Issue Brief: Data Portability and Interoperability

The promise and perils of data portability mandates as a competition tool

September 10, 2020

Authored by:

Geoffrey A. Manne (President & Founder, International Center for Law & Economics)
Sam Bowman (Director of Competition Policy, International Center for Law & Economics)

ICLE | 1104 NW 15th Avenue Suite 300 | Portland, OR 97209 | 503.770.0076
icle@laweconcenter.org | @laweconcenter | www.laweconcenter.org

I. Introduction

Lawmakers and regulators are increasingly exploring the imposition of data portability requirements on technology companies, in particular large digital platforms.[1] These would require them to allow users to download their data from those services and/or have it sent to another service on their behalf, either on a one-off or ongoing basis, depending on the proposal.[2]

In this comment, we explore the calls for data portability that arise from distinct and often opposing parts of antitrust law and competition policy, privacy law, and data security. Specifically, we focus on claims that data portability mandates can be used to increase market competition, considering the potential costs and benefits of such requirements, and the relationship between data portability as a pro-competition tool and other moves towards stronger laws governing user privacy.

We begin by discussing the concepts involved in mainstream proposals for data portability. We then examine the various competition issues involved in calls for data portability and discuss the case for and against data portability in these cases. Finally, we discuss in detail the UK's experience with its Open Banking mandate—the most comprehensive data sharing scheme imposed to effect a competition objective—and assess its effects, both intended and unintended.

II. Background

Data portability refers to an entitlement of users of a digital service to easily move data relating to them from one platform to another without them having to manually re-enter that data.[3] Under the

---

[1] The International Center for Law & Economics (ICLE) is a nonprofit, nonpartisan research center based in Portland, OR. ICLE promotes the use of law & economics to inform public policy debates. We believe that intellectually rigorous, data-driven analysis will lead to efficient policy solutions that promote consumer welfare and global economic growth. ICLE has received financial support from numerous companies, foundations, and individuals, including firms with interests both supportive of and in opposition to the ideas expressed in this and other ICLE-supported works. Unless otherwise noted, all ICLE support is in the form of unrestricted, general support. The ideas expressed here are the authors' own and do not necessarily reflect the views of ICLE's advisors, affiliates, or supporters. Please contact the authors with questions or comments at icle@laweconcenter.org. A modified version of this document was submitted as comments to the FTC's September 2020 workshop on data portability.

[2] See, e.g., Article 29 Data Protection Working Party, *Guidelines on the Right to Data Portability* (2017), http://ec.europa.eu/newsroom/document.cfm?doc_id=44099 [hereinafter *Art. 29 Guidelines*]; Personal Data Protection Commission of Singapore, *Public Consultation on Review of the Personal data Protection Act 2012—Proposed Data Portability and Data Innovation Provisions* (May 22, 2019), *available at* https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/PDPC-Public-Consultation-Paper-on-Data-Portability-and-Data-Innovation-Provisions-(220519).pdf; JACQUES CREMER, YVES-ALEXANDRE DE MONTJOYE, & HEIKE SCHWEITZER, COMPETITION POLICY FOR THE DIGITAL ERA (2019), *available at* https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf [hereinafter *European Commission Digital Competition Report*]; UK Department for Business, Energy & Industrial Strategy, *Smart Data Review: Terms of reference* (June 11, 2019), *available at* https://www.gov.uk/government/publications/smart-data-review/smart-data-review-terms-of-reference; *See also* Alexander Macgillivray & Jay Shambaugh (Obama OSTP), *Exploring Data Portability* (Sept. 30, 2016), https://obamawhitehouse.archives.gov/blog/2016/09/30/exploring-data-portability.

[3] *See, e.g.*, Regulation (EU)2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing

California Consumer Privacy Act (CCPA), for example, consumers have the right to receive their data "in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance."[4] Under the EU's General Data Protection Regulation (GDPR), portability is a constituent part of the broader set of consumer privacy rights necessary to "creat[e] the trust that will allow the digital economy to develop."[5]

Although such provisions are directly aimed at effecting a putative consumer "right" to control "their" data, data portability mandates are also commonly defended on competition grounds, as a mechanism for facilitating new entry and intensifying competition by reducing lock-in and hence switching costs between digital platforms.[6] As the European Commission asserted in its Impact Assessment Report on the then-proposed GDPR: "Portability is a key factor for effective competition."[7] The Commission elaborates:

> The possibility to move data from one service provider to another would increase competition in some sectors, e.g. between social networks, and could also make data protection an element in this competition, when users decide to move away from a service they do not consider appropriate in terms of data protection.[8]

Data portability is distinct from data *interoperability*. Data portability generally refers to a one-off transfer—the removal of data from one service and its transfer to another service—whereas interoperability refers to an ongoing transfer or alignment of data as it is created on one service with another. Although this report focuses on *portability*, the distinction is smaller than it may appear: ultimately interoperability means giving customers the ability to "port" their data on an ongoing basis without leaving the original service. As discussed below, the most significant use of data portability as a competition remedy—Open Banking in the UK—requires interoperability.[9]

Directive 95/46/EC, OJ L119/1, 04/05/2016 [hereinafter *GDPR*] at Article 12(3). *See also* International Organization for Standardisation, ISO/IEC 19941:2017, Information Technology—Cloud Computing—Interoperability and Portability (2017), *available at* https://www.iso.org/obp/ui/#iso:std:iso-iec:19941:ed-1:v1:en.

[4] California Consumer Privacy Act of 2018, CA Civ. Code §1798.100, *et seq.* (2018) [hereinafter *CCPA*] at §1798.100(d).

[5] *GDPR*, *supra* note 3, at Prelim., ¶7.

[6] *See, e.g.,* Inge Graef, Jeroen Verschakelen & Peggy Valcke, *Putting the Right to Data Portability into a Competition Law Perspective*, L.: J. HIGHER SCH. ECON., ANN. REV. 53, 59 (2013) ("In the proposal for the [GDPR], the reduction of user lock-in is not mentioned as an objective of the right to data portability. . . . Nevertheless, both the right to data portability and competition enforcement for facilitating data portability will remedy user lock-in. By enabling users to transfer their data easily from one system to another, switching costs are reduced and the risk of lock-in is lowered."). For more on switching costs, *see infra* Section III.A.

[7] Commission Staff Working Paper, Impact Assessment accompanying the General Data Protection Regulation and the Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, SEC (2012) 72 final, at 28.

[8] *Id.* at 106 (Annex 5).

[9] *See infra* Section IV.

As well as markets with perceived insufficient levels of customer switching, portability mandates have been proposed for markets where weak competition is perceived to give companies the ability to collect "too much" data from their users, or markets where customers do not understand the value of their data until after they have agreed to a set of terms.[10]

A. Which data?

It is not simple to define in principle what kinds of data should be portable, and data portability regulations in practice usually require some kind of delineation of what data counts as "belonging" to the user and what counts as the company's data.

The most straightforward distinction may be between data *provided by* a user and data *inferred about* the user. As the Art. 29 Guidelines explain the distinction:

> [T]he term "provided by" includes personal data that relate to the data subject activity or result from the observation of an individual's behaviour, but does not include data resulting from subsequent analysis of that behaviour. By contrast, any personal data which have been created by the data controller as part of the data processing, e.g. by a personalisation or recommendation process, by user categorisation or profiling are data which are derived or inferred from the personal data provided by the data subject, and are not covered by the right to data portability.[11]

An uploaded photograph is an unambiguous example of data provided by a user, as might be a playlist the user has compiled, whereas an algorithmically generated playlist created by a music streaming service based on the user's listening history may be an example of data inferred from the user (and then provided back to the user, in this case). Factual or descriptive data is gathered when the end-user actively provides the data to a firm while observational or predictive (i.e., inferred) data is generated by the firm itself as a result of an individual's use of its services. [12]

The semantic distinctions are not entirely clear, nor consistently implemented, however. For example, the Art. 29 Guidelines include much observational data in the "provided" category:

---

[10] For example, a few months before introducing the ACCESS Act, a bill that would force data portability between large tech firms and smaller competitors, Senator Hawley introduced the DASHBOARD Act, a bill that would force disclosure of the information large tech platforms collect to the Securities & Exchange Commission on the premise that users were unaware of the value of the data they trade for online services. *See* S.2658, Augmenting Compatibility and Competition by Enabling Service Switching Act of 2019, *available at* https://www.congress.gov/bill/116th-congress/senate-bill/2658/text; S.1951, Designing Accounting Safeguards To Help Broaden Oversight and Regulations on Data, *available at* https://www.congress.gov/bill/116th-congress/senate-bill/1951/text.

