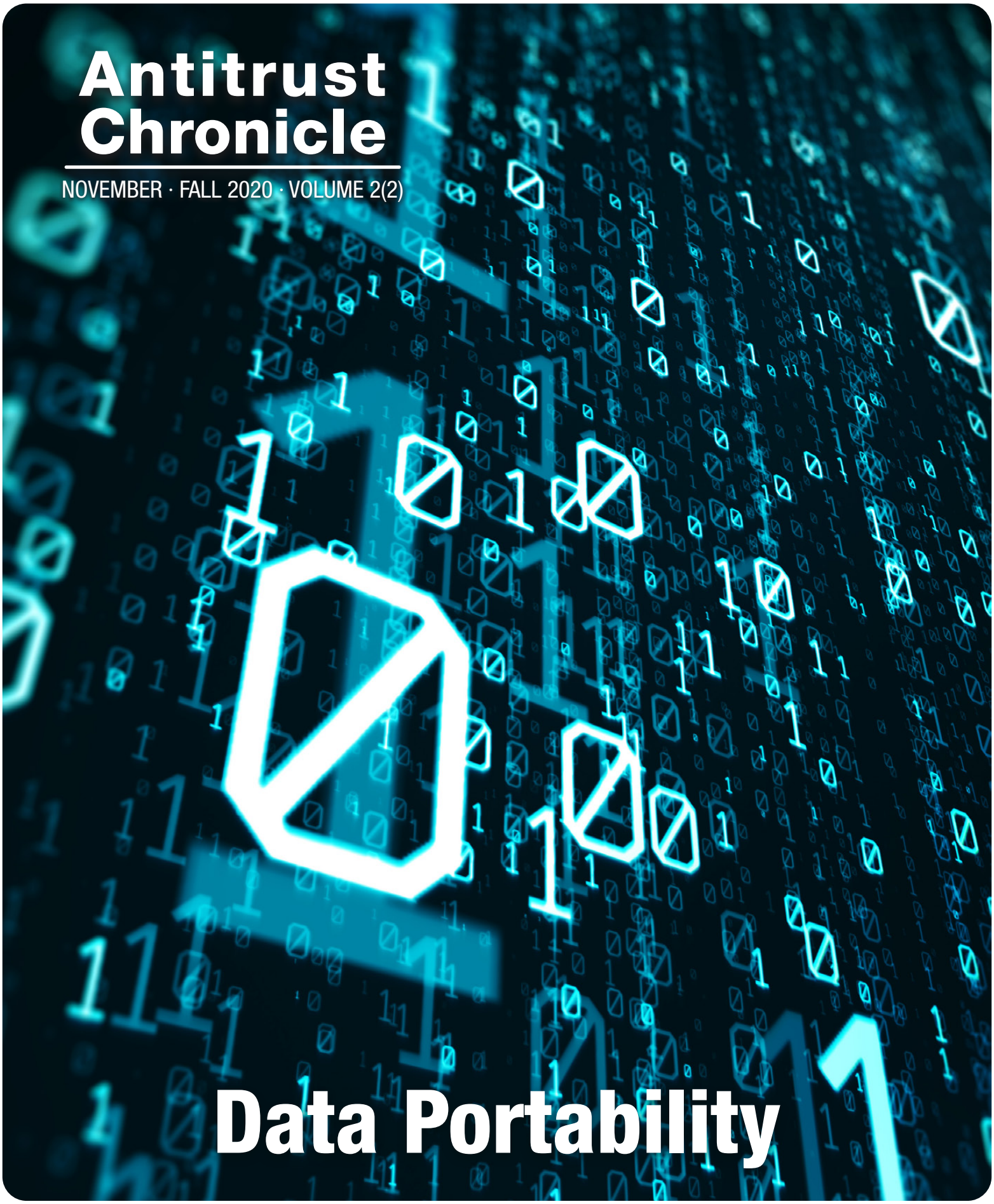


Antitrust Chronicle

NOVEMBER · FALL 2020 · VOLUME 2(2)

Data Portability

CPI COMPETITION POLICY INTERNATIONAL

TABLE OF CONTENTS

LETTER FROM THE EDITOR

Dear Readers,

The question of data portability, in its many forms, has long been an antitrust issue. This stems back as far as the Microsoft interoperability cases of the 1990s, or even further (notably such as in telecoms markets).

Today, however, data portability has taken on even greater importance in antitrust discourse. Like many concepts, it is a double-edged sword.

On the one hand, regulators wish to ensure that competitors are not foreclosed by dominant platforms who maintain walled gardens of data that erect barriers to entry. On the other hand, particularly in light of data protection rules such as those enacted in California and the EU, it has been recognized that consumers have a right to protect their own data, which renders complex the imposition of antitrust remedies mandating its portability. Mandating data portability can also create other unintended consequences, by potentially distorting companies' incentives to innovate.

Navigating the strait between portability and consumer data protection will be one of the key dilemmas facing regulators in years to come.

The contributions to this volume plot a course through this dilemma by discussing the latest developments in both data portability around the world, and its interaction with other laws and regulations.

As always, thank you to our great panel of authors.

Sincerely,

CPI Team

SUMMARIES

08

CPI Talks…

…with Jon Leibowitz

In this month's edition of CPI Talks… we have the pleasure of speaking with Mr. Jon Leibowitz, Counsel in Davis Polk's Washington DC and New York offices. Mr. Leibowitz was Chairman of the Federal Trade Commission from 2009 through 2013 and Commissioner from 2004 to 2009.

10

Data to Go: The FTC's Workshop on Data Portability

By Guilherme Roschke & Andrea Zach

On September 22, 2020, the Federal Trade Commission ("FTC") held a public event, "Data to Go: An FTC Workshop on Data Portability." At the event, the FTC gathered regulators, industry representatives, consumer advocates, and academics for a virtual public discussion of the potential benefits and challenges posed by data portability, as well as issues and best practices related to its government- or industry-led implementation. The workshop was a joint project of the FTC's Bureaus of Competition and Consumer Protection and benefitted from the participation of expert panelists from around the world.

16

Data Portability

By Daniel L. Rubinfeld

Data portability (the ability to transfer data without affecting its content) and interoperability (the ability to integrate two or more datasets) significantly affect the use of data, with important implications for antitrust policy. Allowing for improved data portability can facilitate the ability of consumers to switch services, which would substantially increase competition. However, barriers to data portability can increase market power and be a major source of social inefficiency. This paper lays out the pros and cons of a move towards requirements of data interoperability and portability. Of further note is the need to account for the fact that increasing the scale and scope of data analysis can create negative externalities in the form of better profiling, increased harms to privacy, and cybersecurity risks.

23

Using the Portability and Other Required Transfers Impact Assessment ("PORT-IA") in Antitrust Law

By Peter Swire & John Snyder

Data portability is attracting attention, especially due to recent portability laws in Europe and California, and the hope that it can reduce the market power of digital platforms. This article discusses the potential pro-competitive and other benefits of new data portability requirements, including for lock-in effects, network effects, and barriers to entry. There are significant risks and costs from mandating portability, including privacy and cybersecurity risks if individuals' personal data is not carefully protected. The discussion applies the framework of the Portability and Other Required Transfers Impact Assessment ("PORT-IA") to antitrust law. The PORT-IA provides a structured set of relevant questions, to assist legislators, regulators, enforcement officials, and others to evaluate whether proposed mandatory data sharing is likely to be net beneficial. The article concludes with analysis of how the PORT-IA may appropriately be included in merger review, enforcement discretion, fashioning of remedies and other aspects of antitrust law.

SUMMARIES

Unpacking Data Portability

By Christopher S. Yoo

Data portability has become a hot topic in competition law. Although some commentators have suggested that data portability represents low hanging fruit compared with more complex remedies such as interoperability, the debate about how to implement any such mandate, presumably under the essential facilities doctrine, remains underdeveloped. Key issues that remain unresolved include the impact of the distinction between structure and unstructured data on essentiality, the significance of regulatory regimes that can provide access to data, the tension between portability and privacy, and the difficulties associated with ordering, provisioning, compatibility, and standardization of data. Closer examination of these challenges reveals that data portability is not a panacea and that enforcement officials will have engage in the type of nuanced, fact-specific determinations that characterize classic antitrust analysis and the implicit limitations of the essential facilities doctrine.

The Opportunities and Limits of Data Portability for Stimulating Competition and Innovation

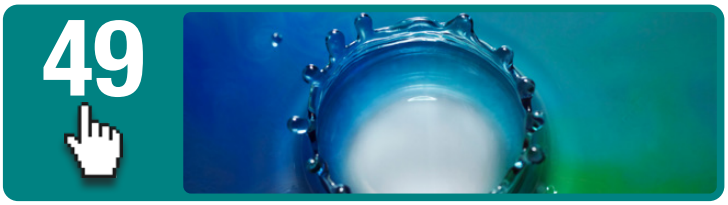
By Inge Graef

Data portability has a hybrid nature. What emerged as a data protection concept is now also becoming part of policies aiming to stimulate competition and innovation. To reap the full benefits of data portability, this article argues that there is a need for regulators to steer its implementation and to provide guidance on how data controllers should handle tensions between different interests and overlapping legal entitlements. Data portability can empower individuals and business users to make better choices but more asymmetric enforcement is needed to ensure that data portability will stimulate competition. And as a tool to promote data-driven innovation, data portability is a necessary but probably not a sufficient condition to keep data-driven markets open to newcomers.

Online Search Competition and the Risk of Unintended Consequences of Data Access

By Jordi Casanova

Mandatory access to digital platforms' data is one of the remedies proposed to address potential failures in digital markets. In addition to the high costs of implementing a governance framework for data access, such remedy is likely to involve important trade-offs that should be carefully balanced by regulators. In particular, data access is likely to undermine competition on the merits and the incentives to offer services to consumers free of charge. Furthermore, it could distort companies' incentives to innovate with user data. To avoid these unintended effects, this article proposes to focus instead on prohibiting exclusionary practices by large digital platforms.

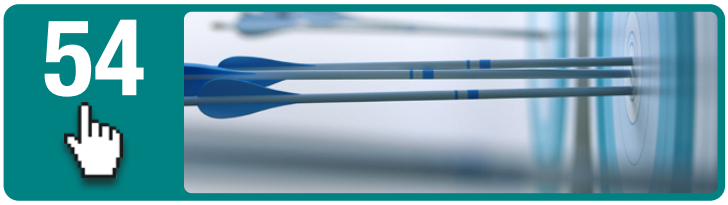


The Impact of Data Portability on Platform Competition

By Emanuele Giovannetti & Paolo Siciliani

Data (number) portability increased switching activity in telecoms markets, but not so far in banking. Data portability is, however, particularly relevant in platform markets dominated by Big-Techs in order to allow an entrant to compete on quality through profiling and matching algorithms. This article discusses results from a model on incumbency advantage among two-sided platforms, whereby agents face different levels of switching costs. Interestingly, policies aimed at lowering switching costs, especially for consumers with higher costs due, for example, to behavioural inertia, might unintendedly hurt entry, as the incumbent platform becomes less accommodative. Moreover, higher switching costs help to avert "winner-takes-all" outcomes preventing sustainable entry. Again counterintuitively, these results show the incumbent preferring a multihoming regime, whereas users might be worse-off. These findings raise deep questions from a regulatory perspective, given that data portability policies are typically motivated by the desire to facilitate competition through multihoming and reducing switching costs.

SUMMARIES



Data Portability Rights: Limits, Opportunities, and the Need for Going Beyond the Portability of Personal Data

By Daniel Gill & Wolfgang Kerber

This paper uses the example of data of connected cars for showing the difficulties of solving data access problems through data portability rights. Especially the privacy law-based data portability of Art. 20 GDPR proves insufficient for solving competition and innovation problems caused by data access problems, due to a too narrow definition of the scope of portable data and the need for additional complementary regulations for making data portability effective. Therefore, data portability rights outside of privacy laws, e.g. based upon the consumer data rights approach or in competition policy, can offer more flexible and effective solutions for fostering competition and innovation.

Data Access and Portability and EU Competition Law

By Björn Lundqvist

This short paper will discuss the right to access and port data under EU Competition Law and EU sector-specific regulations. While general Competition Law is not readily available, stipulating a difficult test for the plaintiff, the EU Commission seems very keen on granting access and portability rights to data under newly enacted sector specific regulations, without any scrutiny in reference to the competitive effects of such rights. Indeed, to access and port data under these sector specific regulations are available to any comers. The paper concludes that enacting sector-specific regulations granting access to data without utilizing competition law principles may prove disastrous, and the Commission should rethink the aim of granting access to data to all and everyone.

WHAT'S NEXT?

For December 2020, we will feature Chronicles focused on issues related to (1) **Vertical Restraints**; and (2) **Patent Licensing**.

ANNOUNCEMENTS

CPI wants to hear from our subscribers. In 2020, we will be reaching out to members of our community for your feedback and ideas. Let us know what you want (or don't want) to see, at: antitrustchronicle@competitionpolicyinternational.com.

CPI ANTITRUST CHRONICLES JANUARY 2021

For January 2021, we will feature Chronicles focused on issues related to (1) **GDPR v. CCPA**; and (2) **Telecommunications**.

Contributions to the Antitrust Chronicle are about 2,500 – 4,000 words long. They should be lightly cited and not be written as long law-review articles with many in-depth footnotes. As with all CPI publications, articles for the CPI Antitrust Chronicle should be written clearly and with the reader always in mind.

Interested authors should send their contributions to Sam Sadden (ssadden@competitionpolicyinternational.com) with the subject line "Antitrust Chronicle," a short bio and picture(s) of the author(s).

The CPI Editorial Team will evaluate all submissions and will publish the best papers. Authors can submit papers on any topic related to competition and regulation, however, priority will be given to articles addressing the abovementioned topics. Co-authors are always welcome.

CPI TALKS…

…with Jon Leibowitz

In this month's edition of CPI Talks… we have the pleasure of speaking with Mr. Jon Leibowitz, Counsel in Davis Polk's Washington DC and New York offices. Mr. Leibowitz was Chairman of the Federal Trade Commission from 2009 through 2013 and Commissioner from 2004 to 2009.

Thank you, Mr. Leibowitz, for sharing your time for this interview with CPI.

1. You have recently stated that "Congress must pass a federal privacy law that gives consumers the choice, clarity, and enforcement they deserve." What should be the main features of this law?

First, national privacy legislation should give consumers the statutory right to control how their personal information is used and shared — including rights of access and deletion — and provide increased corporate transparency. To do so, the law should 1) require companies to solicit affirmative consumer consent before collecting sensitive data (e.g. health and financial data, Social Security numbers); and 2) allow consumers to opt out of collection of *non*-sensitive personally identifiable data. Implied consent can be permitted for certain types of company operational-use data which most consumers assume is being collected (e.g. shipping addresses, for online orders).

Second, any federal privacy requirements should be technology- and industry-neutral. In other words, companies that collect, use, and share the same kinds of covered personainformation should be subject to the same privacy requirements, rather than differing requirements based on how companies classify themselves in the marketplace.

Third, for any privacy legislation to be successful, Congress needs to ensure that the Federal Trade Commission ("FTC") has the resources to enforce the law and bring cases where necessary. To that end, the law should empower the FTC to be the primary authority to administer and enforce the new legislation. This should include the ability to impose penalties even for first-time violations, targeted APA rulemaking authority, and more resources to be able to appropriately fulfill these duties. State attorneys general will be critical allies in enforcement, and they should also be empowered to fully enforce any new federal privacy law, like they are under the Children's Online Privacy Protection Act ("COPPA").

Finally, the new federal law needs to pre-empt state laws. Americans deserve strong and consistent privacy protections no matter where they live, work, and travel — not a crazy-quilt patchwork of differing laws based on the vagaries of state legislatures. And consumers deserve to understand their rights, which militates strongly for one robust standard.

2. What would such a law learn from the experiences of the EU, and, more recently, California, in how such a law would operate in practice? What pitfalls are to be avoided?

State and regional regimes such as GDPR have shown us the promise of uniform privacy legislation across broad geographical areas. Such regimes, when at their best, can provide a more even playing field to allow for consistency and predictability in companies' compliance efforts — big and small alike — and can boost consumer confidence that their personal data is being protected.

However, due to the complexity of the privacy requirements of GDPR as it stands, large players can more easily comply with it while small players cannot.[1] Many business leaders in the EU are confused about data security concepts, like encryption.[2] EU consumers are similarly confused: only 34 percent of respondents in a survey recognized the law, and even fewer knew what it covered.[3] The EU should think carefully

1 Millions of Small Businesses Aren't GDPR compliant, Our Survey Finds, GDPR.eu, https://gdpr.eu/2019-small-business-survey/.

2 *Id.*

3 Kirsty Cooke, Data Shows Awareness of GDPR Is Low amongst Consumers, KANTAR, March 27, 2018, https://uk.kantar.com/public-opinion/policy/2018/data-shows-awareness-of-gdpr-is-low-amongst-consumers/.

about the practical effects of its law, as large amounts of uncertainty may chill new business and leave consumers unsure of their own rights. In the meantime, in designing its own federal privacy legislation, the United States should avoid viewing GDPR as a default model, given that its complexity inhibits businesses' ability to implement compliance and consumers' understanding of their rights.

California's CCPA — while proving that a legislature can pass a privacy law — can be improved and strengthened at a national level. Research also shows an exceedingly high cost of compliance, with a recent study commissioned by the California Attorney General's office finding the "total cost of initial compliance with the CCPA" to be a whopping $55 billion.[4] And now, before the ink is even dry on the original CCPA regulations, a ballot initiative that passed earlier in November will create even more changes and uncertainty in the California privacy landscape.

The United States needs a powerful federal privacy law to avoid a patchwork of conflicting state requirements. Congress should focus not only on stronger safeguards for all Americans and more consumer control over data, but also on protections that are more easily understood. If consumers and businesses do not know what their rights and obligations are, the law is destined for a rocky future.

3. Opponents to a federal privacy law cite the need not to preempt "nimble privacy protections that let states meet [their] varying challenges." Is there an argument that states should be allowed to test the field before a federal law is enacted? Or do the overarching challenges of the Internet require the federal government to set common standards?

Fundamentally, it does not make sense to have 50 different state laws for consumer privacy when the very same data travels across state (and international, for that matter) boundaries. A crazy quilt patchwork of state laws is neither enforceable nor advisable. Moreover, every American deserves the same strong privacy protections no matter where she lives, works, or travels. Having one uniform set of requirements throughout the country accomplishes this and also prevents consumer and business confusion.

Notably, Attorney General Becerra — a terrific AG, and the speaker quoted above — was describing California's CCPA, which itself preempted California's own municipalities' regulations — for precisely the same reasons.

4. How do you see such a law interacting with antitrust rules? The German regulator recently issued a controversial decision (under appeal) holding a breach of EU privacy rules to constitute a breach of competition rules. Should a U.S. law contain provisions defining clearly the scope of each body of rules?

Privacy issues can sometimes overlap with antitrust — we thought a lot about when and to what extent when I was on the FTC — and a number of jurisdictions are clearly beginning to grapple with that issue. Having said that, we should all be happy if, in the next two years, the United States just passes a law that empowers consumers to control their own data. A successful federal privacy law will, like our long-standing antitrust laws, help ensure that the marketplace is free from anticompetitive and privacy-stripping business behavior that harms consumers.

5. How should such a law be enforced? Should the FTC be vested with enforcement power at a federal level? Or is there a need for a separate regulator?

The FTC has been the United States' top privacy cop for the past 40 years. The biggest thing missing from its arsenal is the authority to fine first-time violators. Today, there is bipartisan support in Congress to vest the FTC with that authority, which will make the agency considerably more effective. In order to fuel the FTC's ability to enforce the new law, Congress should also grant the FTC targeted privacy rulemaking authority and significantly more resources. Fortunately, there is bipartisan support for that as well.

My view is that there is no need for a separate regulator. All too often, industry-specific regulators suffer from something called "agency capture," where an agency established to regulate a certain type of business ends up being influenced and controlled by that industry, typically to the detriment of consumers. The FTC, by having effective privacy oversight as part of a broader jurisdiction over virtually the entire economy, is somewhat more immune to that type of capture. In my view, the FTC should be the primary agency enforcing the new federal privacy law, and state attorneys general should also be empowered to enforce the law to complement the FTC's efforts.

4 California Attorney General's Office, "Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations" (August 2019), http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.

DATA TO GO: THE FTC'S WORKSHOP ON DATA PORTABILITY

BY GUILHERME ROSCHKE & ANDREA ZACH[1]

1 Guilherme Roschke is Counsel for International Consumer Protection, and Andrea Zach is a staff attorney in the Bureau of Competition's Office of Policy and Coordination at the Federal Trade Commission.

On September 22, 2020, the Federal Trade Commission ("FTC") held a public event, "Data to Go: An FTC Workshop on Data Portability."[2] The FTC gathered regulators, industry representatives, consumer advocates, and academics for a virtual public discussion of the potential benefits and challenges posed by data portability, as well as issues and best practices related to its government- or industry-led implementation. The workshop was a joint project of the FTC's Bureaus of Competition and Consumer Protection and benefitted from the participation of expert panelists from around the world.

Andrew Smith, Director of the FTC's Bureau of Consumer Protection, delivered the opening remarks, noting that the primary objective of the workshop was not a "broad policy pronouncement or legislative recommendation." Rather, the goal was to contribute to the broader policy discussion about how data portability can empower consumers and promote competition without compromising data security. He then identified some of the touted benefits of data portability, such as giving consumers more control over their data and empowering them to switch service providers. Freeing up data, however, is not without risk. For example, increased data flows can raise serious questions about how to ensure the data is secure.

Peter Swire, Professor of Law and Ethics at Georgia Tech Scheller College of Business, next presented an overview of data portability, including describing some key concepts and terminology. He characterized the dilemma posed by data portability—that is, the tension between opening data flows to promote competition and allow for user control, and closing data flows to protect consumers' privacy and prevent against unauthorized access. Professor Swire developed the "Portability and Other Required Transfers Impact Assessment" ("PORT-IA"), an analytical framework created after reviewing case studies from a variety of sectors. Modeled on privacy impact assessments that are routinely conducted by all types of organizations (including the FTC) whenever a new project would collect data from consumers, the PORT-IA includes a series of structured questions to assess the potential competition, privacy, and cybersecurity costs and benefits of a data portability initiative.

Four panel discussions followed. **The first session** focused on the European Union's General Data Protection Regulation[3] ("GDPR"), the California Consumer Privacy Act[4] ("CCPA"), and India's Data Empowerment Protection Architecture ("DEPA"). Panelists Karolina Mojzesowicz, the European Commission's Deputy Head of Unit for Data Protection, and Stacey Schesser, Supervising Deputy Attorney General of the California Office of Attorney General's Privacy Unit, described the GDPR and CCPA rights to data portability. Both statutory regimes are examples of a general approach to data portability based on a consumer's personal data rights. Each framework applies to a wide range of organizations that process personal data, with only limited exceptions. By contrast, India has taken a narrower, sectoral approach. In the absence of a comprehensive privacy law (although a personal data protection bill is making its way through Parliament), India created DEPA, a technology and regulatory framework that facilitates the transfer of data between various financial institutions using "just-in-time" digital consent, which provides informed consent for every data transaction rather than blanket consent for data use. As explained by Rahul Matthan, a partner at Trilegal in Bangalore, faced with the possibility that India would become "data rich" before it became "economically rich" due to India's rapid digitization, policymakers wanted a different data management system—a portability infrastructure—that would allow India's population, much of which is unbanked, to use their personal data to their benefit. Under DEPA, users can log into authorized apps and pull together their financial data—such as their transaction histories—that they can then share to obtain loans and other financial services. According to Mr. Matthan, government-licensed consent managers mediate the interaction between the user, the data requester (e.g. the lender), and the data controller (e.g. the user's bank or other entity). They also serve as a conduit for the encrypted data flows. DEPA launched in the financial sector earlier this year, and is expected to launch relatively soon in the health and telecom sectors as well.

Panelists also discussed the dual or "hybrid" nature of data portability. Professor Inge Graef, Associate Professor of Competition Law at Tilburg University in the Netherlands, explained that data portability promises both to ease restrictions on data flows while allowing consumers to control their personal data, and to spur economic growth while protecting consumers' right to privacy. Panelists generally agreed that it is too early to tell how the GDPR and CCPA portability rights will affect competition or innovation. The CCPA only went into effect in January 2020, and although the GDPR has been in effect for more than two years, very few consumers have exercised their data portability rights. Karolina Mojzesowicz noted that the European Commission is focused on how to standardize formats and interfaces to expand portability to more sectors and encourage the portability of data in real time.

2 Fed. Trade Comm'n, Data to Go: An FTC Workshop on Data Portability (Sept. 22, 2020), https://www.ftc.gov/news-events/events-calendar/data-go-ftc-workshop-data-portability.

3 European Parliament and Council of European Union (2016) Regulation (EU) 2016/679, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN.

4 California Consumer Privacy Act, Cal. Civ. Code § 1798.140, *available at* https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.140.

Implementation challenges were another topic. Gabriela Zanfir-Fortuna, Senior Counsel at the Future of Privacy Forum, and Professor Graef identified several challenges, including proper authentication of users, legal risks and responsibilities if data is ported to a service provider with weak privacy or security protections, and onward transfers or other downstream uses of data. Professor Graef also called for more guidance on data controllers' obligation to comply with a data portability request involving data that relates to more than one individual or data that is protected by the intellectual property rights of the data controller. If multiple interpretations are possible, data controllers might use such ambiguities as a pretext to deny data portability requests.

Finally, participants compared general and sectoral approaches to data portability. Professor Graef noted that one disadvantage to a sectoral approach is that it makes it more difficult to transfer data across different markets, such as in the context of the Internet of Things. However, she further noted that a sectoral approach might be the better choice to start, even for implementing a general approach like the GDPR. First, a sectoral approach offers certain advantages, such as the ability to be more concrete in standard setting and infrastructure design. A general approach, because of its broad application, may need to avoid referring to specific standards or technologies. Second, a sectoral approach may make a general approach more effective because the portability infrastructure already will have been created.

The second session explored case studies from the financial and health care sectors, including the new health care interoperability rule from the Office of the National Coordinator of Health Information Technology at the U.S. Department of Health and Human Services[5] ("ONC") and the United Kingdom's Open Banking initiative.[6] Panelists also discussed whether Section 1033 of the Dodd-Frank Act provides authority to issue similar standard-setting rules in the U.S. financial sector.

Dr. Don Rucker, the U.S. Department of Health and Human Services' National Coordinator for Health Information Technology, kicked off the discussion by explaining the ONC's rule, which is designed to support and advance the access, exchange, and use of electronic medical records. Both Dr. Rucker and Dan Horbatt, Chief Technology Officer of Particle Health, noted the importance of standard setting rules in maximizing the benefits of health data portability. In its rule, ONC adopted certain standards to support data exchange via secure application programming interfaces ("APIs").

