May 28, 2020

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

Peter Swire*

These public comments are submitted in response to the request from the European Commission for comments on the proposed European Strategy for Data ("Data Strategy"), published on February 19, 2020.[1] The Data Strategy mentions data portability at least nine times. My comments highlight some aspects of an ongoing research project that proposes a new framework for assessing issues of data portability and other required transfers of data. These comments draw on my presentation to an online expert discussion on data portability in April, 2020 hosted by the Organization for Economic Cooperation and Development.[2]

From a competition perspective, greater portability and other transfers of data can have pro-competitive effects. Portability also can enhance individuals' autonomy or freedom of choice about their personal 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 freedom of choice, and other values, and closing data flows, for reasons including protecting privacy and cybersecurity.

For consideration with the Data Strategy, these comments:

1. Suggest new terminology for addressing portability and other required transfers of data.
2. Introduce the concept of a a Portability and Other Required Transfer Impact Assessment ("PORT-IA"), similar in important respects to the Data Protection Impact Assessment required under GDPR.
3. Present 14 structured questions (with sub-questions) in a PORT-IA to assess competition, autonomy, privacy, cybersecurity, and other issues. The questions presented here derive from the largely-completed research on the following case studies: (1) phone number portability in the United States and European Union; (2) EU financial services (PSD2); (3) US financial services; (4) Open Data; (5) US health

* 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, the Georgia Tech Scheller College of Business, and Microsoft. The views expressed here are those of the author, and do not represent the views of any research sponsors or clients of Alston & Bird LLP. Contact: peter.swire@scheller.gatech.edu; www.peterswire.net.

[1] https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf; https://ec.europa.eu/eusurvey/runner/DataStrategy.

[2] https://peterswire.net/wp-content/uploads/PORT-IA.Swire_.March-27-2020.pdf.

care; (6) EU health care; and (7) automobile dealer statutes passed in Arizona and other states.

Going forward, more complete versions of the research project will be published, and will likely be available initially at www.ssrn.com.

Part I: Introduction and Overview of 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 GDPR mandates that individuals have a right to data portability,[3] with a somewhat similar portability requirement in the California Consumer Privacy Act, which entered into effect at the beginning of 2020.[4] In light of these laws, the research project reserves the term "**portability**" to a required transfer when **one** person wishes to port (transfer) the data.

As documented in the case studies, 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").[5] To promote clarity, this research project limits the term "inter-operability" to the technical ability of two or more systems to exchange information. The research project uses the term "**other required transfers**" for those transfers that are required and transfer the data of **more than one person**. Taken together, the research project 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. The PORT-IA.

[3] 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").
[4] California Consumer Privacy Act, Section 1798.100(d).
[5] https://www.hhs.gov/about/news/2020/03/09/hhs-finalizes-historic-rules-to-provide-patients-more-control-of-their-health-data.html.

In order to enable a consistent and disciplined evaluation of PORT initiatives, the. research project 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[6] or Data Protection Impact Assessments required by GDPR.[7]

As shown by the detailed set of structured questions below, 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.[8] There are also non-competition rationales for a PORT, including: user control/autonomy and other non-commercial benefits; innovation and other commercial benefits; and regulatory or other legal benefits of the initiatives. The benefits discussion also assesses whether the benefits contemplated by proponents of 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

[6] E-Government Act of 2002, Pub. L. 107-347, Sec. 208.
[7] GDPR, Article 35.
[8] 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.

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."[9] With that said, implementing portability can have substantial cybersecurity and other risks, and may actually reduce consumer welfare.[10] 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.

C. The Case Studies.

The research and some writing is now complete for the following case studies: (i) US and EU phone number portability;[11] (ii) the new US health care interoperability regulation;[12] (iii) EU portability requirements concerning health care data;[13] (iv) the EU Payment Services Directives, requiring transfers among financial services organizations;[14] (v) similar issues in the US financial services sector, implementing Section 1033 of the Dodd-Frank Act;[15] (vi) Open Data requirements for government agencies, for both the US[16] and EU;[17] and (vii) a lesser-known set of recent laws in Arizona and other states in the US that mandate portability for the data of automobile dealers.[18]

---

[9] 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.
[10] Id. at 380.
[11] 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.
[12] https://www.hhs.gov/about/news/2020/03/09/hhs-finalizes-historic-rules-to-provide-patients-more-control-of-their-health-data.html.
[13] *E.g.,* https://ec.europa.eu/health/ehealth/electronic_crossborder_healthservices_en.
[14] 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.
[15] 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.
[16] *E.g.*, OPEN Government Data Act, 44 U.S.C. § 3501.
[17] *Policy: European legislation on open data and the re-use of public sector information*, EUROPEAN COMMISSION, *available a*t https://ec.europa.eu/digital-single- market/en/european-legislation-reuse-public-sector-information.
[18] *E.g.*, Arizona Revised Statute Section 28-4651 to 4655.

