



August 21, 2020

Federal Trade Commission  
Office of the Secretary  
Constitution Center  
400 7th St. SW  
5th Floor, Suite 5610  
Washington, DC 20024

**Re: *FTC Data Portability Workshop, Docket No.: FTC-2020-0062***

Consumer Reports<sup>1</sup> writes to respond to the Federal Trade Commission’s (“FTC” or “Commission”) request for comment<sup>2</sup> on its forthcoming workshop, “Data To Go: An FTC Workshop on Data Portability.” Data portability and interoperability will play increasingly important roles in the digital economy, and we appreciate the Commission holding this event to study these issues.

**POLICY CONSIDERATIONS**

In general, Consumer Reports supports data portability obligations on companies to allow consumers to take their data to competing services. Data access has long been considered a Fair Information Practice Principle;<sup>3</sup> data portability should be considered as a logical extension of this right. In fact, under the California Consumer Privacy Act, these rights are explicitly merged: consumers have a right to access the data that

---

<sup>1</sup> Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For over 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers’ interests. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace.

<sup>2</sup> *Data To Go: An FTC Workshop on Data Portability*, FED. TRADE COMM’N (last visited Aug. 21, 2020), <https://www.ftc.gov/news-events/events-calendar/data-go-ftc-workshop-data-portability>.

<sup>3</sup> See, e.g., *Privacy Online: A Report to Congress*, FED. TRADE COMM’N at 9 (June 1998), <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf>.

companies have about them, and “the information shall be in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance.”<sup>4</sup> However, while these rights are related, they play somewhat different roles: data access is primarily about accountability, to enable us to shine a light on the data that companies have collected about us. It is also often paired with a right of deletion<sup>5</sup> or a right of correction<sup>6</sup> so that consumers can get rid of unnecessary or unwanted data, or amend records that could otherwise be used to draw incorrect inferences about them.

Data portability on the other hand empowers consumer agency and facilitates competition by allowing consumers to take their data and move it to another service or repository. If a consumer becomes dissatisfied with one provider that processes personal information (such as an email service or cloud storage for photographs), they can simply move their data to a competing provider. Portability rights limit providers’ ability to lock consumers into their service, whereby consumers could be coerced into accepting deteriorating quality or higher prices because of switching costs. Humans are still creatures of habit and tend to accept the status quo;<sup>7</sup> even with completely seamless data portability, there would still be costs associated with researching other providers and learning a new interface. Nevertheless, portability rights can help reduce friction and increase competition in products and services that increasingly rely on computer processing and personal information.

Nevertheless, there should be reasonable context specific limits to data portability rights, especially in the use case of shared data. Data often describes more than one person: a chat group, an email thread or call log. Data collecting products and services should balance the right to data portability without exposing data from others. For example, platforms that offer the ability to tag multiple friends in a photo creates a challenge to determine who is the owner of the photo. Even among connections on a social network who have access to each other’s profiles, allowing one individual to download every piece of personal data related to another person could violate reasonable expectations and undermine privacy. The other extreme — limiting any data portability would leave users with zero choice and power to leave a platform and use a different service. The same can be said about genetic data, where donating saliva

---

<sup>4</sup> Cal. Civ. Code §1798.100(d), <https://theccpa.org/#1798.100>.

<sup>5</sup> See, e.g., the California Consumer Privacy Act, Cal. Civ. Code §1798.105, <https://theccpa.org/#1798.105>.

<sup>6</sup> See, e.g., the Fair Credit Reporting Act, 15 U.S.C. §1681(i), <https://www.law.cornell.edu/uscode/text/15/1681i>.

<sup>7</sup> Jacob M. Nebel, *Status Quo Bias, Rationality, and Conservatism about Value*, ETHICS at 451 (Jan. 2015), <https://philpapers.org/archive/NEBSQB.pdf>.

samples for DNA sequencing may potentially violate the rights of their family members who share similar genes. Platforms must balance data rights with the rights of others connected to that data.