[11] *Art. 29 Guidelines*, *supra* note 2, at 10-11.

[12] *See* INTERACTIVE ADVERTISING BUREAU, DATA SEGMENTS & TECHNIQUES LEXICON 10 (Jan. 2016), https://www.iab.com/wp-content/uploads/2016/01/IAB-Data-Lexicon-Update-2016.pdf ("The process of generating an attribute can be defined whether the user actively supplies the information (i.e. 'declared' data) or whether it is generated from a system (i.e. 'inferred' data).").

> Nevertheless, data "provided by" the data subject also result from the observation of his activity. As a consequence, the WP29 considers that to give its full value to this new right, "provided by" should also include the personal data that are observed from the activities of users such as raw data processed by a smart meter or other types of connected objects, activity logs, history of website usage or search activities.[13]

Such data is not strictly "inferred," in that it entails no algorithmic or manual operation to identify it. Yet it is also not exactly "provided" by the user, and it would not exist were it not for the user's interaction with the service. It is far less clear that this data should be treated the same way.

> It seems clear that people should be able to transfer data such as the photos they upload to a service or the posts they make to a social network. It's less clear what other data should be included.
>
> Should people be able to export the information that a service provider receives as they use its features—information like search history, location data, and activity logs? What about information generated about people by the service provider on the basis of people's uploaded data or their interactions with the service, like the inferences used to personalize music, events, and ads, or to identify potentially fraudulent activity?[14]

As we discuss below, determining the appropriateness of mandatory portability of such data requires assessing the purposes of the data portability mandate, and its effects along several dimensions.

First- and third-party relationships are also relevant. Data collectors can have either a first-party or third-party relationship with end-users. For example, Google and Facebook are two of the most prominent first-party collectors of data. They have first-party relationships because users create accounts directly with the companies and agree to their privacy policies and terms of service. By contrast, data brokers such as Acxiom or Experian, which serve as intermediaries between data suppliers and data demanders, do not have a direct relationship with users and therefore fall into the third-party category.

Undoubtedly there are other meaningful distinctions when considering the legal definition of data. Data portability mandates must wrestle with these nuances and clearly define which categories of data firms are required to make available for exporting, and to which firms the mandates will apply. For example, it is certainly easier to allow users to export descriptive data they have provided to the platform. By contrast, inferred and predictive data have been created either solely by the platform owner or at the very least "co-created" between the user and the platform. In the latter case, the predictive data itself can be used to make inferences about a firm's algorithms and other trade secrets.

---

[13] *Art. 29 Guidelines*, *supra* note 2, at 9-10.

[14] Erin Egan, Facebook, *Charting A Way Forward: Data Portability and Privacy* 10 (Sept. 2019), *available at* https://about.fb.com/wp-content/uploads/2020/02/data-portability-privacy-white-paper.pdf.

Even where such data does not implicate commercially sensitive property interests, the data itself might be so idiosyncratically tied to the service that it makes little sense to impose costs on a firm to support export. For example, it would probably not be worth requiring a video game company to incur the expense necessary to make records about players' in-game performance exportable, as this is mostly irrelevant outside the context of that game.

In other cases, the data, though potentially not entailing property interests, arises as a result of repeated observations about a user's behavior. These repeated interactions with a platform in particular patterns allow for more accurate inferences to be made and thus provide a competitive advantage to that firm as a result of its theoretically superior market performance.

When considering the incentive effects of data portability on companies, there may also be a meaningful distinction between data that has been sought by the company for other uses, such as targeting advertising or for use in developing other software, where the data is "payment" by the user for a service (or where the service is payment by the company for the data), and data that has been generated as an incidental by-product of another commercial relationship, such as bank transaction data. In the former case, there may be a more significant effect on business behavior from widespread use of data portability.

B. Implementation and trade-offs

Most legislation that imposes a data portability mandate raises further, indeterminate questions about specifics. Which data are subject to these mandates? How should firms and enforcers judge what counts as "easy" transfer technologies? Which systems and formats are companies required to support? What qualifies as "without hindrance"? These questions are perhaps answerable in principle, but doing so involves trade-offs, for example of greater constraints on the companies involved versus lower compliance or user friendliness of the mandated data portability. At some point, legislators, regulators, or the companies themselves must make concrete decisions about these trade-offs.

At one end of the spectrum, companies could be expected to create and maintain open application programming interfaces (APIs) to facilitate real-time importing and exporting of data. These could end up constituting interoperability for the data concerned, with users able to automatically share data between services in real time as the data is uploaded or created.[15] At the other end of the spectrum, companies could be required to report limited personal data for each user as some form of downloadable file.[16] Timing is also a question: should a company be required to provide data immediately, or within a longer time period? The GDPR requires that data be provided within one month

---

[15] *See, e.g.*, Toby Beresford, *Why the Data Portability Provisions of GDPR Might Force Companies Like LinkedIn to Reopen Their API*, MEDIUM (May 26, 2017), https://medium.com/@tobyberesford/why-the-data-portability-provisions-of-gdpr-might-force-companies-like-linkedin-to-reopen-their-api-d914b18bc9c4.

[16] *See* Eric Null & Ross Schulman, *The Data Portability Act: More User Control, More Competition*, NEW AMERICA OPEN TECHNOLOGY INSTITUTE (Aug. 19, 2019), https://www.newamerica.org/oti/blog/data-portability-act-more-user-control-more-competition/.

of the request,[17] which makes easy migration of data from one service to another less practical for users. On the other hand, shorter time frames may involve greater compliance costs—which may slow down product development or impose other costs on users—and increased risk of inadvertent exposure of others' data.

The trade-off facing policymakers is increased specificity about things like transfer methods, file formats, and response times, potentially constraining companies' ability to innovate by changing their product, and less specificity with less benefit to users. Depending on how these are addressed, data portability mandates may also run into conflicts with other legal goals, such as privacy and data security. The GDPR's long compliance period may be related to its fundamental nature as a set of privacy and data protection rights, not as a competition tool.

There are also potential privacy issues that arise from data that relates to other people. If Facebook was required to export or provide access to its social graph (the information that lists a user's contacts on the service and which some scholars have argued creates a moat that makes competition with Facebook difficult or impossible[18]), data pertaining to other users would inevitably be included. Even a relatively simple requirement to make photos available for download can implicate the interests of others: if friends' faces are contained in a user's photos, making her photos more available may tread upon the privacy interests of her friends. And importing those photos into a new service potentially subjects those individuals to increased and un-bargained-for security risks.

Of course, this is exactly what happened with Facebook and its Social Graph API v1.0, ultimately culminating in the Cambridge Analytica scandal.[19] Because v1.0 of Facebook's Social Graph API permitted developers to access information about a user's friends without consent, it enabled third-party access to data about exponentially more users than authorized access. In the case of Cambridge Analytica, for example, it appears that some 270,000 users granted data access, from which Cambridge Analytica was able to obtain information on 50 million Facebook users.

It is important to note that the basic Social Graph information—the connections between users themselves—would constitute "provided" information subject to porting under the Art. 29 Guidelines definition, which includes "observable" data like friend connections.[20] It is unlikely that any form of data portability mandate would intentionally include further data derived from friends' profiles (whether "provided" or "inferred"), but, as noted above, virtually any portability mandate in the social context will inadvertently include at least some such data.

---

[17] *See GDPR*, *supra* note 3, at Art. 12(3).

[18] *See, e.g.*, Luigi Zingales and Guy Rolnik, *A Way to Own Your Social-Media Data*, NY TIMES (June 20, 2017), https://www.nytimes.com/2017/06/30/opinion/social-data-google-facebook-europe.html.

[19] *See, e.g.,* Nathaniel Fruchter, Michael Specter, & Ben Yuan, *Facebook/Cambridge Analytica: Privacy lessons and a way forward,* MIT INTERNET POLICY RESEARCH INITIATIVE (Mar. 20, 2018), https://internetpolicy.mit.edu/blog-2018-fb-cambridgeanalytica/.