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. The research project will seek to "show my work" – explain how details of the structured questions grew out of specific takeaways from the case studies. These public comments highlight two points about the case studies.

First, the earliest implemented PORT initiatives, for phone number portability in the EU and US, represent uncharacteristically asymmetrical examples of the potential benefits of PORT initiatives. To the extent observers or policymakers implicitly are relying on the phone number case study, they may have an unrealistically positive view about how easy and beneficial PORT initiatives will generally be. On the one side, phone number portability has significant pro-competitive benefits. Absent portability, individuals would be required to give up their cell phone numbers when switching to another carrier. The individual can suffer from "lock in" – losing the current cell phone number 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.[19] 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.

[19] *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).

The larger publication will document how the structured questions in the PORT-IA are consistent with the case studies and other research to date. 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. My belief is that the work to date, once published, will provide 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."

My own work on relevant issues dates back to: (i) 2007 testimony to the Federal Trade Commission on antitrust and privacy,[20] which was the first publication to explain that privacy can be a quality or non-price aspect of competition; and (ii) a lengthy law review article in 2013 on the right to data portability.[21] The research project draws on my experience as a professor of privacy, cybersecurity, and antitrust/competition 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.

In addition to informing the Data Strategy, one result of the research project may be to assist single-issue regulators, such as competition or data protection authorities, to recognize the legal and policy considerations that may arise from other disciplines. For instance, a competition 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. Data protection 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."[22] 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."[23] 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

[20] 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.

[21] 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.

[22] GDPR, Art. 4(11).

[23] Article 29 Data Protection Working Party, "Guidelines on Consent under Regulation 2016/679," (Nov. 28, 2017), at 8.

competition, data protection, and cybersecurity. The assessment of such initiatives, and the European Data Strategy, should be similarly multi-disciplinary.

===

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 that can be better managed, arising from the method of transmission, such as the means for transferring credentials or other sensitive data?

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

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

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

a. Onward transfer: risks from access following authorized PORTing
   i. The concern is that once data is transferred from the controller to the recipient, there may be security or privacy risks arising after transfer to the recipient of the data.
   ii. To what extent is there notice about, and consent by, the data subject to explain privacy and security risks after transfer to the recipient? For instance, if the transfer is from a controller under stricter legal rules, to a recipient with less strict rules, is the data subject notified and does the data subject provide consent to any increased risk?

iii. Would the goals of the PORT be met by transfer of pseudonymous or de-identified data? Are there other technical, administrative or other steps that can mitigate risk once data is transferred to the recipient?
iv. To what extent are the goals of the PORT initiative impeded by steps taken to reduce risks from access following authorized porting?

b. Fair, reasonable, and non-discriminatory (FRAND) terms for security and privacy
i. To what extent, if any, are security requirements different in their application to the controller initially holding the data than for the recipient of the PORT? Are such differences justified on security grounds, or do they appear to unfairly discriminate against transfers to the recipient?
ii. To what extent, if any, are privacy requirements different in their application to the controller initially holding the data than for the recipient of the PORT? Are such differences justified on privacy grounds, or do they appear to unfairly discriminate against transfers to the recipient?

11. Assess risks to competition from the PORT

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

12. Assess regulatory or legal risks of the initiative

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

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

a. Are there any other significant costs or risks from the PORT? For instance, one obstacle to adoption of a PORT can be the expense and time required to create standards for implementing the PORT.
b. To what extent can such costs or risks be mitigated, such as by altering the design of the PORT initiative?

14. Assess incentives for those presenting evidence of risks

a. What parties have an economic or other incentive to oppose the PORT? Explain the incentives. Assess the asserted risks in light of the incentives of some actors to

oppose the initiative. Just because a party has an economic interest to support or oppose an initiative does not mean the facts it cites are incorrect; however, assess the evidence opposing the initiative in light of possible bias. Where available, identify evidence based on sources that are as objective as possible.

Conclusion: 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.

==#==