Next, Bill Roberts, the Head of Open Banking at the UK's Competition and Markets Authority ("CMA"), explained the UK's open banking rules. The CMA established its Open Banking initiative to fulfill one of the remedies mandated by the CMA following its investigation into competition in UK retail banking. The CMA found that older and larger banks were not competing hard enough for customers' business, taking advantage of the fact that consumers rarely move their accounts even when fees are high. The CMA required the UK's nine largest banks to develop APIs that would allow bank customers to securely share their financial data with regulated third parties so a broad range of businesses could compete to provide financial services. Open banking, also referred to as consumer-directed banking, relies on common standards for APIs, data formats, and security rather than "screen scraping" to access and transfer data; this approach is considered safer and more secure for both account holders and financial providers. (Screen scraping is a process in which users provide their online banking login credentials to a third party. The third party then uses these credentials to access users' bank account data.) Two years after implementation, there are over a million active users of UK Open Banking and over 700 providers of UK Open Banking services, with no material security events.

Michael Barr, Dean of Public Policy and Professor of Law at the University of Michigan, suggested that an open banking system could similarly empower U.S. consumers and encourage competition and innovation. Professor Barr noted that although the U.S. banking system is not as concentrated as that of the UK, U.S. consumers are similarly locked in at their banks and do not switch accounts. However, unlike the UK, the U.S. lacks clear rules for secure portability of financial data. Section 1033 of the Dodd-Frank Act authorizes the U.S. Consumer Financial Protection Bureau ("CFPB") to write rules implementing a consumer's right to access their own financial data, and that authority could be the basis for improving data portability. In July, the CFPB announced a potential rulemaking under the Dodd-Frank Act on consumer-authorized access to financial records.[7]

Panelists next discussed the practical challenges of setting up a portability regime, citing authentication as a significant obstacle. Speaking from the experience in the UK, Bill Roberts noted that friction encountered during the customer authentication process appeared to be a significant obstacle to customer usage of UK Open Banking, particularly if customers had to go through multiple steps to complete the authorization process and allow their bank to share their data. To resolve this challenge, the UK enabled biometric authentication as a secure and frictionless

5 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 45 C.F.R. Parts 170 and 171, *available at* https://ecfr.federalregister.gov/current/title-45/subtitle-A/subchapter-D.

6 Open Banking Ltd., *What is Open Banking*, OpenBanking.org.uk, https://www.openbanking.org.uk/customers/what-is-open-banking/ (last visited Nov. 3, 2020).

7 Press Release, Consumer Financial Protection Bureau, "CFPB Announces Plan to Issue ANPR on Consumer-Authorized Access to Financial Data (July 24, 2020), https://www.consumerfinance.gov/about-us/newsroom/cfpb-anpr-consumer-authorized-access-financial-data/.

alternative. Dan Horbatt and Dr. Rucker also noted the difficulty of authentication in the health sector, both with patients and with the vendors that hold their data. However, the private sector has made some inroads through the development of reference databases that use a combination of technology and data matching to authenticate individuals, and through biometric and multifactor authentication. Michael Barr noted that in the U.S. financial sector, the government may need to set standards in order to let banks know which authentication procedures are appropriate, and use those same authentication procedures to move money more quickly and efficiently. He also expressed concern that the current methods used to authenticate identity can impose very high costs on the financial sector and on consumers, and limit consumers' access to the financial system.

Shifting the conversation to ongoing and emerging benefits derived from existing data portability regimes, Michael Barr described how consumer-focused data portability could help small businesses operate efficiently and provide consumers with control over their data. In addition, Bill Roberts emphasized how data portability can increase competition by allowing companies to expand outside of their typical markets and services. For instance, once the infrastructure is in place to provide secure and authenticated access to financial data, banks might decide to offer the same data transfer services for other types of data. Considering the health care sector, Dan Horbatt envisioned a world where a patient or health care provider could use health data from a variety of sources to monitor the patient's health in between provider visits. According to Dr. Rucker, health apps and wearable technology would drive this shift.

The third session discussed the benefits and risks of data portability more broadly, with an eye toward the twin aims of protecting consumers and promoting competition. To begin, Ali Lange, Public Policy Manager at Google, described Google's data portability initiatives, which include Google Takeout and the Data Transfer Project ("DTP"). Google Takeout allows users to export a copy of the content in their Google account to back it up or use with a service outside of Google. The DTP is a collective initiative with Apple, Facebook, Microsoft, and Twitter that extends data portability beyond the ability to download (and re-upload) data, to providing users with the ability to directly transfer their data between participating online service providers. It relies on tools that can convert a participating service provider's APIs to and from a set of standardized data formats. These tools, which are being built by the open-source community and are available on GitHub, make it possible to transfer data using existing industry-standard infrastructure and authorization mechanisms. According to Ms. Lange, centralizing the engineering effort makes data portability more scalable and allows other companies to participate. The direct transfer of data also benefits users who lack access to reliable high-speed internet service because it does not require users to download and re-upload their data, which means consumers do not incur charges or face interruptions when moving their data.

Panelists then discussed the policy goals for data portability. Gabriel Nicholas, Research Fellow at New York University School of Law, discussed two goals of data portability—giving consumers access to their data and encouraging competition. He suggested there has been a lot of progress on the first goal, but not much on the second. He also explained that any data portability effort must focus on the consumer's experience, asking the following questions: Is privacy maintained? Is the transfer secure? Is it easy to use? In addition, in order to enhance competition, the data must be of the type that would allow a new entrant to use the data to compete or innovate.

Pam Dixon, Founder and Executive Director of the World Privacy Forum, discussed the need to manage privacy risks, especially in sectors like health care where the data is especially sensitive. In the United States, there are statutes that protect consumers' personal data or concern cybersecurity, such as the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Gramm-Leach-Bliley Act (also known as the Financial Services Modernization Act of 1999). But these statutes primarily regulate certain industries and categories of data (such as health and financial data), and leave significant gaps in coverage. For example, HIPAA's privacy protections do not attach to an individual's health data. Under HIPAA, an individual's health data is protected only if it is held or maintained by a "covered entity," such as a health care provider or health plan. Data that is held or maintained by a patient (or anyone else who is not a "covered entity") is not protected under HIPAA. Thus, patients may not appreciate that when they transfer data out of their personal patient portal, that data is leaving a HIPAA-protected regulatory structure. The FTC brings privacy and data security cases under the FTC Act's prohibition against unfair or deceptive trade practices. However, no single U.S. law regulates the collection and use of consumers' personal data.

Hodan Omaar, Policy Analyst at the Center for Data Innovation, emphasized the opportunities for innovation made possible by data portability. She stated that if companies can be moved away from thinking about how they can collect and store data to how they can use and analyze data, there will be more innovation and benefits to overall consumer welfare. Noting that data is a different type of economic asset that does not have value until it is used, Ms. Omaar asserted that data portability can help firms focus on which types of data would help promote transparency, provide new choices for consumers, and spur innovation.

Peter Swire joined the third panel to identify four goals of data portability based on his review of case studies. According to Professor Swire, data portability can: (1) increase the data available for research; (2) reduce the "lock in" effect that can inhibit competition; (3) increase multihoming, in which users share data with more than one service; and (4) provide a mechanism to distinguish when security concerns are being used as a pretext to prevent interoperability. However, he noted that with any regime, there needs to be security features built in, and that includes authentication, security in transit, and privacy standards that determine who has access privileges to the data. These security features are especially critical in jurisdictions where there is no baseline privacy protection (in contrast to the GDPR, for example). Baseline privacy protections can fill in the gaps that exist in sector-specific data portability regimes.

Panelists also identified areas where additional research or guidance is needed in order to realize data portability's benefits and manage its risks. For instance, panelists explained that although the process may be difficult, there is a real need to develop technical standards. Another area is what to do with data that relates to more than one individual, or data that is provided by a user and then enhanced through analytics performed by the data controller. Finally, panelists suggested that in order to address the network effects that feature prominently on some social platforms, policymakers may need to consider group portability, which would allow a set of users to move the data they share together to another platform. Reciprocity may also be an important part of any data portability initiative—that is, should firms that import data also be expected to export data?

The workshop's **final session** turned to a discussion of how to solve some of the most challenging aspects of data portability, including privacy, security, standards, and interoperability. Several panelists pointed to the need for comprehensive federal privacy legislation as a first step to managing the risks that exist, with or without data portability. According to Sara Collins, Policy Counsel at Public Knowledge, baseline privacy protections would make data portability easier both by establishing minimum standards for how data should be treated, and by removing pretextual arguments for refusing to import or export data. Michael Murray, President of Mission: data Coalition, and Julian Ranger, Executive President and Founder of digi.me, emphasized the role of explicit informed consent. In their view, if data is collected with a clear consent certificate from a consumer who understands what they are sharing, then data portability reduces the privacy risk because the consumer will know what the data will be used for, and whether it will be shared with third parties (and if so, who and why).

As the conversation turned to the security risks of data portability, panelists discussed competing incentives for companies considering data portability. According to Erika Brown Lee, Senior Vice President and Assistant General Counsel for Privacy and Data Protection at Mastercard, the threat of liability stemming from a security incident should lead companies to prioritize preventative verification and identification. Likewise, Michael Murray and Julian Ranger echoed the role of liability as an incentive for companies to share data responsibly. Other panelists stressed that cybersecurity concerns should not be used as a pretext for obstructing data portability efforts. Erika Brown Lee noted that a strong verification and identification system can minimize the impact of liability pitfalls in the event of a security breach. Bennet Cyphers, Staff Technologist at Electronic Frontier Foundation, cautioned that security practices must evolve or there is a risk that they become outdated. Julian Ranger explained that digi.me minimizes security risks by never seeing or collecting the data; an individual's data is decentralized and encrypted, and only the consumer has the key.

The panel next discussed the concept of screen scraping or credential sharing as a means of enabling data portability. Panelists agreed that data portability driven by APIs is preferable to screen scraping partly because consumers do not need to share their credentials with third parties. Julian Ranger noted that legislation allowing for use of APIs could subsequently outlaw screen scraping. However, Bennett Cyphers argued for the value of screen scraping to subvert anticompetitive practices or outdated API regulations, and cautioned against any effort to make it illegal. He also touted screen scraping's ability to incentivize companies or industries to develop APIs.

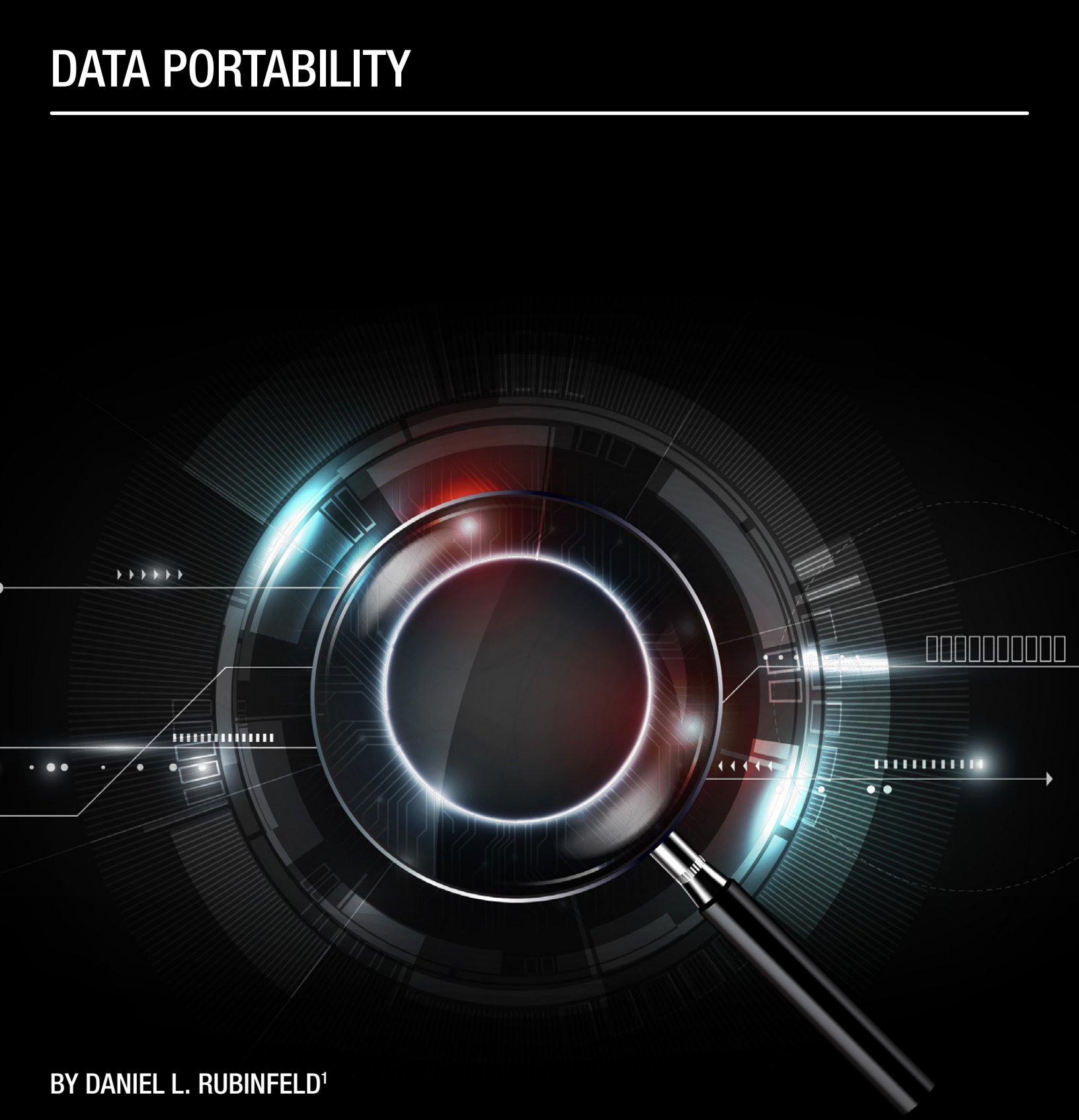
Turning to the last topic, panelists explored data standardization and interoperability. While Julian Ranger agreed that data standardization is important, he cited Australia as an example where focusing first on standards has significantly delayed interoperability. In contrast, regimes that have prioritized the development of well-formed APIs have found that businesses use those APIs to solve the problem of interoperability, and data can begin to flow. Michael Murray, Sara Collins, and Bennet Cyphers emphasized the need for standards to promote interoperability in industries that do not otherwise have incentives to facilitate data sharing. Erika Brown Lee highlighted the importance of industry participation in standards creation in order to ensure widespread adoption and compliance. Michael Murray shared that in his experience, electric utilities will adopt standards but not achieve true interoperability because there is no incentive for them to share a customer's usage data with another utility, for instance if the customer moves to another part of the country.

In conclusion, panelists reiterated the salience of data portability through closing remarks. Julian Ranger and Erika Brown Lee highlighted the importance of data portability to promote competition and user control, respectively. While acknowledging these benefits, Sara Collins emphasized the importance of examining the interconnectedness of privacy, data security, and competition while considering data portability policy.

Expanding on this point, Michael Murray asked the FTC to provide guidance on digital informed consent as data portability policy moves forward. Sara Collins further supports the creation of a digital regulator with the expertise and technical experience to make data portability decisions on a sector-by-sector basis. Throughout, the panelists agreed that technology is moving toward data portability and expressed excitement for the possibilities that will come along with it.

Ian Conner, Director of the Bureau of Competition at the FTC, delivered the closing remarks. He noted that although the agency relies primarily on law enforcement to stop practices that harm consumers and undermine competition, finding the right remedy for a given violation of the law can be challenging, particularly in digital sectors where competition is data-driven. Often, understanding whether data is available and can be moved among competitors is key to understanding the competitive implications of a particular acquisition or business practice. Without understanding the role of data portability, the agency cannot fully assess the remedy necessary to address those harms. He concluded by noting that making more users' data accessible and held by more entities could itself raise privacy and data security concerns that must be considered in fashioning competition remedies.

DATA PORTABILITY



BY DANIEL L. RUBINFELD[1]

1 Robert L. Bridges Professor of Law and Professor of Economics Emeritus, U.C. Berkeley, and Professor of Law, NYU. Many thanks to Michal Gal for her collaborative work on data standardization, to Benjamin J. Hartman for his able research assistance, and to Hal Varian for helpful comments.

I. INTRODUCTION

Data is an essential raw material in our economy. Predictions based on relationships identified in data affect numerous aspects of our lives, yet much of this data is collected in a world that is largely modular.[2] To illustrate, it is predicted that by 2025 seventy-five billion Internet of Things devices, controlled by numerous market players, will be connected to the internet, collecting and using data.[3] Furthermore, for those concerned about privacy, data lie at the core of personal profiling in all of our social networking sites.

In each and every case, data portability (the ability to transfer data without affecting its content) and interoperability (the ability to integrate two or more datasets) significantly affect the use of data, with important implications for antitrust policy. Currently, it can be difficult for users to move personal data in a social network to a competing service.[4] Allowing for improved data portability could facilitate the ability of consumers to switch services, which would substantially increase competition. To illustrate, a Facebook user could readily connect with users of other social networks, irrespective of their initial social network provider. In addition, data interoperability can create data synergies: combining data from different sources can improve the knowledge that can be mined from it.

Barriers to data portability and the interoperability that greatly increases the private benefits of portability can be a major source of social inefficiency in our data-intensive economy.[5] In response to concerns of this type, the European Commission has promulgated its General Data Protection Regulation ("GDPR"). Put simply, the GDPR puts into place a regulatory overlay under which the Competition Directorate and the member states can manage competition policy.[6]

To this point, the U.S. has yet to follow suit. At the core of data-related concerns in the Biden administration are likely to be interoperability and portability.[7] Questions abound. Does imposing a regulatory overlay, perhaps modeled on our telecom regulation, make sense? Short of creating a new federal agency, can the FTC utilize its rule-making functionality to achieve substantial *ex ante* regulatory-like benefits? Or, can the DOJ achieve similar benefits through litigation and/or the use of its typically *ex post* consent decree power? Will active antitrust enforcement improve efficiency, or will it lead to remedies that stifle innovation?

There is a real concern that barriers to data sharing could result in the balkanization of data within particular sectors or even firms, thereby not only impeding innovation within markets, but also reducing spillovers to other markets. Indeed, it is quite possible, when all is considered, that private concerns and private regulation could prevent the sharing of data that would otherwise be efficiency-enhancing.[8]

The discussion that follows lays out some of the pros and cons of a move towards requirements of data interoperability and portability, whether through regulation or through antitrust enforcement.[9] There are technological obstacles to widening the use of data that can be overcome through data portability. Whether the push for interoperability and portability will require a more interventionist role for our competition authorities in order to deal with those obstacles is an open question. On the plus side, standardizing data so that they are portable can lead to

2 Greg Allen & Taniel Chan, Artificial Intelligence and National Security 27 (2017).

3 *Internet of Things (IoT) Connected Devices Installed Base Worldwide from 2015 to 2025 (in Billions)*, Statista, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (last visited November 1, 2020).

4 But, Google's Data Transfer Project has made the movement of photos and other personal data easier. See https://github.com/google/data-transfer-project (accessed on November 7, 2020). According to the Project, "We are establishing a common framework, including data models and protocols, to enable direct transfer of data both into and out of participating online service providers."

5 Oscar Borgogno & Giuseppe Colangelo, *Data Sharing and Interoperability: Fostering Competition Through APIs*, 35 Comput. L. & Sec. Rev. (2019).

6 Commission Regulation 2016/679, 2016 O.J. (L119) Art. 18 ¶ 2 [hereinafter GDPR]. See European Commission, *A Digital Single Market Strategy for Europe*, 14-15(2015). See also Jan Kramer, Pierre Senellart & Alexandre de Streel, Making Data Portability More Effective for the Digital Economy: Economic Implications and Regulatory Challenges (2020).

7 The European Commission has seen APIs (Application Programming Interfaces) as vital to achieving interoperability and through portability to make possible the flourishing of Artificial Intelligence and the Internet of Things. See Borgogno &Colangelo, *supra* note 5, at 4 (noting that the GDPR (Article 20) envisions a series of data portability rights that will support the free-flow of non-personal data and the re-use of government data). The authors stress that data sharing through APIs requires a complex implementation process and standardization for success. Similarly, Article 6 of the GDPR creates a right to business-to-business data portability. For further background, see, e.g. Orla Lynskey, *Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability*, 42 Eur. L. Rev. 793 (2017). See also Jorg Hoffman & Begona Gonzelez Otero, *Demystifying the Role of Data Interoperability in the Access and Sharing Debate* (Max Planck Institute for Innovation & Competition Research Paper No. 2016, 2020).

8 See Catherine Tucker, *Online Advertising and Antitrust: Network Effects, Switching Costs, and Data as an Essential Facility*, CPI Antitrust Chronicle (April 2019). See also Aysem Diker Vanberg & Mehmet B. Unver, *The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo*? 8 Eur. J. L. & Tech. 1 (2017) (suggesting that lessons can be learned from EU competition law to limit the potential adverse consequences of the right to data portability).

9 For a more extensive discussion of the benefits and costs of data standardization that is essential for portability to be effective, see Michal Gal & Daniel L Rubinfeld, *Data Standardization*, 94 N.Y.U. Law Rev. 737 (2019).

smoother data flows, better machine learning, and easier policing of infringement, and can reduce any adverse effects of data-fed algorithms. Standardization might also support a more competitive and distributed data collection ecosystem. At the same time, increasing the scale and scope of data analysis can create negative externalities in the form of better profiling, increased harms to privacy, and cybersecurity concerns.

II. DATA: ANALYSIS AND MARKETS

To understand interoperability and portability issues, it is important to explore the relevant characteristics of data, data analysis, and data markets, as well as some technological obstacles to the use of data and to data integration. While some types of data are not fungible,[10] other datasets can be relevant for multiple users, operating in a wide variety of markets.[11] Moreover, many of those markets are two-sided, as for example the market for Google search advertising, with consumers on one side and advertisers on the other.[12] Furthermore, big data has increased the ability of algorithms to reveal interesting relationships between attributes of datasets and to mine valuable knowledge for descriptive as well as predictive functions.

In an ideal world, data would be transferable or replicable at very low marginal cost. In principle, interoperability can be achieved because data are divisible and can potentially be integrated with other data. Moreover, when economies of scaleand scope cannot be achieved by a single entity or by a single source of data, data integration has the potential to significantly increase data's predictive value. While obstacles abound, in some cases portability will be essential if the benefits of the integration of large amounts of data into one high-quality dataset can be achieved. The challenge is to integrate data that are not necessarily similar in source or structure and to do so quickly and at a reasonable cost.[13]

Competition for data collection, analysis, and storage, as well as competition in markets for data-based products or services, is shaped by the height of entry barriers at various points in the vertical chain, from manufacturer to wholesaler-distributor to retailer and finally to the consumer. The demand for data has created an ecosystem of numerous firms that trade in data.[14] This, in turn, enables firms to use data collected elsewhere to scale up their datasets.

Currently, a number of collaborative projects directed towards improving data interoperability and portability are underway. Founded by Google, Microsoft, Yahoo, and Yandex, schema.org is a collaborative effort to create, maintain, and promote schemas for structured data – in essence, to achieve data standardization. Projects include "dataset search" and "the data commons." Built by schema.org, datacommons.org is an open knowledge repository that combines data from public datasets using mapped common entities. In addition, Google Takeout allows users to export their data in an "industry standard" form.[15]

There are three obstacles to achieving substantial benefits from portability. The first involves *metadata uncertainties*.[16] Metadata comprise the data that describe the data included in a dataset. Metadata uncertainties limit others' ability to understand what different data points signify (e.g. does the label "address" relate to billing or to shipping). As such, metadata can increase information asymmetries regarding the content of datasets, thereby reducing incentives to engage in mutually beneficial data sharing.

The second limitation involves *obstacles to data transformation*, which can raise the costs of combining the available data into coherent datasets i.e. achieving data interoperability. One such obstacle results from data granularity, as when similarly attributed data are collected at different times. Another obstacle can arise from the need to reorganize data into a new, combined dataset with a different structure or internal organization.

10 Maurice Stucke & Alan Grunes, Big Data and Competition Policy (2016).

11 See Anja Lambrecht & Catherine E. Tucker, *Can Big Data Protect a Firm from Competition?* Competition Policy Int'l (2017).

12 James Ratliff & Daniel L. Rubinfeld, *Is There a Market for Organic Search Engine Results and Can Their Manipulation Give Rise to Antitrust Liability*, 10 J. Competition L. & Econ. 517 (2014).

13 *The 6 Challenges of Big Data Integration*, flydata, https://www.flydata.com/the-6-challenges-of-big-data-integration/ (last visited November 3, 2020).

14 U.S. Senate Comm. on Commerce, Sci., & Transp., Off. of Oversight & Investigations, Majority Staff, A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes 20 (Dec. 18, 2013), http://educationnewyork.com/files/rockefeller_databroker.pdf.

15 See, for example, www.lifewire.com/what-is-google-takeout-4173795.

16 Avigdor Gal, Uncertain Schema Matching (2011).

The third obstacle involves *missing data*. This limitation, which is difficult to correct ex post, arises when some necessary data were not collected, or the costs of ex post collection is prohibitive. Missing data may also result, for example, from limited capacity of a database to store the data,[17] or from data collectors' limited foreseeability of the value of data interoperability.

These three limitations reduce users' incentives and ability to extend the use of data and to achieve data synergies. Indeed, a European Commission study found that "merging different datasets and making them interoperable is one of the most resource-intensive activities for data (re-)users and that, even within the same value chain, datasets are rarely interoperable by default."[18]

III. THE BENEFITS AND COSTS OF PORTABILITY

Making data interoperable and portable can potentially reduce all of the obstacles to data use by others. At the same time, creating functional standards can increase the potential value of portability. Data standardization can increase interoperability (of datasets), lower switching costs for consumers (from one data collector to another), and limit duplication (of data collection, storage and analysis). The threat or actuality of increased competition can reduce the market power of economically powerful platforms, lowering prices paid, directly or indirectly, by consumers.

Supporting the interoperability of different data sources also reduces investment risks associated with data collection, organization and storage. By reducing data portability costs and enabling more market players to utilize data, data standardization may increase incentives for data sharing. Increased use of data may also facilitate cumulative and synergetic knowledge production.[19]

Data portability can support a competitive and distributed data collection ecosystem. Not only can it increase the incentives of firms to collect and to share data, it can make markets more competitive. It can also increase the ability of firms to integrate different datasets and reduce the need to rely on one source for data, either internal or external. For example, Google may combine data regarding a user's email, geo-location, and browser history, to better predict her preferences. Other firms, which lack such a variety of data sources, may find it difficult to match these capabilities.

The quality gap created by such network effects carries the potential to entrench or strengthen the dominance of some firms. As a result, data-based markets could exhibit highly concentrated structures, with a single dominant firm possessing a massive share. Benefits arising from data collection and analysis that are not the result of artificial entry barriers do not in themselves raise antitrust issues.[20] However, some have advocated the need for a regulatory overlay.[21]

The difficulty of achieving scale may be overcome if competitors could combine data collected by numerous sources. The lower the costs and obstacles to data portability and interoperability, the stronger the potential competitive pressures on large data collectors. And, since data are non-rivalrous and often easily replicable, data collectors could share their data with many potential users, potentially strengthening competition even further. But the potential has yet to be fully achieved. To illustrate, the recipients of data obtained from Google Takeout may use a variety of different industry standards.