[20] *See Art. 29 Guidelines*, *supra* note 2, at 9-10.

As we discuss in the remainder of this comment, there is no simple solution for implementing data portability, and any data portability program—whether legally mandated or voluntarily adopted—will necessarily be faced with these and other trade-offs that complicate the competition and privacy dimensions of the issue.

III. Assessing the arguments for data portability

A. User lock-in and switching costs

As noted, data portability mandates are sometimes proposed as a means to lower switching costs and prevent consumers from being locked in to a single online platform.[21] Lock-in occurs when various decisions made by users and providers make it unattractive or excessively costly for an "installed base" of users to switch to a rival's product, often because of incompatibility between prior interactions or purchases from the original provider and future interactions or purchases from a prospective competing provider.[22] Data created by or about a user can contribute to lock-in if the value of an existing service is increased by virtue of the data it uses, and if that data is not accessible or usable by an alternate provider.[23] Although lock-in is not a standalone theory of harm under US antitrust law, it can have a significant bearing on the outcome of cases. This was notable in the *Microsoft* antitrust proceedings, where the cost of switching from Microsoft's products played an important role in defining the relevant market and in establishing Microsoft's market power.[24]

An inability to easily move data across platforms has sometimes been identified as a source of consumer lock-in. Thus, numerous commentators have argued that the inclusion of a right to data portability in the European Union's General Data Protection Regulation ("GDPR") could promote competition between online platforms.[25]

Similarly, a report on competition in digital markets prepared for the UK's Treasury by an expert panel led by Jason Furman argued that data portability and/or interoperability could make it easier

---

[21] *See, e.g.*, Null & Schulman, *supra* note 16 ("Users of certain services may spend years developing a social following and creating content; the inability to transfer that work to another service likely serves as a significant switching cost that a data portability right could alleviate.").

[22] *See generally* Joseph Farrell & Paul Klemperer, *Coordination and Lock-in: Competition with Switching Costs and Network Effects*, 3 HANDBOOK OF INDUSTRIAL ORGANIZATION 1967 (Mark Armstrong & Robert H. Porter, eds. 2007); CARL SHAPIRO & HAL VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY (1998).

[23] *See, e.g.*, Aysem Diker Vanberg & Mehmet Bilal Ünver, *The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?*, 8 EUR. J. L. & TECH. (2017), at 6 *available at* https://arro.anglia.ac.uk/701565/1/Diker%20Vanberg_2017.pdf ("For instance, without data portability a consumer using Yahoo's email service might not want to move to Gmail due to the risk of losing invaluable personal data. This type of consumer lock-in could be seen as creating a more fragile marketplace, as it is open to exclusionary acts of dominant players. As such, the right to data portability needs to be considered also from a competition law viewpoint.").

[24] *See U.S. v. Microsoft*, 253 F.3d 34 (2001).

[25] *See*, e.g., Wolfgang Kerber, *Digital Markets, Data, and Privacy: Competition Law, Consumer Law and Data Protection*, 11 J. INTELL. PROP. L. & PRAC. 861 (2016). *See also* Diker Vanberg & Ünver, *supra* note 23; Orla Lynskey, *Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability*, 6 EUR. L.J. 793 (2017).

for smaller firms to compete with larger, established platforms, by allowing customers to switch more easily.[26] The UK's Competition and Markets Authority (CMA) imposed data interoperability on the retail banking market in 2017 after concluding that low levels of customer switching were a significant cause of weak competition in the UK's banking market (and this policy, Open Banking, was cited heavily by the Furman report as a model for interoperability in digital markets[27]). A report prepared for the European Commission by Jacques Crémer and others also argued that a presumption in favor of a data interoperability requirement should be considered for dominant platforms in certain cases.[28]

The empirical evidence, however, is quite thin on the question of data "stickiness" affecting customer switching, let alone measuring its importance in consumer tech markets. Although there is a theoretical link between data portability and switching costs, it is unclear how much effect, if any, these data-related switching costs exert on consumers' actual behavior. Though consumers may find it less costly to switch platforms if they can carry their data with them (rather than re-enter it in the new platform), they likely take dozens of other parameters into account and there is no clear sense that data-related switching costs have a significant bearing on these calculations.

Moreover, the type and use of data is essential to assessing the extent to which it may impede competition. Phone number portability, for example, seems to have a fairly significant effect on users' incentives to switch to competing providers.[29] In that case, the loss of the relevant data—primarily the users' previous phone number itself[30]—is viewed by consumers as particularly costly because of the costs of informing contacts of a new number and the risk of lost calls (especially business calls) from prospective contacts unaware of the number change.[31] At the same time, the privacy risks from phone number portability are presumably extremely low, as the vast majority of users want others to be able to find their phone numbers.

But in other cases the competition benefits of mandated data portability are less clear. Most obviously, when the data subject to a portability mandate is incidental to the functioning of the relevant service from users' perspective, lock-in is unlikely to arise from the non-portability or non-interoperability of the data. Thus, for example, the inability to port customer data collected and used by ISPs

---

[26] *See* UNLOCKING DIGITAL COMPETITION: REPORT OF THE DIGITAL COMPETITION EXPERT PANEL 87 (Mar. 2019) [hereinafter *Furman Report*], *available at* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf.

[27] *See id.* at 69-70.

[28] *See European Commission Digital Competition Report*, *supra* note 2, at 4.

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

[30] Although other data is involved in phone number portability, as well. *See How LNP Works*, NUMBER PORTABILITY ADMIN. CTR. (last accessed Aug. 20, 2020), *available at* https://www.npac.com/number-portability/how-lnp-works.

[31] *See Telephone Number Portability*, 11 FCC Rcd 8352, 8368 (1996) ("[A] lack of number portability likely would deter entry by competitive providers of local service because of the value customers place on retaining their telephone numbers.").

and cable providers for advertising, billing, and the like is extremely unlikely to have an effect on a user's decision to switch to a competing provider.

One notable indication that lock-in and switching cost arguments may be weaker than proponents suggest is the near-ubiquity of multi-homing in today's digital markets. "[A]lmost all positive-price customers in multi-sided markets multi-home."[32] The willingness of consumers to use the services of multiple, competing (although sometimes only partially substitutable) platforms without porting their data between them indicates that the lack of portability is not necessarily a substantial impediment to users' willingness to switch between rivals. Moreover, users' willingness to spread their data among competing platforms—meaning no one platform will have access to all of a user's relevant data at any given time—indicates that the putative lock-in effect from past data transactions is weaker than commonly supposed. And the presence of multiple viable competitors further indicates that the competitive concerns from the lack of data portability may be less significant than commonly presumed.

Finally, it should be noted that the consumer welfare effects of switching costs are ambiguous. On the one hand, the presence of switching costs can, as noted, make it harder for new competitors to enter, thus reducing competition and enabling incumbents to charge more for locked-in users. On the other hand, however, *for the same reason*, the presence of switching costs can induce entry by competitors looking to capture new customers (those not yet locked-in to an incumbent's platform) who they can lock-in to their own service, and thus from whom they can expect to extract higher prices.[33] Thus, efforts to induce competition by encouraging data portability may backfire, as potential new competitors, facing the prospect of a reduced ability to lock-in users themselves, may have a reduced incentive to enter in the first place.[34]

This does not mean we should dismiss the possibility that data portability may strengthen competition by lowering switching costs, but we should be wary of assuming that it will deliver benefits, especially when (as we discuss below) the experience so far is that data portability requirements have had modest effects on switching rates, at best.

---

[32] Cristina Caffarra & Kai-Uwe Kühn, *The competition analysis of vertical restraints in multi-sided markets*, in OECD, RETHINKING ANTITRUST TOOLS FOR MULTI-SIDED PLATFORMS 213, 223 (2018), *available at* www.oecd.org/competition/rethinking-antitrust-tools-for-multi-sided-platforms.htm. On multi-homing in two-sided markets generally, see Jean-Charles Rochet & Jean Tirole, *Platform Competition in Two-Sided Markets*, 1 J. EUR. ECON. ASS'N. 990 (2003).

