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

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.

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.

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").

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).

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 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.

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/.

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.

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.