Interoperability is related to data portability: instead of transferring a consumer's data to another company (and then deleting their own copies), companies make available the data on their systems to third-party applications and other platforms to copy, change, or otherwise process. Because the concepts are similar, some policy solutions try to achieve both: for example, the bipartisan ACCESS bill requires large internet platforms to both make data portable to move to other systems, but also requires that these companies make available technical interfaces to give others the ability to process data on their platforms.<sup>8</sup>

Interoperability especially presents unique policy challenges, placing values such as innovation, quality control, competition, and privacy sometimes at odds with each other. Interoperability, like data portability, can reduce companies' power to lock consumers into their silos, but can also lead to unfavorable outcomes if bad actors are able to exploit the platform to exfiltrate data or otherwise harm consumers or worsen the user experience. Cambridge Analytics presents a stark example of the downsides of interoperability, where one rogue developer was able to deceptively harvest the data of users — as well as that of their friends — for political microtargeting.<sup>9</sup> Even before the Cambridge Analytica scandal came to light, Facebook begin restricting apps' access to data; while this move pleased privacy advocates who had called for the change for

---

<sup>8</sup> S. 2658, Augmenting Compatibility and Competition by Enabling Service Switching Act of 2019, <https://www.congress.gov/bill/116th-congress/senate-bill/2658/text>; Press release, Senator Mark R. Warner, *Senators Introduce Bipartisan Bill to Encourage Competition in Social Media*, (Oct. 19, 2019), <https://www.warner.senate.gov/public/index.cfm/2019/10/senators-introduce-bipartisan-bill-to-encourage-competition-in-social-media>. The ACCESS bill also smartly mandates interoperability for *privacy controls*, requiring that large internet companies create interfaces for third parties to access and set them. Companies like Google and Facebook offer many privacy settings, but they are often byzantine and confusing for most users; empowering consumers to designate a trusted third party to manage those settings for them would give consumers more control over their personal data without requiring them to expend the time and effort to understand the ever-shifting nuances of companies' data processing activities and how their controls operate in practice.

<sup>9</sup> Sam Meredith, *Facebook-Cambridge Analytica: A timeline of the data hijacking scandal*, CNBC, (Apr. 10, 2018) <https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html>.

years,<sup>10</sup> it frustrated others who complained that the changes made the Facebook platform less open.<sup>11</sup>

## POLICY RECOMMENDATIONS

While Consumer Reports supports policies that would promote competition by incentivizing or mandating data portability and interoperability, those policies must be supplemented by other legal protections to compensate for the greater exposure of personal information. Simply put, reasonable privacy and security obligations are a condition precedent for interoperability to work. Even the best of privacy protections will be imperfect, due to the difficulties in detection and enforcement; portability and interoperability, by expanding the universe of companies with access to data, unavoidably invite some degree of risk. In many cases, that risk will be outweighed by the value to consumer agency and competition. To minimize that risk in all cases, companies should be legally obligated to use reasonable security measures and to limit data processing to what is reasonably necessary to deliver the services requested by the consumer.<sup>12</sup>

Further, data portability and interoperability mandates should be paired with *nondiscrimination* obligations, to ensure that companies cannot charge fees or set discriminatory conditions on individuals who prefer to use another service to process their data. As privacy protections are a necessary condition for meaningful interoperability, nondiscrimination is a necessary condition for consumers to enjoy meaningful privacy protections.<sup>13</sup>

---

<sup>10</sup> Letter from the American Civil Liberties Union of Northern California *et al.* to Mark Zuckerberg (Jun. 16, 2010), [https://www.eff.org/files/filenode/social\\_networks/openlettertofacebook.pdf](https://www.eff.org/files/filenode/social_networks/openlettertofacebook.pdf).

<sup>11</sup> Dell Cameron, *Alex Stamos, Ex-Facebook Security Chief, Blames Journalists for Cambridge Analytica Fallout*, GIZMODO (Aug. 23, 2019) <https://gizmodo.com/alex-stamos-ex-facebook-security-chief-blames-journal-1837520235>.