[33] See Luís Cabral, *Dynamic pricing in customer markets with switching costs*, 20 REV. ECON. DYNAMICS 43, 55 (2016) ("In a competitive environment, switching costs have two effects. First, switching costs increase the market power of a seller with attached customers. Second, switching costs increase competition for new customers."). *See also* Farrell & Klemperer, *supra* note 22.

[34] *See, e.g.*, Toker Doganoglu, *Switching costs, experience goods and dynamic price competition*, 8 QUANTITATIVE MARKETING & ECON. 167 (2010); Jean-Pierre Dubé, Günter J. Hitsch, & Peter E. Rossi, *Do Switching Costs Make Markets Less Competitive?*, 46 J. MARKETING RES. 435 (2009).

B. Access to data as a barrier to entry

In a similar vein, numerous commentators have suggested that incumbents' access to user data—e.g., the click and query data that allows a search engine to refine its results based on user behavior—acts as a barrier to entry, allowing incumbents to improve their services in ways that new entrants may not be able to match, thus deterring new entry and insulating incumbent firms from effective competition.[35]

> It's not just that digitisation has made economies of scale more important than before. It's also that the huge amount of data that some platforms have, and the huge networks behind them, can give them an edge that smaller rivals can't match.[36]

The concern about data barriers to entry is related to but distinct from the concern over user lock-in. Most significantly, the animating theory behind the idea of a data barrier to entry is the creation of "data network effects": essentially, the increased value of a service to users arising from its ability to draw on the data of a large number of users.

The argument goes that superior access to data from more users allows incumbent firms to improve their products and gain more users. This then leads to even more data, thereby creating a self-reinforcing circle that eventually causes one firm to dominate the market: thus, "data network effects."[37] As one critic puts it with respect to Google:

> While there are a number of network effects that come into play with Google, ["its intimate knowledge of its users contained in its vast databases of user personal data"] is likely the most important one in terms of entrenching the company's monopoly in search advertising.
>
> * * *
>
> Google's overwhelming control of user data… might make its dominance nearly unchallengeable.[38]

In a related vein, data portability and interoperability have been proposed as solutions to the alleged ability of incumbent platforms to extend their data advantage into related markets. Senator Warner, for example, proposed the imposition of an "interoperability" mandate on platforms in his 2018 Platform Regulation White Paper, stating that an interoperability mandate would "blunt [tech

---

[35] *See, e.g.*, Nathan Newman, *Search, Antitrust, and the Economics of the Control of User Data*, 31 YALE J. ON REG. 401 (2014); *Furman Report*, *supra* note 262626, at 33.

[36] MARGRETHE VESTAGER, EUROPEAN COMMISSION, COMPETITION AND THE DIGITAL ECONOMY at OECD/G7 Conference (2019).

[37] *See, e.g.*, Maurice E. Stucke & Allen P. Grunes, *Debunking the Myths Over Big Data and Antitrust*, 5 CPI ANTITRUST CHRONICLE 1, 6 (2015) ("Data-driven industries can be subject to several network effects, including: Traditional network effects, such as social networks like Facebook; Network effects involving the scale of data; Network effects involving the scope of data…").

[38] Newman, *supra* note 35, at 420 & 423.

platforms'] ability to leverage their dominance over one market or feature into complementary or adjacent markets or products."[39] According to Senator Warner, such a measure would enable startups to offset the advantages that arise from network effects on large tech platforms by building their services more easily on the backs of successful incumbents.[40] He offered similar comments on social media accompanying the release of the ACCESS Act.[41]

Thus, the concerns surrounding data as a barrier to entry arises from the collection and use of large, aggregated sets of data, whereas the concerns around data lock-in and switching costs arise from the collection and use of any given user's particular data.

The alleged problem of data barriers to entry is sometimes used as an argument for data portability at the user level. But if unequal access to large agglomerations of data is a problem, *individual* data portability is unlikely to be an effective solution. This is true for at least three reasons. First, to the extent that a new service would benefit from an aggregated network of data, the transfer of small, disconnected bits of data seriatim as individual users switch to the new service will not readily provide this input. Second, and related, to the extent that a competing service relies on individual users' decisions to decamp to the rival service and bring their data with them, this is unlikely to happen: If a new service is unable to compete with an incumbent because it does not have access to certain data, it is unlikely that users will want to switch to it in the first place. Third, the real value of a large agglomeration of data comes not in the data per se, but in the *analysis* of the data. It may not often be the case that simple *access* to data is sufficient to engender effective competition.[42]

It should also be noted that data portability mandates may actually *create* barriers to entry. It is well-known that "a potential risk in privacy regulation is the entrenchment of the existing incumbent firms and a consequent reduction in the incentives to invest in quality."[43] The same dynamic applies to potentially costly data *sharing* mandates, and "in some cases where entry had been profitable without regulation, [some firms] will choose not to enter."[44] As Baroness Neville-Rolfe, the UK's former parliamentary Under-Secretary of State for the then-Department for Business, Innovation and Skills aptly noted in commenting on the GDPR:

---

[39] *See* Sen. Mark Warner, *Potential Policy Proposals for Regulation of Social Media and Technology Firms* (White Paper, Jul. 13, 2018), at 21, *available at* https://graphics.axios.com/pdf/PlatformPolicyPaper.pdf.

[40] *Id.* at 21-22.

[41] Mark Warner (@MarkWarner), TWITTER (Oct. 22, 2019, 10:12 AM), https://twitter.com/MarkWarner/status/1186646478753800192. *See* ACCESS Act, *supra* note 10.

[42] *See* Geoffrey Manne & Ben Sperry, *Debunking the Myth of a Data Barrier to Entry for Online Services*, TRUTH ON THE MARKET (Mar. 26, 2015), https://truthonthemarket.com/2015/03/26/debunking-the-myth-of-a-data-barrier-to-entry-for-online-services/.

[43] James Campbell, Avi Goldfarb & Catherine Tucker, *Privacy Regulation and Market Structure*, 24 J. ECON. & MGMT. STRATEGY 47, 68 (2015).

[44] *Id.* at 48-49.

> The technical feasibility and the cost to platforms of providing data in a suitable format obviously needs to be considered because if the costs are too high then that perversely becomes a barrier to entry. . . . So you have got these tensions in these innovative areas. We're wanting to move forward, we're wanting to protect the consumer but you are wanting to ensure that the real friends to the consumer which is new ideas, innovation and competition are coming through and that new regulations don't stop that.[45]

Indeed, there is evidence that the introduction of GDPR has likely reduced the rate of competitive entry in Europe. Empirical work by Jia, Jin, and Wagman demonstrates "negative and pronounced effects following the rollout of GDPR on the number of venture deals, particularly in the period immediately after GDPR's rollout, and particularly for newer, data-related, and consumer facing ventures."[46]

The Furman Report, for its part, appears to agree that data portability has limited competition benefits,[47] and instead pushes for "data openness" and "open standards" in order to make certain datasets held by large, "strategically significant" incumbents available for access by would-be competitors.[48] In other words, whatever the merits of enabling or mandating *these* sorts of data access, the Furman Report appears to agree that the goal of overcoming data barriers to entry is unlikely to be furthered by a data *portability* mandate.

But the existence of meaningful data barriers to entry is dubious in the first place. Access to large amounts of data does not, by itself, represent an anticompetitive barrier to entry. Data is simply one input in a panoply of inputs necessary for a firm to compete effectively:

> Information is important to companies because of the value that can be drawn from it, not for the inherent value of the data itself…
>
> Consider companies like Uber, Lyft, and Sidecar that had no customer data when they began to challenge established cab companies that did possess such data. If data were really so significant, they could never have competed successfully. But Uber, Lyft, and Sidecar have been able to effectively compete because they built products that users wanted to use—they came up with an idea for a better mousetrap. The data they have accrued came after they innovated, entered the market, and mounted their successful challenges—not before.

---

[45] Remarks of Baroness Neville Rolfe to the UK House of Lords EU Internal Market Sub-Committee, Dec. 14, 2015, reported in *New data porting rules mustn't overburden businesses with costs, says UK minister*, THE REGISTER (Dec. 16, 2015), https://www.theregister.com/2015/12/16/data_portability_requirements_must_not_impose_too_great_a_cost_burden_on_businesses_says_uk_minister/.

