Before the
National Telecommunications and Information Administration
Washington, DC 20230

In the Matter of	)	
	)	
Developing the Administration's	)	Docket No. 180821780–8780–01
Approach to Consumer Privacy	)	

COMMENTS OF NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE

November 9, 2018

Eric Null
Becky Chao
New America's Open Technology Institute
740 15th St NW, Suite 900
Washington, D.C. 20005

Introduction

New America's Open Technology Institute (OTI) files these comments in response to the National Telecommunications and Information Administration's (NTIA) Request for Comments on Developing the Administration's Approach to Consumer Privacy (RFC).[1] The desired outcome of the NTIA's proposal is a "reasonably informed user."[2]

OTI's comments will focus on two issues. First, data minimization, user controls, and strong enforcement should be central pillars of the NTIA's approach to consumer privacy. Data minimization provides many benefits to both users and companies. It reduces the amount of information companies have to convey to their users, it reduces risks associated with collecting and storing data including harms brought about by data breaches, and it reduces company costs associated with data processing. User controls are also necessary for "reasonably informed users" to control how their data is collected and used. And strong enforcement is necessary to ensure that companies have incentives to follow the law.

Second, some of the goals identified by the NTIA are contradictory or misplaced. Primarily, while the NTIA's proposal focuses on a comprehensive approach that would apply to all sectors, it should allow for different requirements for broadband providers—there are salient differences between broadband providers and online companies that necessitates a different approach. Moreover, the idea of creating legal clarity through an outcomes-based approach is difficult because focusing on outcomes necessarily requires leaving substantial room for interpretation of the law.

I. Data minimization, user controls, and strong enforcement should be central to any approach to consumer privacy.

The NTIA proposes seven different "outcomes" for a consumer privacy regime, with the ultimate "outcome" being a "reasonably informed user."[3] These seven outcomes are transparency, control, reasonable minimization, security, access and correction, risk management, and accountability. These outcomes are laudable, and each should play a role in the NTIA's regime. Some of the outcomes, however, require more emphasis. The NTIA's regime should place heavy focus on data minimization, user access and ability to correct *or delete* information, and robust enforcement of the law.[4]

A. Data minimization provides many benefits to users and companies.

To achieve the goal of a reasonably informed user, data minimization (the practice of reducing the total amount of data collected, used, and stored) *must* play a prominent role in any

[1] 83 Fed. Reg. 48600 (Sept. 26, 2018) ("RFC").
[2] *Id.*
[3] *Id.*
[4] These principles are included in the Public Interest Privacy Legislation Principles, submitted with these comments.

consumer privacy regime. The federal notice-and-consent privacy regime has, for two decades, placed the primary privacy burden on users—companies set their own policies and users have to determine their willingness to agree to long, legalistic privacy policies they often do not read. Companies should start minimizing the data they collect and justify why they collect that data and how they use it.

Data minimization has several benefits. For one, it reduces the amount of information a company has to convey to its users. Users can only read, understand, and internalize so much information about data practices at a time. Already, our privacy regime (incorrectly) assumes that users read privacy policies, something the NTIA criticizes.[5] Further, a Deloitte survey found that 91% of consumers consent to legal terms and services without reading them.[6] If the NTIA truly wants users to be informed, and indeed, if *users* want to be informed, the amount of information they have to absorb must be reduced.[7] Minimizing the data collected, and minimizing its uses, would lead to such a reduction.

Second, data minimization reduces the risks associated with data collection and storage, such as data breaches and other unauthorized access.[8] As the IAPP has stated, "we are all suffering from data overload" and "more data means more problems; the hackers and data thieves couldn't be happier."[9] Further, "[t]he value of data decreases very quickly, and storing it 'just in case' is a dangerous path."[10] Data breaches can be ruinous for companies, and the more data companies have on their users, the higher the likelihood that they will be a target and that a breach would have catastrophic consequences.[11]

Third, data minimization reduces costs for companies that no longer have to maintain such extensive data collection and storage systems.[12] Collecting, storing, and using data is costly.[13] And sifting through large amounts of data to find the needle in the haystack can increase costs as well: "the dangers of data hoarding are similar to those of physical hoarding: mounds of