Other barriers, such as switching costs, may still exist.[22] Moreover, a more dispersed market structure might come with its own costs. In particular, intermediary platforms that connect the data gathered from different players could themselves possess market power.[23]

---

17 For an in-depth analysis of the problems involved in collecting and storing data, see, e.g. Blue Ribbon Task Force on Sustainable Dig. Preservation & Access, Sustainable Economics for a Digital Planet: Ensuring Long-term Access to Digital Information (2010), https://www.cs.rpi.edu/~bermaf/BRTF_Final_Report.pdf.

18 Eur. Comm'n, *supra* note 6, at 89.

19 This was recognized by the European Commission: *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Towards a Thriving Data-Driven Economy* 14-15, COM (2015). Realizing potential data synergies also depends on the information market participants possess regarding relevant datasets. See Barbara Engels, *Data Portability Among Online Platforms*, 5 Internet Policy Rev. 1, 9 (2016).

20 See, e.g. Stucke & Grunes, *supra* note 10, at 279.

21 See, e.g. Eleanor Fox, *We Need Rules to Rein in Big Tech*, CPI Antitrust Chronicle (Oct. 2020).

22 *Id.* at 166.

23 Michal S. Gal & Niva Elkin-Koren, *Algorithmic Consumers*, 30 Harv. J. L. & Tech. 309, 338 (2017).

There is a further risk of lock-in to an inefficient standard. To illustrate, assume that a data standard requires all medical data collectors to gather certain types of data at specified intervals, but these intervals are too far apart for the data to be meaningful. While data could be collected at shorter intervals, the standard might send a wrong signal as to the appropriate interval. In addition, data standards can impose high compliance costs on all market players, potentially countering some or all of the competition-driven portability benefits just described.[24] Last but not least, data standards can also negatively affect competition by raising some competitors' costs,[25] and could make coordination and collusion easier.[26]

Data interoperability and portability also raise privacy concerns. The easier it is to share data, the greater the concern that private data will fall into more hands.[27] Portability could also reduce the willingness of potential data subjects to allow their private data to be collected, thereby potentially affecting data collection and innovation.

Data portability can also affect cybersecurity.[28] Integration of databases may enable security systems to more efficiently detect patterns of suspicious activity, and the scale of data may allow algorithms to more rapidly learn from past patterns to detect future attacks.[29] Yet, the more standardized the data, the easier it might be for hackers to access and use it. The potential harm becomes even greater to the extent that data portability enables the creation of larger, less-dispersed databases, given that the size of the dataset may be positively correlated with the potential harm from security breaches.[30] Finally, an inefficient standard can reduce organizations' ability to detect cyber threats and make its implementation costly.

The costs and benefits of requiring interoperability of data sets and making portability possible are likely to differ among different types of data or its uses. As a result, in some cases it may be better to prevent certain uses of data, including its sharing under certain circumstances. At the same time, in some settings, encouraging portability of data must be accompanied by safeguards – legal, technological or even cultural – that ensure that its overall effects on social welfare are positive.

Should the U.S not take an active role in examining and in some cases possibly even facilitating data standards, American firms might find themselves bound by foreign standards.[31] Given that the European Union has acknowledged the importance of data standards for ensuring a comprehensive data sharing environment,[32] and its market players are currently in the process of setting such standards in order to comply with portability requirements, it is important to ensure that domestic data interoperability and portability considerations are not disregarded.

---

24 Peter Swire & Yianni Lagos, *Why the Right to Data Portability likely Reduces Consumer Welfare*, 72 Maryland L. Rev. 335, 352 (2013); Orla Lynskey, *Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability*, 42 Eur. L. Rev. 793, 808 (2017).

25 *Chapter One: Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance*, 13 Harv. L. Rev. 1722, 1733-34 (2018) (suggesting that the requirements for data storage applied by the Second Circuit created a comparative advantage to Microsoft relative to its competitors).

26 Ariel Ezrachi & Maurice Stucke, Virtual Competition: The Promises and Perils of the Algorithm-Driven Economy (2016); Michal S. Gal, *Algorithms as Illegal Agreements*, 34 Berkeley Tech. L. J. 1 (2018).

27 Peter Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, 72 Maryland L. Rev. 335 (2013).

28 Security harms do not involve privacy alone but can also engender economic harms, for example through the loss of financial data and identity theft. See, e.g. Clare Sullivan, Digital Identity: An Emergent Legal Concept 113–16 (2011).

29 Tatiana Tropina & Cormac Callanan, Self- and Co-regulation in Cybercrime, Cybersecurity and National Security 14 (2015).

30 Wolfgang Kerber & Heike Schweitzer, *Interoperability in the Digital Economy*, 8 J. Intell. Prop. Info. Tech. & Electronic Comm. 39, 54 (2017).

31 See generally Anu Bradford, *The Brussels Effect*, 107 Nw U. L. Rev. 2 (2012).

32 Article 29 Data Protection Working Party, Guidelines on the Right to "Data Portability" 2 (2017), http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.

IV. ANTITRUST ENFORCEMENT AND/OR REGULATION?

Can we rely on the market to create and implement efficient data standards that support interoperability and portability? In a number of settings the answer is in the affirmative, given the large benefits to be had from data standardization. Interestingly, private endeavors have mainly focused on data portability, rather than on data interoperability.[33] Yet, in some settings, significant market failures may prevent socially beneficial data standardization, a vital prerequisite to achieving the benefits of interoperability and portability. Consider the world of music recordings, where songs and other types of music have been saved in a variety of formats (e.g. cartridges, CDs, audio tapes, digital audio recordings, etc.) that can be hard for individuals to use.

This section explores some reasons for this market failure as well as the policy implications. First, the incentives of different market players may differ and may affect their ability to create an efficient standard. Some market participants may favor the status quo with the benefits being high switching costs, greater lock-in and reduced data portability. For some, this characterizes the large platforms – Google, Amazon, Facebook, and Amazon -- incumbents enjoying data-based comparative advantages that cannot be easily matched by others. By preventing the creation of the standard, the claim is that incumbents essentially raise their rivals' costs relative to their own.

Second, even if a standard is voluntarily created, its content may serve the interests of some market players and not others. Concerns arise from the private interests of those involved in setting the standard, especially given the knowledge that competitive entry may involve substantial sunk costs. Furthermore, the chosen standard may impose costs as well as benefits in the rivals of its creators.[34]

Third, collective action problems might lead market players not to make portability possible, even when it is beneficial for all of them to do so. In the absence of an arbiter, the market may be sufficiently fragmented that no single approach gains critical support, leading to a patchwork of inconsistent data standards that slow data flows.[35] Furthermore, there might be insufficient time for deliberation before the market sets on its course. Most importantly, the uncertainty resulting from the fact that users cannot be assured that others will follow their move to the new standard, creates a coordination problem.[36] Coordination incentives could also be limited by lack of knowledge among data collectors about the data's potential uses and concerns about the obstacles to integrating it with other types of data. Antitrust concerns, too, could limit incentives to standardize. And, the creation of efficient data standards might be inhibited by internal constraints, short-term strategic conduct, or historical legacies.

Even if the portability of data that serves the interests of all market players is achieved, private standard-setters may disregard the positive spillovers they create on data subjects, on firms in other markets, and on social welfare. An inherent tension also exists between temporal beneficiaries of data analysis: while tomorrow's users may benefit from past data collection, their gains are not always easily shared with the collectors of such data.

Market failures may also arise with regard to the implementation of an acceptable standard. There is arguably an important regulatory role in the acknowledgment, evaluation, and – in the right cases – the possible facilitation of data portability. The potential benefits from increased uses of data, as well as the costs accruing from the potential loss of international competitiveness and from the continuing use of a patchwork of (inefficient) standards, should act as a catalyst for data portability issues to be seriously considered.

As an initial first-stage effort, Congress and the competition authorities should carefully study market dynamics and characteristics to identify where data portability's benefits outweigh its costs. Such costs include the costs of standard setting, implementation, and oversight, of compliance with the standard, and lock-in to an inefficient standard. The need for study is strengthened by the fact that the current situation is characterized by a patchwork of inconsistent legacy data collection and organizational methods, developed over time by various market players, which are not particularly conducive to data integration.

The competition authorities are well positioned to analyze the pros and cons of data portability. They have or can acquire the appropriate technical expertise. They have the ability to understand the implications of their decisions on all market players, to evaluate whether industry standards are economically efficient, and to assess whether the market could and would develop timely and efficient standards without governmental intervention. However, there is a case to be made for the creation of a regulatory overlay, perhaps through the promulgation of a set of regulatory constraints under which the competition authorities should operate.

33 See, e.g. Lynskey, at 793; Data Portability Project, http://www.dataportability.org (last visited Nov. 3, 2020); & Open Data Institute, https://theodi.org/ (last visited Nov. 3, 2020).

34 Stanley M. Besen & Joseph Farrell, *Choosing How to Compete: Strategies and Tactics in Standardization*, 8 J. Econ. Persp. 117, 128 (1994).

35 Kevin Werbach, *Higher Standards: Regulation in the Network Age*, 23 Harv. J. L. & Tech. 179, 201 (2009).

36 See Joseph Farrell & Garth Saloner, *Coordination Through Committees and Markets*, 19 Rand J. Econ. 235, 236 (1988).

Creating an ecosystem of standards that can work in different contexts, and that can interoperate where required, is likely to also require consultation with industry, or even a coordinated governance process that includes the participation of market players. Both suggestions build on the fact that market players often have substantial knowledge and understanding of existing technical needs and the merits of a variety of possible solutions. The particular governmental agency that takes the lead in doing so, and the specific agenda it pursues, may vary across industries.

Once it is established that allowing for data portability will likely increase social welfare, it is important to facilitate the creation of efficient data standards. Regulators face a range of options with regard to how standards can be set, each with its own costs and benefits. These include adopting private solutions, establishing standard-setting organizations (SSOs) or determining standards themselves. The preferred regulatory model may differ among industries and among types of data, depending on the relative competence of different standard setters, the extent of divergence between private and social interests, and the way such a divergence might affect the costs of portability. Yet it seems that in most cases a supervised delegation to an industry-based SSO, comprised of professional data scientists, will be more advantageous than performing the task by a new governmental entity. While regulators play an important role in determining when market failures prevent the creation of welfare-enhancing data standards, they generally have less competence in evaluating the standards that will work best in a given market setting. Where private SSOs are preferred, the regulator may need to set and enforce some basic rules for their operation.

Once a data standard is agreed upon, the regulator must decide how to facilitate its adoption. Options include setting best-practices, mandating the adoption of data standards, and creating soft incentives for their adoption.[37] It might come as no surprise that the Data Transfer Project undertaken in June 2018 by Microsoft, Google, Facebook, and Twitter, which sets a standard to enable user-initiated data portability among project participants, was initiated amidst increased calls for the government to reign in the power of large digital firms resulting from the control of data.[38]

It is noteworthy that in some situations the government may have no choice but to set data standards if it is to make portability work. This might be the case where the government collects and organizes data internally (such as meteorological, demographic or legal data), or where it contracts with others to provide it with certain types of data.

V. CONCLUSION

There are substantial benefits, along with some potentially significant costs, to increasing data portability. The private sector has been active in making efforts, individually or jointly, to improve data portability. Nevertheless, private benefits and social benefits are not fully aligned and there is a clear role for intervention by the public sector. Adding a regulatory overlay to our current regulatory and enforcement authorities that recognizes the potential effects of data portability is appealing. The value of adding such an overlay substantially, short of the creation of an entirely new governmental entity, makes sense. Of course, given the costs and risks involved in intervening in the market, caution is required before any such intervention.

37 The Office of the National Coordinator for Health Information Technology, for example, releases an annual list of best available standards, to be used by technology developers and to inform coordinated governance efforts. See Office of the Nat'l Coordinator for health info. Tech., 2015 Interoperability Standards Advisory 1 (2015).

38 See also Greg Fair, *Our Work to Move Data Portability Forward*, The Keyword (Sept. 21, 2020), https://blog.google/technology/safety-security/data-portability (discussing Googles efforts to improve data portability through the Data Transfer Project). Of further note, Google Takeout was created on June 28, 2011 to allow users to export their data from most of Google's services. See www.wikipedia.com (las visited Nov. 8, 2020).

USING THE PORTABILITY AND OTHER REQUIRED TRANSFERS IMPACT ASSESSMENT ("PORT-IA") IN ANTITRUST LAW

BY PETER SWIRE & JOHN SNYDER[1]

1 Peter Swire is the Elizabeth and Tommy Holder Chair of Law and Ethics in the Georgia Tech Scheller College of Business, and Senior Counsel, Alston & Bird LLP. John Snyder is Partner, Alston & Bird LLP.

I. INTRODUCTION

This edition of the CPI Antitrust Chronicle reflects growing public attention to the issue of data portability.

Three key trends contribute to this new attention: (1) an individual right to data portability has recently come into effect in Europe and California, with federal legislation an increasing possibility; (2) there are intense public debates about whether and how to bring antitrust enforcement actions against prominent digital platforms such as Google and Facebook, with portability as an oft-mentioned possible remedy; and (3) beyond digital platforms, multiple sectors of the economy increasingly have data portability requirements.[2]

The Federal Trade Commission ("FTC") in September hosted a day-long workshop on the topic.[3] In announcing that workshop, the FTC noted that data portability may "promote competition by allowing new entrants to access data they otherwise would not have, enabling the growth of competing platforms and services."[4] In so doing, the FTC echoed the reasoning of numerous other leading observers.[5]

This article discusses the potential pro-competitive and other benefits of new data portability requirements, including potentially addressing lock-in effects, reducing network effects, and lowering barriers to entry. At the same time, we note that there are significant risks and costs from mandating portability, including privacy and cybersecurity risks if individuals' personal data is not carefully protected. Importantly, mandated data sharing also has the potential to diminish incentives to innovate and potentially can lock-in advantages for incumbents.

The discussion follows the framework of the Portability and Other Required Transfers Impact Assessment ("PORT-IA"), as proposed in Swire's report. The PORT-IA is agnostic about whether a portability initiative, on balance, has net benefits or costs; instead, the proposal provides a structured set of relevant questions, to assist legislators, regulators, enforcement officials, and others to evaluate whether proposed mandatory data sharing is likely to be net beneficial.

This article concludes with analysis of how the PORT-IA, with its attention to multiple goals including promoting competition, may appropriately be included in merger review, enforcement discretion, fashioning of remedies and other aspects of antitrust law.

2 Peter Swire, "The Portability and Other Required Transfers Impact Assessment (PORT-IA): Assessing Competition, Privacy, Cybersecurity, and Other Considerations," Peter Swire, (Sept. 8, 2020), available at https://ssrn.com/abstract=3689171.

3 *Data to Go, An FTC Workshop on Data Portability Agenda*, available at https://www.ftc.gov/system/files/documents/public_events/1568699/agenda-dp-workshop.pdf. Swire was both a speaker and a panelist for this workshop.

4 *Data To Go: An FTC Workshop on Data Portability*, Fed. Trade Comm'n (Sept. 22, 2020) available at https://www.ftc.gov/news-events/events-calendar/data-go-ftc-workshop-data-portability.

5 See Gabriel Nicholas & Michael Weinberg, "*Data Portability and Platform Competition: Is User Data Exported from Facebook Actually Useful to Competitors*" Engelberg Center on Innovation Law & Policy, NYU School of Law, (Nov. 2019) available at https://www.law.nyu.edu/centers/engelberg/pubs/2019-11-06-Data-Portability-And-Platform-Competition. See also Stigler Report on Digital Platforms, Final Report, STIGLER CT. FOR THE STUDY OF THE ECONOMY AND THE STATE, CHICAGO BOOTH SCH. (2019) at 32; available at https://research.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler center.pdf.

II. PORT IMPACT ASSESSMENT: A TOOL TO FACILITATE INFORMED LEGISLATING AND DECISION-MAKING

The PORT-IA offers a set of structured questions, based on case studies of historical mandates in a range of industries, that draw out the facts that legislators, regulators and enforcers can rely on to make informed policy and enforcement decisions.

Structured Questions for the PORT-IA: Top-level Questions

Q1: Define the challenge or opportunity that leads to a possible data portability or other required transfer ("PORT")

Data PORTability Benefits:
Q2: Assess PORT rationales based on competition
Q3: Assess innovation and other commercial benefits due to the PORT
Q4: Assess non-commercial benefits due to the PORT
Q5: Assess regulatory or legal benefits of the initiative
Q6: Assess any reduced benefits due to lack of technical or market feasibility
Q7: Assess incentives for those presenting evidence of benefits

Data PORTability Risks and Costs:
Q8: Assess privacy risks from the PORT
Q9: Assess security risks from the PORT
Q10: Assess risks from the PORT that may arise for either security or privacy
Q11: Assess risks to competition from the PORT
Q12: Assess regulatory or legal risks of the initiative
Q13: Assess any other significant costs or risks from the PORT, including obstacles to adoption
Q14: Assess incentives for those presenting evidence of risks or cost

As a matter of terminology, the word "portability" has become a term of art, under the E.U. General Data Protection Regulation, for transfers of an individual's data. We use "other required transfers" for mandated transfers of two more people – these transfers are sometimes described by the vague term "data sharing" in the antitrust literature. "PORT" is a general term for Portability and Other Required Transfers. Figure 1 shows the top-level questions in the PORT-IA – there are also more detailed questions in each portion. The PORT-IA begins by requiring a clear description of the proposed data flows at issue. What is the data, where is it originating, what is the destination, and what obligations are being imposed? When the topic is portability, no accurate analysis can be conducted without a data map and understanding of the law or other constraints that may affect the data transferred. It is equally critical to outline the public policy goals that a data PORTability regime is designed to achieve because implementing any data PORTability regime is likely to require tradeoffs between competing public policy goals.

A. Identifying the Likely Pro-Competitive Benefits

The PORT-IA next examines the procompetitive benefits of the proposed PORT from a range of perspectives.[6] Based on learnings from historical case studies of portability initiatives in a range of industries, the PORT-IA asks whether a required PORT initiative would 1) eliminate lock-in, 2) reduce network effects, 3) lower barriers to entry or repositioning, or 4) otherwise enhance competition in effected markets. The potential for data PORTability to achieve these pro-competitive benefits will differ by industry and depending on the specifics of the proposed obligation.

The PORT-IA first asks whether a data PORTability initiative has the potential to enhance competition by *reducing lock-in effects*. As used in the PORT-IA, lock-in is related to -- but distinct from -- network effects. Lock-in doesn't necessarily depend on a firm having a high market share or other indicia of market power; instead it may reflect practical or technological barriers to switching behavior. For example, absent a legal obligation to facilitate number portability, even a very small mobile carrier with no meaningful market power could lock-in its customers and discourage switching to competing carriers. The extent to which a data PORTability initiative will reduce lock-in effects will turn on the nature of the initiative and the industry to which it will apply.

6 Beyond the potential pro-competitive benefits from PORTability initiatives, there are also non-competition rationales for a PORT, including increased user control/autonomy over their data, a related but separate policy objective.

PORT-IA next enquires into the potential of data PORTability to reduce or eliminate network effects. Network effects can be direct or indirect. *Direct network effects* occur where the value of a service increases as the number of users of that service increase. For example, the value of a telephone or social network to a user increases as the number of other users on the network grows. More recently, some have observed that direct network effects can create and enhance the market power of digital platforms.[7] Enforcement officials have noted that where network effects are significant, tipping can occur, resulting in a "winner take all," or "winner take most" outcome.[8] However, other observers have argued that these direct network effects may be overblown, or that they don't always constitute a significant barrier to entry. They point to the speed at which Facebook displaced MySpace as the leading social network, as well as the ability of competing platforms, like LinkedIn and Twitter, to thrive, due in part to multi-homing behavior.[9]

Where applicable, the PORT-IA also requires an assessment of the potential impact on *indirect network effects*. Indirect network effects are driven by complementary products or services, which work together to increase the value of a network. Indirect network effects are often identified in connection with two-sided platforms, where the value of the platform to one group of participants depends on how many members of a different group participate.[10] Where data PORTability can reduce indirect network effects it can facilitate entry in adjacent markets and prevent a firm from extending dominance into related products and services.

As the FTC, the Antitrust Division of the Department of Justice ("DOJ") and Congress all wrestle with antitrust concerns about leading digital platforms, observers have noted that data PORTability has significant potential to eliminate lock-in and erode barriers to entry. Most notably, in September 2019, the influential Stigler Committee on Digital Platforms identified data interoperability as its top solution to remedy the market power of digital platforms and restore competition. In so doing, it pointed to data PORTability's proven potential to reduce network effects:

A major cause of this lack of competition is the presence of very sizable network externalities: that is, I want to be on the social media where my friends are. Network externalities as a potential barrier to entry are not a new phenomenon: It plagued the early phone industry. To eliminate this problem, the United States forced interoperability among the various phone companies — AT&T is obliged to connect calls started by T-Mobile consumers. The same should be done with social media. Mandating not only an open but also a common Application Program Interface ("API") would allow different messaging systems to connect to one another. In so doing, a common API guarantees interoperability and eliminates the network externalities that drive the winner-take-all nature of the social media market.[11]

Other policy makers, including top legislators, have advanced data PORTability as a critical tool to address consumer lock-in and reduce barriers to entry caused by network effects. Congressman David Cicilline (D-RI), Chair of the House Subcommittee on Antitrust, Commercial and Administrative Law has called for giving consumers more rights and greater control over their data, by using data PORTability to take down the "walled gardens that block start-ups and other competitors from entering the market through high switching costs."[12]

Despite strong theoretical basis to expect these procompetitive benefits, reality may differ substantially in some circumstances. For example, Gabriel Nicholas and Michael Weinberg have cautioned that many of the pre-existing PORTability tools offered by major digital platforms have failed to live up to their theoretical promise.[13] The PORT-IA, therefore, includes questions designed to reveal any practical and technical 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).

---

7 Stigler Report, *supra* note 5 at 38.

8 Prepared Remarks of Renata B. Hesse, Deputy Assistant Attorney General, Remarks as Prepared for the Confrence on Competition and IP Policy in High-Technology Industries: At the Intersection of Antitrust & High-Tech: Opportunities for Constructive Engagement, 6 (Jan. 22, 2014), available at https://www.justice.gov/atr/file/517776/download.

9 See, e.g. Catherine E. Tucker, *Network Effects and Market Power: What Have We Learned in the Last Decade?*, Antitrust, Spring 2018, at 79-80 available at http://sites.bu.edu/tpri/files/2018/07/tucker-network-effects-antitrust2018.pdf; D'Arcy Coolican & Li Jin, *The Dynamics of Network Effects*, Andreessen Horowitz, available at https://a16z.com/2018/12/13/network-effects-dynamics-in-practice/.

10 As the Supreme Court has explained, these indirect network effects are especially pronounced in transactional platforms, where a platform cannot make a sale unless participants on both sides of a platform agree to use their services. *Ohio v. Am. Express Co.*, 138 S. Ct. 2274, 2286 (2018).

11 Stigler Report on Digital Platforms, *supra* note 5, at 16.

12 Congressman David Cicilline, Address at New America Open Technology Institute: A Deep Dive Into Data Portability: How Can We Enable Platform Competition and Protect Privacy at the SameTime?" (June 6, 2018), video available at https://www.newamerica.org/oti/events/deep-dive-data-portability-how-can-we-enable-platform-competition-and-protect-privacy-same-time/.

13 Gabriel Nicholas & Michael Weinberg, "Silicon Valley's Favorite Idea for Encouraging Competition," Slate, Nov. 19, 2019, available at https://slate.com/technology/2019/11/data-portability-facebook-competition-antitrust.html.

B. Identifying the Likely Harms to Competition, Data Security and Data Privacy

Once the expected competitive benefits of a data PORTability initiative have been catalogued and evaluated, the PORT-IA turns to an equivalent analysis of likely harms. As Swire & Lagos noted in a 2013 article, the right to data portability can in some circumstances reduce incentives to innovate. It might also impose unreasonable and disproportionate compliance costs on small companies with no appreciable market power, thereby disadvantaging them relative to better capitalized competitors.[14] Such potential harms to competition should not be ignored.

More generally, PORT-IA requires consideration of whether a proposed PORT would create privacy risks. 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.

III. HOW TO INCORPORATE THE PORT-IA INTO ANTITRUST LAW AND PRACTICE

A basic theoretical point of the PORT-IA is that the overall costs and benefits of a PORT initiative include both the effects on competition and effects on other significant legal and policy goals, such as privacy, cybersecurity, and user control of their information. These multiple categories or costs and benefits raise the issue of how antitrust law can and should take account of these other goals.

A. Use of the PORT-IA in Legislation, Regulation, and Company Product Choice

Multiple policy goals can and should be considered in enacting legislation – it is the province of the legislature to consider potentially conflicting goals such as competition, privacy, and cybersecurity. Hearings on proposed PORTability legislation could include witnesses able to shed light on these important topics so that lawmakers can craft laws that avoid mistakes that could harm consumer welfare.

PORTability legislation and proposals have increased in recent years. The General Data Protection Regulation in the EU, which went into effect in 2018, includes a Right to Data Portability, as does the California Consumer Privacy Act, which went into effect in 2020. In 2019, Senators Josh Hawley (R-MO), Mark R. Warner (D-VA) and Richard Blumenthal (D-CT) introduced S.2658, the Augmenting Compatibility and Competition by Enabling Service Switching ("ACCESS") Act. At the time, Senator Blumenthal remarked that, "[a]s we learned in the *Microsoft* antitrust case, interoperability and portability are powerful tools to restrain anti-competitive behaviors and promote innovative new companies. The bipartisan ACCESS Act would empower consumers to finally stand up to Big Tech and move their data to services that respect their rights."[15] The ACCESS Act would impose obligations on income-generating, consumer-facing communications services with more than 100 million monthly active U.S. users, requiring them to enable users to safely download their own data or directly port it to a competing communications provider. In addition, as discussed in detail in the PORT-IA report, the leading proposals for comprehensive federal privacy legislation contain a Right to Data Portability, as do pending proposals in numerous states.[16]

For rulemaking, unless there is some limit created by the statute that authorizes regulation, it similarly is in the public interest to consider both competition and other regulatory goals. The structured questions can serve as a check-list to ensure that regulators appreciate competing considerations and work to impose and enforce regulations that minimize the tensions that can exist between competition, privacy and data security goals. For example, the U.S. Department of Health and Human Services issued a major rule in March 2020 on health care interoperability, which attempted to balance a range of competition, privacy, cybersecurity, and other issues.[17]

14 Peter Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, 72 Md L. Rev. 335 (2013).

15 Press Release, Senators Introduce Bipartisan Bill to Encourage Competition in Social Media (Oct. 22, 2019) available at https://www.warner.senate.gov/public/index.cfm/2019/10/senators-introduce-bipartisan-bill-to-encourage-competition-in-social-media.

16 International Association of Privacy Professionals, Resource Center: State Comprehensive-Privacy Law Comparison Bills Introduced 2019-2020 (2020), available at https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law.pdf.

17 See 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 84 Fed. Reg. 7424, 7469 (proposed March 4, 2019) (codified at 45 C.F.R. parts 170 and 171), available at https://www.federalregister.gov/documents/2019/03/04/2019-02224/21st-century-cures-act-interoperability-information-blocking-and-the-onc-health-it-certification.

