORTABILITY ADMIN. CTR., *available at* https://www.npac.com/number-portability/the-npac-neustar-lnp (last accessed Mar. 11, 2020).

[28] *Id.*

[29] *Id.* NPAC also operates in Canada where their phone numbers are administered and regulated by Neustar.

[30] WIRELESS LOCAL NUMBER PORTABILITY, FED. COM. COMM'N, *available at* https://www.fcc.gov/general/wireless-local-number-portability-wlnp.

Service Type; (6) Alternative SPID (to identify a reseller); (7) billing ID; and, (8) end user location and type.[31]

1.5. **Applicable Law.** Phone number portability is mandated by the Telecommunications Act of 1996 and regulated by the Federal Communications Commission (FCC).[32] 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."'"[33] 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.[34]

1.6. The European Union similarly mandated phone number portability via Article 30 of the Universal Services Directive ("**USD**") of 2002.[35] 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 when the number is activated with another operator, 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.[36]

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."[37] This is true also for business customers whose costs could include revising marketing materials, keeping track of customers'

[31] *How LNP Works*, NUMBER PORTABILITY ADMIN. CTR., *available at* https://www.npac.com/number-portability/how-lnp-works (last accessed Mar. 11, 2020).

[32] *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 4.

[33] William Drexel, *Telecom Public Policy Schizophrenia: Schumpeterian Destruction Versus Managed Competition*, 9 VA. J.L. & TECH. 5, 13-14 (2004).

[34] *See* Stephen M. Kessing, *Wireless Local Number Portability: New Rules Will Have Broad Effects*, 2004 DUKE L. & TECH. REV. 6.

[35] 2002 O.J. (L 108/56) 30 *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0022&from=EN (last accessed Mar. 31, 2020).

[12] *Id.* at art. 30.

[37] 11 FCC Rcd 8352, 8368, 1996 FCC LEXIS 3430, *34-35, 3 Comm. Reg. (P & F) 600.

information once they change numbers, and the possibility of losing customers because a business changed its phone number.[38]

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.[39] 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.[40] 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 change in number. Therefore, retaining a phone number reduces the network effects that a dominant phone carrier may have because a consumer does not have to worry about the significant number of contacts that will have to be informed about a new phone number.[41] Additionally, when there is an increase in willingness of a "consumer to change to another service provider" there is consequently an increase in competition.[42] Thus, consumers have "more choices and reduce[d] prices."[43] Prices for wireless services decreased after number portability was mandated for wireless service providers.[44]

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

[38] *Id.*

[39] FED. COM. COMM'N, No. 96-325, FIRST REPORT AND ORDER: IN THE MATTER OF IMPLEMENTATION OF THE LOCAL COMPETITION PROVISIONS IN THE TELECOMMUNICATIONS ACT OF 1996 AND INTERCONNECTION BETWEEN LOCAL EXCHANGE CARRIERS AND COMMERCIAL MOBILE RADIO SERVICE PROVIDERS, 12 (1996), *available at* 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."). *See also In the Matter of Telephone Number Portability*, 1996 FCC LEXIS 3430, *34, 11 FCC Rcd 8352, 8368, 3 Comm. Reg. (P & F) 600 ("[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.").

[40] *See* What is LNP? Number Portability Administration Center, *available at* https://www.npac.com/number-portability/what-is-lnp ("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.").

[41] 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.).

[42] *What is LNP?* NUMBER PORTABILITY ADMIN. CTR., *available at* https://www.npac.com/number-portability/what-is-lnp (last accessed Mar. 11, 2020).

[43] *Id.*

[44] Minjung Park, *The Economic Impact of Wireless Number Portability*, 59 J. INDUS. ECON. 714, 715 (2011).

portability was not an option when number portability became required.[45] LECs were required to use current available number portability measures.[46] These portability requirements took place over a long period of time, and the FCC has continuing legal authority to update requirements for portability.[47]

3. RISKS AND COSTS OF PORT INITIATIVE

3.1. Security. At the time the wired and wireless phone number PORTs were implemented, few potential or anticipated security risks existed. Enrollment for a new phone service has often been done in person, with an opportunity for relatively strong authentication of the user.

3.2. Recently, however, mobile number portability hacking has been on the rise.[48] Hackers have convinced phone carriers to port numbers, and then the hacker can reset the passwords on every online account that uses that phone number for account authentication.[49] In order to carry out a "port-out scam" all a hacker generally needs to know, depending on the carrier is a person's phone number, name, address, last four digits of a social security number, the person's account login information.[50] Hacker can obtain this information through theft or phishing. Particularly with one-time passwords sent through SMS text being used for authentication, phone numbers are increasingly important because a hacker can change the user's account passwords and steal money, information, or identification easily.[51] Phone number portability vulnerabilities can be

[45] *See* 11 FCC Rcd 8352, 8356, 1996 FCC LEXIS 3430, *7-8, 3 Comm. Reg. (P & F) 600.

[46] *Id.*

[47] "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." Separate Statement of Chairman Michael K. Powell, *In re Tel. Number Portability*: CTIA Petitions for Declaratory Ruling on Wireline-Wireless Porting Issues, CC Docket No. 95-116, FCC-03-284 (2003), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-284A2.pdf.

[48] Alix Langone, *My Cell Phone Number Was Stolen. It Nearly Ruined My Life*, MONEY (Jun. 8, 2018), *available at* https://money.com/cell-phone-porting-scam-t-mobile/ ("A T-Mobile spokesperson said these are industry-wide issues, but did acknowledge a recent 'uptick' in cell phone hijacking.").