---

[5] RFC at 48600 ("In many cases, lengthy notices describing a company's privacy program at a consumer's initial point of interaction with a product or service does not lead to adequate understanding.").
[6] Caroline Cakebread, *You're not alone, no one reads terms of service agreements*, Business Insider (Nov. 15, 2017), https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11.
[7] Currently, if users want to stay informed about their privacy choices, it could take up to 304 hours per year of time to read those policies. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf (at 17).
[8] *See* FTC Staff Report: Internet of Things: Privacy & Security in a Connected World, Federal Trade Commission (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (at IV).
[9] Reducing Risk Through Data Minimization, International Association of Privacy Professionals, https://iapp.org/resources/article/reducing-risk-through-data-minimization.
[10] Bernard Marr, *Why Data Minimization is an Important Concept in the Age of Big Data*, Forbes (Mar. 16, 2016), https://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-age-of-big-data/#7bd907211da4.
[11] *Id.*
[12] *Id.*
[13] Shantha Kumari, *Data Minimization in the Age of Big Data!*, Sysfore Blog (Apr. 22, 2016), https://blog.sysfore.com/data-minimization-in-the-age-of-big-data.

useless junk that make it very difficult to find what we need when we need it. It costs money and time...."[14] Processing less data means reducing spending on processing data.

As a result of these benefits, minimizing data collection, use, and storage will likely increase trust between users and companies, to the benefit of both.

B. Users must be able to control the data companies have about them.

A reasonably informed user is essentially powerless without easy-to-use, easy-to-find controls, and the ability to access, correct, and delete information that a company has on them. These user controls must include broad access to data portability and platform interoperability tools. Without these controls, efforts to streamline notice would be for naught.

1. Users want more control over the data they provide companies.

Consumers have lost control over their data, but they want more control.[15] According to a PwC survey conducted in 2017, 92% of consumers in the U.S. believe they should be able to control the information available about them on the internet, but only 10% feel they have complete control over their personal information.[16] Further, consumers have growing anxiety over data privacy and security. A survey by the Harris Poll on behalf of IBM conducted in March 2018 found that 85 percent of consumers think businesses should be doing more to actively protect their data, and that 73 percent believe businesses are focused on profits over consumers' security needs.[17] And 7 out of 10 survey respondents think that government intervention is appropriate given that businesses have not been able to do enough.[18]

Consumers are skeptical of companies' ability to protect their data. For an overwhelming majority of consumers (88%), the extent to which they are willing to share personal information depends on how much they trust a given company.[19] Nearly the same number (87%) state that they will take their business elsewhere if they do not trust that a company is handling their data responsibly.[20] And over half of consumers have stated that if given the option, they would make an effort to get their personal information back from a company.[21]

---

[14] Bernard Marr, *Why Data Minimization is an Important Concept in the Age of Big Data*, Forbes (March 16, 2016), https://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-age-of-big-data/#7bd907211da4.
[15] Comments of OTI in FCC Broadband Privacy proceeding, at 21-27, https://ecfsapi.fcc.gov/file/10707717014775/2016-07-06%20-%20OTI%20Broadband%20Privacy%20Reply%20Comments%20FINAL.pdf.
[16] Consumer Intelligence Series: Protect.me, PwC, https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/cybersecurity-protect-me.html.
[17] IBM Cybersecurity and Privacy Research, The Harris Poll (Apr. 13, 2018), https://newsroom.ibm.com/Cybersecurity-and-Privacy-Research.
[18] *Id.*
[19] Consumer Intelligence Series: Protect.me, PwC, https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/cybersecurity-protect-me.html.
[20] *Id.*
[21] *Id.*

Thus, users want more and better controls over data, and they should have the ability to access, correct, and delete data about them. The NTIA's framework should account for those desires and expectations.

2. Data portability and platform interoperability should be part of any privacy approach.

The NTIA overlooks data portability and platform interoperability, which are both critical to ensuring that consumers have control over their data. Over the past several years, we have seen private companies trend toward locking down their data rather than opening it up. This provides tech companies the ability to further entrench themselves in the market by making it harder for consumers to switch services or leverage their own data elsewhere. But to improve the competitive landscape, the NTIA should work toward creating opportunities for data portability and platform interoperability.[22]

C. Companies must be held accountable for privacy violations.

Companies should be held accountable for their privacy transgressions. Without accountability, any privacy regime falls apart because there are essentially no consequences for violating the standards or rules put in place. Users need more, not less, enforcement.[23] When companies know that they can get away with violating the rules without punitive action, there is no deterrent. The Federal Trade Commission (FTC) should be emboldened to seek civil penalties for privacy and data security violations in the first instance, and it should be provided more resources to accomplish its mission.[24] State attorneys general, who play an extremely important role in protecting user privacy,[25] must continue to be empowered to enforce their laws against transgressors. The NTIA can help push for increased enforcement by pushing for federal legislation.