<sup>12</sup> Justin Brookman, *A Comparison of the COVID-19 Privacy Bills*, MEDIUM (May 19, 2020), <https://medium.com/cr-digital-lab/a-comparison-of-the-covid-19-privacy-bills-76f8e037cffe>; Consumer Reports and Privacy Rights Clearinghouse Letter to Chair Reuven Carlyle, Environment, Energy & Technology Committee, Washington State Senate, Re: PSSB 6281, The Washington Privacy Act (Jan. 21, 2020), <https://advocacy.consumerreports.org/wp-content/uploads/2020/01/CR-PRC-Letter-to-Senate-EET-1.21.19.pdf>.

<sup>13</sup> Consumer Reports letter to Chairman Crapo and Ranking Member Brown, Committee on Banking, Housing, and Urban Affairs, United States Senate, Re: Hearing on Data Ownership: Exploring Implications for Data Privacy Rights and Data Evaluation (Oct. 24, 2019), <https://advocacy.consumerreports.org/wp-content/uploads/2019/10/Consumer-Reports-data-ownership-letter-10.24.19.pdf>.

Platforms that make their data available to third parties to access and manipulate should also exercise effective monitoring and moderation to ensure that this data access is not being abused. For at least fifteen years, the FTC has interpreted its Section 5 unfairness authority to require companies to use reasonable data security to prevent third-party abuse of their networks. In a number of other contexts, too, the FTC has interpreted Section 5 to require policing of others' actions: *Neovi* and *LeadClick* are just two examples of the FTC holding platforms liable for third-party abuses.<sup>14</sup> The FTC's Endorsement Guides arguably hold advertisers *strictly liable* for third-party endorsements that do not disclose material conflicts of interest,<sup>15</sup> though the related FAQs clarify that the Commission would be unlikely to bring an action against a company if it has a reasonable monitoring program in place.<sup>16</sup> Nevertheless, even the more relaxed FAQ guidance implies an affirmative legal obligation to monitor and remediate the illegal behavior of others. Last year in its \$5 billion settlement with Facebook, the Commission charged Facebook for failing to implement a reasonable privacy program by not implementing controls to address the risks associated with third-party interoperability and data access.<sup>17</sup>

In general, companies that operate a platform that allows for third-party interoperability with their systems should have an obligation to implement reasonable and cost-effective measures proportionate to the risks associated with potential abuses. On the other hand, companies should not have the same policing obligations for data portability requests, as the transfer of data to another entity should generally constitute a transfer of responsibility for that data as well.

---

<sup>14</sup> *FTC Action Results in Contempt Order Against Online Check Writing Marketers*, FED. TRADE COMM'N (Jul. 27, 2012), <https://www.ftc.gov/news-events/press-releases/2012/07/ftc-action-results-contempt-order-against-online-check-writing>, *U.S. Circuit Court Finds Operator of Affiliate Marketing Network Responsible for Deceptive Third-Party Claims Made for Lean-Spa Weight-Loss Supplement*, FED. TRADE COMM'N (Oct. 4, 2016), <https://www.ftc.gov/news-events/press-releases/2016/10/us-circuit-court-finds-operator-affiliate-marketing-network>.

<sup>15</sup> Fed. Trade Comm'n, *Guides Concerning the Use of Endorsements and Testimonials in Advertising*, 85 Fed. Reg. 10104 (Feb. 21, 2020), <https://www.federalregister.gov/documents/2020/02/21/2020-03447/guides-concerning-the-use-of-endorsements-and-testimonials-in-advertising>.

<sup>16</sup> *The FTC's Endorsement Guides: What People are Asking*, FED. TRADE COMM'N (last updated Sept. 2017), <https://www.ftc.gov/tips-advice/business-center/guidance/ftcs-endorsement-guides-what-people-are-asking>.

<sup>17</sup> *FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, FED. TRADE COMM'N (Jul. 24, 2019), <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions>.