[49] *See* Lorrie Cranor, "Your mobile phone account could be hijacked by an identity thief," FTC, *available at* https://www.ftc.gov/news-events/blogs/techftc/2016/06/your-mobile-phone-account-could-be-hijacked-identity-thief (Jun. 7, 2016) ("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.").

[50] Erik Hyrkas, *Port-Out Scams and SIM Hijacking: How to Protect Yourself*, LET'S TALK (Mar. 28, 2019), *available at* https://www.letstalk.com/cellphones/guides/port-out-scams/.

[51] Richi Jennings, *Mobile number portability hacking (it's WAY too easy): The 2FA FAIL-factor*, TECH BEACON, *available at* https://techbeacon.com/security/mobile-number-portability-hacking-its-way-too-easy-2fa-fail-factor.

mitigated by the phone user making it more difficult for hackers to gain their information such as: altering their security questions so that they are difficult to guess, getting a virtual phone number or VoIP plan and using that number publicly rather than the assigned 10-digit phone number.[52] 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.

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. In instances where 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.[53]

4. LESSONS LEARNED

4.1. This case study shows that the US 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 is significant 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

[52] Gabriel Wood, *Phone Porting: How Hackers Can Hijack Your Mobile Phone Number*, NEXT ADVISOR (Jan. 12, 2018), *available at* https://www.nextadvisor.com/phone-porting-how-hackers-can-hijack-your-mobile-phone-number.

[53] *See Memorandum Opinion and Order and Further Notice of Proposed Rulemaking* (FCC 03-284), FED. COMM. COMM'N. at n. 62 (2003), *available at* 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.").

become greater recently). The other case studies have not generally shown this pattern of clearly large benefits and clearly 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 occur now 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. Then, the hacker steals information and accounts associated with the phone number.

4.6. Consumers have utilized the benefits of phone number portability, with millions of customers taking advantage of it once the PORT went into effect.[54]

[54] *FCC Observes First Anniversary of Wireless Local Number Portability*, FED. COMM. COMM'N (2004), *available at* https://www.fcc.gov/general/wireless-local-number-portability-wlnp#recent.

III.B EU Financial Services.

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")[55] as updated and expanded in the Payment Services Directive of November 2015 ("PSD2").[56] In the UK, after study by the Open Banking Working Group,[57] the Competition & Markets Authority ("CMA") created the Open Banking Implementation Entity ("OBIE") to set software standards and industry guidelines to implement PSD2.[58] 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.

---

[55] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007L0064&from=EN. The European Commission explained the need for PSD1 and PSD2 on a dedicated payments homepage. *See* Payment Services, EUROPEAN COMM'N, *available at* https://ec.europa.eu/info/business-economy-euro/banking-and-finance/consumer-finance-and-payments/payment-services/payment-services_en. For the differences between PSD1 and PSD2, *see* MEMO/15/5793 *Payment Services Directive: Frequently Asked Questions*, 12 *available at* https://ec.europa.eu/commission/presscorner/detail/en/MEMO_15_5793. *See also* an explanation from the European Payments Council: *Why was the Revised Payment Services Directive (PSD2) created?*, EUROPEAN PAYMENTS COUNCIL, *available at* https://www.europeanpaymentscouncil.eu/sites/default/files/infographic/2018-04/EPC_Infographic_PSD2_April%202018.pdf.

[56] Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366 [hereinafter PSD2].

[57] The Open Data Institute set up the Open Banking Working Group in September 2015 – at the request of the UK Government. *See Open Banking: Setting a Standard and Enabling Innovation*, OPEN DATA INST., *available at* https://theodi.org/project/open-banking-setting-a-standard-and-enabling-innovation/; and, Open Banking Working Group: Roster and Forthcoming Report Announced, OPEN DATA INST., *available at* http://oldsite.theodi.org/news/open-banking-working-group-roster-report-announced.

[58] *See generally About Us*, OPEN BANKING, *available at* https://www.openbanking.org.uk/about-us/: "The Open Banking Implementation Entity was created by the UK's Competition and Markets Authority to create software standards and industry guidelines that drive competition and innovation in UK retail banking. [….] The Open Banking Implementation Entity (OBIE) is the company set up by the CMA in 2016 to deliver Open Banking. Our trading name is Open Banking Limited. We are governed by the CMA and funded by the UK's nine largest banks and building societies."

1.3 **Destination**. (1) Consumers. (2) PSPs, including 'account servicing payment service providers,' 'payment initiation service providers,' and 'account information service providers.' as defined in PSD2.[59]

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.[60] The relevant product market is the retail payments market, including card, internet and mobile payments.

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").[61] PSD2 notably widened the scope of PSD1 to cover third party 'payment initiation services.'[62] Prior to PSD2, such new providers had not been regulated at the EU level, so PSD2 covered them, addressing issues such as confidentiality, liability and security of transactions with such providers.

1.6 **Some Helpful Resources:**

- Green Paper: Towards an Integrated European Market for Card, Internet and Mobile Payments, Com/2011/0941/final (2017), available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52011DC0941.

---

[59] See the definitions provided for these terms of Article 4, PSD2, *e.g.* "'account servicing payment service provider' means a payment service provider providing and maintaining a payment account for a payer."

[60] Pursuant to, respectively, Articles 45, 46, 47, 48, and 49 of PSD2:

- 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.
- 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.
- 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.
- 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.
- 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.

