Comments for the Record

Comments regarding “Data to Go: An FTC Workshop on Data Portability”

JENNIFER HUDDLESTON | AUGUST 21, 2020

Agency: Federal Trade Commission

Comment Period Closes: 8/21/2020

Comment Submitted: 8/21/2020

Docket No.: FTC-2020-0062

I appreciate the opportunity to provide comments prior to the Commission’s workshop “Data to Go: An FTC Workshop on Data Portability.” This comment does not represent the views of any particular party or special interest group but is intended to assist regulators in creating a policy environment that will continue to facilitate a regulatory approach that allows innovation to flourish while addressing harms to consumers.

The questions posed by the Commission seek to learn from existing policies aimed at data protection and to minimize unnecessary tradeoffs. These questions also illustrate that as with many policy decisions related to data, data portability may impact not only the regulation of data security or privacy, but also innovation and competition. In this regard I seek to address the following in my comments:

1. The interaction between data portability requirements and data privacy policy;
2. The interaction between data portability and data privacy as illustrated by the General Data Protection Regulation (GDPR) and potentially remaining policy questions; and
3. The impact data portability requirements may have on competition.

Data Portability and Data Privacy

Data portability is often touted as a policy solution to improve consumer control over data and provide additional options for those who desire a more privacy-centric option. The relationship between data privacy and data portability is not straightforward.

While some data may clearly belong to one user, much of the data that users would desire to be portable is generated by interactions, or it is not obvious which user has control over it. For example, to port a social graph of a user’s connections or contacts with others from one service to another would require information about other users. Even something as simple as porting photos can involve data from multiple users (for example, who are tagged in the photo) or other relevant information (such as other users’ interactions with the photo) is also included. In these scenarios, questions arise about the consent (or lack of consent) of other users whose information may be ported to the new service if a friend chose to invoke his or her rights to data portability. So,

while data portability might increase control for the user porting information, it may not increase and even decrease the control of associated users. If a user can only port his or her own information without these connections, it may not have the usefulness or advantages they believed it would.

At the same time, many voluntary elements of data portability currently available may provide more privacy-sensitive users with options. For example, the ability to download one's own data or use systems that are interoperable may provide a greater sense of control or increase efficiency. But mandating such requirements may limit the options available in an attempt to create interoperability and uniformity. In setting such standards, it is possible that they could easily be too rigid to evolve quickly with innovative improvements and solutions that would better solve the problem.[1]

Data Portability and Data Security

One of the key questions in any policy that requires data portability is where responsibilities fall in the event of a breach during or after a transfer. Particularly given the potential for significant fines as a result of such incidents and the loss of consumer trust associated with them, providing innovators with clarity around the responsibility and liability associated with data that has been transferred would provide needed legal certainty. This greater certainty would better allow companies to make informed choices about the potential risks associated with allowing data portability.

The GDPR, a complex regulatory regime governing data collection, usage, and security in the European Union, has shown that a request for data often associated with data portability or deletion requirements also has its own data security risk. In some cases, the speed with which companies are expected to comply with requests has resulted in poor verification of the identity of the individual submitting the request. For example, a researcher found he was able to obtain his fiancée's data invoking GDPR consumer rights with minimal identity checks.[2] This illustrates how requirements intended to promote privacy and control can also result in incentives that may increase certain risks.

Data portability can be a tool for providing user control and flexibility; however, it also has potential to increase uncertainty and risk for data security. This is particularly true when mandated portability creates an improper incentive for speed in response over thorough vetting. A flexible approach can allow improved and innovative solutions to data security; this flexibility can also yield uncertainty for innovators, however.

Data Portability and Competition

In addition to individual control, proponents of data portability of argue that by lowering switching costs, such requirements will increase competition among platforms that rely on data. But data portability requirements can also create additional costs and regulatory barriers for new entrants. The relationship between portability or interoperability and competition is complicated.

In many cases, it is not the data itself that is valuable to a company, but the various assumptions, algorithmic applications, and efficiency that large platforms offer with that data.[3] Additionally, a single user or piece of data is often not exclusive to a single platform or firm and firms may benefit in user growth by offering portability that allows consumers to not feel locked into a single product.[4] As a result, in some scenarios incentives may lead a company to offer portability while retaining a successful market position through its superior product or algorithms.[5] But mandating interoperability or data portability might actually harm consumer welfare unlike when companies choose to voluntarily offer such solutions based on market demands.[6]

Portability or interoperability requirements may come at a cost that is particularly burdensome on new entrants, and thus have a detrimental impact on consumers. The costs of these requirements are high and would likely both be passed along to the consumer and deter new entrants into the market, thus harming consumer welfare.[7] An analysis by the Information Technology and Innovation Foundation's Alan McQuinn and Daniel Castro found that data portability requirements similar to the GDPR or the California Consumer Privacy Act would cost American organizations subject to these requirements about $510 million.[8] A high cost of compliance and the increased risk of penalties might deter smaller companies from entering the market or deter investment. For example, following the GDPR in Europe there has been decreased investment in new and small firms.[9]

Conclusion

In some cases data portability can be an excellent way for companies to provide individuals with more choice and control over their own data; this portability is not without its own costs and tradeoffs to both consumers and the companies with which they interact, however. Clarity around the liability for data during and after transfer would be needed to provide a degree of legal certainty given the patchwork of data breach and security laws.

[1] Ryan Hagemann, Jennifer Huddleston, and Adam Thierer, *Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future*, 17 Colo. Tech. L. J. 41 (2019), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3118539 (discussing the role of soft law and risks with over regulation in regards to the "pacing problem" in technology policy).

[2] Bradley Barth, *Researcher: GDPR's Right of Access policy can be abused to steal others' personal info*, SC Media, Aug. 9, 2019, https://www.scmagazine.com/home/security-news/researcher-gdprs-right-of-access-policy-can-be-abused-to-steal-others-personal-info/.

[3] Thomas M. Lenard, *If Data Portability is the Solution, What's the Problem?*, Technology Policy Institute, Jan. 2020, *available at* https://techpolicyinstitute.org/wp-content/uploads/2020/01/Lenard_If-Data-Portability.pdf.

[4] *Id*. at 3.

[5] *Id.* at 3.

[6] Peter Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critiques*, Public Law and Legal Theory Working Paper No. 204, May 31, 2013, *available at* https://fpf.org/wp-content/uploads/2013/07/Swire-Lagos_Why-the-Right-to-Data-Portability-Likely-Reduces-Consumer-Welfare1.pdf.

[7] *Id*.

[8] Alan McQuinn & Daniel Castro, *The Costs of Unnecessarily Stringent Federal Data Privacy Law*, Information Technology & Innovation Forum, Aug. 5, 2019, https://itif.org/publications/2019/08/05/costs-unnecessarily-stringent-federal-data-privacy-law.

[9] Jian Jia, Ginger Zhe Jin, & Liad Wagmann, *The Short Run Effects of GDPR on Technology Venture Investment*, NBER Working Paper No. 25248, Nov. 2018, https://www.nber.org/papers/w25248.