Finally, while interoperability mandates may in some cases be appropriate to ensure that consumers have choices in providers and how to communicate, we would be deeply skeptical of proposals that would mandate providing competitors access to consumer data simply in order to allow them to improve their own products and services.<sup>18</sup> Consumers make decisions about the companies with whom to trust their personal information. The conceit that other companies should be entitled to that data in order to develop their own products is anathema to privacy values and consumer autonomy. In many cases, the competitive edge afforded by access to data may be overblown: often the marginal returns of data decrease rapidly, suggesting that having ever-increasing stores of data may not in reality be all that advantageous for various tasks.<sup>19</sup> While some Big Data enthusiasts have previously suggested that the massive amounts of data generated in the modern age will render scientific theory and analysis obsolete,<sup>20</sup> in reality, differentiating between signal and noise is a nontrivial task that may be rendered more difficult when combining different data sets, each of which may contain their own errors and biases.

The appropriate remedy to companies like Google and Facebook having access to too much personal data is not to franchise that extremely detailed and sensitive data set to any data broker who wants it: rather, it is to rein in Google's and Facebook's own collection and use of personal information. They are — by far — the biggest harvesters of third-party data by virtue of being embedded into a huge number of other companies' websites and mobile applications.<sup>21</sup> Privacy law should strictly constrain their ability to access and use that data. Privacy law should also limit the collection and use of first-party data as well: where a product functions merely as a platform allowing a consumer to communicate with others and access others' content, in many cases those

---

<sup>18</sup> Steve Lohr, *How Should Big Tech Be Reined In? Here Are 4 Prominent Ideas*, N.Y. TIMES (Aug. 20, 2019), <https://www.nytimes.com/2019/08/20/technology/big-tech-reined-in.html> (see "Unlock the Data"); *Stigler Committee on Digital Platforms Final Report*, CHICAGO BOOTH/STIGLER CTR FOR THE STUDY OF THE ECONOMY AND THE STATE at 276 (2019), <https://www.publicknowledge.org/wp-content/uploads/2019/09/Stigler-Committee-on-Digital-Platforms-Final-Report.pdf>.

<sup>19</sup> Pilászy, István & Tikk, Domonkos. (2009). Recommending new movies: Even a few ratings are more valuable than metadata, Conference: PROCEEDINGS OF THE 2009 ACM CONFERENCE ON RECOMMENDER SYSTEMS at RecSys 2009, New York, NY, USA, October 23-25, 2009, [https://www.researchgate.net/publication/221141047\\_Recommending\\_new\\_movies\\_Even\\_a\\_few\\_ratings\\_are\\_more\\_valuable\\_than\\_metadata#:~:text=Recommending%20new%20movies%3A%20Even%20a%20few%20ratings%20are%20more%20valuable%20than%20metadata,-Conference%20Paper%20](https://www.researchgate.net/publication/221141047_Recommending_new_movies_Even_a_few_ratings_are_more_valuable_than_metadata#:~:text=Recommending%20new%20movies%3A%20Even%20a%20few%20ratings%20are%20more%20valuable%20than%20metadata,-Conference%20Paper%20).

<sup>20</sup> Chris Anderson, *The End of Theory: The Data Deluge Makes the Scientific Method Obsolete*, WIRED Jun 23, 2008), <https://www.wired.com/2008/06/pb-theory/>.

<sup>21</sup> Steven Englehardt and Arvind Narayanan, *Online Tracking: A 1-million-site Measurement and Analysis*, CCS '16 PROCEEDINGS OF THE 2016 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY at 5.1 (Oct. 2016), [https://www.cs.princeton.edu/~arvindn/publications/OpenWPM\\_1\\_million\\_site\\_tracking\\_measurement.pdf](https://www.cs.princeton.edu/~arvindn/publications/OpenWPM_1_million_site_tracking_measurement.pdf)



companies should be prohibited from monitoring or monetizing those communications.<sup>22</sup> To the extent that their position as a platform gives them privileged insight into competitors' products, the law should constrain their use of that information to gain an unfair competitive advantage as well.<sup>23</sup>