[61] *See Fair, Reasonable and Non-Discriminatory (FRAND) Licensing Terms. Research Analysis of a Controversial Concept*, EUROPEAN COMM'N, *available at* https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/fair-reasonable-and-non-discriminatory-frand-licensing-terms-research-analysis-controversial.

[62] *See Payment Services Directive: Frequently Asked Questions*, EUROPEAN COMM'N, *available at* https://ec.europa.eu/commission/presscorner/detail/en/MEMO_15_5793.

- Opinion dated 5 December 2013 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, *available at* https://edps.europa.eu/sites/edp/files/publication/13-12-05_opinion_payments_en.pdf.
- Concerning delays in implementation of PSD-2: Nick Caley, *PSD2 in 2019: A Year of Yet More Delays*,FINTECH FUTURES (Dec. 30, 2019), *available at* https://www.fintechfutures.com/2019/12/psd2-in-2019-a-year-of-yet-more-delays/; The Sobering September Preview: Banks' PSD2 APIs Far From Ready, TINK (Jun. 14, 2019) available at https://blog.tink.com/blog/2019/06/14/psd2-updated-sandbox.

- Markos Zachariadis and Pinar Ozcan, *The API Economy and Digital Transformation in Financial Services: The Case of Open Banking*, SWIFT Institute Working Paper No. 2016-001, section 1. (June 15, 2017). *available at* http://dx.doi.org/10.2139/ssrn.2975199.

III.C. US Financial Services.

1. Summary of the 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.[63]

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."[64] 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."[65] The Consumer Financial Protection Bureau ("CFPB") has the authority to issue rules for "standardized formats for data,"[66] but has not done so.

1.5 Some Helpful References:

- *"Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation"* (2017), available at https://www.consumerfinance.gov/data-research/research-reports/consumer-protection-principles-consumer-authorized-financial-data-sharing-and-aggregation.

- "*Consumer Financial Protection Bureau Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act*," available at https://files.consumerfinance.gov/f/documents/cfpb_heironimus-statement_symposium-consumer-access-financial-records.pdf

- U.S. Dept. of Treasury, "*A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation"* (2018), available at

[63] *See* Greg Johnson, *12 Mint.com Alternatives You'll Love: Our Top Picks for 2020*, CLUB THRIFTY (Jan. 14, 2020) (providing current list of similar providers), *available at* https://clubthrifty.com/mint-com-alternative.

[64] Dodd-Frank Act Wall Street Reform and Consumer Protection Act, 12 U.S.C. § 5481(6) (2020).

[65] Dodd-Frank Act Wall Street Reform and Consumer Protection Act, 12 U.S.C. § 5533 (2020).

[66] 12 U.S.C. § 5533(d).

https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation_0.pdf.

Michael S. Barr, Abigail DeHart, and Andrew Kang, *Consumer Autonomy and Pathways to Portability in Banking and Financial Services* (University of Michigan Center on Finance, Law & Policy Working Paper), available at https://ssrn.com/abstract=3483757.

III.D. Open Data.

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 principally on the United States, with reference to the European Union.

1.2. **Origination:** The data comes from public agencies. Previously, this data was in printed form or 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.[67]

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 data regarding populations.[68] In addition to the federal Data.Gov, more than 260 cities and municipalities have launched their own open data initiatives.[69] Each of the individual states have also made data publicly available and accessible online, to varying degrees.[70]

1.5. **Applicable law:** The federal Data.Gov portal launched in 2009.[71] The federal Data.Gov portal is now mandated by the OPEN Government Data Act, 44 U.S.C. § 3501 (Jan. 24,

---

[67] *See* Beth Simon Novak, Forum: Is Open Data the Death of FOIA, The Yale Law Journal (Nov. 21, 2016), *available at* https://www.yalelawjournal.org/forum/is-open-data-the-death-of-foia; Martin, Kristen et al., *Privacy Interests in Public Records: An Empirical Investigation*, 31 HARV. J. LAW & TECH. 111, 114-17 (2017), *available at* http://jolt.law.harvard.edu/articles/pdf/v31/31HarvJLTech111.pdf.

[68] *See* John Whittington et al., *ARTICLE: Push, Pull, and Spill: A Transdisciplinary Case Study in Municipal Open Government*, 30 BERKELEY TECH. L. J. 1899, 1926-30 (2015); 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*, Data.Illinois.Gov, available at https://data.illinois.gov/.

[69] *U.S. City Open Data Census*, OPEN KNOWLEDGE INTERNATIONAL, *available a*t http://us-cities.survey.okfn.org/.

[70] Meta S. Brown, *States Offer Information Resources: 50+ Open Data Portals*, FORBES (Apr. 30, 2018) *available a*t https://www.forbes.com/sites/metabrown/2018/04/30/us-states-offer-information-resources-50-open-data-portals/#3c5ff1245225.

[71] *See Memorandum: Transparency and Open Government*, THE WHITE HOUSE BRIEFING ROOM, *available at* https://obamawhitehouse.archives.gov/the-press-office/transparency-and-open-government.

2019).[72] The OPEN Government Data Act requires "timely and equitable access to the agency's public information."[73] However, each agency is left to interpret the meaning of "public information," design its own Open Data policy, and decide which datasets to publish.[74] The various state and local open data portals are each governed by state and municipal laws, regulations, policies, terms of use and privacy policies.

1.6. Some Helpful References:

- *Open government data powers software applications that help consumers make informed decisions*, DATA.GOV, *available at* www.data.gover/consumer//consumer-apps-page**.**

- Stefaan Verhulst, et al., *Open Data's Impact: When Demand and Supply Meet,* GOVLAB (Mar. 2016), *available at* https://www.thegovlab.org/static/files/publications/open-data-impact-key-findings.pdf.