[46] Jian Jia, Ginger Zhe Jin, & Liad Wagman, *The Short-Run Effects of GDPR on Technology Venture Investment*, Working Paper (May 22, 2020) (forthcoming in MARKETING SCIENCE) at 30, *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3278912.

[47] *See Furman Report, supra* note 2626, at 68 ("[GDPR] legislation has been an important step in enshrining personal data portability rights. However, these rights do not go so far as to create the conditions necessary to achieve data mobility and support value generation from personal data.").

[48] *See id.* at 71-77.

> In reality, those who complain about data facilitating unassailable competitive advantages have it backward. Companies need to innovate to attract consumer data, otherwise consumers will switch to competitors (including both new entrants and established incumbents). As a result, the desire to make use of more and better data drives competitive innovation, with manifestly impressive results: the continued explosion of new products, services, and apps is evidence that data is not a bottleneck to competition but a spur to drive it.[49]

As Anja Lambrecht and Catherine Tucker argue in a recent paper, in order for "big data" to provide a sustainable competitive advantage, it would need to be inimitable, rare, valuable, and non-substitutable. It fails on all counts.[50]

Most importantly, "it is only when combined with managerial, engineering and analytic skill in determining the experiment or algorithm to apply to such data that it proves valuable to firms."[51] As Ben Thompson put it during the recent FTC Hearings on Competition and Consumer Protection in the 21st Century:

> The data that Facebook gets from you is worth very little if you could give that to another company, but once Facebook combines that with all the other data they get, and then has the scale on the advertising side to take advantage of that, it is a massive, meaningful economic difference, where Facebook is really adding tremendous value and is appropriately valued because of that.[52]

Mandatory sharing of data will thus often have quite limited value in overcoming a supposed barrier to entry, as the availability of data per se will often do little to facilitate competitive entry.

Moreover, the very notion of data as an antitrust-relevant barrier to entry is deeply problematic.[53] By definition, data produced as a consequence of ongoing market operations is something only incumbents will have—and incumbents will always have. Defining the possession of data in this context as

---

[49] Geoffrey A. Manne & Ben Sperry, *The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework*, CPI ANTITRUST CHRONICLE, 9 (May 2015), https://ssrn.com/abstract=2617685.

[50] Ana Lambrecht & Catherine E. Tucker, *Can Big Data Protect A Firm From Competition*, CPI ANTITRUST CHRONICLE (Jan. 2017), https://www.competitionpolicyinternational.com/wp-content/uploads/2017/01/CPI-Lambrecht-Tucker.pdf.

[51] *Id.* at 5.

[52] *Competition and Consumer Protection in the 21st Century: FTC Hearing #3 Day 1: Multi-Sided Platforms, Labor Markets, and Potential Competition; Before the FTC*, FTC Transcript 201 (Oct. 15, 2018) (statement of Ben Thompson, Founder and Author, Stratechery).

[53] The general notion that large datasets held by incumbent firms constitute an "essential facility" or should be subject to a duty to deal is problematic at a fundamental, conceptual level, as well, as we have discussed at length elsewhere. *See, e.g., Comments of the International Center for Law & Economics, Topic 5: Are there policy recommendations that would facilitate competition in markets involving data or personal or commercial information that the FTC should consider?*, FTC Hearings on Competition & Consumer Protection in the 21st Century, (Jan. 7, 2019), *available at* https://laweconcenter.org/wp-content/uploads/2019/07/Understanding-Competition-in-Markets-Involving-Data-or-Personal-or-Commercial-Information-FTC-hearings-ICLE-Comment-7.pdf.

an entry barrier would be tantamount to inviting antitrust challenges on the basis of a company's mere existence (and even more so, success).

Data in this respect is like reputation. Nearly all new entrants suffer reputational disadvantages. And yet new entry happens all the time. Likewise, the more successful the incumbent—the larger its network, the stronger its reputation, the better its product—the more difficult is new entry. And yet this is competition.[54] There are numerous, well-known cases where new entrants have broken into markets where big data was supposed to have created an impenetrable moat, including WhatsApp in the communications market, King Digital Entertainment in the online gaming market, and Tinder in the online dating market.[55] Similarly,

> we've had already a situation of significant entry by a startup into the search space starting from no data or market share, and that was Google. Google did it. And it did it because it scraped the web itself for information and was able to, you know, through page rank and other means, contextualize it.[56]

In the end, it is not the data that makes the difference, but the "superior ability to understand and meet customer needs."[57] Contrary to the claims of many proponents of data portability as a solution to alleged data barriers to entry, rarely is it data that confers power on incumbents; rather, their power derives from how they structure, process, and contextualize the data.

> It is a fundamental misread to think that Facebook's control of its API. . . is the source of Facebook's competitive advantage. In building for scale, Facebook and other social media sites have developed many interconnected computational assets, and it is the sum total of these pieces that makes them competitive, not simply one piece.[58]

Ultimately, as Catherine Tucker concludes, "empirically there is little evidence of economies of scale and scope in digital data in the instances where one would expect to find them."[59]

---

[54] US courts have consistently rejected the idea that reputation operates as a barrier to entry. See, e.g., *Omega Environmental, Inc. v. Gilbarco, Inc.*, 127 F.3d 1157, 1164 (9th Cir. 1997) ("We agree with the unremarkable proposition that a competitor with a proven product and strong reputation is likely to enjoy success in the marketplace, but reject the notion that this is anticompetitive. It is the essence of competition.").

[55] *Id.* at 6 (statement of Rohit Chopra, Comm'r, FTC).

[56] *Competition and Consumer Protection in the 21st Century: FTC Hearing #7 Day 1: Competition and Consumer Protection Issues of Algorithms, Artificial Intelligence and Predictive Analytics*; Before the FTC, FTC Transcript 159 (Nov. 13, 2018) (statement of Joshua Gans, Professor, University of Toronto).

[57] *Id.* at 7.

[58] Will Rinehart, *Why A Data Portability Act Might Not Be An Effective Policy Path*, AM. ACTION FORUM (Feb. 6, 2018), https://www.americanactionforum.org/insight/data-portability-act-might-not-effective-policy-path/.

[59] *See* Catherine Tucker, *Digital Data, Platforms and the Usual [Antitrust] Suspects: Network Effects, Switching Costs, Essential Facility*, 54 REV. INDUS. ORG., 685, 686 (2019).

C. Pro-incumbent bias

Although proponents of a data portability mandate presume that data will flow from large incumbents to small entrants, of course it can and sometimes will go the other way.[60] As noted above, one potentially unintended consequence of data portability mandates may be to make it harder for smaller platforms to compete with larger ones by reducing user "stickiness" that may otherwise keep users on their platform. Consumers would not necessarily be worse off in this scenario, but the effects on market structure that some proponents of data portability have in mind may not materialize.

Most of the incumbent tech companies do seem to believe that some degree of data portability will be good for them. Google, for example, broadly supports a data portability mandate and was a founding member of the Data Transfer Project (DTP).[61] The DTP is a voluntary scheme run by Google, Facebook, Microsoft, Twitter and Apple, intended to create a set of API standards to allow users to transfer their data between participating services.[62] Its first application went online in April 2020, giving users the ability to transfer their photos directly between Facebook and Google Photos. The DTP is intended by these companies to act as a set of standards to make data portability functionality easier to set up, and the DTP's intention is to be open to other parties.

Hal Varian, chief economist at Google, explained the company's position by saying that Google wants increased data portability because the search giant believes its competitive advantage lies not in the *amount* of proprietary data (alone) the company has but in how it *processes* that data, given its strengths in machine learning and cloud computing.[63]

Facebook is likewise a supporter of the DTP and data portability mandates more generally.[64] Facebook has voluntarily allowed some form of data portability since at least 2010, and, since GDPR, updated the export format to modern JSON standards.[65] More broadly, Facebook believes that

---

[60] *See, e.g.,* Ben Thompson, *The Bill Gates Line*, STRATECHERY (May 23, 2018), https://stratechery.com/2018/the-bill-gates-line/ ("The problem with data portability is that it goes both ways: if you can take your data out of Facebook to other applications, you can do the same thing in the other direction.").

[61] *See* DATA TRANSFER PROJECT (last accessed Aug. 18, 2020), https://datatransferproject.dev/. The major members include Google, Apple, Facebook, Microsoft, and Twitter.