Similarly, the multiple goals evaluated in a PORT-IA can assist a business deciding whether and how to build PORTability into its services. For such a company, considering privacy and cybersecurity may be good for its customers or its bottom line. In addition, however, the company may be under legal requirements pertaining to privacy and cybersecurity. For instance, a company may be subject to a privacy or cybersecurity consent decrees with the FTC, or covered by comprehensive data protection laws in the European Union ("EU") or elsewhere. Companies need to carefully evaluate whether enhancing PORTability would risk violation of these competing obligations.

B. PORT-IA Can Also be Used by Antitrust Enforcers to Make More Informed Enforcement Decisions and to Design More Effective Remedies

The use case for PORT-IA is more complex for law enforcement agencies. Enforcers like the FTC, which enforces both antitrust and consumer protection laws, arguably have broader leeway to balance competition, data security and data privacy considerations. But even dedicated competition enforcers, such as the Antitrust Division, can reach more informed decisions by considering the questions posed by the PORT-IA.

1. PORT-IA Can Contribute to More Informed Enforcement Decisions

Most U.S. antitrust authorities appear unwilling generally to stretch the antitrust laws to target data privacy and data security breaches by major digital platforms. As FTC Commissioner Christine Wilson has argued, "[t]he antitrust laws are designed to address anticompetitive conduct; absent such conduct, they are not the right tool to protect the legitimate and important privacy rights and expectations of consumers."[18] And U.S. antitrust enforcers have historically declined to enforce the antitrust laws to protect consumer privacy rights.

But one doesn't need to be a proponent of *hipster* antitrust to appreciate that data privacy and cybersecurity concerns can play a supporting role in antitrust enforcement decisions. Swire first wrote in 2007 that privacy can be a quality, non-price aspect of competition.[19] FTC Commissioner Noah Phillips has acknowledged, "[p]rivacy is not necessarily irrelevant to antitrust law. If, in fact, firms are competing on privacy, then that is an aspect of competition at which we should look."[20] Assistant Attorney General Makan Delrahim has likewise indicated that "it would be a grave mistake to believe that privacy concerns can never play a role in antitrust analysis…. Like other features that make a service appealing to a particular consumer, privacy is an important dimension of quality…. As I have said before, these non-price dimensions of competition deserve our attention and renewed focus in the digital marketplace."[21]

Moreover, there is an argument that data privacy and security considerations may be relevant to a traditional antitrust analysis of a business's data portability and interoperability practices and policies. In monopolization cases, for example, a businesses' *bona fide* interest in protecting data security and privacy might well bear on *intent*, and therefore serve as evidence that challenged conduct is not fairly characterized as exclusionary or anticompetitive.[22] Relatedly, provided they are not pretextual, a company's proffered concerns that more robust data PORTability functionality might expose its user's data to security or privacy risks could also serve as a legitimate *procompetitive justification* for its practices, particularly if there are no less competitively restrictive means to avoid those concerns.[23] Finally, in exercising prosecutorial discretion in close cases, enforcement agencies focused on consumer welfare arguably should not turn a blind eye to the real-world tensions that emerge as businesses work to balance competing considerations relating to competition, data security and data privacy.

---

18 Christine S. Wilson, Commissioner, Fed. Trade Comm'n, Remarks at University of Illinois at Chicago John Marshall Law School: Global Innovation, Local Regulation: Navigating Competition Rules in the Digital Economy, 7 (Mar.13, 2020); available at https://www.ftc.gov/system/files/documents/public_statements/1569053/wilson_- global_innovation_local_regulation_ui_chicago_speech_3-13-20.pdf.

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

20 Noah Joshua Phillips, Commissioner, Fed. Trade Comm'n, Keynote Address at Stanford Law School: Should We Block This Merger? Some Thoughts on Converging Antitrust and Privacy, 13 (Jan. 30, 2020) available at https://www.ftc.gov/system/files/documents/public_statements/1565039/phillips_-_stanford_speech_10-30-20.pdf.

21 Makan Delrahim, Assistant Attorney General, Dept. of Justice, Antitrust Division, Remarks at Harvard Law School & Competition Policy International Conference on "Challenges to Antitrust in a Changing Economy": "Blind[ing] Me With Science": Antitrust, Data, and Digital Markets, 8-10 (Nov. 8, 2019) available at https://www.justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers-remarks-harvard-law-school-competition.

22 See, e.g. *Aspen Skiing Co v. Aspen Highlands Skiing Corp.*, 472 U.S. 585, 602 (1985).

23 See, e.g. *United States v. Microsoft Corp.*, 253, F.3d 34, 59 (D.C. Cir. 2001).

2. PORT-IA Can Allow Enforcers and Judges to Design Remedies that Avoid Unnecessary Harm to Data Security and Privacy

Enforcers can also benefit from conducting a PORT-IA in the event they are considering imposing data PORTability obligations as a remedy to an anticompetitive merger or practice. As the Director of the FTC's Bureau of Competition explained recently, the FTC recognizes an obligation to consider data privacy and consumer protection concerns in fashioning data-related remedies for anticompetitive mergers and other conduct challenged by the agency:

> Data's competitive role and its portability is not just a question to be assessed in looking at the effects of a proposed transaction or practice. It is key to understanding what it is going to take to remedy the potential or actual competitive harms from those transactions and that conduct. Without understanding the role of data portability, we can't fully assess the remedy necessary to address those competitive harms. *And making more and more users data more accessible and held by more entities can itself actually raise privacy and consumer protection concerns that we must consider in crafting our competition remedies.*[24]

In short, the FTC's top antitrust enforcer has acknowledged that the agency has an obligation to consider the risks to privacy and consumer protection when fashioning remedies for antitrust violations. To date, the DOJ leadership has not addressed this issue so directly. However, the Division's recently issued Merger Remedies Manual notes that a proposed remedy should not only effectively redress the violation, but "just as importantly, be no more intrusive than necessary to cure the competitive harm."[25] In using data PORTability as a remedy, the DOJ at least has an interest in imposing remedies that don't unnecessarily expose consumer data to security or privacy risks. The importance of considering privacy and cybersecurity is even more compelling where a proposed remedy threatens to create a conflict with a party's privacy or data security legal obligations, such as compliance with a privacy or data security law, regulation or consent decree. The PORT-IA is intended to be a tool to ensure that these remedy decisions are fully informed and reflect a comprehensive view of the impact of the costs and benefits of data PORTability.

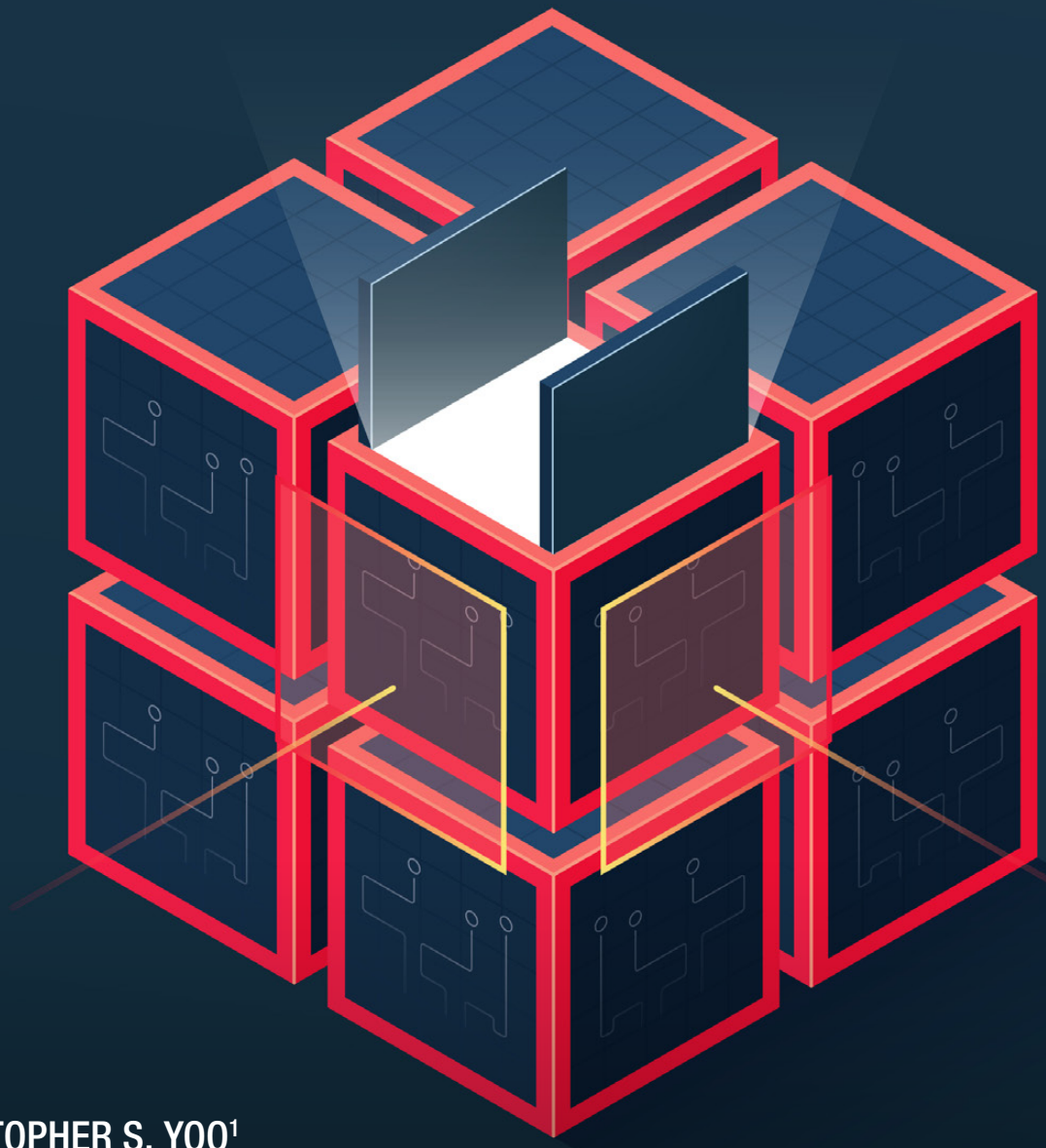
IV. CONCLUSION

There are compelling reasons for decision-makers to explore the use of data PORTability to enhance or restore competition by reducing switching costs and lowering barriers to entry. Increased transfers of personal data, however, often carry risks to cybersecurity and personal privacy. The PORT-IA provides a structured set of questions to investigate the range of relevant effects of a PORTability proposal. As discussed here, attention to these competing public policy goals makes sense for legislation, regulation, and for decisions within individual companies of when and how to enhance PORTability. In addition, even under traditional antitrust frameworks, there are opportunities for antitrust enforcement officials to recognize these privacy and cybersecurity considerations, both in connection with enforcement decisions and when fashioning antitrust remedies.

24 Ian Conner, Director, Federal Trade Commission Bureau of Competition, Closing Remarks at Data to Go: An FTC Workshop on Data Portability, September 22, 2020, at 6:18:50-6:19:30 (emphasis added); video available at https://www.ftc.gov/news-events/audio-video/video/data-go-ftc-workshop-data-portability.

25 U.S. Dept. of Justice Antitrust Division, Merger Remedies Manual § II (Sept. 2020), available at https://www.justice.gov/atr/page/file/1312416/download. See also *id.* at fn.4 ("In contrast to the limited public-interest inquiry under the Tunney Act, the Division's prosecutorial discretion encompasses a broader set of considerations, including the facts developed in the investigation, the judgment of the prosecuting attorneys, and the allocation of the Division's limited resources.").

UNPACKING DATA PORTABILITY



BY CHRISTOPHER S. YOO[1]

1 John H. Chestnut Professor of Law, Communication, and Computer & Information Science and Founding Director of the Center for Technology, Innovation and Competition, University of Pennsylvania.

I. INTRODUCTION

Data portability has become a hot topic in competition law. Now well established as a matter of privacy law by the enactment of the California Consumer Protection Act ("CCPA") and the European Union's General Data Protection Directive ("GDPR"), legislators and enforcement officials around the world have shown increasing interest in data portability as a competition law remedy. It was endorsed by recent high-profile reports issued by expert panels convened by the European Commission and the UK in 2019. The 2019 report released by the Australian Competition and Consumer Commission ("ACCC") was more circumspect, concluding that data portability was unlikely to provide any short-term benefits to competition in digital platform markets. At the same time, the ACCC promised to revisit the issue when considering how to apply the 2017 consumer data right to other sectors.

The topic began to attract interest in the U.S. this fall. For example, the Federal Trade Commission conducted a workshop on the topic on September 20. In addition, the October 6 majority staff report that capped off the U.S. House Judiciary Committee's sixteen-month investigation into digital markets recommended mandating data portability through legislation requiring data portability under competition law. Although both the U.S. Supreme Court and the European Court of Justice have yet to adopt the doctrine, their discussions of related principles and lower court decisions imply some clear prerequisites for it to apply. Both jurisdictions require that the resource to which competitors are demanding access be *essential* or *indispensable*, in that the competitor is practically unable to duplicate it or obtain it from another source.[2] U.S. law also requires the absence of a regulatory regime through which the competitor could obtain access to the resource and the feasibility of providing access.[3] European law limits mandating access to "exceptional circumstances," further requiring that refusal to provide access excludes effective competition and prevents the appearance of a new product or new technological development, which precludes the use of data portability to provide me-too products.[4]

These requirements represent important prerequisites that must be satisfied before mandating data portability under competition law. In addition, the fact that options for data portability remain virtually unused despite being mandated by GDPR and CCPA and offered by leading digital platforms, such as Google and Facebook, suggests that the implementation of data portability may present important practical considerations that must be taken into account.

II. ALL DATA ARE NOT CREATED EQUAL: STRUCTURED VS. UNSTRUCTURED DATA

An essential prerequisite for mandating data portability under competition law is the inability for the competitor to duplicate the data or obtain them from another source. To date, discussions have largely treated data as a monolithic phenomenon without drawing any distinctions among particular types of data and their different uses. A proper evaluation of the opportunities for self-provisioning and the availability of similar data from third parties requires a better understanding the precise types of data to which access is sought and their uses.

For example, although advocacy rhetoric tends to talk about "big" data, the trade press repeatedly emphasizes that size is not the only thing that matters. Gartner famously articulated in 2001 that data consists of 3 Vs: Although volume is an important characteristic of data, so are its velocity (rate of change) and variety (differences in type and source). From there, other commentators have expanded the list, with one consulting firm listing as many as 42 Vs.[5] Although this framework has yet to be subject to rigorous academic analysis, the basic point about the multidimensionality of data is clear enough.

There is another more important distinction that has yet to arise in competition law circles but has begun to attract attention among academics: the distinction between structured and unstructured data. *Structured data* are collected intentionally to inform a specific model. Examples include traditional column-row databases that record names, dates, addresses, and transaction histories, which represent the type of data with which people are most familiar. *Unstructured data* are collected incidentally and used to inform emergent models. Examples include video, audio, social media feeds, photos, and sensor data. *Semi-structured data*, which are structured data used to inform other, emergent models, represent an intermediate case. A common example of semi-structured data is email analyzed for purposes other than person-to-person communications.

2 Case T-201/04, *Microsoft v. Commission*, 2007 E.C.R. II-3601, 3725 ¶ 328; 3B Phillip E. Areeda & Herbert Hovenkamp, Antitrust Law ¶ 773b2, at 242-43 (3d ed. 2008).

3 *Verizon Commc'ns Inc. v. Law Offices of Curtis V. Trinko*, 540 U.S. 398, 411 (2004); *MCI Commc'ns Corp. v. AT&T Co.*, 708 F.2d 1081, 1133 (7th Cir. 1983).

4 *Microsoft*, 2007 E.C.R. at II-3726 ¶¶ 331-332, II-3818 ¶ 647.

5 Tom Safer, *The 42 V's of Big Data and Data Science*, Elder Research (Apr. 1, 2017), https://www.elderresearch.com/blog/42-v-of-big-data.

Structured and unstructured data serve very different purposes. The user-facing side of online transactions (such as search results or purchase recommendations) tends to be based on structured data . The profiles used to support advertising incorporate significant amounts of unstructured data.

More importantly for purposes of competition law, structured and unstructured data have different economic characteristics relevant to the essential facilities doctrine. Empirical studies have shown the scale economies with respect to structured data to be modest enough that relatively small competitors should be able to achieve them on their own without gaining access to the resources of others. That fact would tend to vitiate claims that the facility is essential. The scale economies for unstructured data are more significant, but the number of alternative sources of the demographic and other information used to create advertising profiles are legion. Indeed, industry observers suggest that more than 80 percent of all available data is unstructured data.

These considerations suggest some key factual propositions regarding scale economies and substitutability that must be established by any antitrust court faced with a request to mandate data portability. They also underscore the importance of considering such requests in the context of specific types of data and not lumping all forms of data into the same bucket.

III. THE SIGNIFICANCE OF REGULATORY ALTERNATIVES

As noted earlier, different legal regimes draw different inferences from the existence of a regulatory regime that could provide access to the resource in question. U.S. law holds that the presence of a regulatory regime through which competitors can obtain access renders the essential facilities doctrine inapposite, while the recent decision of the German Federal Court Justice in the Facebook case ruled the presence of related relief under privacy law does not foreclose actions under competition law.[6] This distinction accord with the U.S. tradition of treating competition law and regulation as substitutes and the European approach of treating them as complements.[7]

These jurisprudential differences suggest that each regime may accord different effect to the fact that CCPA and GDPR already provide for the right of data portability, with the U.S. regarding the existence of a regulatory mechanism for compelling sharing rendering access under the antitrust laws nonessential. The fact that the relevant European privacy law did not cover the precise conduct in question in the German Facebook case does leave some room for a different outcome with respect to data portability.

IV. THE TENSION BETWEEN PORTABILITY AND PRIVACY

One of the central raised concerns at the FTC hearing was the possibility that data portability may impair efforts to protect consumer privacy. As an initial matter, any data portability regime must take great care to verify that the person requesting the data is actually the data subject. Any failure to verify the person's identity risks giving unauthorized actors access to their personal information.

In addition, one of the fundamental cornerstones of U.S. privacy law is notice and consent, in which the parties enter into an agreement as to the permitted uses of any data collected. This makes the enforcement of promises made in privacy policies a matter of contract. While data subjects have sufficient privity of contract with the firm that collects their data in the first instance to have standing to sue them for any breaches of that agreement, that contract does not provide any enforceable rights against third parties that obtain the information through data portability. Thus, exercises of data portability carry some risk of weakening privacy protections.

The same problem arises with respect to re-identification of data. The most common way to de-anonymize a dataset is by correlating it against an identified dataset. The best practices identified by the FTC's 2012 report require holders of de-identified data to "(1) take[] reasonable measures to ensure that the data is de-identified; (2) publicly commit[] not to try to re-identify the data; and (3) contractually prohibit[] downstream recipients from trying to re-identify the data."[8] The reliance on contract to protect against de-identification again places data portability in tension with privacy by potentially limiting the data subjects' rights against firms that use data portability to obtain access to their personal information.

---

6 Compare *Trinko*, 540 U.S. at 411-13, with *BGH* June 23, 2020, KVR 69/19 ¶ 126, https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2020-6&nr=109506&linked=bes&Blank=1&file=dokument.pdf.

7 Compare *Pac. Bell Tel. Co. v. linkLine Commc'ns, Inc.*, 555 U.S. 438 (2009), with Case C-280/08P, *Deutsche Telekom v. Commission*, 2010 E.C.R. I-9555.

8 Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers iv, 21 (2012), available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

V. IMPLEMENTATION CHALLENGES

Beyond the conceptual challenges discussed above, mandating data portability under antitrust law would raise significant practical challenges as well. It would require establishing new systems for ordering and provisioning requests for data. It would also raise significant presume to mandate data compatibility as well.

Ordering and provisioning: Lower U.S. decisions also predicate the essential facilities doctrine on the feasibility of providing access.[9] As the Supreme Court noted, services that are not already offered as separate products "exist only deep within the bowels" of the company, which means that access mandates would force companies to design and implement new systems to make that access possible.[10]

In short, a data portability mandate would require firms to establish new systems for ordering and provisioning request for data. Court considering implementing such mandates will need to decide how much metadata will be disclosed. If the data are substantial, the process may take some time and require considerable resources to transfer the data. Past experience has shown that antitrust courts will have to supervise an increasing scope of the business relationship when the quality of the product varies and when the interfaces are complex.[11]

Compatibility: The fact that firms base their operations on different and often incompatible data structures means that simply mandating data portability will require competitors to fit the proverbial square peg into a round hole. To promote competition, the data that is being shared must be compatible.

The need for compatibility suggests two natural solutions, both of which have considerable drawbacks. The first is reconfiguration of the data, most likely by the competitor who requested them. The problem is that enterprise-grade databases are often prohibitively expensive to reconfigure. In addition, any process of conversion or translation runs the risk of introducing errors.

The second is standardization. Any form of standardization of data formats necessarily structures interactions in ways that can limit the functionality of these systems. Requiring that a firm use a particular data structure thus inevitably has a direct impact on innovation.[12] In addition, antitrust officials have become increasingly concerned that standard setting processes may be vulnerable to strategic behavior.

VI. CONCLUSION

Some of the participants in the FTC workshop have somewhat ingenuously pointed to data portability as low hanging fruit in terms of antitrust remedies for big tech firms compared with the challenges posed by more complex remedies such as interoperability. The need to differentiate between structured and unstructured data; the relevance of alternative regulatory mechanisms for obtaining access to data; the potential for portability to weaken privacy; and implementation challenges relating to ordering, provisioning, and compatibility reveal that data portability is not the panacea for which some would hope. Instead, a closer examination confirms that such cases require the type of nuanced, fact-specific inquiry that characterizes classic antitrust analysis and the implicit limitations of the still provisional essential facilities doctrine.

9 *MCI*, 708 F.2d at 1133.

10 *Trinko*, 540 U.S. at 410. *But see* Case C-418/01, *IMS Health GmbH & Co. OHG v. NDC Health GmbH & Co. KG*, 2004 E.C.R. I-5069, I-5084 ¶ 43 (noting that service need not be marketed separately to fall within essential facilities doctrine).

11 *Trinko*, 540 U.S. at 414; 3B Areeda & Hovenkamp, *supra* note 2, ¶ 774e, at 275-79.

12 Christopher S. Yoo, *When Antitrust Met Facebook*, 19 Geo. Mason L. Rev. 1147, 1155 (2012).

THE OPPORTUNITIES AND LIMITS OF DATA PORTABILITY FOR STIMULATING COMPETITION AND INNOVATION

BY INGE GRAEF[1]

1 Associate Professor of Competition Law at Tilburg University, affiliated to the Tilburg Law & Economics Center (TILEC) and the Tilburg Institute for Law, Technology, and Society (TILT). This article is based on oral remarks made by the author at the 'Data To Go' workshop on data portability organized by the US Federal Trade Commission on September 22, 2020. For more information about the workshop, see https://www.ftc.gov/news-events/events-calendar/data-go-ftc-workshop-data-portability.

I. INTRODUCTION

The concept of data portability has been heralded as a key enabler of consumer empowerment, competition and innovation. Despite its potential, data portability does not seem to have had the impact yet it was expected to have. Against this background, this article explores the opportunities as well as limits of data portability and provides suggestions to make data portability more effective – both as a data protection concept and as a tool for stimulating competition and innovation.

To reap its full potential, this article submits that there is a need for regulators to steer the implementation of the right to data portability in the General Data Protection Regulation ("GDPR") through guidance to data controllers on how to balance different interests and through asymmetric enforcement by imposing additional requirements on data controllers with market power. Attention is also paid to merger review, where the GDPR's right to data portability has been relied upon as a limit that can prevent competition concerns from arising despite the current problems with data protection enforcement. Because of its hybrid nature that brings together considerations of data protection, competition and innovation, data portability can also be implemented through other regimes beyond data protection law. In particular, data portability may be imposed under competition law on dominant firms and under the upcoming ex ante regulation in the Digital Markets Act on gatekeeping platforms. These regimes are not bound by the limits of the GDPR's right to data portability and can therefore impose additional forms of data portability, including portability of non-personal data for business users, portability of inferred data and real-time continuous portability. The article concludes that, nevertheless, data portability in itself is unlikely to be sufficient in order to address the risk of market tipping and to keep data-driven markets open to newcomers.

II. HYBRID NATURE OF DATA PORTABILITY

The nature of data portability is a hybrid between various interests. The concept originated in the GDPR, which is a data protection instrument and aims to empower individuals by strengthening the control over their personal data. The right to data portability of Article 20 GDPR was one of the tools introduced to pursue this objective by giving individuals the right to receive personal data provided to a data controller in a structured, commonly used and machine-readable format and to transmit this data to another controller. In this sense, one can argue that the right to data portability fits with the fundamental rights nature of data protection by enhancing informational self-determination.[2]

At the same time, one can characterize data portability by the sharing and reuse of data that it facilitates.[3] During the legislative discussions in the Council, a number of Member States doubted whether to retain the right to data portability in the GDPR because they considered data portability not to be within the scope of data protection but rather in consumer or competition law.[4] However, one should keep in mind that the GDPR serves a dual objective of, on the one hand, protecting the fundamental right to data protection and, on the other hand, promoting the free flow of personal data.[5] This second objective, which is more about stimulating the EU's internal market, is very much present in the right to data portability and brings the concept close to other policy areas, in particular those of competition and innovation.

In EU law and policymaking, the concept of data portability is now emerging in many areas: from data protection to consumer law,[6] it has been integrated into competition analysis already in some merger cases,[7] and it also forms part of broader innovation policies for instance in the context of the European Commission's data strategy.[8] In addition, notions of data portability and data access are appearing in sector-specific

2 Orla Lynskey, "Aligning data protection rights with competition law remedies? The GDPR right to data portability," European Law Review 2017, p. 809-810.

3 Inge Graef, Martin Husovec & Nadezhda Purtova, "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law," German Law Journal 2018, p. 1369.

4 Council of the European Union, Interinstitutional File: 2012/0011 (COD), 10614/14, June 6, 2014, p. 3 footnote 1.

5 Article 1 of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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 (GDPR) [2016] OJ 119/1.

6 Article 16(4) of Directive (EU) 2019/770 of the European Parliament and of the Council of May 20, 2019 on certain aspects concerning contracts for the supply of digital content and digital services (Digital Content Directive) [2019] OJ L 136/1.

7 See Case M.7813 - Sanofi/Google/DMI JV, February 23, 2016 and Case M.8124 - Microsoft/LinkedIn, 6 December 2016 as discussed in section VI. below.

8 Commission Communication, "A European strategy for data," COM(2020) 66 final, 19 February 2020, p. 20.

frameworks, for instance in the banking,[9] energy[10] and automotive[11] industries. This makes data portability a concept with a hybrid nature. This hybrid nature also determines what impact data portability can have on consumers and competition. Because of the various interests that come together in the concept of data portability, there are still questions about how tensions between these interests should be reconciled in concrete cases. These tensions can stand in the way of data portability reaching its potential for stimulating data protection, competition and innovation.