Further, all enforcers should work coextensively and concurrently to ensure the maximum privacy protections. Agencies at the federal level, like the NTIA and FTC, should coordinate with each other on enforcement and identify ways to strengthen privacy protections. Federal agencies should also work with state attorneys general to offer guidance and aid where possible.

---

[22] *See* Comments of New America's Open Technology Institute, In the Matter of Competition and Consumer Protection in the 21st Century: The Intersection Between Privacy, Big Data, and Competition (filed Aug. 20 2018) (submitted with these comments).

[23] *Consumer Data Privacy: Examining the European Union's General Data Protection Regulation and the California Consumer Privacy Act*, Hearing before the Senate Committee on Commerce, Science, and Technology (Oct. 10, 2018), Testimony of Laura Moy, https://perma.cc/3HDL-9ZY5 (at 10-14).

[24] Current FTC Chair Joseph Simons has discussed the limits of Section 5 of the FTC Act, particularly that it does not provide for civil penalties, in capturing all privacy and data security concerns in testimony before the House Committee on Energy and Commerce in a hearing on Oversight of the Federal Trade Commission on July 18, 2018.

[25] Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 91 Notre Dame Law Review 747 (Feb. 16, 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2733297.

II. The goals identified by the NTIA are laudable, but some of them are contradictory or misplaced.

The NTIA's stated goals are laudable. However, at least two are either contradictory or misplaced: first, the NTIA should allow for separate rules for broadband providers and online companies; and two, the NTIA overemphasizes harmonizing the state and federal regulatory landscape.

A. The NTIA's regime should allow for separate rules for broadband providers and other online companies

The NTIA praises the sectoral approach that has developed in the U.S. over the past several decades, yet also argues that any regime should apply to all entities that are not covered by the current sectoral approach. The NTIA claims that the regime should, instead, account for any particularized differences in the *application* of the policies, not in the rules themselves. This approach unfortunately is not likely to be sufficient for differentiating between broadband providers and online content providers.

Broadband providers are different. The broadband provider versus online company debate played out at the Federal Communications Commission (FCC), while the agency and the public deliberated over broadband privacy.[26] Broadband providers are sufficiently different to merit privacy rules tailored to them, and the law itself established network providers as a separate sector deserving of its own privacy rules.[27] Among the reasons they deserve their own privacy rules is that they have nearly comprehensive access to all traffic that flows over their networks including, in some cases, content. Broadband providers routinely collect data on users' geo-location, web browsing and app usage history, and more.[28] The risks of misusing this data are enormous: they can be used for aggressive product marketing and exploited by identity thieves, for example.[29] Broadband customers generally cannot refuse to provide data to their providers because it is needed to provide the service. Further, broadband providers are third parties to communications between a user and the content they seek online, making privacy violations by their broadband providers based on their control over the infrastructure unexpected and unreasonable.

[26] *See* Comments of New America's Open Technology Institute in FCC Broadband Privacy proceeding, at 3-11, https://ecfsapi.fcc.gov/file/60002081381.pdf.
[27] *See* 47 U.S.C. §222.
[28] Broadband Privacy: What Consumers Need to Know, Consumers Union (Sept. 20, 2017), https://consumersunion.org/research/broadband-privacy-what-consumers-need-to-know.
[29] *Id*.

The FCC has long imposed privacy obligations on telephone providers,[30] and it is even more important to impose privacy rules on broadband providers that reflect their vital role in providing internet access to hundreds of millions of Americans.

B. An outcomes-based proposal would not provide enough clarity for online companies, particularly small businesses, to comply with the law.

An outcome-based approach to privacy would leave online companies with insufficient guidance on how best to comply with the law. Any flexibility for companies would only be marginal, as companies would have difficulty determining what actions and processes compliance requires. The lack of clear, prescriptive rules disproportionately burdens small businesses, and stifles innovation from these smaller firms. This ambiguity would also make it harder for enforcers to determine whether a company has violated the law, and would likely create an unpredictable regulatory regime. Ultimately, an outcome-based approach inadequately protects users, and undermines the system of accountability it seeks to create.