[62] *Id.*

[63] *Why the Techlash? Antitrust Policy and Big Tech*, AMERICAN BAR ASSOCIATION (interview of Hal Varian by John Roberti, Nov. 11, 2019), https://ourcuriousamalgam.com/episode/15-why-techlash-antitrust-big-tech/ (question starting at 21:44) (Roberti: "Why does Google like data portability if that's something that gives your competitors a potential leg up? Why is it in your interest to do it as well?" Varian: "Because we think we'd be better utilizing that data than our competitors are. The question is if everybody is required to do this, to make their data portable to one degree or another, then the party that thinks they can get the most value from that data is going to find that very attractive. If somebody thinks they can't do that, then they're going to find that not very attractive.").

[64] *See* Facebook, *Charting a Way Forward*, *supra* note 1414, at 6.

[65] *Id.*

"people should be able to transfer their information directly to a provider of their choosing, similar to how people use Facebook Login today."[66]

After all, in most conceptions of data portability the mandates cut both ways—incumbents and start-ups alike must share data with each other. If data portability mandates extend beyond merely descriptive data which, given the size of incumbent firms they likely already largely possess, those mandates could be tantamount to sharing critical insights into the proprietary secrets of start-up firms. As Tyler Cowen has observed, a data portability requirement could end up being analogous to a de facto interoperability requirement to the detriment of start-ups:

> Presumably data portability would be imposed on Facebook's competitors and potential competitors as well. That would mean all future competing firms would have to slot their products into a Facebook-compatible template. **Let's say that 17 years from now someone has a virtual reality social network innovation: does it have to be "exportable" into Facebook and other competitors? It's hard to think of any better way to stifle innovation**.[67]

Depending on many factors, such a result could become a net drag on innovation incentives, despite the best of intentions of lawmakers. If new products and services must comport with legacy standards, there will be less disruptive innovation and more sustaining innovation, which could harm consumers in the long run.

Lastly, if there is no exemption in the data portability requirement for small firms, then large firms will be at a relative advantage in terms of compliance, because regulatory compliance is a fixed cost and large incumbents will more easily shoulder the burden of hiring lawyers and privacy engineers to ensure compliance.[68]

Some proponents of data portability and interoperability requirements rely on the example of the local number portability mandate embedded in the Telecommunications Act of 1996. Most notably, Zingales and Rolnik believe that local number portability mandates provide a useful framework for designing a "social graph portability" mandate.[69] That mandate placed a "duty to provide, to the extent technically feasible, number portability in accordance with requirements prescribed by the Commission."[70] Further, the law declared that "[t]he cost of establishing telecommunications

---

[66] *Id.* at 7.

[67] Tyler Cowen, *Why Forced Data Portability is a Mistake*, MARGINAL REVOLUTION (May 18, 2018) (emphasis added), https://marginalrevolution.com/marginalrevolution/2018/05/forced-data-portability-mistake.html.

[68] *See* Diker Vanberg & Ünver, *supra* note 23, at 4 ("[M]any small and medium-sized companies do not have the resources to fully understand the GDPR, comply with it and write an EIM to move data to another provider.").

[69] *See* Zingales & Rolnik, *supra* note 18.

[70] 47 U.S.C. § 251 (2018).

numbering administration arrangements and number portability shall be borne by all telecommunications carriers on a competitively neutral basis."[71]

The analogy to number portability is flawed, at least with respect to social graph portability. Because phone numbers were limited by area code, and because users understandably were reluctant to relinquish a number that other people used to reach them, controlling phone numbers was much more of a zero-sum game than hosting a social graph, which users can obviously create as many of as there are services to host them.

Zingales and Rolnik believe that that "owning" a phone number and being able to take it to a new phone company is akin to an individual owning his social graph and being able to take it to a new social network.[72] But a phone number, as a personal identifier, is much more similar to other personal attributes—like name and date of birth—and much less like the set of social connections one has on a particular social network. Such descriptive data is non-rivalrous and non-exhaustive; a user can just as easily provide his personal information to a new firm.

Requiring social graph portability would be much more like requiring that a phone company provide competing phone companies with all the metadata related to an individual's use of a phone network so that the new company could tailor a custom phone book for the new user.

The core convenience of social graph portability is that a new service can recreate all the connections for a user based on their use of a previous service. Yet most, if not all, apps that depend on social connections implement features that allow an individual to use their contact list to identify other users they know on the new service.[73]

In some cases, users wouldn't want their existing connections to automatically be connected to them on new services. For example, a person on a professional network like LinkedIn may not want all or any of her contacts to be able to automatically friend her on Facebook or a dating service. The existing method of allowing contact list matching and new friend-requests presents a reasonable compromise between data portability and user privacy.

D. Incentives to collect data

Proposals for data portability often do not consider that changing rights over data ownership and access may significantly change existing business models that provide valuable services in exchange

---

[71] *Id.*

[72] *See* Zingales & Rolnik, *supra* note 18.

[73] *See* Manne & Sperry, *supra* note 42 ("[M]any competitors end up voluntarily sharing access to data. For instance, I can use the friend-finder feature on WordPress to find Facebook friends, Google connections, and people I'm following on Twitter who also use the site for blogging. Using this feature allows WordPress to access your contact list on these major online players.").

for access to people's data, and that it is often far from obvious that one party or another should have exclusive ownership rights over a dataset.

Many retail stores have schemes that give customers vouchers if they swipe a loyalty card when they pay for their shopping. Though these are described as loyalty schemes, they are as much about collecting data about customers, again for both aggregate and individual-level usage.[74] Shoppers at large super markets like Kroger effectively receive refunds on their shopping through points earned on purchases, and in exchange Kroger gets information about individual consumption habits for marketing purposes. The famous example of Target knowing that a customer was pregnant based on her shopping history, and hence being able to target maternity goods to her, is an example of how data can be used for aggregate analytics (of other pregnant women's shopping histories) and for individual-level targeting.[75]

Aldi, on the other hand, does not have a loyalty scheme and has no easy way of getting access to its customers' shopping history. The investment Kroger has put in to gathering customer data, in terms of loyalty points and designing analytics and marketing systems to gain insights from the data, gives it a competitive advantage over Aldi in this respect, and it is reasonable to assume that the data only exists because Kroger has "paid" customers for it in loyalty points.

If portability meant that Aldi could easily and cheaply induce customers to port their shopping history over to them from Kroger, effectively free riding on the investment Kroger has made in generating this data, then some of the incentive for Kroger to maintain this program, or for other stores to innovate similar kinds of program, would be eliminated.

Thus, making it easy for users to transfer data from one provider to another may be harmful to innovation if it allows free riding on the data collection efforts of other companies.

E. Commercial flexibility

Data interoperability mandates, which require data to be made available to third party services on an ongoing basis, usually need to specify what format the data takes, how it can be accessed, and other aspects of how the data is used by the original company. These may risk constraining the original company's flexibility to, for example, change its product, if doing so may break the functionality of third-party apps that users have connected to that service. As described below in the section on Open Banking, there may be a tradeoff between the efficacy of a data interoperability remedy and the constrictions on commercial flexibility to innovate that it involves.

---

[74] *See, e.g.*, Christina Donnelly, Geoff Simmons, Gillian Armstrong & Andrew Fearne, *Digital Loyalty Card 'Big Data' and Small Business Marketing: Formal versus Informal or Complementary?*, 33 INT'L SMALL BUS. J. 422 (June 2015).

[75] Kashmir Hill, *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/.

Apart from the risk of constraining *technological* flexibility is the risk of constraining *business model* flexibility. Platforms, especially, differ in how open they are to third parties as a matter of business strategy. As the debate over Apple's App Store demonstrates, while closed platforms can provide significant benefits to consumers (for example, through increased security and moderation) they can also be unpopular with businesses dependent on those platforms.[76]

Mandating openness, interoperability, or the like is not without costs, most importantly in terms of the effective operation of the platform and its own incentives for innovation. It is not clear *a priori*, that a more open platform is necessarily a better one for consumers, yet in many respects moves toward data portability assume that they are.[77] Yet platforms have an incentive to optimize openness and to assure complementors of sufficient returns on their platform-specific investments. This doesn't mean that maximum openness is optimal, however; in fact, typically a well-managed platform will exert some control where doing so is most important, and openness where control is least meaningful.[78]

This is the state of affairs that leads to the indeterminate and complex structure of platform enterprises. Consider the big online platforms like Google and Facebook, for example. These entities elicit participation from users and complementors by making access to their platforms freely available for a wide range of uses, exerting control over access only in limited ways to ensure high quality and performance. At the same time, however, these platform operators also offer proprietary services, or offer portions of the platform for sale or use only under more restrictive terms that facilitate a financial return to the platform. Thus, for example, Google makes Android freely available to device makers, but imposes contractual terms that require installation of certain Google services in order to ensure that it realizes a return sufficient to justify the maintenance and continued development of Android in the first place. Mandating equal access to Android, in other words, may undermine Google's ability to monetize Android.