III. OVERLAPPING LEGAL ENTITLEMENTS

The existence of different legal entitlements over the same dataset can result into tensions between the various interests relevant to data portability. This issue takes different shapes. Personal data can relate to more than one individual, for instance one's interactions on a social network. And personal data of an individual may at the same time be protected by intellectual property rights held by a data controller.

Such overlapping legal entitlements can limit the effectiveness of data portability, depending on the extent to which they stand in the way of requests of individuals to have their personal data transferred to another provider. For example, Facebook has claimed before that its trade secrets and intellectual property prevent the company from sharing all the personal data it holds about a user in response to access requests under data protection law.[12] How exactly these interests and legal entitlements should be balanced against each other is not entirely clear from the text of the GDPR.

Article 20(4) GDPR states that the application of the right to data portability should not adversely affect the rights and freedoms of others. Such third-party rights and freedoms include the data protection rights of others as well as the intellectual property rights held by data controllers. Some guidance on how to balance these interests has been provided by the Article 29 Working Party[13] in its 2017 guidelines on the right to data portability.

As regards mixed datasets containing personal data from more than one individual, the guidelines from the Article 29 Working Party suggest data controllers to set up mechanisms to obtain consent from third parties. This would ease data transmission in situations where third party data subjects are willing to consent to the porting of their personal data in response to someone else's data portability request. In the absence of such consent, the new data controller should identify another legal basis for the processing of third party personal data, such as its legitimate interests to provide a service to the data subject that invoked the data portability request. Beyond this purpose, the data controller is not allowed to use the transmitted third party data to serve its own interests, for instance for proposing marketing products or for enriching the profile of the third party data subject.[14]

With regard to intellectual property rights, the Article 29 Working Party states in its guidelines that intellectual property cannot be a reason for data controllers to refuse to port all the personal data. Data controllers should try to transmit personal data in a form that does not release information covered by trade secrets or intellectual property rights.[15] However, the guidelines do not clarify what should happen in case this is not possible. And if data controllers would be obliged to facilitate portability requests for personal data over which they hold intellectual property claims, another question is whether this also implies that new controllers should be able to reuse the ported data free of charge without having to obtain a license from the original intellectual property rights holder.[16] More clarity about these issues will hopefully follow, now the European Commission announced in its February 2020 Communication 'A European strategy for data' its intention to evaluate the intellectual property framework with a view to further enhance data access and use, including a possible clarification of the application of the Trade Secrets Directive as an enabling framework.[17]

9 Article 66 and 67 of Directive (EU) 2015/2366 of November 25, 2015 on payment services in the internal market (Payment Services Directive 2) [2015] OJ L 337/35.

10 Article 23 of Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity (Electricity Directive) [2019] OJ L 158/125.

11 See the discussion in Commission Communication, "On the road to automated mobility: An EU strategy for mobility of the future," COM (2018) 283 final, May 17, 2018, p. 13

12 Emil Protalinski, "Facebook: Releasing your personal data reveals our trade secrets," ZDNet, October 12, 2011, available at https://www.zdnet.com/article/facebook-releasing-your-personal-data-reveals-our-trade-secrets/.

13 The Article 29 Working Party is a former advisory body composed of, among others, representatives from the national data protection authorities in the EU Member States and is now replaced by the European Data Protection Board.

14 Article 29 Working Party, "Guidelines on the right to data portability," 16/EN WP 242 rev.01, 5 April 2017, p. 11-12.

15 Article 29 Working Party, "Guidelines on the right to data portability," 16/EN WP 242 rev.01, April 5, 2017, p. 12.

16 For an analysis, see Inge Graef, Martin Husovec & Nadezhda Purtova, "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law," German Law Journal 2018, p. 1375-1386.

17 Commission Communication, "A European strategy for data," COM(2020) 66 final, February 19, 2020, p. 13.

How to precisely strike the balance between different interests will need to be addressed through future measures and cases. Despite the (non-legally binding) guidance from the Article 29 Working Party, the concrete application of the right to data portability in practice still raises issues. This can also be seen from the White Paper on data portability that Facebook published in September 2019 to launch a debate about how to develop privacy-protective data portability.[18] In addition, Facebook called upon regulators to step in to balance the desirability of data portability with the greater risks for privacy when announcing a photo transfer tool.[19] These are important trade-offs that should not be completely left up to private companies.[20]

Until more clarity is provided through further guidance or cases, there is quite some discretion for data controllers themselves to strike the balance between the various interests. This may not always lead to desirable outcomes, because data controllers could point to the existence of these overlapping legal entitlements as an excuse to limit the scope of the data that should be ported.

The message here is that the impact of data portability is not an abstract or static issue; it is something that regulators and enforcers can and should influence by guiding and steering implementation. This is true for how data portability interacts with the privacy interests of other individuals as well as the intellectual property rights of data controllers, and it also holds for the impact of data portability on competition and innovation.

IV. POTENTIAL OF DATA PORTABILITY TO STIMULATE COMPETITION AND INNOVATION

It is still unclear what impact the GDPR's right to data portability exactly has on competition and innovation and if it can indeed foster competition between data controllers and encourage data-driven innovation, as was expected as a positive side effect of the new right at the time of adoption.[21] In particular, competition may increase in markets where data portability would make it easier for individuals to switch between services by taking their data with them.[22] A prerequisite for this is that individuals actively invoke their right to data portability.[23]

Despite its potential to stimulate competition and innovation, concerns are now expressed that data portability can strengthen the position of established players by letting their users invoke the right to data portability to get even more data.[24] This would lower competition because smaller firms would then see their users move with their data to the established players. For instance, economic modelling has suggested that data portability's prospect of easier switching can lure consumers into providing more data to the incumbent. Because of the additional data, the incumbent gets a competitive advantage in performing data analytics that can raise entry barriers for newcomers.[25] A recent review of economic literature expects data portability not to lead to less or more competition in established digital markets by itself, but does point at its ability to encourage innovation in complementary and new digital markets by letting innovation at the service and at the data analytics levels take place within different firms at the same time.[26]

18 Facebook White Paper, "Charting a Way Forward on Privacy and Data Portability," September 2019, available at https://about.fb.com/wp-content/uploads/2020/02/data-portability-privacy-white-paper.pdf.

19 Matthew Newman, "Facebook wants EU lawmakers to weigh up data portability's risks and rewards, Clegg says," MLex, December 2, 2019.

20 See the discussion in Inge Graef, "Paving the Way Forward for Data Governance: a Story of Checks and Balances (Editorial)," Technology and Regulation 2020, p. 26-27, available at https://techreg.org/index.php/techreg/article/view/57/13.

21 However, see the concerns about the costs that the GDPR's right to data portability would impose on small businesses expressed by Peter Swire & Yianni Lagos, "Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique," Maryland Law Review 2013, p. 349-353.

22 See the comments by the then Competition Commissioner Almunia in the speech "Competition and personal data protection," November 26, 2012, available at https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_12_860: 'I believe that a healthy competitive environment in these markets requires that consumers can easily and cheaply transfer the data they uploaded in a service onto another service. The portability of data is important for those markets where effective competition requires that customers can switch by taking their own data with them'.

23 There are some indications that the GDPR's right to data portability is not so actively invoked or effectively implemented yet. See for instance Janis Wong & Tristan Henderson, "The right to data portability in practice: exploring the implications of the technologically neutral GDPR," International Data Privacy Law 2019, p. 173–191; Sarah Turner, July Galindo Quintero, Simon Turner, Jessica Lis & Leonie Maria Tanczer, "The exercisability of the right to data portability in the emerging Internet of Things (IoT) environment," new media & society 2020 (forthcoming), p. 1-21, available at https://doi.org/10.1177/1461444820934033.

24 See also Esmeralda Florez Ramos & Knut Blind "Data portability effects on data-driven innovation of online platforms: Analyzing Spotify," Telecommunications Policy 2020, who argue that online platforms not facing real competition do not have a substantial need to increase investments in data-driven innovation due to possible risk and opportunity of increased user switching that could result from the GDPR's right to data portability.

25 Wing Man Wynne Lama & Xingyi Liu, "Does data portability facilitate entry?," International Journal of Industrial Organization 2020, p. 1-24, available at https://doi.org/10.1016/j.ijindorg.2019.102564.

26 Jan Krämer, Pierre Senellart & Alexandre de Streel, "Making data portability more effective for the digital economy: Economic implications and regulatory challenges," CERRE report June 2020, p. 55-64, available at https://cerre.eu/publications/report-making-data-portability-more-effective-digital-economy/.

V. ASYMMETRIC ENFORCEMENT OF THE GDPR'S RIGHT TO DATA PORTABILITY

A way to ensure that data portability creates opportunities for newcomers to innovate and that limits the undesirable effect of consolidating the market position of established players is to introduce asymmetric regulation and enforcement. Asymmetric enforcement implies that the level of obligations applicable to a business are tailored to its market share or the scope of its activities. In other words, powerful firms (which could for instance be determined by looking at whether they hold market power from the perspective of competition law) would be subject to stricter requirements for enabling data portability. The GDPR's risk-based approach already provides room for such an approach.

While the GDPR applies to all forms of processing of personal data regardless of the market position of the data controller, it does take into account the level of risk for determining the extent of the obligations to which controllers are subject. When the risk of processing is higher, data controllers have to comply with more detailed requirements. For instance, 'the risks of varying likelihood and severity for the rights and freedoms of natural persons' need to be taken into account for determining the extent of technical and organizational measures a data controller has to implement to ensure and be able to demonstrate that the processing of personal data is performed in compliance with the GDPR.[27] The 2019 expert report on 'Competition Policy for the Digital Era' commissioned by EU Commissioner Vestager also refers to the relevance of a firm's market power under the GDPR's risk-based approach.[28]

In terms of compliance with Article 20 GDPR, asymmetric enforcement could mean that an additional responsibility is imposed on powerful data controllers to facilitate data portability. One of the open questions is whether the right to data portability requires one-off portability only, where personal data is transferred once to a new controller at the request of the data subject, or whether it can also be interpreted to include continuous and real-time portability of personal data until the data subject revokes her portability request. While some have argued that the GDPR's right to data portability has not been designed for real-time data sharing,[29] others have pleaded for a broader interpretation beyond one-off portability to make the right more suitable for the dynamic needs of data-driven markets.[30] Considering that data controllers with market power have more resources to implement the technical measures for enabling real-time portability, it would be justified to require such firms to do so in order to comply with Article 20 GDPR. This would make the GDPR's right to data portability more effective without burdening small data controllers with the same level of obligations. However, to avoid adverse effects on small data controllers, the compliance measures taken by powerful data controllers should be carefully monitored to prevent that technical standards are established that would squeeze out smaller firms or that would otherwise limit their ability to develop innovative services.

Criticism against making data protection obligations, such as the right to data portability, scalable may be that such an approach provides data subjects of data controllers holding market power with a higher level of protection as compared to data subjects of data controllers without market power. One could argue that this is at odds with the general applicability of the data protection rules. Furthermore, the fundamental right to data protection that the GDPR promotes requires to be respected irrespective of the market position of the data controller. After all, small data controllers may also engage in far-reaching data processing activities and can cause harm to their data subjects. However, there is reason to be particularly concerned about data controllers holding market power whose behavior is less constrained by the competitive forces of the market. In this regard, one could even claim that data subjects of powerful firms are less protected if the data protection rules would not take into account market power for interpreting the extent of protection to be offered to data subjects under the GDPR. Important to note here is that the scalability of data protection obligations would serve as a tool to impose stricter requirements on powerful data controllers and not to provide small businesses with an opportunity to bypass the minimum requirements laid down in the GDPR.[31]

27 Article 24(1) GDPR.

28 Jacques Crémer, Yves-Alexandre de Montjoye & Heike Schweitzer, "Competition policy for the digital era," April 2019, p. 77, available at https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.

29 Jacques Crémer, Yves-Alexandre de Montjoye & Heike Schweitzer, "Competition policy for the digital era," April 2019, p. 81-82.

30 Josef Drexl, "Data access and control in the era of connected devices: Study on Behalf of the European Consumer Organisation BEUC," 2018, p. 110, available at https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf.

31 For a detailed discussion, see Inge Graef & Sean van Berlo, "Towards Smarter Regulation in the Areas of Competition, Data Protection and Consumer Law: Why Greater Power Should Come With Greater Responsibility," European Journal of Risk Regulation (forthcoming).

VI. DATA PORTABILITY, COMPETITION ENFORCEMENT AND THE DIGITAL MARKETS ACT

Considering its hybrid nature, data portability is also relevant for competition enforcement. Market power is an inherent part of competition analysis, so that additional requirements can be imposed on powerful firms in several ways under competition law. Restrictions on data portability by dominant firms could be qualified as an exclusionary or exploitative abuse. Or a requirement to facilitate data portability could be imposed as a condition to approve a merger that gives rise to data-related competition concerns, for instance because the merging parties hold overlapping or complementary datasets. It is interesting to note in this regard that the European Commission has pointed at the right to data portability and other requirements in the GDPR as legal limits preventing competition concerns from arising in a number of merger cases.[32]

In its *Microsoft/LinkedIn* merger decision, the Commission argued that the applicability of data protection law limited Microsoft's ability to access and undertake any treatment of LinkedIn full data after the merger.[33] Although the merger was approved about 1.5 years before the GDPR started applying in May 2018, the Commission already pointed at the ability of the GDPR to 'further limit Microsoft's ability to have access and to process its users' personal data in the future' by strengthening the rights of data subjects such as through data portability.[34] As such, the Commission relied on (then still future) GDPR requirements to substantiate its reasoning that the combination of datasets of the two merging parties did not raise competition concerns. Even more remarkably, in its *Google/Sanofi* merger decision the Commission relied on the ability of the GDPR's right to data portability to prevent diabetes patients from becoming locked-in to a digital e-medicine platform to be offered by the future joint venture while the text of the GDPR was not even adopted at the time the merger was approved.[35]

Although the integration of GDPR requirements into merger analysis is a welcome development for the coherent application of different regimes of EU law, it also gives rise to risks when the conclusion that competition concerns are absent assumes compliance with and effective enforcement of existing, and let alone future, data protection rules. As acknowledged by the Commission in its June 2020 Communication evaluating the two years of application of the GDPR, a bottleneck in current data protection enforcement against big tech firms is that they are typically established in Ireland and Luxembourg. Because the GDPR automatically assigns the national data protection authority of the data controller's main establishment as the lead supervisory authority for the entire EU, the Irish and Luxembourg data protection authorities have to act as lead authorities in many important cross-border cases for which they need larger resources than their population would otherwise suggest.[36]

Considering these enforcement problems in data protection law, the Commission could make compliance with the GDPR (or at least those GDPR requirements relevant to the merger analysis) a condition for approving a data-driven merger to prevent that competition concerns occur afterwards because data protection rules like the GDPR's right to data portability are not effectively implemented or enforced. This would give the Commission the ability to intervene itself if necessary after the merger when competition concerns still occur because of a lack of data protection compliance by the merged entity and a lack of enforcement by data protection authorities. Even though the GDPR is now in full force, its ability to prevent competition concerns from arising due to the limits it imposes on merging parties to combine their datasets is still suffering from the enforcement issues.

Beyond competition enforcement, the European Commission is currently preparing a legislative proposal to adopt a Digital Markets Act. The Digital Markets Act will include ex ante regulation for so-called gatekeeping platforms.[37] Data portability could be one of the ex ante obligations imposed on these platforms. While there are still questions about how to design and enforce requirements of data portability under competition law and new ex ante regulation, their asymmetric approach would be welcome in an effort to increase the opportunities for smaller firms and newcomers to compete and make markets more contestable.

---

32 For a detailed discussion, see Inge Graef, Damian Clifford & Peggy Valcke, "Fairness and enforcement: bridging competition, data protection, and consumer law," International Data Privacy Law 2018, p. 215-217.

33 Case M.8124 - Microsoft/LinkedIn, December 6, 2016, par. 254–255 and 375.

34 Case M.8124 - Microsoft/LinkedIn, December 6, 2016, par. 178.

35 Case M.7813 - Sanofi/Google/DMI JV, 23 February 2016, par. 67-69. Note that the final text of the GDPR was adopted on April 27, 2016.

36 Commission Communication, "Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation," COM(2020) 264 final, June 24, 2020, p. 5-6.

37 European Commission, "Inception Impact Assessment of the Digital Services Act Package," Ares(2020)2877686 , July 2, 2020, available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Digital-Services-Act-deepening-the-Internal-Market-and-clarifying-responsibilities-for-digital-services.

In particular, competition enforcement and new ex ante regulation are not bound by the limits set by the GDPR's right to data portability. Data portability is also relevant in business-to-business relations where business users may face difficulties in switching service providers when they cannot take their business data with them.[38] To make data portability effective for dynamic digital markets (such as the Internet of Things),[39] real-time and continuous data portability would be required. This could be implemented through requirements on dominant firms or gatekeeping platforms (either within or beyond the GDPR as discussed in section V. above). Furthermore, the scope of application of the GDPR's right to data portability is limited to personal data 'provided by' the data subject. This notion is interpreted by the Article 29 Working Party as including data knowingly and actively provided by the data subject (such as one's contact details or age) as well as data observed by virtue of the data subject's use of a service or device (such as one's search history). However, inferred or derived data created by the data controller through subsequent analysis of provided or observed data (such as algorithmic results or results of user profiling) are excluded from the scope.[40] Since inferred or derived data carry a lot of value and would be particularly relevant for enabling competition in markets for data analytics, data portability requirements enforced against dominant or gatekeeping platforms through competition law and new ex ante regulation could include such data.

VII. BEYOND DATA PORTABILITY

Despite its potential to empower individuals or business users in their individual relationship with a data controller, a question is whether data portability (irrespective of whether it is enforced under the GDPR, competition law, or new ex ante regulation and irrespective of how expansive its scope is interpreted) is enough to stimulate competition and innovation in data-driven markets. How data portability affects competition and innovation will mainly depend on how actively individuals and businesses overall request transfers of their data. In order for overall competition in data-driven markets to increase, it is not enough that just a few individuals or businesses invoke data portability.

To address risks of market tipping and increasing market concentration in data-driven industries, requirements for market players to share data directly with competitors or new entrants may be needed in certain circumstances.[41] This would mean that the exchange of data is no longer dependent on a portability request of an individual or a business. Data protection and privacy interests of course have to be taken into account when personal data is involved. Illustrative here is that the UK Competition and Markets Authority ("CMA") recommended in its July 2020 market study into online platforms and digital advertising to require Google to open up its click and query data to allow rival search engines to properly compete by improving their algorithms. According to the UK CMA, such an intervention can be designed in a way that does not involve the transfer of personal data to prevent data protection concerns.[42]

Porting of data creates a positive externality through the better service (in terms of better predictions or search results for instance) that all users will receive when an additional user brings her data to a new provider. However, users typically do not take this benefit for other users into account when deciding to port data, so that we should expect too little data portability requests to remedy market tipping.[43] To stimulate data-driven innovation, there is a need to consider additional data access requirements beyond data portability.[44]

---

38 See the self-regulatory codes of conduct that the Commission should facilitate to enable businesses to port data and switch cloud service providers based on Article 6 of Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L 303/59.

39 See also Jan Krämer, Pierre Senellart & Alexandre de Streel, "Making data portability more effective for the digital economy: Economic implications and regulatory challenges," CERRE report June 2020, p. 79-83.

40 Article 29 Working Party, "Guidelines on the right to data portability," 16/EN WP 242 rev.01, 5 April 2017, p. 9-11.

41 Cédric Argenton & Jens Prüfer, "Search Engine Competition with Network Externalities," Journal of Competition Law and Economics 2012, p. 73-105 and Jens Prüfer & Christophe Schottmüller, "Competing with Big Data," Journal of Industrial Economics (forthcoming), available as TILEC Discussion Paper No. 2017-006 at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2918726.

42 UK CMA, "Online platforms and digital advertising Market study final report," July 1, 2020, p. 365-367, available at https://assets.publishing.service.gov.uk/media/5efc57ed3a6f4023d242ed56/Final_report_1_July_2020_.pdf.

43 Inge Graef & Jens Prüfer, "Mandated data sharing is a necessity in specific sectors," Economisch Statistische Berichten 2018, p. 300, available at https://esb.nu/incoming/20042404/mandated-data-sharing-is-a-necessity-in-specific-sectors.

44 For a discussion, see Bertin Martens, Alexandre de Streel, Inge Graef, Thomas Tombal & Néstor Duch-Brown, "Business-to-Business data sharing: An economic and legal analysis," *JRC Digital Economy Working Paper 2020-05* July 2020, available at https://ec.europa.eu/jrc/sites/jrcsh/files/jrc121336.pdf; and Richard Feasey & Alexandre de Streel, "Data Sharing for Digital Markets Contestability: Towards a Governance Framework," CERRE report September 2020, available at https://cerre.eu/publications/data-sharing-digital-markets-competition-governance/.

VIII. CONCLUSION

Data portability has a hybrid nature. What emerged as a data protection concept is now also becoming part of policies aiming to stimulate competition and innovation. To reap the full benefits of data portability, this article has argued that there is a need for regulators to steer its implementation and to provide guidance on how data controllers should handle tensions between different interests and overlapping legal entitlements. Data portability can empower individuals and business users to make better choices but more asymmetric enforcement is needed to ensure that data portability will stimulate competition.

Merger analysis should not assume effective enforcement of GDPR requirements, like the right to data portability, if they are determinative for the question whether a data-driven merger raises competition concerns. Instead, competition authorities should proactively consider the imposition of conditions for approving a data-driven merger to prevent that competition concerns occur afterwards because data protection rules are not complied with. And as a tool to promote data-driven innovation, data portability is a necessary but probably not a sufficient condition to keep markets open to newcomers.

ONLINE SEARCH COMPETITION AND THE RISK OF UNINTENDED CONSEQUENCES OF DATA ACCESS

BY JORDI CASANOVA[1]

1 Jordi Casanova is a Regulatory Economist at the EFTA Surveillance Authority's Competition and State Aid Directorate. The views expressed in this article are those of the author and do not represent the views of the EFTA Surveillance Authority or its members.

Brennan Hawkings, an 11-year-old boy from Utah, was found after being lost for more than four days in rugged terrain at a Boy Scout camp.[2] Brennan's parents later discovered why it had taken so long to find him: he had avoided passers-by, including the search teams looking for him. The boy was afraid that someone would steal him, as he'd been told "not to talk to strangers."

Brennan's case is a textbook example of the so-called Law of Unintended Consequences. Not talking to strangers is a universal lesson taught by well-intentioned parents to protect their children. In the context of Brennan's disappearance, however, it had the unintended effect of leaving him unprotected.

This article discusses how data access regulation of online search aggregators may similarly result in unintended negative effects, risking a not so happy ending for consumers as in Brennan's story.

I. UNDERSTANDING ONLINE SEARCH COMPETITION

The first challenge we face is in understanding the business models of individual platforms and aggregators and their implications for consumer welfare.[3] This is a critical question that is likely to determine whether one supports regulatory intervention at all and, if so, its form. Unfortunately, despite significant research, we are far from a consensus view on the features and impacts on competition and consumers of online search business models.

One view suggests that these markets are characterized by high barriers to entry, due to supply-side economies of scale, switching costs and demand-side network effects.[4] Accordingly, dominant firms' competitive advantage stems from the inherent features of the market in the form of entry barriers, making it all but impossible for other businesses to compete on the merits.

Another view, found in the research on "killer acquisitions" and platform envelopment suggests that dominant online search engines ("OSEs") are engaged in a myriad of acquisitions of potential entrants, which they acquire to avoid entry and competition in their core market(s).[5]

That a market could be characterized by entry barriers and at the same time the existence of many potential entrants, purchased by dominant firms to avoid entry and competition, seem in our view two propositions that are at least difficult to reconcile.

Conversely, some commentators argue that the scope for barriers to act as a deterrent of entry or expansion in online search markets may have been overstated.[6] First, the investments needed in physical assets are significantly lower than those required in industries typically associated with high barriers to entry, such as utilities. In fact, small online search engines such as DuckDuckGo, Ecosia, Yahoo, or even Microsoft's Bing (with market shares below 5 percent worldwide each) have managed to enter and remain viable.

Second, low user switching costs, combined with the same zero-pricing applied by virtually all OSEs, may explain why consumers have the incentives and ultimately switch in great proportions to the OSE that they consider offers the highest quality, providing an alternative explanation for the relatively high levels of concentration observed in these markets.

2 https://edition.cnn.com/2005/US/06/22/missing.scout/.

3 Caffarra C., Eto F., Scott Morton F. & Latham O. (2020), *Designing regulation for digital platforms: Why economists need to work on business models*, Voxeu, 4 June, https://voxeu.org/article/designing-regulation-digital-platforms.

4 See, for example, Zingales L., Rolnik G. & Lancieri F. M. (2019), *Stigler Committee on Digital Platforms*, Final Report, Stigler Center for the Study of the Economy and the State, https://research.chicagobooth.edu/stigler/media/news/committee-on-digital-platforms-final-report; Furman J. (2019), *Unlocking digital competition*, Report of the Digital Competition Expert Panel, 13 March, Furman Report, https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel; Competition and Markets Authority (2020), *Online platforms and digital advertising*, Market study final report, 1 July, https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study#final-report; Crémer J., Montjoye Y.A. & Schweitzer H. (2019), *Competition policy for the digital era*, Special Advisers Report, https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.

5 See, for example, Condorelli D. & Padilla J. (2020), *Harnessing Platform Envelopment in the Digital World*, Journal of Competition Law and Economics, 1-45, https://www.condorelli.science/ENVELOP.pdf; Zingales L., Rajan R.G. & Kamepalli S.K. (2020), *Kill zone*, CEPR Discussion Paper No. DP14709, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3594344.

6 For a review of the literature, see Casanova (2020), *Online Search Engine Competition with First-Mover Advantages, Potential Competition and a Competitive Fringe: Implications for Data Access Regulation and Antitrust*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3647092.

Third, there is an ongoing debate about the role played by network effects resulting from feedback loops in data, which allow to train and improve search algorithms. This is a technical issue on which we are still far from reaching a consensus in the literature.[7] Consider that a small online search engine such as DuckDuckGo (with a 0.5 percent market share worldwide) received as many as 60 million daily queries in 2020.[8] Thus, it would seem that even small OSEs gather very large samples of queries that they can use to train their algorithms.

As digital businesses are built upon large investments in innovation, it would seem reasonable to pay particular attention to the role played by innovation in explaining market outcomes. In online search, as businesses do not differentiate in price, quality and innovation are likely to be important determinants of competitive advantage. Accordingly, dominant positions may not be the result of differences in the *amount of data* that search engines collect, but rather of the difference in the *amount of research and innovation* that they conduct to train their search algorithms with the data collected.

Consider that Google is the worldwide leader in R&D, with more than 27,000 employees dedicated exclusively to this activity. Compare this to DuckDuckGo's total workforce of around 100 employees. Even a large company such as Microsoft had R&D investments in 2019 that were 40 percent lower than those of Google, and potentially focused to a much lesser degree on online search. Yet Microsoft's Bing has been able to attract an increasing number of users, particularly in the US, and to remain viable.