1. An outcome-based approach creates too much ambiguity, leading to insufficient protections and an unpredictable enforcement regime

On its surface, an outcome-based approach may provide more flexibility for companies to determine how best to comply with the goals laid out by the law. However, this flexibility is not only overstated, but it also leaves inadequate protections for users. Without prescriptive rules that enable companies to apply clear, formulated instructions to their particular circumstances, regulated companies cannot easily determine what the law requires.[31] Furthermore, the flexibility of a principles-based approach would enable some firms to "backslide" and get away with the minimum level of compliance possible.[32] The lack of certainty therefore undermines the protections and accountability that the laws seek to ensure.[33]

Moreover, the ambiguity also generates problems for enforcers by creating an unclear regulatory regime.[34] Whereas prescriptive rules provide enforcers with a more straightforward roadmap for determining whether a company has violated the law, an outcomes-based approach makes it difficult for enforcement agencies to determine which processes violate the laws in question *and* enable them act retrospectively.[35]

---

[30] *See* Protecting Your Privacy: Phone and Cable Records, Federal Communications Commission, https://www.fcc.gov/consumers/guides/protecting-your-privacy.
[31] Christopher Decker, *Goals-Based and Rules-Based Approaches to Regulation*, Department for Business, Energy & Industrial Strategy BEIS Research Paper Number 8 (May 2018).
[32] Julia Black, Presentation: *Principles based regulation: risks, challenges and opportunities*, Banco Court, Sydney (March 27, 2007), http://eprints.lse.ac.uk/62814/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_Black%2C%20J_Principles%20based%20regulation_Black_Principles%20based%20regulation_2015.pdf.
[33] *Id.*
[34] *Id.*
[35] *Id.*

2. The lack of clear rules would stifle innovation from small businesses

An outcome-based approach particularly burdens small businesses. Small businesses are constrained by resources much more than incumbent firms. For small businesses to invest the time and capital in interpreting the principles and compliance exacerbates their resource allocation problem much more than for bigger, more established firms that are better equipped with the resources to comply. Small businesses would disproportionately invest more resources into compliance.[36] This process not only detracts from resources they could've otherwise invested in innovation, but also deters small businesses from further investment and innovation.[37]

Stating that small businesses would not likely be targeted for enforcement actions is not the solution. Instead, small businesses must be subject to enforcement, but the rules must be clear and easy to follow. As President and CEO of the Center for Democracy and Technology Nuala O'Connor testified before the U.S. Senate Committee on Commerce, Science, and Technology in October 2018, implementing clear rules "favors … small and start up businesses over incumbents, or at least levels the playing field…. A clear, simple standard for U.S. companies to know what they are allowed to do with our … personal data ... is a good move."[38] Clear rules will better support small businesses because those businesses can more efficiently engineer their products and services to comply with those rules.

Conclusion

OTI commends the NTIA on proposing a high-level privacy regime. While the proposal covers a lot of issues, several issues still need to be addressed. OTI looks forward to working with the NTIA on its proposal.

---

[36] *See* Sean Hackbarth, *How Regulations at Every Level Hold Back Small Business*, U.S. Chamber of Commerce (Mar. 28, 2017), https://www.uschamber.com/series/above-the-fold/how-regulations-every-level-hold-back-small-business ("The costs [of federal regulations] to smaller businesses with 50 employees or fewer are nearly 20% higher than the average for all firms.")

[37] *See* Robb Mandelbaum, *The $83,000 Question: How Much Do Regulations Really Cost Small Businesses?*, Forbes (Jan. 24, 2017), https://www.forbes.com/sites/robbmandelbaum/2017/01/24/the-83000-question-how-much-do-regulations-really-cost-small-business/#5572ff5f1b25. ("About 40 percent of respondents claim that they have held off making a new investment because of a regulation at some point in the past.")

[38] *Consumer Data Privacy: Examining the European Union's General Data Protection Regulation and the California Consumer Privacy Act*, Hearing before the Senate Committee on Commerce, Science, and Technology (Oct. 10, 2018) (Testimony of Nuala O'Connor), https://www.c-span.org/video/?452550-1/senate-panel-data-privacy-protection#&start=6053.

Public Interest Privacy Legislation Principles

Unregulated data collection and use in the United States has eroded public trust in companies to safeguard and use data responsibly. Surveys show that, while individuals often try to remove or mask their digital footprints,[1] people think they lack control over their data,[2] want government to do more to protect them,[3] and distrust social media platforms.[4]

The current U.S. data privacy regime, premised largely upon voluntary industry self-regulation, is a failure. Irresponsible data practices lead to a broad range of harms, including discrimination in employment, health care, and advertising, data breaches, and loss of individuals' control over personal information. Existing enforcement mechanisms fail to hold data processors accountable and provide little-to-no relief for privacy violations.