- Raphael Duguay, et al., *The Impact of Open Government on Public Procurement*, (Nov. 2019), *available at* https://ssrn.com/abstract=3483868.

- An Yan and Nicholas Weber, *Mining Open Government Data Used in Scientific Research*, THE INFORMATION SCHOOL, UNIVERSITY OF WASHINGTON (Mar. 24, 2018) *available at* https://arxiv.org/pdf/1802.03074.pdf.

- *Policy: European legislation on open data and the re-use of public sector information*, EUROPEAN COMMISSION (Mar. 8, 2020) *available a*t https://ec.europa.eu/digital-single-market/en/european-legislation-reuse-public-sector-information.

[72] *See* Summary H.R.4174 – 115th Congress (2017-2018), Public Law No: 115-435, *available at* https://www.congress.gov/bill/115th-congress/house-bill/4174; 44 USCS §3501.

[73] 44 USCS §3506(d)(1).

[74] *See* 44 USCS §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.").

III.E: US Health Care

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

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"),[75] 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.[76]

1.3 The Final Rule was published on March 9, 2020, with regulatory text and accompanying material of over 1200 pages.[77]

1.4 Note - the term "interoperability" is used in the Proposed Rule and the Final Rule to apply broadly, to: (1) technical interoperability; (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.

---

[75] 21st Century Cures Act, Pub. L. No. 114-255, 130 Stat. 1033, *available at* https://www.congress.gov/bill/114th-congress/house-bill/34; 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 84 Fed. Reg. 7424 (Mar. 4, 2019), *available at* https://www.federalregister.gov/documents/2019/03/04/2019-02224/21st-century-cures-act-interoperability-information-blocking-and-the-onc-health-it-certification.

[76] Elise Sweeney Anthony & Michael Lipinski, *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Proposed Rule*, THE OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., *available at* https://www.healthit.gov/sites/default/files/page/2019-02/HITACNPRMPresentation.pdf.; 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 84 Fed. Reg. 7424, 7469 (proposed March 4, 2019) (to be codified at 45 C.F.R. parts 170 and 171), *available at* https://www.federalregister.gov/documents/2019/03/04/2019-02224/21st-century-cures-act-interoperability-information-blocking-and-the-onc-health-it-certification.

[77] 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 45 C.F.R. 170, 1149 *available at* https://www.healthit.gov/cerus/sites/cerus/files/2020-03/ONC_Cures_Act_Final_Rule_03092020.pdf.

1.2.1 PORT Initiative A: Information Blocking

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

1.2.3 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").[78]

1.2.4 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. [79]

1.2.5 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."[80] 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.[81] 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.[82]

1.3 PORT Initiative B: Health IT Developer Certification Requirements

1.3.1 Origination: Software of a covered health IT developer.

1.3.2 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

---

[78] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191,110 Stat. 1936 (codified as amended in scattered sections of Title 42).

[79] 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 1149, *available at* https://www.healthit.gov/cerus/sites/cerus/files/2020-03/ONC_Cures_Act_Final_Rule_03092020.pdf ("*Electronic health information* (EHI) is defined as it is in § 171.102.").

[80] *Id.* at 45 C.F.R. 171.103.

[81] *Id. at* 45 C.F.R. 170, 170.200-205.

[82] *Id.* at 45 C.F.R. 171.300 -171.303.

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

1.3.4 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 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.[83]

1.4 PORT Initiative C: Standardized API

1.4.1 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."[84] For instance, the API would enable export of the patient's data from a health care provider to a smartphone app.[85]

1.4.2 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).

1.4.3 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.[86]

1.4.4 Legal requirements: The Proposed 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

[83] Elise Sweeney, *supra* note 2.

[84] 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 45 C.F.R. 170, 170.404(a).

[85] 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 84 Fed. Reg. 7424, 7481 (March 4, 2019) (to be codified at 45 C.F.R. parts 170 and 171), *available at* https://www.federalregister.gov/d/2019-02224/p-830.

[86] 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 45 C.F.R. 170, 170.404(a).

Users to interact with the API technology,"[87] and (4) the API be licensed on reasonable and non-discriminatory terms, and include limits on fees.

1.5 Some Helpful References:

- In addition to the Federal Register notice for the final rule, the most readable discussion that I found is Elise Sweeney Anthony & Michael Lipinski, *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Proposed Rule*, The Office of the Nat'l Coordinator for Health Info. Tech., *available at* https://www.healthit.gov/sites/default/files/page/2019-02/HITACNPRMPresentation.pdf. (Download archived documents from NPRM.)

[87] Elise Sweeney, *supra* note 2 at 20.

III.F. EU Health Care.

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[88] (the Cross-Border Healthcare Directive), 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 many efforts further described below and 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 mandates 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 Member State; and (2) with respect to Patient Summary data, the data will be received by a 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 health-related information about the individual such as an individual's allergies, current medication, previous illness, and surgeries[89], as well as data for the administration of the patient, such as identifying data and contact information.[90]

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. Examples of actions and initiatives are included below.

---

[88] Council Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02011L0024-20140101.

[89] *See* Electronic cross-border health services, EUROPEAN COMM'N, *available at* https://ec.europa.eu/health/ehealth/electronic_crossborder_healthservices_en.