If one accepts that innovation is an important parameter of competition in online search, then the high and increasing levels of innovation by dominant online search firms is another observation that is difficult to reconcile with a finding of a lack of competition due to high barriers to entry. In markets characterized by entry barriers, market forces do not typically constrain dominant players to continuously re-invest in innovating. Yet, well-known dominant OSEs such as Google, Yandex (Russia) or Baidu (China) have done precisely that, as shown in Table 1: R&D expenses ($ millions) by major online search engines (2013-2019) below.

Table 1: R&D expenses ($ millions) by major online search engines (2013-2019)

		2013	2014	2015	2016	2017	2018	2019
Google	R&D expenses	7,137	9,832	12,282	13,948	16,625	21,419	26,018
	% YoY increase	*24%*	*38%*	*25%*	*14%*	*19%*	*29%*	*21%*
	% earnings	*13%*	*15%*	*16%*	*15%*	*15%*	*16%*	*16%*
Yandex	R&D expenses	84	127	193	228	272	325	421
	% YoY increase	*36%*	*52%*	*52%*	*18%*	*19%*	*20%*	*29%*
	% earnings	*15%*	*17%*	*22%*	*21%*	*20%*	*18%*	*17%*
Baidu	R&D expenses	575	977	1,425	1,421	1,810	2,208	2,568
	% YoY increase	*78%*	*70%*	*46%*	*0%*	*27%*	*22%*	*16%*
	% earnings	*13%*	*14%*	*15%*	*14%*	*15%*	*15%*	*17%*

Source: Casanova (2020)[9] from companies' income statements.

There are at least several factors that may explain this behavior by dominant search engines. The first is that entry by fringe competitors is viable in the long term: DuckDuckGo, Bing or Ecosia are examples of small search engines that have entered the market and remained viable over the long term. The evidence from Russia, China, the Czech Republic or South Korea also seem to suggest that entry and viable competition against large players such as Google is possible.

The second factor has to do with the way competition works in sectors characterized by technological innovation and low end-user switching costs. In technology-driven markets, late movers are able to "free-ride" on pioneering firms. First, because "imitation costs" are considerably lower than the "innovation costs" of the first mover. Second, because innovations are subject to "inter-firm diffusion."[10] This can be seen in how smaller OSEs largely compete with incumbents by copying their innovations and investing less than the dominant players, as shown

7 *Idem.*

8 https://duckduckgo.com/traffic.

9 Casanova (2020), *supra* note 6.

10 See Ghenawat P. & Spence A.M. (1985), *Learning curve spillovers and market performance', Quarterly Journal of Economics, 100, pp. 839-852; Lieberman M. (1987), The learning curve, barriers to entry, and competitive survival in the chemical processing industries*, Graduate School of Business, Stanford University, March; Lieberman M.B. and Montgomery D.B. (1988), *First-mover advantages*, Strategic Management Journal 9 (Special Issue: Strategy Content Research): 41–58.

by the example of Microsoft's Bing.

Furthermore, shifts in technology or customer needs may be exploited by new entrants to displace existing incumbents,[11] as Google itself did with Altavista and Yahoo. Due to low costs, user switching can be quick, and because platforms and aggregators have a tendency to tip in short time, growth of new businesses can be exponential, with limited ability for incumbents to react. There are many past examples of incumbents being displaced by new competitors through technology shifts. Think of how IBM lost its dominance in the 90s due to its failure to foresee the relevance of software and the personal computer; how Microsoft misjudged the importance of mobile operating systems, leading to the appearance of new global players in that market; how Microsoft lost its dominance in web browsers to new players such as Firefox and Chrome; or more recently the rapid success of Zoom in video-conferencing services and TikTok in social media.

A third factor has to do with potential competition or, alternatively, the way we define the markets in which we assume these businesses compete. In the case of Google, several factors suggest that there is at least a large business that is already competing with Google to some extent[12] and that could enter its core online search market with relatively low incremental costs: Amazon.[13] Amazon is already an online (product) search engine; it has the computer scientists needed; data center capabilities (it is the worldwide leader in that market); it is the fourth largest company worldwide in digital ad revenues, including with its own ad tech business; and it owns Alexa, its window to website insights only comparable to those obtained by Google from being the most visited website worldwide. Furthermore, China's Amazon equivalent (Alibaba) entered Baidu's core online search market in China in 2014 with Shenma, a hybrid OSE.[14]

These combined features could explain why dominant online search aggregators are constrained to continue to deliver for consumers through ever greater investments in innovation. They also distinguish them from the network industries that we typically regulate, such as telecoms, water or railway. Namely, the viability of entry at lower scale and cost and the scope for technological discontinuities and inter-firm diffusion to displace incumbents through exponential growth in short time, with limited ability for reaction by incumbents. Overall, these factors seem to suggest that we should carefully consider the need for and the potential impact of regulation on the high levels of innovation that we observe in online search markets.

II. REGULATING ONLINE SEARCH AGGREGATORS: THE RISK OF UNINTENDED CONSEQUENCES

It could be argued that online search markets represent the perfect conundrum. They tend to be highly concentrated markets, at least when the market is defined without taking into account potential competition. Yet, they exhibit high levels of innovation,[15] quality and low prices.[16] Arguably, the opposite outcomes that one would expect from a highly concentrated market.

This paradox has driven some economists to recognize the large consumer benefits of digital platforms, yet to presume that a regulatory framework can be engineered that would deliver "even greater benefits for consumers." However, there is an inherent risk in this presumption at a time where we still have relatively little certainty on digital platforms' business models and their impact on consumers. As eloquently put by US Judge Stephen Breyer (now Justice Breyer) in a different context, "antitrust laws very rarely reject […] 'beneficial birds in hand' for the sake of more speculative […] 'birds in the bush.'"[17]

---

11 See, for example, Foster R. N. (1986), *The Attacker's Advantage*, Summit Books, New York; Scherer F. M. (1980), *Industrial Market Structure and Economic Performance*, Rand McNally, Chicago, pp. 431-438; Gomez J., Lanzolla G. & Maicas J. P. (2016), The Role of Industry Dynamics in the Persistence of First Mover Advantages, Long Range Planning, 49(2), pp. 265-281; Varadarajan R., Yadav M.S. & Shankar V. (2013), *First-Mover Advantage in the Internet-Enabled Market Environment*, Handbook of Strategic e-Business Management, pp. 157-185.

12 Business Insider (2020), *Google may cut commission fees for sellers, attempting to compete with Amazon for ecommerce-related search dollars*, July 27, https://www.businessinsider.com/google-beefs-up-ecommerce-to-compete-with-amazon-2020-7?r=US&IR=T.

13 For a more detailed description see Casanova (2020), supra 7.

14 Tait Lawton (2018), *What is Shenma Search? China's Lesser-Known Mobile Chinese Search Engine*, Nanjing Marketing Group, https://www.nanjingmarketinggroup.com/blog/what-is-shenma-search#:~:text=Shenma%20comes%20with%20UC%20Browser,to%20search%20via%20the%20PC accessed June 30, 2020.

15 A recent study by the Boston Consulting Group of the 50 most innovative companies worldwide ranked Apple first, Google second, Amazon third, Microsoft fourth and Facebook tenth, see Boston Consulting Group (2020), *The Most Innovative Companies 2020 – The Serial Innovation Imperative*, June, https://image-src.bcg.com/Images/BCG-Most-Innovative-Companies-2020-Jun-2020-R-4_tcm9-251007.pdf accessed July 28, 2020.

16 For a discussion of the levels of innovation, quality and prices in online search markets, see Casanova (2020), *supra* note 6.

17 *Barry Wright Corp. v. ITT Grinnell Corp.*, 724 F.2d 227, 1984, para 24, https://law.resource.org/pub/us/case/reporter/F2/724/724.F2d.227.83-1292.html.

One potential risk is that we elevate the achievement of lower market concentration to such a pivotal objective of regulatory policy that it should be attained at any cost, discounting the potential for unintended consequences for innovation, competition and ultimately consumers. As the example of Brennan shows, there are rarely universally valid rules. Thus, we shouldn't assume that the achievement of lower market concentration will always deliver net benefits for consumers independently of the costs, particularly if such objective is attained by law rather than market forces. Instead, it would seem preferable to assess policy proposals on a case-by-case basis and to act with restraint, recognizing that our relative ignorance is likely to be prone to unintended consequences.

In this sense, we focus on two areas in which regulatory intervention in online search should carefully balance potential trade-offs: (i) trade-offs between competition *for* data and competition *with* data and (ii) trade-offs between data access and competition *with* data.

A. Trade-Offs Between Competition for Data and Competition with Data

Dominant OSEs compete *for* data by offering multiple services to consumers for free. Google invested in Android to compete with Apple, provided a free Gmail service to compete with Microsoft's Outlook and Hotmail, a free web browser Chrome to compete with Microsoft's Internet Explorer and Apple's Safari, a free Sheets and Docs service to compete with Microsoft's Office, a Google Shopping e-commerce aggregator and drone delivery service[18] to compete with Amazon, and more recently is aiming to acquire Fitbit to compete with Apple's wearables.

Additionally, dominant OSEs compete *with* data by offering mainly online search services and digital ads. The most likely outcome of an obligation of access to a dominant online search engine's data, if successful, is that it would increase competition in prices from alternative OSEs in search advertising. This could have a significant impact on these businesses: consider that out of all the services it provides, Google derives around 70 percent of its earnings from online advertising through Google Search.[19] Thus, mandatory access to data is likely to impact the regulated OSE's incentives to compete for data by offering free services to consumers, because any competing OSE could now request access to the user data obtained from those services, and use it to undercut its prices in online advertising.

Faced with decreasing online advertising revenues in search, dominant online search businesses are most likely to either reduce their investments in free-of-charge services or to rebalance their tariffs through higher prices for the other services they provide. That would be similar to what Google proposed to do following the European Commission's *Android* remedies: charge a $40 fee for licensing Android in the EEA, combined with an auction process amongst online search engines.[20]

Access to dominant OSE's data will also alter the incentives of other platforms and startups to provide valuable end user services in exchange for user data only. Why would other platforms and startups risk their capital in competing on the merits for data by providing valuable end user services, if they will have access to the best dataset out there, that of dominant OSEs?

Consider that Microsoft developed its own Windows Mobile/Phone and lost ignominiously the battle for a successful mobile operating system, with its CEO laughing at iPhone's launch because it did not have a keyboard.[21] Only in 2015, Microsoft had to write-off more than $7bn invested in Nokia before completely exiting the market.[22] Through mandatory data access, Microsoft's Bing could be able to require access to user location data obtained by Google through Android and use this to undercut Google in search advertising – the market in which it recovers the vast majority of the costs of investing in Android. It is hard to see how that could qualify as "competition on the merits." Furthermore, it could distort the incentives of other firms to compete for the data that Google gathers through Android – remember that not only Microsoft but also Amazon, another business active in digital advertising, could give another shot in the future to the smartphone market after the failure of its Fire phone.

---

18 Luke Dormehl (2020), *When it comes to delivery drones, Google's Wing is miles above the competition*, Digital Trends, January 27, https://www.digitaltrends.com/cool-tech/google-wing-drone-deliveries/ accessed June 30, 2020; Isabella Lee (2019), *Google Overtakes Amazon in Race to Make Consumer Drone Deliveries a Reality*, UAV Coach, April 10, https://uavcoach.com/google-wing-drone-delivery/ accessed June 30, 2020 and Urban Air Mobility (2020), *Google's Wing drone deliveries soar during pandemic with 500% volume increase*, May 26, https://www.urbanairmobilitynews.com/express-delivery/googles-wing-drone-deliveries-soar-during-pandemic-with-500-volume-increase/ accessed June 20, 2020.

19 CMA (2020), *supra* note 4, Appendix D, page D11.

20 Simonetta Vezzoso (2018), *Android Remedies: Tearing Down the Wall?*, CPI International, November 19, 2018 https://www.competitionpolicyinternational.com/android-remedies-tearing-down-the-wall/#_edn12 accessed July 28, 2020.

21 https://9to5mac.com/2016/11/04/microsoft-versus-apple-smartphones/.

22 Tom Warren (2015), *Microsoft writes off $7.6bn from Nokia deal, announces 7,800 job cuts*, The Verge, July 8, https://www.theverge.com/2015/7/8/8910999/microsoft-job-cuts-2015-nokia-write-off accessed July 20, 2020.

The concerns above would be greatly accentuated if access to a dominant OSE's data was imposed at a zero price, because the dominant OSE did not acquire that data at zero cost. To balance this, regulators could set a "reasonable price" for access to data, as they do for access to utilities' networks. The challenge is that economists have the right tools to set the prices for access to the physical infrastructure of mature businesses such as network industries, but we are not well equipped to assess the reasonable return on services of highly innovative companies, such as Google.[23] Let alone of new services that these companies may offer in the future to compete for data. Therefore, the answer to whether we should or should not mandate access to data should depend on whether regulators can set an appropriate price for it, one that does not undermine incentives to offer free-of-charge services to collect it.

Overall, given the trade-off described, it would seem that an important question facing regulators wishing to impose an access to data remedy is whether consumers will be better-off by trading more competition with data in online search and advertising, relatively immature markets that are experiencing increasing levels of innovation and decreasing prices, for potentially less competition for data.

B. Trade-Offs Between Data Access and Competition with Data

There will also be important trade-offs in terms of the data that is allowed to be accessed and the extent by which alternative OSEs will be able to effectively compete with it. Greater anonymization of user data will be more respectful of privacy. However, there will be a trade-off between privacy and the value for alternative OSEs of the data shared. This is because anonymized user data is of relatively little value to perform search engine analytics and to personalize advertising.

Conversely, it is likely that an effective remedy will require sharing as much personal information as possible. As noted by the CMA, search query data alone is unlikely to be particularly valuable for alternative OSEs, unless it is shared combined with other information such as the click-through behavior of the user.[24] However, the greater the amount of data shared, the easier it will become for competitors to understand the workings of the dominant OSE's search algorithm. In turn, the easier it will be for alternative OSEs to reverse-engineer it.

In sectors characterized by a high degree of innovation that is subject to inter-firm diffusion, such as pharmaceutical companies or technology equipment vendors, we typically guarantee these companies' exclusivity to their innovations through a patent protection system, in order to maintain their incentives to continue innovating. Instead, the proposal to mandate access to data could result in the opposite extreme, by further facilitating inter-firm diffusion in a sector that is similarly characterized by high levels of innovation and inter-firm diffusion.

Just like with patented drugs, the risk is that cash-restricted alternative OSEs will spend their resources in cheaper reverse-engineering of the dominant OSE's algorithm, rather than in considerably more costly and risky innovation. This could in turn distort the incentives for dominant OSEs to dedicate resources to improving their online search service. Ultimately, we could end up with a system that resulted in a "level-playing-field-to-the-bottom" which reduced both, competition for data and the incentives of dominant OSEs to compete in improving their OSEs with that data.

Thus, even if regulation resulted in the desired lower market concentration over time, it could come at the cost of lower innovation and quality. Particularly, if this greater competition was not on the merits but rather triggered by regulation that artificially facilitated inter-firm diffusion, diminished the incentives of successful dominant firms to invest, and resulted in "imitators" competing away "innovators" in the market.

23 See Jordi Casanova (2020), *Estimating Reasonable Prices for Access To Digital Platform's Data: What Are the Challenges?*, European Competition and Regulatory Law Review, Volume 4, Issue 3, https://core.lexxion.eu/article/CORE/2020/3/4.

24 This is recognized by the CMA (2020), Appendix V, paragraph 96, *supra* note 4, where the CMA states that "other stakeholders suggested that without associated insights into users' behaviours on the search engines, such as which websites they choose to visit after making such a query, the provision of access to user queries may limit the ability of search engines to train their algorithm and improve the relevance of their search results."

III. CONCLUSION

The important and complex trade-offs involved in regulating access to data require careful consideration to avoid unintended consequences. As OSE markets are characterized by relatively low switching costs and competitive advantages that are contestable by both a competitive fringe and potential competitors, our focus should not be on undermining a dominant players' earned market position through access regulation, but rather on ensuring that competition is on the merits and not maintained through anti-competitive foreclosure. Compared to access regulation, which involves significant trade-offs, focusing on prohibiting exclusionary practices is unlikely to risk undermining competition and investment incentives. There may be a need for an ex ante regulator that monitors dominant OSEs' behavior to avoid exclusionary practices and to ensure that intervention is timely.

These proposals would be in line with the objectives of competition authorities of ensuring that online search markets remain fair and contestable. As mentioned by Professor Philip Marsden, "competition authorities do not try to take the crown from a victor in any competition on the merits – but try to stamp out illegal behavior so that legitimate competition and innovation can thrive."[25]

25 Ahron Peskin (2020), *Tech & Competition – A Conversation with Professor Philip Marsden*, LinkedIn, 8 June, https://www.linkedin.com/pulse/tech-competition-conversation-professor-philip-marsden-ahron-peskin/ accessed June 30, 2020.

THE IMPACT OF DATA PORTABILITY ON PLATFORM COMPETITION

BY EMANUELE GIOVANNETTI & PAOLO SICILIANI[1]

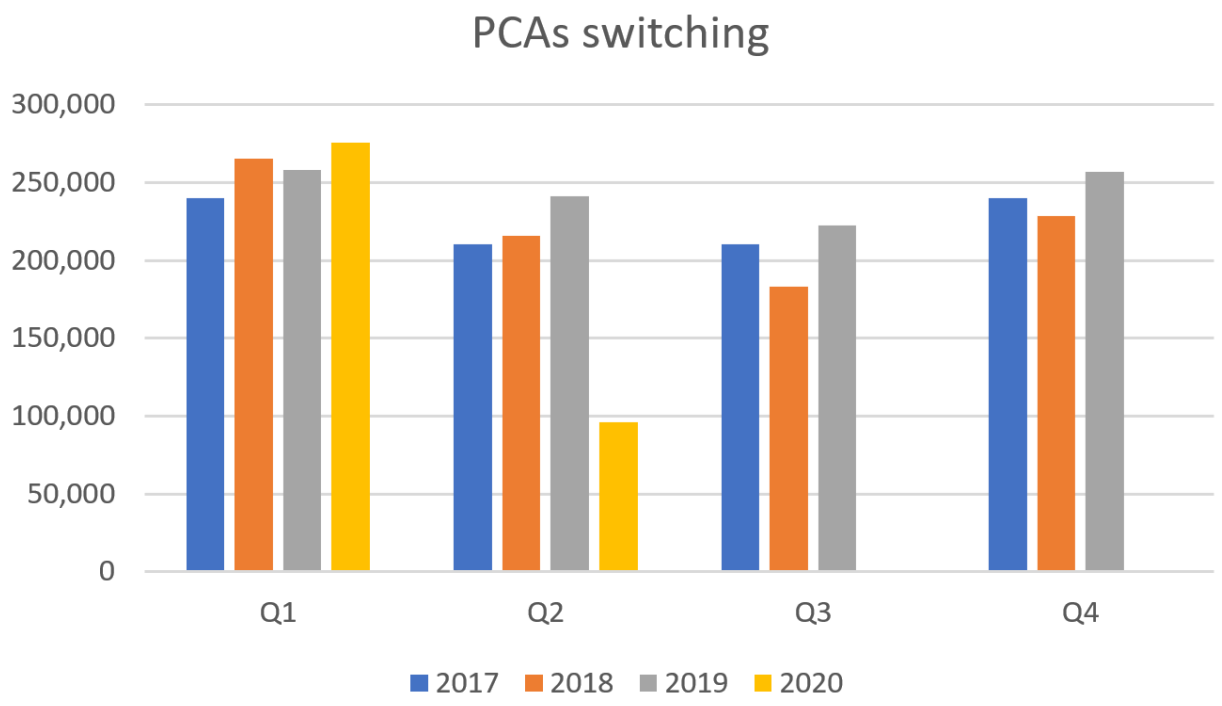
1 Emanuele Giovannetti, Anglia Ruskin University & Hughes Hall, University of Cambridge; and Paolo Siciliani, Bank of England. The views expressed in this paper are those of the authors, and not necessarily those of the Bank of England or its committees.

I. FROM NUMBER PORTABILITY TO DATA/IDENTITY PORTABILITY

The remedy of imposing data portability to promote competition against a dominant incumbent by reducing switching costs was first introduced by telecoms regulators. Specifically, under number portability consumers can change their fixed or mobile operator while keeping their old phone number. By losing a personal number a consumer would have to spend time to alert all of her contacts, as well as a number of essential service providers (e.g. banking, insurance and utilities), about the changed contact details. There is no doubt that number portability was an effective tool in increasing switching activity, especially in mobile markets.[2]

In contrast, the imposition of data portability failed to ignite switching activity when applied to other commoditized service markets, most notably in banking. In the UK, the process of switching personal current account has been entirely automated since 2014 under the industry-run Current Account Switching Service, which allows consumers to transfer seamlessly all of their recurring transaction arrangements, both outgoing (e.g. utility bills and mortgage repayments) and incoming (e.g. monthly salary), within seven days. Nevertheless, the level of switching activity has remained anemic at below 5 percent.[3] In contrast, in the absence of data portability, switching activity has materially increased over the last decade in other commoditized service markets, such as general insurance (e.g. car and home insurance) and retail energy (gas and electricity). Arguably, one of the key difference is the "evergreen nature" of personal current accounts (i.e. with the lack of regular triggers for shopping around), whereas consumers have to periodically renew their insurance policies and energy provider (i.e. once the fixed-rate promotional period expires).

While data portability is typically aimed at reducing switching costs, recently it has also been mandated to facilitate the comparison of complex tariffs based on a specific usage profile, thus lowering search costs. Specifically, Open Banking was launched in the UK in 2018, a remedy imposed by the Competition and Markets Authority to facilitate tariff comparability and thus reverse the persistent low level of switching activity in the market for personal current accounts. Under this data portability remedy, the largest incumbent banks are required to adopt standardized application programming interfaces ("APIs") to allow seamless access to user data (with consent) by third-party apps. The figure below shows that although there was a slight uptick in the level of switching activity up to the first quarter of 2020,[4] it is still too early to tell whether Open Banking will ultimately have a lasting impact.



Source: Current Account Switching Service

2 S. Buehler, R. Dewenter & J. Haucap (2006), "Mobile number portability in Europe," Telecommunications Policy, 30, 385-399.

3 See CMA, Retail Banking Market Investigation – Final Report, August 2016, Chapter 6, available at https://assets.publishing.service.gov.uk/mwg-internal/de5fs23hu73ds/progress?id=UAGn5g0D6ECgy5mzUrSc08vdMQP8TAdsPM2_tdakhL0,&dl.

4 The drastic fall in Q2-2020 is most certainly due to lockdown restrictions.

The holistic approach to data portability showcased with Open Banking is seen as a template for the kind of ground-breaking regulatory intervention called for to rain back the super-dominance of a few essential digital platforms run by Big Tech.[5] These cases differ from the ones highlighted above in that the incumbency advantage is often further strengthened by the presence of network effects,[6] both within the same category of users (i.e. direct network effects – e.g. connecting with social peers) and across separate ones (i.e. indirect network effects under multi-sided platform competition – e.g. e-marketplace). Similarly to switching costs, network effects give rise to a first-mover advantage due to the belief that the challenger platform might fail to reach a viable scale.

In these cases, data portability is not only aimed at lowering switching costs, but also at allowing the challenger platform to match the quality of the incumbent's match-making service: that is, the ported data is used to improve the precision of its matching/predictive algorithms. In this sense, switching costs and network effects feed off each other to buttress the incumbency advantage.[7] This can be especially the case where the same platform provides a bundle of personalized services that hinges on the creation of a shared, detailed and multifaceted digital profile of users' identities and individual preferences.

In this respect, drawing the boundaries of data portability can be very contentious, to the extent that attributes of a digital identity are not only the reflection of data inputs provided by the user, but also the results of added inferences obtained from proprietary algorithms. For example, location services, browsing histories, site reviews, dedicated advertising, driving directions, all different tailored services based on algorithmic profiling relying on personal data gathered through tracking methods.[8] Therefore, changing platform could entail a deterioration of the relevance in these personalized services. Arguably, this new type of "lock-in effect" increases the longer the customer relationship with the platform in question has been in place.

II. THE IMPORTANCE OF DIFFERING LEVELS OF SWITCHING COSTS

This multi-contact feature of dominant platforms can be a source of heterogeneity in switching costs, to the extent that users differ in the range of services that they rely on, and the challenger platform only competes on a subset of those.[9] This is the typical disruptive innovation scenario whereby the new entrant does not initially develop a fully-fledged offer, but instead focuses on a narrow scope with the strategy to broaden it as the customer base grows. Different degrees of "lock-in effects" can also be the result of demographic and behavioral factors. For example, young cohorts may be less invested into the incumbent platform and therefore face lower switching costs. The presence of inertia due to a default or status quo bias, may be particularly relevant in the context of switching to a new platform, given the risk of failed "take-off."

Different levels of switching costs across a group of users in not only relevant for the consumer/end-user side of multi-sided platforms, but often also at work on other sides. For example, in e-marketplaces and payment systems, SMEs on the, respectively, seller and merchant sides can be affected by the same type of behavioral biases outlined above. More subtly, end-users can become sellers themselves, as with the provision of media content over social networks (e.g. online social gaming platforms).

Therefore, in the presence of heterogeneous levels of switching costs, the impact of mandating data portability at the expense of the incumbent platform can be conceptualized as compressing the range of switching costs, thus in principle benefiting high-switching cost users the most, as it should be the case. We have developed a model to assess the incumbency advantage among two-sided platforms whereby agents

5 Coyle, D. (2018), "Practical competition policy implications of digital platforms," Antitrust Law Journal, 82, 835-860. Gans, J. (2018), "Enhancing Competition with Data and Identity Portability," The Hamilton Project, Brookings, available at https://www.brookings.edu/wp-content/uploads/2018/06/ES_THP_20180611_Gans.pdf. Scott Morton, F., P. Bouvier, A. Ezrachi, B. Jullien, R. Katz, G. Kimmelman, A.D. Melamed and J. Morgenstern (2019), Committee for the Study of Digital Platforms - Market Structure and Antitrust Subcommittee, Report, George J. Stigler Center for the Study of the Economy and the State, available at https://www.judiciary.senate.gov/imo/media/doc/market-structure-report%20-15-may-2019.pdf.

6 Competition in telecoms markets was not affected by the presence of network effects thanks to the imposition of interoperability among firms' networks.

7 Nevertheless, Franck and Peitz (2019) pointed out that switching costs may stems from the requirement, under data protection rules, to obtain consent from "friends" to transfer (i.e. under data portability) the related data from one platform to another. Franck, J.-U. and M. Peitz (2019), *Market Definition and Market Power in the Platform Economy*, Report, Centre on Regulation in Europe, available at https://www.cerre.eu/sites/cerre/files/2019_cerre_market_definition_market_power_platform_economy.pdf.

8 In addition, trackers are not only ubiquitous, but also largely run by a few Big Tech firms (OECD, 2020). OECD (2020), "Consumer Data Rights and Competition - Background note," available at https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf.

9 The use of bundling discounts, such as under a monthly subscription fee that gives preferential access to a range of services (e.g. Amazon Prime), could further strengthen this effect.

have heterogeneous switching costs that, critically, also differ in range and average across the two platform's sides.[10] Given the duopolistic setting, where an incumbent platform is facing a new entrant, the assumption that agents on different sides have heterogeneous switching costs can also encompass the impact of different propensities to shop around in the first place (i.e. search costs).