In the same way, data portability mandates may constrain the ability of platforms to monetize the content they host. Twitter's move from relatively open APIs for third-party apps to relatively closed ones in order to prevent users from using apps that block advertising, or bypass its spam and content

---

[76] Benedict Evans, *App stores, Trust and Anti-trust* (Aug. 18, 2020), https://www.benevans.com/benedictevans/2020/8/18/app-stores.

[77] *See* Dirk Auer, *On the Origin of Platforms: An Evolutionary Perspective*, TRUTH ON THE MARKET (July 7, 2020), https://truthonthemarket.com/2020/07/07/on-the-origin-of-platforms-an-evolutionary-perspective/.

[78] See, e.g., Jonathan M. Barnett, *The Host's Dilemma: Strategic Forfeiture in Platform Markets for Informational Goods*, 124 HARV. L. REV. 1861 (2011); David J. Teece, *Profiting from technological innovation: Implications for integration, collaboration, licensing and public policy*, 15 RES. POL'Y 285 (1986); Andrei Hagiu & Kevin Boudreau, *Platform Rules: Multi-Sided Platforms As Regulators*, in PLATFORMS, MARKETS AND INNOVATION (Annabelle Gawer, ed. 2009); Kevin Boudreau, *Open Platform Strategies and Innovation: Granting Access vs. Devolving Control*, 56 MGMT. SCI. 1849 (2010).

moderation filters, may be an example, or Facebook's preventing advertisers from accessing its users' data directly in order to protect their privacy and protect its own ability to monetize its service.[79]

As well as potentially leading to suboptimal outcomes by constraining potentially valuable business practices, universal data portability mandates may prevent some business models from ever being tried, creating a potentially significant cost that is never visible and so can never be corrected.

Relatedly, mandating portability may limit the ability of businesses to compete on the dimension of data security. Numerous digital platforms impose restrictions on the use and sharing of data intended to appeal to users' security and privacy interests. The existence of some consumers' "preference for and competitive cooperation within walled gardens suggest caution before enacting [regulations] that uniformly impose[] interoperability mandates on both small and large providers of online services."[80]

Strong data portability mandates will necessarily entail tradeoffs that, if not considered (or perhaps even if they are considered) can lead to a reduction in consumer welfare.[81] By forcing firms to be in a position to provide users with personal data in an easily accessible format, mandated data portability increases the risk of identity theft and of personal data leaks.[82] As the EU prepared to implement the GDPR, the European Commission's Working Party on Data Protection recognized there were data security risks inherent in data portability:

> As data portability aims to get personal data out of the information system of the data controller, the transmission may become a possible source of risk regarding those data (in particular of data breaches during the transmission).[83]

In data security, the set of vulnerable points in a system is known as the "attack surface."[84] By mandating data portability, regulators are necessarily increasing the attack surface by adding another attack vector (i.e., another vulnerability for bad actors to exploit) in the form of large, downloadable data sets of comprehensive user information.

The European Data Protection Board ("EDPB")—the body tasked with overseeing implementation of GDPR's data portability requirements—has thus far been unwilling to weigh the benefits of a data portability requirement against the costs (including to data security), however. Instead of seeking the

---

[79] *See* Matthew Hughes, *Twitter to Place New Restrictions on its API to Stop Abuse*, THE NEXT WEB (July 24, 2018), https://thenextweb.com/twitter/2018/07/24/twitter-to-place-new-restrictions-on-its-api-to-stop-abuse/.

[80] Peter Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, 72 MD. L. REV. 335, 378 (2012).

[81] *See generally*, *id.*

[82] *See id.* at 373-75.

[83] *See Art. 29 Guidelines*, *supra* note 2, at 19.

[84] *See* Lily Hay Newman, *Hacker Lexicon: What Is an Attack Surface?*, WIRED (Mar. 12, 2017), https://www.wired.com/2017/03/hacker-lexicon-attack-surface/.

optimal balance between mandated data portability and data security, the EDPB notes that "[s]uch security measures must not be obstructive in nature and must not prevent users from exercising their rights, e.g., by imposing additional costs."[85]

Finally, these restrictions on commercial flexibility may also manifest itself by requiring the portability of data that is idiosyncratic, such as the video game performance history described above, or customers' history of viewing certain forms of media or adverts that are unique to that service. In cases like these, data portability mandates may end up forcing services to comply in a cumbersome way that slows down product development, without corresponding benefit.

IV. The Cautionary Tale of Open Banking

Open Banking is a data interoperability scheme in the UK imposed by the Competition and Markets Authority (CMA) on the nine largest UK banks after the CMA's Retail Banking Market Inquiry. That Inquiry concluded that low rates of customer switching between banking products was a key reason for weak competition in the banking sector and required those banks to make customer data shareable on a persistent basis.[86] Bank customers can give approved third party apps access to their bank data (for example, transaction history and balance data) and initiate payments through approved third party apps. Because the interoperability that Open Banking involves requires much more standards-setting and precise rules about compliance than data portability measures typically do, an independent agency was set up by the CMA to design and roll out Open Banking to the banks, the Open Banking Implementation Entity (OBIE).

Open Banking was launched to customers in early 2018 but it has not been widely adopted by consumers in the UK. Although the OBIE reported in early 2020 that one million customers were now using Open Banking products,[87] as of the date of this writing there are only a handful of consumer products on the market based on Open Banking, and none that has achieved widespread adoption.

Open Banking is particularly significant for three reasons. One, unlike most other examples of data portability mandates, it was imposed as an explicit *competition* remedy; two, it shows the amount of money and effort needed for even relatively simple functionality; and three, unlike many proposals for data portability, it was imposed on a market—banking—where the relevant data to be shared is *incidental* to the commercial relationship between the business and the customer.

The first of these makes Open Banking particularly relevant to further discussions of data portability and interoperability as a competition remedy. Whereas increased competition may be a theoretical

---

[85] *See Art. 29 Guidelines*, *supra* note 2, at 19.

[86] *See* Final report, Competition & Markets Authority, Retail banking market investigation (Aug. 9, 2016), *available at* https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf.

[87] *Open Banking Adoption Surpasses One Million Customer Mark*, OPEN BANKING (Jan. 20, 2020), https://www.openbanking.org.uk/about-us/latest-news/open-banking-adoption-surpasses-one-million-customer-mark/.

by-product of Article 20 of the GDPR, it is the express focus of Open Banking. And yet, although Open Banking has not yet reached maturity, the early signs are not promising that it has succeeded in increasing competition in banking.

While Open Banking was initially proposed as a way of driving increased customer switching between current accounts,[88] if it succeeds it may ultimately do so by allowing for an easier unbundling and re-bundling of services *related* to the current account—overdraft borrowing, mortgage borrowing, savings, and so on, by allowing customers to more easily access cheaper complementary products from third parties than they would get by 'defaulting' to their current account provider bank.[89] It is noteworthy, however, that there is no evidence or suggestion whatsoever that Open Banking has actually increased customer switching rates, nor that consumers are accessing cheaper credit thanks to it.

If Open Banking continues on this trend (increasing bank customers' use of third party complementary products but not increasing switching between bank accounts), it may suggest that similar remedies will not have the desired effect in markets where complementary services already function effectively and consumers already use them.

The second of these points relates to the costs of Open Banking. Despite an early estimate for HM Treasury that compliance would cost no more than £1 million per bank,[90] funding for the OBIE itself—the entity responsible for overseeing and designing the Open Banking APIs and security framework—exceeded £80m by 2019,[91] and the banks themselves report their internal costs of compliance as being far above that, some in the hundreds of millions. Because many of these costs involved the upgrading of internal systems that may have needed to be upgraded at some stage anyway, it is difficult to determine the true cost of the scheme, but it is clear that costs have vastly exceeded what was originally hoped.