The public needs and deserves strong and comprehensive federal legislation to protect their privacy and afford meaningful redress. Privacy legislation is essential to ensure basic fairness, prevent discrimination, advance equal opportunity, protect free expression, and facilitate trust between the public and companies that collect their personal data. Legislation should reflect at least the following ideas and principles:

1. Privacy protections must be strong, meaningful, and comprehensive

Privacy concerns cannot be fully addressed by protecting only certain classes of personal data held by some companies. Legislation should mandate fairness in all personal data processing, respect individuals' expectations for how data should be treated, provide for data portability, and include safeguards against misuse of data, including de-identified and aggregate data. Legislation should advance fundamental privacy rights and require all entities that collect, store, use, generate, share, or sell (collectively, "process") data both online and offline to comply with Fair Information Practices[5] (collection limitation, data

---

[1] *The State of Privacy in Post-Snowden America*, Pew (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america.
[2] Bree Fowler, *Americans Want More Say in the Privacy of Personal Data*, Consumer Reports (May 18, 2017), https://www.consumerreports.org/privacy/americans-want-more-say-in-privacy-of-personal-data.
[3] Lee Rainie, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, Pew (Mar. 27, 2018), http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns.
[4] *Id.*
[5] Fair Information Practices are similar to those adopted by the OECD. *See* OECD Privacy Framework, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

quality, purpose specification, use limitation, security safeguards, openness, access and correction rights, and accountability) across the complete life cycle of the data. Legislation should require all data processing to be clearly and accurately explained, justified, and authorized by the individual. People should have the right to know when their data has been compromised or otherwise breached. Additionally, legislation should require entities processing data to adopt technical and organizational measures to meet these obligations, including risk assessments of high-risk data processing.

2. Data practices must protect civil rights, prevent unlawful discrimination, and advance equal opportunity

Legislation should ensure fundamental fairness of and transparency regarding automated decision-making. Automated decision-making, including in areas such as housing, employment, health, education, and lending, must be judged by its possible and actual impact on real people, must operate fairly for all communities, and must protect the interests of the disadvantaged and classes protected under anti-discrimination laws. Legislation must ensure that regulators are empowered to prevent or stop harmful action, require appropriate algorithmic accountability, and create avenues for individuals to access information necessary to prove claims of discrimination. Legislation must further prevent processing of data to discriminate unfairly against marginalized populations (including women, people of color, the formerly incarcerated, immigrants, religious minorities, the LGBTQIA/+ communities, the elderly, people with disabilities, low-income individuals, and young people) or to target marginalized populations for such activities as manipulative or predatory marketing practices. Anti-discrimination provisions, however, must allow actors to further equal opportunity in housing, education, and employment by targeting underrepresented populations where consistent with civil rights laws. Moreover, decades of civil rights law have promoted equal opportunity in brick-and-mortar commerce; legislation must protect equal opportunity in online commerce as well.

3. Governments at all levels should play a role in protecting and enforcing privacy rights

The public consistently call for government to do more, not less, to protect them from misuse of their data. Legislation should reflect that expectation by providing for robust agency oversight, including enhanced rulemaking authority, commensurate staff and resources, and improved enforcement tools. Moreover, no single agency should be expected to police all data processors; therefore, legislation should empower state attorneys general and private citizens to pursue legal remedies, should prohibit forced arbitration, and importantly, should not preempt states or localities from passing laws that establish stronger protections that do not disadvantage marginalized communities.

4. Legislation should provide redress for privacy violations

Individuals are harmed when their private data is used or shared in unknown, unexpected, and impermissible ways. Privacy violations can lead to clear and provable financial injury, but even when they do not, they may, for example, cause emotional or reputational harm; limit awareness of and access to opportunities; increase the risk of suffering future harms; exacerbate informational disparities and lead to unfair price discrimination; or contribute to the erosion of trust and freedom of expression in society. In recognition of the many ways in which privacy violations are and can be harmful, legislation should avoid requiring a showing of a monetary loss or other tangible harm and should make clear that the invasion of privacy itself is a concrete and individualized injury. Further, it should require companies to notify users in a timely fashion of data breaches and should make whole people whose data is compromised or breached.