The presence of switching costs that favor the incumbent platform can also be thought of as a source of vertical differentiation - in the sense that, all else equal, users would prefer to stay with the incumbent and not incur the disutility due to switching costs – and users differ in their preference for quality. This interpretation is especially appealing where the source of switching costs interacts with the ability of the platform to precisely match agents on the opposite side. Our specification is also isomorphic to a scenario where users have different degrees of brand loyalty, but solely for the incumbent. However, while the presence of unilateral horizontal and vertical differentiation improves consumer welfare, switching costs are socially wasteful. An alternative interpretation is that users face a switching cost when leaving the incumbent, but not when leaving the entrant (i.e. to return to the incumbent). This is especially plausible when switching costs and cross-group network platforms are intertwined (i.e. the incumbent retains the edge in terms of matching quality). In addition, this interpretation fits the static framework adopted in our model, in that, without benefiting from its own "lock-in effects," the entrant would lack the incentive to adopt the "bargain-then-rip-off" dynamic pricing strategy typically associated with the presence of switching costs.

We study the impact of a reduction in switching costs, thanks to the imposition of data portability, under two adoption regimes: *i)* single-homing, whereby agents are restricted to full-switching, in that they must leave the incumbent platform in order to join the entrant platform; and *ii)* multihoming, whereby agents have the option to partially switch to the entrant platform, while keeping their membership with the incumbent platform.

As a general remark, the extent to which switching costs differ across users operates as a separating/partitioning device, whereby the new entrant targets those agents on both sides with relatively lower switching costs, and can do so by charging higher prices as the distance from the high-cost customers targeted by the incumbent platform (on the same side) grows. This is especially the case on the side with comparatively higher switching costs. Therefore, regulatory intervention aimed especially at helping high switching cost users might unintendedly undermine the entrant's prospect to gain a sustainable foothold in the market. This is because the incumbent naturally responds to the reduction in switching costs by setting lower prices, thus squeezing out the entrant. Indeed, under single homing, the incumbent's market shares on either side grow in response to falls in switching costs on either side.

More fundamentally, though, this source of demand-side frictions and preference heterogeneity is needed to avert the kind of tipping, "winner-takes-all" outcomes that would doom the prospect of sustainable entry to start with. That is to say, the range in switching costs has to be sufficiently larger in comparison to the importance of network effects for the coexistence between the two rival platforms to be not only feasible,[11] but also viable from the entrant's perspective.

There can be subtler effects. A reduction in switching cost on one side is detrimental to high switching cost users on the opposite side, when they care more about cross-group (indirect) network effects. This can be the case, for example, with a regulatory intervention aimed at protecting high switching cost end-users of an e-marketplace platform (i.e. switching costs tend to be higher on the consumer side), while sellers on the opposite side are comparatively more concerned about the number of buyers shopping online. Under these circumstances, the incumbent platform can capitalize on the resulting increase in the market share on the buyers side (i.e. as the incumbent becomes more aggressive) by charging sellers more (i.e. to extract the improved network benefits).

All in all, both the new entrant's profit and the network size fall in response to a reduction in switching costs. From a consumer surplus perspective, there is an inverted-U relationship between the aggregate surplus of users and the level of same-side switching costs. This entails that intervention aimed at lowering switching costs would certainly be positive in terms of consumer surplus for very high levels of switching costs, although the entrant's market shares on both sides would fall, but not materially. However, at medium level of switching costs, further reductions in the entrant's market shares in response to a reduction in switching costs would also be detrimental in terms of consumer surplus, that is, to the extent that the incumbent is able to retain a larger proportion of customers paying comparatively higher prices. However, from a distributional perspective, users with high switching costs (i.e. those retained by the incumbent) always benefit from a reduction in switching costs.

10 Siciliani, P. & E. Giovannetti (2019), "Platform competition and incumbency advantage under heterogeneous switching cost — exploring the impact of data portability," Bank of England's Staff Working Paper No. 839, available at https://www.bankofengland.co.uk/working-paper/2019/platform-competition-and-incumbency-advantage-under-heterogeneous-switching-cost. An updated version, which includes a section on welfare assessment, is available on request.

11 It is worth pointing out that the preponderance (with respect to the importance of network effects) of some type of demand-side friction and preference heterogeneity is generally a fundamental assumption in models studying platform competition. The most common choice is to assume that users have differing brand preferences that vary between the two rival platforms (i.e. as under the Hotelling framework).

Arguably, besides the aim of lowering switching costs, the imposition of data portability could be instrumental in making switching a practical option to start with. This would also apply to the option of multihoming (i.e. partial switching). Under multihoming, we find that the incumbent has an incentive to sponsor multihoming on one side only (i.e. by setting a low fee), in order to maintain full coverage on that side, with high switching cost users not switching at all (i.e. partial multihoming). This, in turn, forces the entrant to charge no fee at all on that side. In contrast, on the opposite side the incumbent can set a high price thanks to the fact that users enjoy full cross-group network benefits. The new entrant follows suit (i.e. prices as strategic complements), with the result that no user opts for multihoming, not even those with low switching costs. As a result, both platforms set higher prices on the side with only singlehomers than they would absent multihoming. This outcome is in stark contrast with the classic result under the "competition bottleneck" model where users on the singlehoming side benefit from intense pricing rivalry among platforms; whereas, platform set high membership fees for users on the multihoming side to access singlehoming members.

In addition, we show that the incumbent platform pursues the strategy of sponsoring multihoming on the side with higher switching costs, which entails that prices tend to be higher on the opposite side with lower switching cost. This finding is also in stark contrast with the outcome under the "competition bottleneck" model, where multihoming users (i.e. typically sellers on a marketplace platform) face monopolistic charges to gain access to singlehoming users on the opposite side (i.e. typically buyers facing higher demand-side frictions).

Higher prices on the singlehoming side translates into higher profits for the incumbent than absent multihoming. Therefore, the incumbent should not resist multihoming, even if it is the result of regulatory intervention. By the same token, the incumbent is more accommodative towards the new entrant, in the sense that the degree of preponderance of switching costs (i.e. in comparison to the intensity of cross-group network benefits) required for the sustainable coexistence of the two rival platforms is lower than absent multihoming. Whereas, from a welfare perspective, users, especially those on the singlehoming side, tend to be worse-off than absent multihoming. Therefore, from a policy perspective, facilitating multihoming by imposing data portability can give rise to another trade-off between the prospect of entry and the surplus of user.

III. CONCLUSION

The incumbency advantage of a dominant platform is, arguably, the most prominent competition issue in the area of competition policy nowadays. A new platform trying to enter a market dominated by an incumbent platform may in fact fail to overcome the competitive disadvantage due to the combined impact of network effects and switching costs. This is particularly so where the matching service is commoditized and demand is largely saturated (i.e. lack of a large enough flow of unaffiliated users).

Hence, the imposition of data portability in order to facilitate switching is advocated as a general template for regulatory intervention to address the dominance of digital platforms run by Big Tech. However, the case for entry depends on the range of heterogeneous switching costs. In particular, the preponderance of this demand-side friction over the intensity of cross-group network benefits is a requirement to avert tipping equilibria whereby the incumbency advantage is buttressed by the presence of favorable beliefs regarding the expected network size.

Therefore, intervention aimed at lowering search and switching costs, especially for those consumers facing comparatively higher costs due to, for example, inertia, might unintendedly make entry more difficult as the incumbent's strategic stance becomes less accommodative. Perhaps counterintuitively, this suggests that this type of intervention should take place only after the entrant has managed to gain a foothold in the market, so that, once switching costs have been reduced below the threshold where tipping tendencies resume, the entrant platform is less likely to be disadvantaged by unfavorable beliefs. Again counterintuitively, we find that the incumbent should welcome multihoming, whereas users tend to be worse-off. These findings raise a conundrum from a regulatory perspective, given that the imposition of data portability is typically motivated by the desire to facilitate multihoming and reduce switching costs, thus giving rise to contrasting effects with respect to the prospects for sustainable entry.

DATA PORTABILITY RIGHTS: LIMITS, OPPORTUNITIES, AND THE NEED FOR GOING BEYOND THE PORTABILITY OF PERSONAL DATA

BY DANIEL GILL & WOLFGANG KERBER[1]

1 Daniel Gill, Teaching and Research Assistant (daniel.gill@wiwi.uni-marburg.de); Wolfgang Kerber, Professor of Economics (kerber@wiwi.uni-marburg.de); Marburg Centre for Institutional Economics (MACIE), School of Business & Economics, University of Marburg (Germany). The authors declare no conflict of interests.

I. INTRODUCTION

In recent policy discussions data portability rights are often seen as a very promising instrument for solving problems for competition and innovation that are caused by a lack of access to data. Since the EU data protection law already introduced a data portability right (Art. 20 GDPR) in 2018, the European discussion focusses primarily on this data portability instrument for fostering competition and innovation. However, this right has not fulfilled these expectations so far, which has led to the current policy discussion in the EU on how this right can be made more effective.[2] But data portability rights can also be introduced outside of privacy laws, as, e.g. in the recent approach of consumer data rights, which intends to give consumers more control over their consumer data by granting them, inter alia, a portability right. Australia is implementing such consumer data rights in a sector-specific way,[3] which resembles to some extent sector-specific data access regulations in the EU as, e.g. the access to bank accounts for innovative financial services (PSD2: "Second Payment Service Directive").

This article claims that data portability rights can contribute to the solution of data access problems for competition and innovation but only to a limited extent and under certain conditions. Some of them are already discussed in the policy debate about enhancing the data portability right of Art. 20 GDPR (standardized technical interfaces, continuous data portability). We would like to focus the attention to the need for a careful and deep analysis of the underlying data access problems for competition and innovation as a precondition for deriving conclusions about the appropriate design of data portability rights, and the need for additional complementary regulations for making data portability rights effective enough for achieving these objectives. Therefore section 2 will present some results of our research about the problems of access to data in connected cars for competition and innovation (on secondary markets), and why the data portability right of Art. 20 GDPR is not a suitable instrument for solving these problems. Based upon this case study, section 3 discusses some basic questions about the design, limits, and preconditions of effective data portability rights. After analyzing the limits of a privacy law-based data portability (as Art. 20 GDPR in the EU) for helping to solve data access problems for fostering competition and innovation, we argue that the alternative approach of consumer data rights allows for a more flexible design of data portability rights (e.g. by entailing also non-personal data) that can lead to more targeted and effective solutions for competition, innovation, and consumer empowerment. Therefore, the policy discussion should also focus on data portability rights outside of privacy laws (and beyond personal data) as part of consumer policy, competition policy, and the governance structure of the data economy.

II. CAN DATA PORTABILITY RIGHTS SOLVE ACCESS PROBLEMS TO IN-VEHICLE DATA IN CONNECTED CARS?

The technological transition to connected cars has led to a new regulatory discussion in Europe about access to the large sets of data collected and produced in these cars. Since the car manufacturers have designed their cars as closed systems and transmit all data directly to proprietary servers ("extended vehicle"), they have exclusive de facto control over all data and the technical access to the car. This gatekeeper position allows them to control the access to all secondary markets for services, which require either access to these "in-vehicle data" and/or technical access to the connected car (as, e.g. remote maintenance and repair services). Important is that most of these in-vehicle data are unique, not replicable or substitutable. Concerns of independent providers of aftermarket and other complementary services that this gatekeeper position allows the car manufacturers to foreclose them and leverage market power to these secondary markets is justified from a competition economics perspective, and can lead to negative effects on competition, innovation and consumer choice on these markets.[4] This problem is also not solved by the current EU type approval regulation for motor vehicles, because this well-established mandatory access regime to essential repair and maintenance information for independent service providers is so far not sufficiently updated to the new technology of connected cars, and therefore does not encompass the access to these car data and the remote access to the car for protecting competition on these markets under the new technology.[5]

2 See Communication: A European Strategy for Data. COM(2020) 66 final, 21, and, e.g. Krämer, J., Senellart, P., de Streel, A., Making Data Portability More Effective for the Digital Economy. CERRE, June 2020.

3 See OECD, Consumer Data Rights and Competition – Background Note. DAF/COMP(2020)1, 11-14.

4 See for a market failure analysis from an economic perspective Kerber, W., Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data. 9 JIPITEC 2018, 316-325; see for the general problem of foreclosing service providers on secondary markets in IoT ecosystems through gatekeeper positions of manufacturers J. Crémer, Y.A. de Montjoye, H. Schweitzer, Competition Policy for the Digital Era, 2019, 87-90.

5 See Regulation (EU) 2018/858 (motor vehicle type approval),[2018] OJ L 151/1; Kerber, W. and D. Gill, Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation, 10(2) JIPITEC 2019, 251-256.

Since several years an intense policy debate exists between the car manufacturers defending their approach (with safety and security reasons) and a broad coalition of service providers who demand a regulatory solution.[6] Different options for solving the problem exist: (1) The server with all car data is put directly under the governance of a neutral (data trustee-like) institution (which can grant non-discriminatory access), and (2) the introduction of interoperable telematics platforms, which would allow the storage of the data in the car, and gives the car users direct control over their data and the access to the connected car. Both solutions would eliminate the gatekeeper position of the car manufacturers with respect to the car data and have been assessed as superior compared to the current extended vehicle concept due to its advantages for competition.[7] Other policy options are either (3) mandatory access solutions to essential data in competition law (e.g. Art. 102 TFEU), or (4) a broad extension of the existing mandatory data access regime of the motor vehicle type approval regulation to all data that are necessary for offering services on secondary markets of the connected car (including necessary interoperability requirements).[8] The EU Commission has acknowledged the existence of this competition problem, and announced in its European data strategy a further reform of the type approval regulation.[9]

Since also Art. 20 GDPR is seen as a possible way how consumers can make data of a smart device available to other service providers, (5) this data portability right can also be seen as a possible solution for the data access problems with connected cars. According to Art. 20 GDPR the data subjects (i.e. the car users) have the right to have their personal data directly transmitted from the data-holding car manufacturers to other service providers. In the following, we will show why this data portability right does not offer a sufficiently effective mechanism for solving the above-described problems for competition and innovation.

1) Legal problems: The general critique of the EU data portability right that the scope of the portable data is not clearly defined is also a problem in the case of connected cars. Although most data produced in the connected car are seen as personal data, it is debated which in-vehicle data are personal data and which are not. Since the data portability right only refers to personal data that are "provided" by the data subjects, it is not clear what this means in connected cars that produce the in-vehicle data, mostly through sensors. It is particularly unclear whether this right also entails data that are observed by the connected car. Including also observed data was suggested by the European Data Protection Board, but this is disputed and unclear from a legal perspective.[10] This legal uncertainty about the scope of the portable data and about other legal aspects (as, e.g. liability issues, rights of others, business secrets) is a huge problem for the effectiveness of this data portability solution. In any case, the scope of portable data can be expected to be too narrow for solving the problems for competition and innovation. Another important issue in the connected car example is that the data portability right does not entail a continuous transmission of data in real-time to other service providers, as it would be necessary for many of these services on the secondary markets.

2) Technical problems: Another important limitation is the provision that the data portability right is only applicable if technically feasible. But data controllers have no obligation to implement measures for ensuring technical feasibility, as, e.g. using APIs and developing industry-standards for data formats and interfaces for enabling data interoperability. This is very different in the PSD2 regulation, where banks have an obligation to develop APIs and standardized interfaces for allowing independent service providers to access bank account data. But the technical problems go beyond data interoperability. The provision of many services by independent firms to the users of connected cars would also require a direct technical access to the car. Since the cars are designed as closed systems, the car manufacturers can block the interoperability with other services, and thus can control the markets for all services that need to interoperate with the car. This problem that emerges with many smart devices and IoT applications cannot be solved by a data portability right. Although safety and security problems that can emerge with data portability and interoperability of services have to be solved, the car manufacturers have no obligation to implement a safety and security system which would allow the safe transmission of data and interoperability of services. Also, this is different in the PSD2 regulation about open banking, which entail also strict mandatory rules for safety and security.

3) Economic problems: A huge hurdle for the effectiveness of any data portability rights can be the transaction costs of using these rights. This refers to the consumers, who have to exert these rights, to the service providers to whom data are made available, but also to the data holders that have to port these data without being allowed to demand fees. Most important is whether the consumers are aware of their data portability right and have sufficient incentives for exerting it. Due to the above-described manifold problems, it cannot be expected that consum-

6 See for this debate and the following policy options C-ITS Platform, Final Report 2016, 72-90, TRL, Access to In-Vehicle Data and Resources – Final Report 2017, 32-49, Kerber, *supra* note 4, 312-315.

7 See TRL, *supra* note 6, 160; Kerber, *supra* note 4, 325.

8 See Kerber/Gill, *supra* note 5, 255.

9 See Communication: A European strategy for data (fn.1), 28.

10 See Article 29 Data Protection Working Party, Guidelines on the Right to Data Portability. WP242 rev.01, 10; see for this problem also Krämer et al, *supra* note 2, 78, and Graef, I., Husovec, M., & van den Boom, J., Spill-Overs in Data Governance: The Relationship Between the GDPR's Right to Data Portability and EU Sector-Specific Data Access Regimes, 2019, available at http://dx.doi.org/10.2139/ssrn.3369509, 8.

ers are using it. But even if it would work, i.e. lead to the benefit of being offered additional services, using this data portability mechanism has to be as simple as possible. One option are standardized processes that allow the service providers to initiate the data portability process similar to solutions in the PSD2 regulation (or the old regulations regarding phone number portability), where the consumers only have to give their consent. The current way of applying for data portability in Art. 20 GDPR is too burdensome. An additional problem emerges, if service providers do not need only the individual-level data of specific customers but need aggregate-level data from many connected cars for developing new services (or training algorithms). Then collecting enough data through inducing individual car users to use their data portability right might be too cumbersome and costly for these service providers (collective-action problem).

Also, the costs for the data-holding companies have to be considered. Similar to mandatory data access solutions also a far-reaching data portability right can reduce the incentives for producing certain data sets in the connected car, e.g. through additional sensors.

The result of our analysis is very clear. The data portability right suffers from legal uncertainty, a too narrow scope of data, its slowness and lack of continuous data portability, and missing obligations for ensuring the technical preconditions for data interoperability and interoperability with other services, as well as standardized safety and security solutions, and standardized processes for minimizing transaction costs. The regulations of the PSD2 Directive consist of an entire package of regulatory solutions that address all these problems.[11] If a data portability right would be designed with an adequate scope of in-vehicle data and continuous portability, and complemented with additional regulations for solving these technical and economic problems, then it also might offer a chance for solving the competition and innovation problems in the connected car example.[12] However, such a solution is far away from what can be done with the current data portability right of Art. 20 GDPR.

III. DATA PORTABILITY RIGHTS: THE NEED FOR A FLEXIBLE INSTRUMENT

As part of its European Data Strategy the EU Commission intends to make the data portability right of Art. 20 GDPR more effective, also for fostering competition and innovation, especially also with regard to IoT devices with lock-in effects for consumers. For addressing the current difficulties regarding the use of this right, the Commission considers also "mandating technical interfaces and machine-readable formats allowing portability of data in real-time."[13] Enabling data interoperability and continuous data portability are also important demands in the academic discussion for making the data portability right more effective. Other demands refer to the large legal uncertainty, e.g. about the scope of portable data, which needs a fast clarification, and a better enforcement of the existing data portability rules. Also, the need for developing trustworthy personal information management systems ("PIMS") for helping individuals to self-manage their personal data (consent management) is discussed.[14] All of these proposals would be helpful for a wider use of this data portability right. However, it will be very difficult to implement most of these proposals and they also would not be sufficient for solving many of the existing data access problems for competition and innovation (as, e.g. in the connected car example).

The main problem of using the data portability right of Art. 20 GDPR for solving competition and innovation problems lies in its general cross-sector character and limitation to personal data. Since it is an integral part of EU data protection law (based upon privacy as fundamental value), it is a general right that is granted to all data subjects regarding their personal data. Although EU data protection law has acknowledged that this data protection right can, indirectly, also foster competition and innovation, its basic objective is strengthening the "informational self-determination" of individual persons regarding their personal data. This limits severely the flexibility to adapt this data portability right (e.g. regarding the scope of portable data) to the often very different needs for making data available to other service providers (including additional necessary regulations) for enabling competition and supporting innovation in a sufficient way.[15]

11 See Kerber, W., From (horizontal and sectoral) data access solutions towards data governance systems, 2020, 10-12; available at http://dx.doi.org/10.2139/ssrn.3681263; forthcoming in: Drexl J. (ed.), Data Access, Consumer Interests and Public Welfare.

12 It should be noted that the existing type approval regulation for motor vehicles already encompasses a similar regulatory package, but it would need a huge step for updating this regulatory regime to the challenges of the new technology of connected cars. See Kerber/Gill, *supra* note 5, 255.

13 Communication of the European Commission: Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition - Two Years of Application of the General Data Protection Regulation. COM(2020) 264 final, 9.

14 See, e.g. Krämer et al, *supra* note 3, 75-84.

15 See for this problem also Graef et al, *supra* note 11, 22.

In the policy discussion about mandatory data access/sharing solutions, it has been seen as one of the problems of general ("horizontal") data access solutions that it is much more difficult to apply them in a sufficiently differentiated (targeted) way compared to sector-specific regulatory solutions, with regard to when data access obligations can be justified and how to make them effective.[16] This is the reason why so far the EU and other countries have focused more on sector-specific data access solutions as in sectors like banking (PSD2), energy, and others, which allow for a more targeted approach. The same problem does also exist with data portability rights. From an economic perspective, also data portability rights have to be designed and applied in a differentiated way, because the benefits and costs of solving data access problems through data portability rights can vary widely in different economic and technological contexts (no one-size-fits-all solution). It therefore depends very much on the data access problem in the specific markets, how a data portability right should be designed (scope of data, continuous portability, fees etc.), and whether it has to be complemented with additional regulations for rendering it effective with respect to competition and innovation. It is also necessary to analyze whether other data governance solutions like data access/sharing obligations, data trustee solutions, or technological solutions that change directly who has de facto control over data (as interoperable telematics platforms in the connected car example) would lead to more effective results than data portability rights.[17]

Therefore, the question arises whether the approach to rely primarily on a general privacy law-based data portability right (as Art. 20 GDPR) is the best way for developing effective data portability rights for solving competition and innovation problems, or whether the policy discussion should focus much more on data portability rights outside of privacy laws and beyond the limitation to personal data. Although the EU has taken some steps for introducing data portability rights for non-personal data, these approaches are still in its infancy and suffer from the lack of a coherent concept.[18] It rather is the consumer data rights legislation in Australia, which might help to develop a consistent alternative approach to data portability rights, which is not based upon data protection or privacy laws. The basic idea of consumer data rights is to give consumers more control over their consumer data (consumer empowerment) by granting them directly certain inalienable rights over their consumer data, which also encompass data portability rights.[19] The main advantage of the consumer data rights approach is that it is much more flexible, because consumer data need not be identical with personal data (as defined by privacy laws). They can therefore also encompass non-personal data, and not all personal data need to be consumer data. Therefore, a data portability right regarding consumer data can be much better adapted to different economic and technological conditions.

It is not surprising that in Australia a hybrid version of a general and a sector-specific approach was chosen for the consumer data rights.[20] Although consumer data rights are seen as a general approach for granting consumers (and small businesses) more control over their consumer data and how they can be used, their implementation is done through a step-by-step process in a sector-specific way (banking, energy, telecommunication etc.). This implies that the scope of transferable data as well as the mechanisms for transfer and security protocols can be defined in a sector-specific and problem-oriented way. This allows for a much more targeted approach for designing effective data portability rights for solving specific data access problems in different contexts, and therefore also enables a better balancing of the benefits and costs of data portability rights. With such a sector-specific implementable consumer data rights approach, also data portability solutions might be possible for the connected car example by defining all car data that are necessary for competition and innovation on secondary markets as portable consumer data and complementing this with the necessary additional regulations. It also fits to this approach that the Australian Competition and Consumer Commission ("ACCC") is the lead regulator and enforcement agency for these consumer data rights.[21] The conceptual advantage of consumer data portability rights is that it can encompass both personal and non-personal data, and it can be seen both as an instrument of consumer and competition policy.

Another way of using data portability rights outside of privacy laws for solving competition and innovation problems is to apply them as additional tools in competition law, e.g. as remedies in traditional competition cases or as part of the current competition policy reform discussion.[22] Both in merger cases and in cases of abusive behavior of dominant firms data portability remedies can be used as one of several types of data remedies, as, e.g. also data access/sharing obligations, separation of data sets (internal unbundling), and other limits on the use of data.

16 See for the discussion "Horizontal vs. Sectoral data access solutions" Kerber, *supra* note 12, 4-17.

17 For the need of an economic analysis of entire data governance systems for deriving the proper solutions see Kerber, *supra* note 12, 20-31.

18 See the Digital Content Directive and Free Flow of Data Regulation of the EU.

19 See for this concept OECD, *supra* note 3, 7-14.

20 See ACCC, Consumer Data Right (CDR), available online at https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0, Beaton-Wells, C., Platform Power and Privacy Protection: A Case for Policy Innovation, CPI Antitrust Chronicle September 2018, 6-8, Specht-Riemenschneider, Data access rights - A Comparative Perspective, 2020, forthcoming in: Drexl J. (ed.), Data Access, Consumer Interests and Public Welfare.

21 The ACCC however collaborates with OAIC (privacy protection agency) and the Data Standards Body ("DSB").

22 See for a comprehensive overview Vezzoso, S., Competition Policy in Transition: Exploring Data Portability's Role, forthcoming in: Journal of Competition Law & Practice (JECLAP); available at http://dx.doi.org/10.2139/ssrn.3634736

Data portability remedies can refer both to personal and non-personal data and be complemented with specific conditions for making them effective. Also, strategies of firms with market power that impede data portability can be prohibited as abusive behavior. The German Commission Competition Law 4.0 went one step further by proposing 2019 the introduction of an EU regulation for dominant platforms that would also entail an obligation of these platforms to enable the portability of user and use data in real-time (and to ensure interoperability with complementary services).[23] This leads directly to the question whether (and how) the instrument of data portability rights can and should also be part of a "new competition tool" and an *ex ante* regulation of digital platforms in EU competition policy. We suggest that data portability rights can play a valuable role in both instruments if appropriately designed and applied.

IV. CONCLUSIONS

Data portability rights can be a valuable instrument in the toolbox of policymakers in the data economy. However, they are not a cure-all and will often not be the most effective instruments for solving data access/sharing problems, because they can come with considerable costs and problems, and might require additional regulatory solutions as preconditions for their effectiveness. It is important to understand that they can be used as part of different policies and for achieving different objectives. In privacy laws it is an instrument for informational self-determination regarding personal data, in consumer policy it is about empowering consumers to get more control over the use of their consumer data, and in competition policy it is about solving problems for competition and innovation due to a lack of access to data, e.g. through data-related gatekeeper positions (as in the connected car example). Data portability rights seem to be attractive, because they have positive effects on all these policy objectives, but we also should not underestimate trade off-problems and conflicts between these policies. Therefore, a more integrative policy approach between data protection policy, competition policy, and consumer policy is also necessary with respect to data portability rights, which also have to be integrated well into the overall governance structure of the data economy. For the discussion in the EU we want to warn against relying too much on the data portability right of Art. 20 GDPR (with the danger of over-burdening this instrument), and instead recommend to develop also more data portability solutions outside of EU data protection law, e.g. by using the concept of consumer data rights.