Apart from the costs of the scheme, the difficulty of implementing Open Banking has required the OBIE to take an active role for many years following the roll-out of the scheme, including, for example, by implementing a complete overhaul of the process by which customers authorize third-party apps to access their bank data. Initially left in the hands of the banks, this process was made

---

[88] *See* Report for HM Treasury and Cabinet Office, Open Data Institute & fingleton associates, Data Sharing and Open Data for Banks (Sept. 2014), *available at* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/382273/141202_API_Report_FINAL.PDF.

[89] John Fingleton, *From Open Banking to Open Everything* (May 2018), https://www.regulation.org.uk/library/2018-John_Fingleton_From_Open_Banking_to_Open_Everything.pdf.

[90] Report for HM Treasury and Cabinet Office, Open Data Institute & fingleton associates, Data Sharing and Open Data for Banks (Sept. 2014), *available at* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/382273/141202_API_Report_FINAL.PDF.

[91] Ryan Weeks, *The Cost of Open Banking: £81m and Counting*, FINANCIAL NEWS (May 20, 2019), https://www.fnlondon.com/articles/the-cost-of-open-banking-81m-and-counting-20190530.

unnecessarily unwieldy and was seen as a major barrier to user adoption (in the case of one bank, customers would have to navigate twelve different warning screens to authorize a third party[92]). After it was changed, the rate of customer completions of authorizations rose in some cases by 60%.

The point here is that even relatively simple data—customer account balance and transaction history data, in this case—can still be costly and complicated to make portable or interoperable, and require ongoing management by a *de facto* regulator. While this may be appropriate in some cases, it means that blanket requirements for data portability may either be ineffective—with, in Open Banking's case, unnecessary warning screens putting customers off using it—or require a significant investment and ongoing management.

The final point is that banking, and other already-regulated utilities sectors, may be better suited to data portability mandates than the digital platform markets for which data portability is often proposed. In banking, an existing commercial relationship already exists in which the data to be shared is largely incidental, and requiring it to be open and interoperable with other services may make it easier for customers to access complementary third-party offerings precisely *because* they do not have to switch companies to do so.

This may also be true of, for example, a customer's electricity usage data. In cases such as these, the core data is relatively simple (for example, account transaction histories) and requiring that it be made portable may be unlikely to either diminish the incentive to collect this data or to impose significant restrictions on innovation, since it does not change the nature of the core commercial relationship. In contrast, as discussed above, there are many markets in which the exclusive use of customer data (for marketing purposes, for example) encourages innovation and may lower prices for consumers. In these cases, where the data may be "incidental" to the customer's direct engagement with the service, but hardly "incidental" to the overall value and price of the service being offered, a similar requirement may be damaging to consumers.

As a product becomes more sophisticated and likely to change in nature with increased innovation, applying an Open Banking-like remedy may constrain the ability of the product owner to change it, or else may require a more active and ongoing monitoring and design by a regulator to avoid the remedy becoming obsolete. In both of these cases, a data portability remedy is likely to either come at the cost of reduced freedom to innovate, or be ineffective.

For example, even ignoring the complexities involved in even sharing such data, imposing sharing obligations on such data is far more invasive on a firm like Google or Facebook than it is on a bank required to share balance histories, and non-exclusivity may diminish the value of that data to those firms, in turn diminishing their incentive to invest in consumer products to collect it. The data itself

---

[92] *Open Banking, Preparing for lift off: Purpose, Progress & Potential* 23 (2019), https://www.openbanking.org.uk/wp-content/uploads/open-banking-report-150719.pdf. (This report was co-authored by Sam Bowman, co-author of this submission.)

may also reveal elements of the business model, or not be readily separable from the product. If even something as simple as bank transaction data has been as difficult to make portable as Open Banking has found it, the prospects for mandatory portability of more sophisticated, idiosyncratic data are not encouraging.

The key lessons that emerge from Open Banking thus far are:

1. Open Banking has not significantly driven user switching. User adoption of it in any form is still low, and where it has had some take-up it has been for services that offer cheaper complementary services and make multi-homing of non-substitute products easier, rather than leading customers to switch their bank accounts to rival banks. This may be useful in some markets, but suggests that data portability or interoperability may not drive significantly higher levels of user switching or new entry in markets where that is the competition authority's goal.
2. Open Banking has been costly and time-consuming to implement. This is despite the fact that the data involved—chiefly transaction history and account balance data—is relatively simple and does not differ between different banks. The main difficulties have been around security, user authentication, and the authorization of new third-party services, and it has taken ongoing monitoring by a new agency set up by the CMA and several re-iterations to get these right, and may require more in the future. For services where the data is more sophisticated and unique to each service, the cost of implementing data portability and/or interoperability may be commensurately higher.
3. Open Banking has centered on data that is largely incidental to an existing commercial relationship. The data being shared via Open Banking is valuable and access to it may give banks some advantage over their competitors, for example for the purposes of marketing or targeting products at customers, but it is less central to the relationship than, say, data collected for the sole purpose of marketing. In this case, the indirect costs of making that data more readily available to bank competitors may be relatively small, compared to situations where making data easily available to competitors may eliminate the value of collecting it altogether.

These lessons from Open Banking in the UK should cause policymakers to think carefully about imposing broad-based data portability or interoperability mandates across complex markets, especially when mandated sharing of data may undermine incentives to offer consumers better or cheaper products. Even if Open Banking does end up being a success, it stands as a cautionary tale about the difficulty of getting data portability mandates right.

V. Conclusion and recommendations

The assumption that data "stickiness" is a barrier to users switching between specific services or to new rivals entering an established market readily lends itself to a conclusion that a data portability mandate may be an attractive competition remedy. But, as we have discussed, neither the stated competition concerns, nor the efficacy and desirability of a data portability remedy, are well established. And as the experience of GDPR and Open Banking demonstrate, where such mandates have been put into practice, they are either overly broad, with a relatively minor effect on switching rates

and possibly deleterious effects on entry, or, as in the case of Open Banking, may require significant time, money and intervention to work—and may still not be used by, or useful to, customers.

As a result, it is dramatically premature to conclude that data portability is likely to be an effective, pro-competition policy, even before considering the other trade-offs involved: the reduced freedom to innovate, the potentially detrimental effect on incentives to collect data by offering rewards and attractive products to consumers, the potential for *strengthening* incumbent platforms, and the risks of data and privacy breaches that data portability mandates may entail.

Because of this, we recommend that policymakers exercise great caution and avoid attempting to impose data portability on broad swathes of the economy. Where data portability is imposed at all, it should be done so only in targeted circumstances where there is good evidence that the intervention *will* reduce barriers to switching and ensure that the trade-offs are worth it. Where broad-based portability is viable, it should come from voluntary programs like the Data Transfer Project.

To this end, we recommend that:

1. If data portability is imposed it should be limited only to external, self-reported data, and not data arising from users' interactions with a platform, even where such data is "observable," and not "inferred."
2. Any data portability mandate should defer to industry standards for methods of transmission, and avoid imposing costly administrative obligations on providers where data is incidental to the core functionality of a service.
3. When a data portability mandate is considered, it should be as a narrow remedy, not a ubiquitous requirement on all firms.
4. Competition agencies should adopt a "wait and see" approach to existing moves towards data portability before embarking on their own attempts to mandate data portability. It may also be more useful to consider modifications to existing industry efforts than to duplicate these altogether.
5. Policymakers should be mindful of the trade-offs involved in data portability mandates, particularly if data portability compromises companies' ability to modify or monetize their own products.
6. Any attempts to impose data portability mandates should be done with detailed cost-benefit analyses that consider the specific, desired objectives and the costs of imposing and maintaining those mandates over time on agencies, companies and users. Any such mandates should contain mandatory agency review and sunset provisions to facilitate automatic retirement in the event that they fail to accomplish their stated aims.

While data portability may seem like an attractive option in certain markets, experience suggests it is not simple to impose even in cases where the trade-offs seem small. For markets that are defined by innovation and business models designed to offer customers valuable services in exchange for the

collection of data, the trade-offs are likely to be significantly higher, and implementation even more complex.