[90] *See* eHealth Network Guideline on the electronic exchange of health data under Cross-Border Directive 2011/24/EU, Release 2, Patient Summary for unscheduled care (Nov. 2016), *available at* https://ec.europa.eu/cefdigital/wiki/download/attachments/55878732/%28Adopted%29%20Patient%20Summary%20Guideline%20cross-border%20exchange%20of%20health%20data%20%28release%202%29.pdf?version=1&modificationDate=1512129673394&api=v2.

1.6 Additional helpful 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; [91]

(2) 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;[92]

(3) 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;[93]

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

(5) 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;[94]

(6) the Commission's 2019 *'*Recommendation on a European Electronic Health Record exchange format*'*, 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

[91] *Recommendation of 2 July 2008 on cross-border interoperability of electronic health record systems*, EUROPEAN COMM'N, *available at* https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32008H0594.

[92] *Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and The Committee of The Regions, Towards interoperability for European public services*, EUROPEAN COMM'N, (Dec. 2010), *available at* https://ec.europa.eu/isa2/library/communication-towards-interoperability-european-public-services_en.

[93] *See generally*, *The European eHealth Governance Initiative*, EHEALTH GOVERNANCE INITIATIVE, *available at* http://www.ehgi.eu/Pages/default.aspx?articleID=1.

[94] *See generally*, *EXPAND: Deploying sustainable cross-border eHealth services in the EU*, EUROPEAN COMM'N, *available at* https://ec.europa.eu/digital-single-market/en/news/expand-deploying-sustainable-cross-border-ehealth-services-eu.

Summary) to laboratory results, medical images and hospital discharge reports and puts forward recommended technical specifications for the exchange of this data; [95] and

(7) 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.[96]

(8) Additional sources documenting related initiatives are available at: (a) http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=5168; and (b) https://ec.europa.eu/health/ehealth/cooperation_en.

[95] *See generally*, *Exchange of Electronic Health Records across the EU*, EUROPEAN COMM'N, *available at* https://ec.europa.eu/digital-single-market/en/exchange-electronic-health-records-across-eu.

[96] *See generally*, *New members of eHealth Stakeholder Group start their work*, EUROPEAN COMM'N, *available at* https://ec.europa.eu/digital-single-market/en/news/new-members-ehealth-stakeholder-group-start-their-work.

III.G. US Automobile Dealers

1. DESCRIPTION OF Portability or Other Required Transfer (PORT) Initiative

Automobile dealers typically contract with software companies for "Dealer Management System" ("DMS") services, to assist dealers with their business operations.[97] 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.[98]Automobile dealers have also contracted with systems integrators and application developers ("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.

Reynolds and CDK have changed their position over time concerning a dealer's ability to authorize 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 access by software providers. 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 software providers. The laws are intended to give dealers more control over their data stored in the DMS.

CDK and Reynolds have challenged the Arizona statute in federal court, claiming that the statute is unlawful.[99] Separately, software providers, dealers, and others have brought lawsuits against CDK and Reynolds, alleging (among other things) that they entered into an agreement to exclude software providers in violation of antitrust laws. Peter Swire serves 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.[100]

---

[97] This case study in the U.S. automobile industry focuses on PORTability statutes passed in Arizona and at least three other states in 2019. The states of Montana, North Carolina, and Oregon have enacted substantively similar statutes. *See* H.B. 617, 66th Leg., Reg. Sess. (Mont. 2019) enacted on May 6, 2019, and currently in effect, *available at* https://leg.mt.gov/bills/2019/BillHtml/HB0617.htm; H.R. 3152, 80th Leg. Assemb., Reg. Sess. (Or. 2019) enacted on July 2, 2019, and currently in effect, *available at*: https://olis.leg.state.or.us/liz/2019R1/Downloads/MeasureDocument/HB3152/Introduced; 2019 N.C. Sess. Laws 384 enacted on July 19, 2019, and going into effect on October 1, 2020, *available at*: https://www.ncleg.gov/BillLookup/2019/S384.

[98] *Dealer Mgmt. Sys. Antitrust Litig. v. CDK Glob*., No. 18-cv-864, 2018 U.S. Dist. LEXIS 214398, at *21 (N.D. Ill. Oct. 22, 2018)("Defendants CDK and Reynolds control close to 80 percent of the United States market by number of dealers and approximately 90 of the United States market by vehicles sold.").

[99] *See e.g*., David Muller, *CDK, Reynolds Challenge Ariz. Dealer Data Law*, 93 AUTOMOTIVE NEWS 34 (Aug. 26, 2019), *available at* https://www.autonews.com/dealers/cdk-reynolds-challenge-ariz-dealer-data-law. Peter Swire has submitted an expert declaration on behalf of the Arizona Automobile Dealers Association in *CDK Global, LLC v. Brnovitch*, No. 2:19-cv-04849-GMS (D. Ariz. Mar. 19, 2020).

[100] 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. *Authenticom, Inc. v. CDK Global, LLC*, No. 17-cv-318 (W.D. Wis. 2017), Dkt No. 58 (expert report/declaration of

1.1 **Origination.** A "Dealer Data System."[101] "Dealer Data System" is a defined term under the Arizona law which refers to a DMS.[102]

1.2 **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."[103] For example, a Dealer might contract with an Authorized Integrator to support third party applications for service appointments, inventory management, and customer relationship management.

1.3 **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."[104] 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.

1.4 **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."[105] 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.[106]

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)."

[101] ARIZ. REV. STAT. § 28-4651, *available at* https://www.azleg.gov/legtext/54leg/1r/bills/hb2418s.htm.

[102] *Id.* at 3(b).

[103] *Id.* at 1.