23 Kommission Wettbewerbsrecht 4.0, Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft, 2019, 6.

DATA ACCESS AND PORTABILITY AND EU COMPETITION LAW

BY BJÖRN LUNDQVIST[1]

1 Associate Professor, Stockholm University.

I. INTRODUCTION

This short paper will discuss the right to access and port data under EU Competition Law and EU sector-specific regulations. While general Competition Law is not readily available, stipulating a difficult test for the plaintiff, the EU Commission seems very keen on granting access and portability right to data under newly enacted sector specific regulations, without any scrutiny in reference to the competitive effects of such rights. Indeed, to access and port data under these sector specific regulations are available to any comers. The paper concludes that enacting sector-specific regulations granting access to data without utilizing competition law principles may prove disastrous, and the Commission should rethink the aim of granting access to data to all and everyone.

II. EU EXCEPTIONAL CIRCUMSTANCE DOCTRINE

To use general EU competition law doctrines such as the refusal to supply doctrine to gain access to data in the digital economy may be somewhat problematic. Often platforms, such as Google and Amazon, would be the main targets for a claim for access, and the potential accessees would generally be business users of these respective services. But, these claims for access have several hurdles to overcome to become successful: Is the platform or data holder dominant on a relevant market? How should the relevant market be identified? Are there double or multisided markets? Moreover, in reference to the exceptional circumstance doctrine: accessing data, is that such an "exception" situation, where data access is indispensable for pursuing the user's business? Is there a second (downstream) market that the platform is reserving for itself? Is there an elimination of competition and the prevention of the appearance of a new product? All these requirements can be found in the case law of exceptional circumstance doctrine, i.e. *Magill*,[2] *IMS Health*[3] and *Microsoft*.[4] In the scenario of a competitor wanting access to specific, unique, data sets, indispensable for the business conduct, competition law has an applicability, but, that scenario is perhaps not so common. Multihoming of data makes unique datasets scarce, while from the outset, it may be difficult to find data indispensable for firms that are already active in the relevant market. Indeed, the essential facility, or exceptional circumstance, doctrine sets high thresholds and is very case specific, making it difficult to develop a general doctrine for accessing data in the digital economy under Competition Law.

Notwithstanding the above, the *Magill* "logic" at first glance works well in a data scenario: entities (in the *Magill* case the publicly owned BBC and RTE *et al*), engaging in their primary market or (public) task (producing and distributing TV programmes), create information, (in the form of TV listings) that were copyright protected. They are, under the rules of abuse of dominance, required to give access to this information (the TV listings), due to its indispensability and that a refusal would be unjust, to an undertaking that will create a new product (TV guides). Thus, in the *Magill* case the appellants were not allowed to reserve for themselves a secondary market. However, it was a very special case.[5] Still, *Magill* may be used to argue access to certain specific kind of datasets under the exceptional circumstance doctrine. As will be discussed *infra*, it should also be stressed that the *Magill* logic has inspired sector specific regulation enacting right to access and port public data. To gain access and to port public authority data for business purposes, similar method as under the *Magill* is used. Indeed, given that the exceptional circumstance doctrine is seldomly applicable, access to competitors' data are and will be pursued under sector-specific regulations rather than under general competition law.

2 Joined cases C-241/91 and C-242/91, *RTE, ITP & BBC v. Commission* ECLI:EU:C:1995:98.

3 Case C-418/01 *IMS Health GmbH & Co. OHG v. NDC Health GmbH & Co. KG.* ECLI:EU:C:2004:257.

4 Case T-201/04 *Microsoft Corp. v. Commission of the European Communities* ECLI:EU:T:2007:289.

5 Moreover, as Drexl points out, the *Magill* case could no longer arise as a matter of harmonised copyright law. According to the case-law of the CJEU on the concept of a copyrightable work, the mere listings of TV programs, which are defined by the programming schedule, could no longer be considered as protected by copyright. See, Josef Drexl. in "Data Access and Control in the Era of Connected Devices," Study on behalf of the European Consumer Association BEUC, Brussels 2018, p 32 making reference to inter alia Joined Cases C-403/08 and C-428/08 *Football Association Premier League and Murphy* ECLI:EU:C:2011:631, paras 96-98 (holding that football matches are not protected by copyright);

III. DATA ACCESS UNDER EU COMPETITION LAW

It seems clear that for business users of platforms, accessing customer or user data relating the business user's activity on the platforms, or even more broadly, and the right to transfer such data from a platform to another platform, or in-house, could be very beneficial for the business users commercial strategy. A firm active on, for example, Amazon Marketplace would thus through the data it generates on the Amazon Marketplace website gain in-depth knowledge of the customer base. Something it can use to develop its strategy and product line further. Access and portability right to data may also cause competition to thrive between platforms and in the general data industry if business users could easily shift between platforms and port useful data between the same. Presumably, more data would also be generally traded.

Yet, the exceptional circumstance doctrine, including the essential facility doctrine, is not readily available for gaining access to data, and to port the same. The recent *Google Search* (Shopping) case of the Commission regarding the practice of self-referencing[6] may however reveal a different path to gain data access and be allowed to port data from a platform or competitor. It is worth noting that, notwithstanding the fact that the Commission relied on the argument that the loss of traffic from Google's general search results pages represents a large proportion of competing comparison shopping services' traffic which could not effectively be replaced, the Commission framed this case under a standard leverage theory of harm, rather than the more challenging refusal to supply access to an essential facility, or even under a broader theory of exclusionary discrimination under Article 102(c) TFEU. Indeed, the Commission relied on *TeliaSonera*[7] to argue that it is sufficient to establish that Google's conduct was capable of making it more difficult (i.e. short of impossible) for competing comparison shopping services to access their separate but adjacent markets. This hurdle is clearly lower than a requirement to prove that access to Google's general search pages is indispensable, which would have been required had Google's conduct qualified as a vertical foreclosure case akin to a refusal to supply (the *Oscar Bronner* conditions).[8] Could a self-preferencing or leveraging test be used also to gain access to data?

Generally, the requirements for finding abuse under the monopoly-leveraging, or self-preferencing, concept would then need a finding of two separate markets (data market and device market). The dominant intermediate must adopt a business strategy outside the notion of competition on the merits (e.g. non-access to data or discrimination in access to data) on the primary data market. It must subsequently enter onto the (competitive) secondary market or support a proxy's entry. Entry must cause an exclusionary effect on that market by potentially foreclosing equally efficient, existing competitors due to the lack of access to necessary data held by the dominant platform. Last, the dominant intermediate must have no objective justification for not giving access to the data.[9]

A leveraging test following the steps above implies that certain features need not be present or, for that matter, identified. The service provided, e.g. the platform service, does not need to be indispensable, and neither dominance on the secondary market nor elimination of competition on that market need be proven. It should be admitted that the steps for a general leveraging test are, by the best estimate, ambiguous. Moreover, the Google case is not resolved yet, and it is even more ambiguous whether the Commission, in the end, will be successful it its line of argument. Indeed, it is very uncertain whether the leveraging doctrine could develop into a general doctrine for accessing and porting data.

The issues regarding obstruction, leveraging and self-preferencing have been discussed in great detail in various reports.[10] However, while obstruction of interoperability, data collection and the subsequent use by gatekeeper to enter their customers markets could be addressed as leveraging, self-preferencing or obstruction under Article 102 TFEU, access to, and the right to port of, data is not the natural remedy in these cases. For the porting of and access to data, the exceptional circumstance doctrine is exclusively available, and, as discussed above, not an effective way to pursue.

---

6 Case AT.39740 *Google Search (Shopping)* Commission Decision, C(2017) 4444 final (June 27, 2017), para 339.

7 Case C-52/09 *Konkurrensverket v TeliaSonera Sverige AB* ECLI:EU:C:2011:83.

8 Bjorn Lundqvist, Ioannis Lianos, Wang Xianlin, Matt Strader with Igor Nikolic, and the BRICS teams, Chapter 7. Exclusionary and unfair unilateral practices in reference to Platforms, in Digital Era Competition BRICS Report (2019), http://bricscompetition.org/upload/iblock/6a1/brics%20book%20full.pdf.

9 *Ibid.*

10 Jacques Crémer, Yves-Alexandre de Montjoye & Heike Schweitzer (2019), Competition policy for the digital era, Publications Office of the European Union; Federal Ministry for Economic Affairs and Energy (2019), A new competition framework for the digital economy. Report by the Commission "Competition Law 4.0"; Furman Report: HM Treasury (2019), Unlocking digital competition, Report of the Digital Competition Expert Panel. Various authors, Digital Era Competition BRICS Report, http://bricscompetition.org/upload/iblock/6a1/brics%20book%20full.pdf; Australian Competition and Consumer Commission (2019), Digital Platforms Inquiry. Final Report; BRICS Competition Law and Policy Centre (2019), Digital Era Competition: A BRICS View Committee for the Study of Digital Platforms (2019), Final Report by the Market Structure and Antitrust Subcommittee, George J. Stigler Center for the Study of the Economy and the State.

Forcing porting of data would imply the obligation to collaborate between the platform and the business user. Mandating firms to collaborate is difficult, if they do not want to collaborate. The only case where firms were mandated to collaborate is the US *Aspen skiing* case which, required ski slopes firms to collaborate for the production of joint ski passes. The EU *Microsoft* case did include a requirement for Microsoft to share source code etc., but not to collaborate, yet still it was a very difficult remedy to uphold.[11]

Generally, the right to access and port data under competition law seems difficult.

IV. SECTOR-SPECIFIC REGULATIONS

An alternative route is granting access and portability right under sector specific regulations. To grant access to data, the EU Commission seems keen on using sector-specific regulations Indeed, it seems that rules regarding certain providers, regarding use and access of data (*ex ante* regulations) are currently seeping in as sector or industry specific regulations, implying an obligation to either share data or to grant open and somewhat non-discriminatory access to platforms and devices, which collects the data.[12] However, the sector-specific regulations often address old economy, e.g. banks and transport services, while in reference to regulations for platforms[13] and the free flow or data,[14] no hard rules on access to data is available.

Firstly, the EU Commission did introduce a platform-to-business ("P2B") regulation in 2019, which target the platform-business interface.[15]

The P2B regulation mostly focuses on rules regarding transparency, and it seems clear that the P2B regulation will not directly address access issues. The Commission was somewhat reluctant and hesitant to regulate the P2B in detail. However, the Commission in the P2B addressed the issue with Internet intermediates having access to more data than its customers. The P2B regulation oblige providers of online intermediation services to provide business providers with a clear description of the scope, nature and conditions of their access to and use of customer data generated by the business users' activities on the platform. Moreover, the P2B regulation states that platforms need to be transparent if they intend to discriminate in reference to access to data, by giving better access to affiliated firms then to the business user. Online search engines and platforms should be transparent about any preferential treatment they give to their own products and services offered through their sites. The P2B regulation thus addresses the issue of data and who has access to, while only providing rules regarding transparency.

Second, in the Data Free Flow Regulation, the European Commission has specifically addressed the issue that firms should be given the right to port non-personal data – especially *vis-à-vis* cloud providers. In the regulation, the cloud industry should, through self-regulation, come up with a procedure and standard technology so that data can be ported. The proposed regulation contains a call for self-regulation of the right to port data.[16] It should be acknowledged that a standardisation organisation now has produced a code of conduct for porting data from cloud to cloud. The code is very detailed and applicable for the members of the organisation. It can be difficult for firms to penetrate.[17] Whether the code actually will create a right (*erga omnes*) to port data between clouds seems unclear at this stage. Yet, it is an indication that self-regulation may work.

11 *Aspen Skiing Co. v. Aspen Highlands Skiing Corp.*, 472 U.S. 585 (1985) and *Microsoft Corp v Commission* (2007) T-201/04, ECLI:EU:T:2007:289.

12 Chisholm, A. & Jung, N., (Spring-Autumn 2015), Platform Regulation — Ex-Ante versus Ex-Post intervention: evolving our antitrust tools and practices to meet the challenges of a digital economy. Competition Policy Int'l. Vol. 11, No. 1, 7-21.

13 The proposed P2B regulation: Brussels, 26.4.2018 COM(2018) 238 final 2018/0112 (COD) Proposal for a regulation on promoting fairness and transparency for business providers of online intermediation services.

14 There are French national initiatives to open e-platforms for third party competitors. See e.g. French Senate Report (March 20, 2013), available at http://www.senat.fr/rap/r12-443/r12-443.html.

15 European Commission, Fairness in platform-to-business relations, Ref. Ares(2017)5222469 - 25/10/2017, https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-5222469_en, accessed May 28, 2018.

16 European Commission, Commission Staff Working Document Impact Assessment, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union, SWD/2017/0304 final - 2017/0228 (COD), Brussels, 13 September 2017 (Impact Assessment); Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, COM(2017) 9 Final, January 10, 2017.

17 See the SWIPO Code of Conduct, available at https://valtioneuvosto.fi/en/project?tunnus=LVM019:00/2019. As stated on the EU Commission website, apart from two dedicated Codes of Conduct, respectively on Infrastructure-as-a-Service (IaaS) cloud services and on Software-as-a-Service (SaaS) cloud services, the SWIPO working group also delivered an extensive proposal for a governance structure. This governance structure should make the Codes of Conduct practically enforceable, e.g. through a complaints mechanism for users. The deadline for the implementation of the Codes of Conduct is May 2020, as foreseen by the Regulation on the free flow of non-personal data (FFD). As determined in the FFD Regulation, the European Commission will evaluate the impact of those Codes of Conduct before November 2022. This evaluation will notably focus on the effects that the SWIPO Codes of Conduct will have on the fluidity and competitiveness of the cloud market. https://ec.europa.eu/digital-single-market/en/news/presentation-codes-conduct-cloud-switching-and-data-portability.

The result of the Data Free Flow initiative is somewhat surprising, given the enthusiasm the Commission showed in early policy papers towards implementing a mandatory right to port data for business provider *vis-à-vis* cloud providers,[18] and begs the question whether the right to port should be included in some other legislative effort by the Commission, such as the modernization of the database directive.[19]

The P2B and Free Flow regulations do not stipulate any hard rules that would enable a more equal playing filed. Access and portability are not legal rights, rather topics for contractual discussions.

Access to data is however enacted under sector specific regulations such as the directive for public data,[20] in the field of transport and financial services,[21] and in other legislative initiatives.[22]

The PSI Directive[23] already mentioned, stipulates route for accessing public (government) data.[24] The main focus of the PSI Directive is very specific. It is to create a levelled playing field when making available PSI as input to a commercial activity, i.e. when the PSI is used as components to new products and services. This should then release the full economic potential of a new emerging area of the ICT sector.[25] The PSI Directive is triggered by three prong test:

1. Are the data created (supplied) inside the public task of the Public Sector Body? If yes, the second question is:

2. Are the data being re-used by the PSB or some other body on its behalf? In other words, will the data be used for another purpose than the initial purpose? Moreover, does the re-use constitute a commercial activity, e.g. giving access to the dataset to paying subscribers?

3. If the two first questions are answered in the affirmative, then a number of requirements of requirements for the public authority will apply, including that third parties have the right to access the dataset providing remuneration to the PSB, so to enable the third parties to commercially utilize the data in competition with the PSB and other firms having access to the dataset.

---

18 European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions SWD (2017) 2 Final, COM(2017) 9 Final, 13; European Commission, Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, COM(2017) 9 Final, January 10, 2017, 33, making reference to the works of Zech, who claimed that the right way forward is the creation of a property right to non-personal goods. Cf. Herbert Zech, "Information as a tradable commodity," in Alberto De Franceschi Ferrara (ed), *European Contract Law and the Digital Single Market*, 2016, 51-79.

19 It should be mentioned that there is a right for person under certain circumstances to port data according to Article 20 GDPR. Cf. Björn Lundqvist, "Regulating Competition and Property in the Digital Economy – The Interface Between Data, Privacy, Intellectual Property, Fairness and Competition Law," (January 17, 2018). Faculty of Law, Stockholm University Research Paper No. 55. Available at SSRN: https://ssrn.com/abstract=3103870., accessed 25 March 2018.

20 The Directive on the re-use of public sector information Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, OJ L 172, 26.6.2019, p. 56–83 (The old PSI directive: Directive 2003/98/EC, known as the "PSI Directive") entered into force on December 31, 2003. It was revised by Directive 2013/37/EU which entered into force on July 17, 2013.

21 In order to accelerate retail banking innovation and simplify payments, the European Commission is mandating standardized API access across the EU. The initiative is part of the European Commission's update of the Directive on Payment Services (PSD). The revision to the Directive on Payment Services (PSD2) requires banks to provide access to third parties. See Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance). Cf. EU Commission, (2015) A Digital Single Market Strategy for Europe, COM(2015) 192 final.

22 REACH-Regulation, Article 25 Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC. See furthermore Article 16 of the new Digital Content and Digital Services Directive making reference to GDPR. See also the new Electricity Directive of June 2019 imposes the sharing of consumer data, including metering and consumption data as well as data required for customer switching, demand response and other services. In order to stimulate competition and innovation among electricity suppliers, Article 23(2) of the Directives provides that porting of data should be required. Finally, the Clinical Trials Regulation 536/2014. on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC.

23 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, OJ L 172, 26.6.2019, p. 56–83.

24 See also the INSPIRE directive regarding spatial data, Articles 5 and 8. For the various legal tools making up the INSPIRE initiative see https://inspire.ec.europa.eu/inspire-directive/2.

25 EU Commission, (1998) Public Sector Information: A Key Resource for Europe, Green Paper on Public Sector Information in the Information Society, COM(1998) 585 final, 5.

The PSI directive bears similarities even to the *Magill* case, discussed above. Also, under the *Magill*, the dominant firm create data (TV-listings) in its primary markets, which access is denied to create a business in a secondary market. Yet, the PSI directive seems also to include a non-discriminatory exclusion rules, similar to the ideas put forward in the French competition law cases *GDF*[26] and *EDF*.[27] Indeed, the PSI directive stipulates a prohibition for Governments and Government Authorities to abuse or discriminate using the power inherent in the data collected, without the need to identify dominance in reference to the Authority or the database.

A similar principle for accessing data can be seen in the EU Regulation on providing multimodal travel information services,[28] and to some extent under Directive on Payment Services ("PSD2") that requires banks to provide data access to third parties. PSD2 is well known, however few know about the Regulation on providing multimodal travel information services. The Regulation requires both private and public transport service providers to grant access to travel data at any time in a machine-readable format through the National Access Point (NAP);[29] Those NAPs will gather travel and traffic data from all type of transport from both private and public entities within and, eventually, outside the borders of an EU Member States. The Regulation stipulates that firms have a right to access transport data at any time.

These specific legal systems are examples of rules that are, or are close to, requiring public entities and firms to give access to and the right to port data. It is possibly an indication of an interesting underlying current that the EU legislator try to boost competition and markets by granting access to data, while circumventing general competition law. The idea is to boost competition, without making use of any test of antitrust harm, by opening up the device for collecting data to all-and-everyone. The legal systems do not differentiate between sharing with firms that already possess much data or are indeed hoarding data on several markets, with those firms that do not possess or hoard much data. Whether such a policy is pro-competitive may be disputed. Not only new entrants and small entrepreneurs will be able to obtain data, also incumbent platforms and system leaders will be granted access to these devices or, in reference to government data, the PSI. Indeed, opening up for much information to be available for all and everyone can have large effect of competitive structures of markets, both to the better and the worse.

Moreover, it also begs the question, to be put to the legislator, why similar access rules do not exist for transaction platforms or social platforms. Why not for platform providers when large industries such as the bank sector and the transport sector should be required to give access important and large datasets? Indeed, these sector specific regulations may have the effect of benefiting already large platforms.

Giving access to data is generally pro-competitive, yet a problem with the sector-specific regulations for the data-driven economy is that they do not take into consideration the competitive structure of the markets and market power of the firms that demands data access. Firms that have data-driven business strategies, i.e. hold, seek access to data and use data, and are economically powerful such as certain tech platforms should possibly not be subsidies by having access to data for free. Moreover, if the goal of the digital agenda was to benefit start-ups, entrepreneurial competition and innovation, the sector specific regulations granting access to data, may open up for the possibility to collude.

26 French Competition Authority, Decision 14-MC-02 of 09.09.2014. The case is discussed in the German and French Competition Authorities joint paper, (10 May 2016) Competition Law and Data, 20, available at http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf.

27 French Competition Authority, Decision n°13-D-20 of 17.12.2013, confirmed on that points by the court of appeal on 21.05.2015.

28 Commission Delegated Regulation (EU) 2017/1926 of 31 May 2017 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide multimodal travel information services C/2017/3574 OJ L 272, 21.10.2017, p. 1–13. See also Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport, OJ L 207, 6.8.2010, p. 1–13.

29 See Parliament and Council Regulation (EU) 2017/1926 of 31 May 2017 supplementing Directive 2010/40/EU with regard to the provision of EU-wide multimodal travel information services [2017] OJ L 272/1.

V. CONCLUDING REMARKS REGARDING THE FUTURE

In this paper, I have discussed the right to access and port data under EU Competition Law and EU sector-specific regulations. It seems clear that while general Competition Law is not readily available, stipulating high thresholds for accessing and porting data, the EU Commission seems very keen on granting access and portability right to data under newly enacted sector specific regulations. This is done without any scrutiny in reference to the anticompetitive effects of such rights.

In a recent communication from February 2020, the EU Commission indicates it wants to pursue the strategy of enacting data access regime on a sector specific level even further. It states that the EU will support, with investments and, possibly, sector specific regulations of, so-called "common data spaces." Common data places where both public and private entities should be encouraged and forced to give up their data in data pools, or data commons.[30] According to the Commission the following areas should hold common data spaces:

- A Common European industrial (manufacturing) data space, to support the competitiveness and performance of the EU's industry.
- A Common European Green Deal data space, to use the major potential of data in support of the Green Deal priority actions on climate change, circular economy, zero- pollution, biodiversity, deforestation and compliance assurance.
- A Common European mobility data space, to position Europe at the forefront of the development of an intelligent transport system, including connected cars as well as other modes of transport.
- A Common European health data space.
- A Common European financial data space.
- A Common European energy data space, to promote a stronger availability and cross-sector sharing of data, in a customer-centric, secure and trustworthy manner.
- A Common European agriculture data space.
- Common European data spaces for public administration.
- A Common European skills data space, to reduce the skills mismatches between the education and training system.

Neither these common data spaces,[31] nor the strategy as a whole, seem to take into consideration the competitive structure of the market or the size of the market presence of the entities that should be allowed access to these data spaces. Indeed, all this data may change the structure of these industries radically. They may can become access tools and further fortify the dominance of already powerful platforms or facilitate other forms of anticompetitive conduct. Indeed, enacting sector-specific regulations granting access to data without utilizing competition law principles may prove disastrous.

30 EU Commission A European strategy for data, Brussels, 19.2.2020 COM(2020) 66 final, 21 et seq. See also the Appendix Common European data spaces in in strategic sectors and domains of public interest.

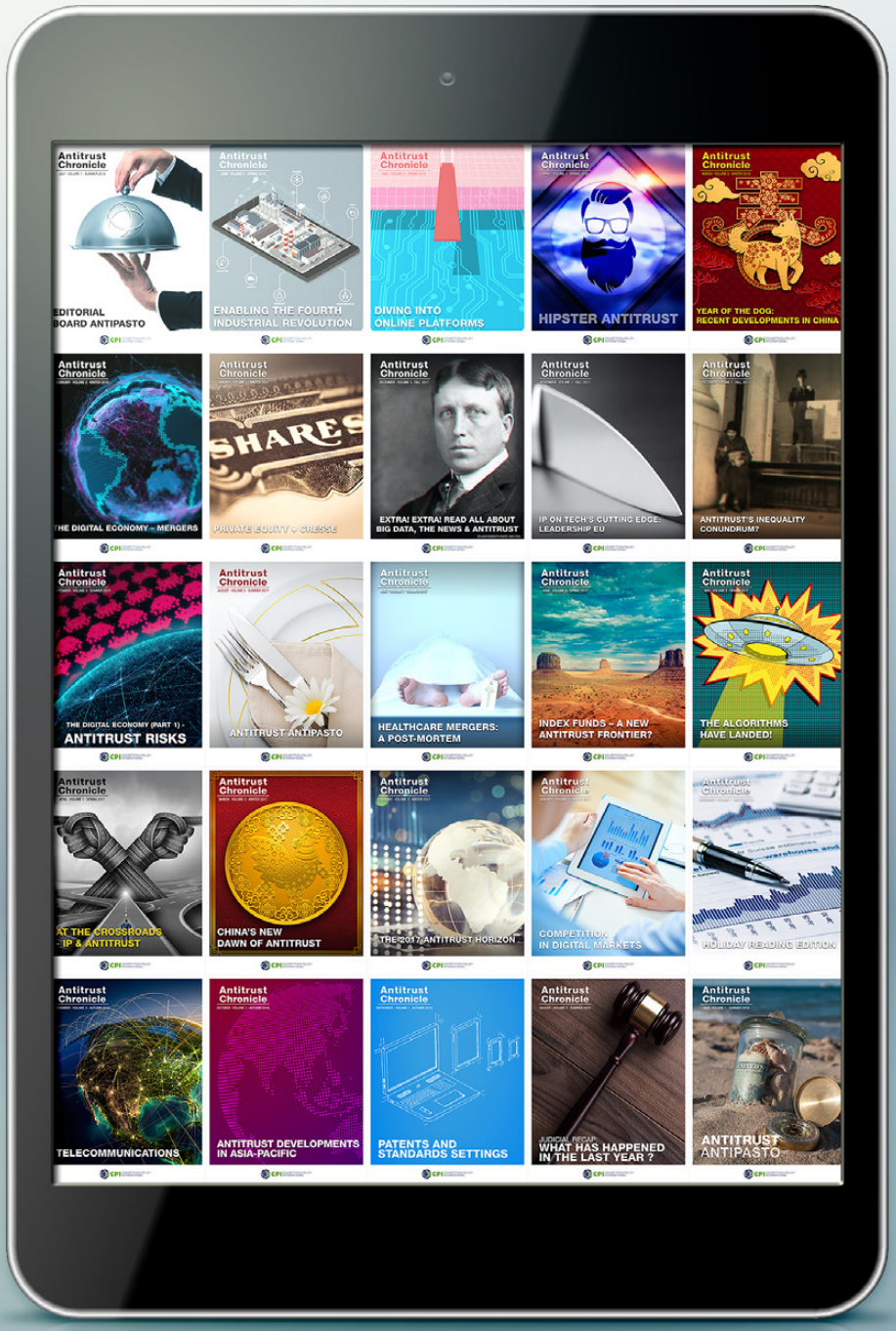
31 Also including the Gaia-x initiative, see https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html.

CPI COMPETITION POLICY INTERNATIONAL

CPI Subscriptions

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

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




CPI
COMPETITION POLICY
INTERNATIONAL