Finally, antitrust agencies have been unduly lax in investigating large internet companies' many acquisitions — both acquisitions in adjacent vertical markets and acquisitions of potential horizontal competitors. These agencies should retrospectively revisit the competitive effects of those acquisitions<sup>24</sup> — including the competitive effects that flow from privacy implications from merged data sets — and where appropriate, seek relief to unwind the acquisition. Looking forward, antitrust enforcers must be more vigilant about acquisitions that could restrict choice or otherwise potentially harm competition and the benefits it creates for consumers.<sup>25</sup> Ultimately, the law needs to be revised to strengthen the ability to stop harmful acquisitions — starting with switching the burden of proof so that the largest platform giants must satisfactorily demonstrate that a proposed acquisition would *not* be anticompetitive.<sup>26</sup>

---

<sup>22</sup> *VIZIO to Pay \$2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent*, FED. TRADE COMM'N (Feb. 6, 2017), <https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it>; Fed. Commc'ns Comm'n, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, FCC 16-148 (Nov. 2, 2016), <https://www.fcc.gov/document/fcc-releases-rules-protect-broadband-consumer-privacy>; 35-A MRSA c. 94, <http://www.mainelegislature.org/legis/bills/getPDF.asp?paper=SP0275&item=9&snum=129>.

<sup>23</sup> Tony Romm, *Amazon, Apple, Facebook and Google Grilled on Capitol Hill Over their Market Power*, WASH. POST (Jul. 29, 2020), <https://www.washingtonpost.com/technology/2020/07/29/apple-google-facebook-amazon-congress-hearing/>; Comments of Consumers Union, *Antitrust and Competition Issues Hearings on Competition & Consumer Protection in the 21st Century*, Fed. Trade Comm'n at 6 (Aug. 20, 2018), [https://www.ftc.gov/system/files/documents/public\\_comments/2018/08/ftc-2018-0048-d-0069-155227.pdf](https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0048-d-0069-155227.pdf); Harold Feld, *Part IV: What Would Real Platform CPNI Look Like?*, Public Knowledge (Jul. 30, 2018), <https://www.publicknowledge.org/blog/part-iv-what-would-real-platform-cpni-look-like/>.

<sup>24</sup> Rebecca Slaughter, *Merger Retrospective Lessons from Mr. Rogers*, Hearings on Competition and Consumer Protection in the 21st Century: Merger Retrospectives (Apr. 12, 2019), [https://www.ftc.gov/system/files/documents/public\\_statements/1513758/slaughter\\_remarks\\_at\\_ftc\\_retrospectives\\_hearing\\_4-12-19.pdf](https://www.ftc.gov/system/files/documents/public_statements/1513758/slaughter_remarks_at_ftc_retrospectives_hearing_4-12-19.pdf)

<sup>25</sup> Consumer Reports letter to Attorney General Barr, *Re: Google-Fitbit Investigation* (Jun. 29, 2020), <https://advocacy.consumerreports.org/wp-content/uploads/2020/06/Google-Fitbit-CR-letter-to-DOJ-6-29-20-FINAL.pdf>.

<sup>26</sup> Consumer Reports letter to Chair Mike Lee and Ranking Member Klobuchar, Subcommittee on Antitrust, Competition Policy, and Consumer Rights, Committee on the Judiciary, United States Senate, *Re: March 10 Hearing on Competition in Digital Technology Markets: Examining Self Preferencing by Digital Platforms* (Mar. 24, 2020), <https://advocacy.consumerreports.org/wp-content/uploads/2020/03/Sen-Judiciary-online-platforms-self-preferencing-CR-letter-3-24-20-FINAL.pdf>.

Thank you very much for instituting this proceeding and for considering our feedback on these important policy issues. Please contact us if there is anything we can do to support your efforts.

Respectfully submitted,

Justin Brookman  
Director of Privacy and Technology Policy

Maureen Mahoney  
Policy Analyst

George Slover  
Senior Policy Counsel

Stephanie Nguyen  
Digital Standard Manager