[104] *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.

[105] ARIZ. REV. STAT. § § 28-4651(2), 28-4653(A)(2).

[106] [106] *Id.* § 28-4653(A)(3).

Part IV: Documenting How the Structured Questions Are Consistent with the Case Studies and Other Research To Date

Part IV of the PLSC version "shows the work" for developing the Structured Questions for the Portability and Other Required Transfers Impact Assessment ("PORT-IA"). The Structured Questions evolved considerably during the research phase of the case studies. For instance, after reviewing multiple case studies, I gave greater emphasis to how each case study and the Structured Questions address issues of authentication and secure transmission (especially through APIs). I added the 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.

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 US and EU, including the lesser-known "Free Flow of Data" Regulation in the EU for non-personal data.[107] It also builds on background research on competition/antitrust issues, for both the US and EU. 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 US legal systems. As currently drafted, the text of the Questions appears to do an effective job of incorporating the lessons from the research performed to date. One hope, therefore, is that readers can use the discussion here to perform their own PORT-IAs of PORTability initiatives.

One note on citation: this draft version for PLSC does not contain full citations to material researched for the case studies. The summaries of case studies, included in Part III of the PLSC version, provide key sources for each case study. As the project continues, the additional citations will be filled in.

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

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

[107] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303.

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. 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 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 has to enable precisely 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. 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. 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. More generally, this 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: who must PORT data, who can request the PORT, what data is covered, and 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 entitles 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 US 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.[108]

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, as well as corresponding system tests."[109] 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 the GDPR or the mandates on a US 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 PORT. 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.

[108] 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." Sec. 314.2(f)(2)(xiii). Such "finders" have not previously been listed as financial institutions.

[109] Peter Swire & Annie Antón, "Engineers and Lawyers in Privacy Protection: Can We Just Get Along?" International Association of Privacy Professionals (Jan. 13, 2014), https://iapp.org/news/a/engineers-and-lawyers-in-privacy-protection-can-we-all-just-get-along.

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. As a linguistic matter, considering 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.
2. Banks and competing financial services. Both PSD2 in the EU and Dodd-Frank in the US 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 initiative services," in hopes of reducing lock-in effects even further.
3. Patient health records. The HHS rule seeks to unlock the ability of a patient to transfer medical records to innovative apps. 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 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 "locked away," inaccessible to the general public. With an Open Data requirement, the data is unlocked.

6. The 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.
7. The Free Flow of Data Regulation. An important motivation for the FFD Regulation was to address "various lock-in issues."

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 US banking market for domestic deposits lacks a dominant firm. The largest firm in the market is Bank of America, which has roughly a 10% market share for domestic deposits.[110] 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.[111]

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."[112] For consumers considering shifting to a new 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 of 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?

[110] https://www.statista.com/statistics/727546/market-share-of-leading-banks-usa-domestic-deposits/

[111] 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 in 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.

[112] Damien Egarius & Laurent Weill, "Switching costs and market power in the banking industry: The case of cooperative banks," 42 Journal of International Financial Markets, Institutions, and Money 155, 156 (2016).

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 barrier to entry that protects 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 seven case studies:

1. Phone portability. This case study shows an important interaction of technical inter-operability with PORT requirements. For phone calls, there is a long history of inter-operability, in the sense that subscribers to one carrier, such as ATT, can easily make a call to subscribers of another carrier, such as T-Mobile or a new start-up. In this respect, easy inter-operability reduces or eliminates the network effect of a consumer choosing the largest carrier.[113] 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 US 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 opening the payments system to non-banks on a fair, reasonable, and non-discriminatory basis. Similarly, a major theme in the U.S. has been to assure that non-banks can inter-operate 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 health-care providers and insurers. 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 current databases of health data, but combatting incumbents' network effects has not been a primary theme in justifying the PORT.[114]

[113] 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 inter-operability 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.

[114] The EU case study primarily concerns overcoming barriers to expanding the geographic scope of health markets, and combatting network effects have not been a major theme.

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) address effects on competition from abuse by a dominant firm. 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 PORT 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.

EU competition law has broader theories of liability concerning dominant firms than US 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. A firm is considered to be dominant when it is able to behave "independently of its competitors, its customers and ultimately of consumers."[115] The Commission uses various tools to determine dominance; it has stated that dominance is not likely with market share below 40%,[116] and that market shares above 50% may lead to a rebuttable presumption of dominance."[117] European competition law places on dominant companies a "special responsibility" to act fairly on the market.[118] 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

[115] European Commission "Communication from the Commission - Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings," (2009/C 45/02), at Paragraph 10, at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009XC0224(01)&from=EN.

[116] Id. at Paragraph 14.

[117] See paragraph 60 in Case C-62/86 *AKZO Chemie BV v Commission*, at http://curia.europa.eu/juris/showPdf.jsf;jsessionid=81DF5712ACC6E6F25B9181918B6969E4.

[118] *E.g.*, Case 322/81 *Nederlandsche Banden Industrie Michelin (Michelin I) v Commission* [1983] ECR 3461, paragraph 57; Case T-83/91 *Tetra Pak v Commission (Tetra Pak II)* [1993] ECR II-755, paragraph 114; Case T-111/96 *ITT Promedia v Commission* [1998] ECR II-2937, paragraph 139; Case T-228/97 *Irish Sugar v Commission* [1999] ECR II-2969, paragraph 112; and Case T-203/01 *Michelin v Commission (Michelin II)* [2003] ECR II-4071, paragraph 97.

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, US antitrust law lacks a comparable counterpart to Article 102. Generally, even dominant firms are encouraged to compete aggressively, and only 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" – without access to which a competitor could not plausibly compete. Where such an essential facility exists, then a logical remedy is to require the facility to mandate access, such as through PORTability obligations. Today, the essential facilities doctrine is rarely successful. However, the FTC and other regulators are apparently contemplating imposing data PORTability as a remedy for a broader range of different antitrust concerns, including, for example, as a remedy for prior acquisitions challenged under the antitrust laws.

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 US and the recommendations of the UK CMA illustrate the regulatory interest in spurring PORTability to address perceived risk to competition by incumbent digital platforms. 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 US antitrust law. The auto dealer case study illustrates the possibility of ex ante regulation instead of ex post enforcement of general antitrust rules. Auto dealers and third-party software providers are currently pursuing an antitrust lawsuit against the two largest Data Management System (DMS) providers, alleging among other things an illegal, contractual 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 mandating transfer of Dealer Data to third-party software providers and others designated by a Dealer.

In conclusion, a PORT-IA should accurately consider any claim about abuse of a dominant market position 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 US 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, allowing entry by fintech and other competitors to provide consumers with new services, such as mobile payments.
- Reducing barriers to entry appears to be a secondary goal for the EU health care initiative. 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.
- For US 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.
- The Arizona statute sought to reduce barriers to entry in the market for software services used by automobile dealers. Under the statute, Dealers can choose to buy from Authorized Integrators, who were previously denied access to the two largest DMS Providers.
- Open Data proponents have discussed positive competitive effects for government procurement, such as by enabling new entrants to bid effectively. 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 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 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 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?**

- 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 quite possibly are smaller than proponents have envisioned -- the supply of data from an Open Data initiative is not necessarily matched with the demand for data by potential entrants.
- One might look for a similar effect if there are regulatory mandates for "data sharing"—for 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. That 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.
- US 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. 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."
- US and EU health care. The US 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. The mandatory APIs are designed to enable patients and others to take advantage of innovations such as smartphone apps. By contrast, the focus of the EU health care PORTability initiative is on smoother data flows among incumbent health systems. There is far less focus on moving patient data from traditional providers to innovations such as smartphone apps.
- US automobile dealers. Proponents of the PORT claim that CDK and Reynolds 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.

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 more often called "user autonomy" in the US and more often called "freedom of choice" in Europe.

- The GDPR Right to Data Portability 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.
- US 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." Similarly, PSD2 emphasized what the Europeans call "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.
- 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 US 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:
    - HHS regulation, because a certified IT health software provider must enable transfer "without special effort" of a medical provider's data to a competing IT software provider.
    - Arizona auto dealer statute, requiring Dealer Data Providers to follow directions of Dealers on the ability to access and transfer Dealer Data.
    - The EU "Regulation on the Free Flow of Non-Personal Data," or "FFD Regulation." A principal goal of the 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."
    - Phone number portability especially 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 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 states that the inter-operability rule's information transfers will benefit medical research.
- 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. 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 can be relevant in other ways, such as for legal proceedings.
- Proponents of Open Data have identified a range of possible public benefits, beyond scientific research. For example: (1) "[O]pening up weather data through NOAA has significantly lowered the economic and human costs of weather-related damage through forecasts." (2) Opening Global Positioning System data has "improved safety, emergency response times and environmental quality." (3) The Opioid Mapping Initiative created a comprehensive map to address the opioid crisis.

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?

- 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 US did not become generally operative until 7 years after passage of the Telecommunications Act of 1996. 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). It appears that this voluntary approach to technical standards has led to even more delays than the mandatory approaches under the Open Banking program in the UK. There are continued, serious problems of incompatible health IT systems across the Member States.

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.
- 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 tend to publish data without regard to 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.

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 US financial services. An important rationale for the benefits of PSD and US financial services portability has been to enable non-banks to compete with banks. Non-banks have often favored the PORT initiatives while banks have sometimes opposed.
- US automobile dealers. Automobile 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.

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?**

- Privacy risks for phone number portability are generally very low – people 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.
- 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.
- 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.
- 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. Due to privacy concerns, courts have amended various rules, such as requiring redaction of Social Security numbers and other sensitive information.
- 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.
- US 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.
- Personal data of the customers of automobile dealers, such as lending data, is often covered by the Gramm-Leach-Bliley Act. Entities processing data on behalf of auto dealers, such as software providers, thus are often service providers that must similarly comply with GLBA requirements.

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?**

- 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?**

- US financial services. There have been press accounts of fintech companies, such as Yodlee, allegedly making de-identified data available to its business customers. This sort of database is subject to possible 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).
- A major constraint on the usefulness of Open Data is the risk of re-identifying individuals in a data set. As one 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.
- 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.

- 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.

Question 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"?**

- Authentication is an important feature in each case study.
- Effective authentication is vital for financial services portability, in both the EU and US, 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.
- 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.
- 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 facilitate transferability of data in cross-border healthcare." It appears that standardized authentication has been difficult to develop.
- For US 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."
- For phone number portability, new phone service has often occurred in the US by in-person visits to retail stores, and 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.

- US 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 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.

  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 arising from the method of transmission, such as transfer of a user's passwords or other sensitive data to the recipient of the transfer?**

- 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.
- Where a data subject seeks to access his or her data from a controller, and port the data to himself or herself, the controller can provide its usual mechanisms for user authentication and transmission of data. By contrast, there are essentially two mechanisms for transfers to third-party data recipients; (a) using the data subject's credentials, often through screen-scraping; or (b) using an API. Screen scraping is generally seen as less secure, especially where users reveal their passwords or other sensitive data to the recipient, in order to enable the recipient to access the data controller.
- Security and cost are important considerations in crafting interoperability standards or other mechanisms for transfers.
  - The 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 in a way in which the exchanged information can subsequently be used." 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.

  - 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.
- The CFPB has not issued regulations, permitted under Dodd-Frank, for "standardized formats for data."
- EU financial services. Implementation of APIs has been a major issue in the implementation of PSD2.
  - 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." PSD2 itself does not provide detailed requirements for the APIs 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.
  - 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."
- 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."
- The Arizona 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."
- In contrast to EU financial services, the HHS Rule, and the Arizona statute, US phone portability has a different model for transfer of the data. Portability exists through a centralized entity, the Number Portability Administration Center.
  - Each participating carrier thus has the relatively simple task of connecting securely to one entity.
  - These 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.
  - 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 (square the number of connections for each new entity).
  - 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.
- 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.
    - When non-banks are data recipients, attackers can use phishing, social engineering or other attacks against the non-bank, which may be a smaller company than the bank, and may often lack the same cybersecurity protections.
    - Attackers can also 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.
- 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."[119] Opening up databases can, however, lead to a greater likelihood of attack on the databases, such as risks to data integrity. 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.[120]
- In 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.[121]
- In the US automobile dealer industry, third-party software providers historically often used screen-scraping, using credentials provided by the Dealers. By contrast, the Arizona statute requires use of an open API, so credentials (user name and password) no longer would need to be shared between Dealers and third-party software providers.

[119] Swire, Peter, "A Model for When Disclosure Helps Security: What Is Different About Computer and Network Security?" 3 Journal on Telecommunications and High Technology Law 163 (2004), https://ssrn.com/abstract=531782.

[120] Competitive Enterprise Institute, "EPA Issues Worst Case Scenario Regulations" (Apr.26, 2000), https://cei.org/content/epa-issues-worst-case-scenario-regulations. 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." Id.

[121] Peter Swire, "Individual Remedies, Hostile Actors, and National Security Considerations," Ch. 8 of testimony submitted to the Irish High Court in *Schrems v. Facebook* (2016), https://www.alston.com/-/media/files/insights/publications/peter-swire-testimony-documents/chapter-8--individual-remedies-hostile-actors-and.pdf?la=en

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

- For US 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.
- For US automobile dealers, the DMS providers have stated that cybersecurity reasons justify blocking authentication and use of APIs by third party software providers.

Question 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?**

- 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/US Privacy Shield both require protections in the event of onward transfers."[122]
- 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.
- For US health care, there is an important onward transfer issue because data often goes from a highly-regulated entity (covered by HIPAA) to a less-regulated entity (not covered by HIPAA). 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. This lack of notice to individuals has been the subject of criticism about the

[122] https://www.privacyshield.gov/article?id=Onward-Transfer-Principle-FAQs.

new HHS rule, and the privacy protections when personal data goes to smartphone apps and other recipients of data have also been criticized.

- US financial services. There have been press accounts of fintech companies, such as Yodlee, allegedly making de-identified data available to its business customers. 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: the 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).
- In contrast, under the Arizona statute, any third party, such as a software provider, cannot authorize onward transfer without prior written consent of the Dealer.
- 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.

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.[123]
    - 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.
- Concerns about discriminatory and possibly pretextual arguments about cybersecurity have been prominent in development of PSD2.
    - PSD1 granted access to payment systems for authorized or registered payment service providers on an 'objective, non-discriminatory and proportionate' basis,

[123] https://publications.jrc.ec.europa.eu/repository/bitstream/JRC96258/jrc96258.pdf

which is similar to the term 'fair, reasonable, and non-discriminatory' used in patent and other settings.
    - In 2011, the European Commission started antitrust proceedings against the European Payments Council ("EPC"). 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.
    - 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.
- 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.
- For US health care, In addition to prohibiting discrimination, the information blocking prohibitions have exceptions for security and privacy, but the exceptions are limited fairly carefully.
    - 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. 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.
    - 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.
- 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.
    - Section 28-4652 broadly states that a Dealer can transfer data to its chosen third parties "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."
    - In addition, the statute prohibits a DMS provider from "placing an unreasonable limit" on access by the chosen third parties.
    - Similar to the HHS rule, the Arizona statute limits the fees that the controller can charge for transfer, roughly to actual costs.

- The FFD Regulation specified that the SWIPO group should create codes of conduct to facilitate professional users to port from one service provider to another, "not least upon termination of their contract with a services provider."
    - The principles document issued with the first two codes stated: "Stakeholders have the right to reuse data under fair, reasonable and non-discriminatory terms, with well-defined and duly justified restrictions."[124]
- In conclusion, 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. The final 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.

[124] https://api.hankeikkuna.fi/asiakirjat/2d0f4123-e651-4874-960d-5cc3fac319b6/1f6b3855-fc1d-4ea6-8636-0b8d4a1d6519/RAPORTTI_20191123084411.pdf.

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 US 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 not generally 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 US 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.
- 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, in some Member States, there may be a distinction in practice between the theoretical legal position and reality on the ground. 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.
- 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. 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 US healthcare, the large incumbent Epic Systems Corporation supported the overall objective of the rule, but commented that the rule "eliminated standard intellectual property protections."
- 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.

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?

- 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

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.
- 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.

Conclusion on Applying the Structured Questions: 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.