Signed,

Access Humboldt
Access Now
Berkeley Media Studies Group
Campaign for a Commercial-Free Childhood
Center for Democracy & Technology
Center for Digital Democracy
Center for Media Justice
Center on Privacy & Technology at Georgetown Law
Color of Change
Common Cause
Common Sense Kids Action
Consumer Action
Consumer Federation of America
Consumers Union
Customer Commons
Demand Progress
Free Press Action Fund
Human Rights Watch
Lawyers' Committee for Civil Rights Under Law
Media Alliance
Media Mobilizing Project
National Association of Consumer Advocates
National Consumer Law Center
National Consumers League
National Digital Inclusion Alliance
National Hispanic Media Coalition
New America's Open Technology Institute
Oakland Privacy
Open MIC (Open Media and Information Companies Initiative)
Privacy Rights Clearinghouse
Public Citizen
Public Knowledge
U.S. PIRG
United Church of Christ, OC Inc.

Before the
Federal Trade Commission
Washington, DC 20580

In the Matter of	)
	)
Competition and Consumer Protection in	)
The 21st Century: The Intersection Between	)
Privacy, Big Data, and Competition	)

COMMENTS OF NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE

August 20, 2018

Kevin Bankston
Eric Null
Ross Schulman
New America's Open Technology Institute
740 15th St NW Suite 900
Washington, D.C. 20005

At the intersection between privacy, big data, and competition (comment topic #4) lies the issue of data portability. New America's Open Technology Institute (OTI) submits these comments to highlight the importance of data portability to online consumers, identify some of the hardest questions around how best to implement meaningful data portability for those consumers, and urge the Federal Trade Commission (FTC) to promote data portability as a critical feature of a competitive internet environment while using its expertise and authority to help address some of those difficult questions. As both the FTC and Congress engage in much-needed efforts to enhance the privacy and security of our personal data, policymakers must simultaneously seek to ensure that consumers' control over their data is also strengthened through broad access to data portability tools and interoperable services. Otherwise, attempts to rein in tech giants' privacy practices may have the unintended effect of locking in their dominance by making it harder for consumers to switch services or leverage their own data elsewhere. Giving consumers real control over their data requires both privacy *and* portability.

I. Consumers Need Meaningful Data Portability

In the wake of the recent privacy controversy over Facebook and Cambridge Analytica,[1] as many users of the social network have considered whether to #DeleteFacebook and spend their time on other social networks instead, consumers and policymakers have had a lot of questions on the topic of data portability: Is my social network data really mine? Can I download it and take it with me to another platform if I'm unhappy with my current platform? What counts as my data that I should be able to download or share, and as my friends' data that I shouldn't? Can I move my network of friends with me to another service or will I have to rebuild it again? Should I even bother to try? Will any other service ever have as many of my friends on it as Facebook does, or are the network effects of Facebook having 2+ billion users—including most of my friends and family—so strong that other services are unlikely to be able to compete? What choices do I as a social network user really have?

Put another way, those inquisitive policymakers and users have been weighing the substantial *switching costs* of moving to another service, often after having spent years on Facebook curating their personal networks, posting content and commenting on others' posts, uploading and tagging photos, and communicating with their friends via direct messages. They are looking hopefully toward data portability as a way to possibly reduce those costs rather than having to abandon their digital life on Facebook and build a whole new digital life elsewhere.

Consequently, there is a growing consensus that being able to easily move your data between different online services (data portability), including being able to interact and communicate between different platforms in an ongoing way (interoperability), is necessary both to respect users' rights in regard to their own data, and to promote competition online and enable

[1] Will Oremus, *The Real Scandal Isn't What Cambridge Analytica Did*, Slate (Mar. 20, 2018), https://slate.com/technology/2018/03/the-real-scandal-isnt-cambridge-analytica-its-facebooks-whole-business-model.html.

new services to emerge.[2] For example, Congressman David Cicilline—the Ranking Member of the House Judiciary Committee's Antitrust Subcommittee—highlighted in a recent keynote address how "[p]eople who may want to leave Facebook are less likely to do so if they aren't able to seamlessly rebuild their network of contacts, photos, and other social graph data on a competing service or communicate across services."[3] Just as Congress gave cellphone users the right to "number portability"—lessening the switching cost of changing your cell carrier by giving you the ability to take your phone number with you—Cicilline argued that social network users should have the right to portability of their social media data. "We need pro-competitive policies that give power back to Americans in the form of more rights and greater control over their data," Cicilline continued, echoing an op-ed he had recently co-authored with then-FTC Commissioner Terrell McSweeny.[4] "This starts by taking on walled gardens that block startups and other competitors from entering the market through high switching costs."

However, the question of how best to ensure meaningful data portability and interoperability raises in turn some difficult technical and policy questions about how to balance users' rights to move and use their data on other services with their friends' privacy interests—and how to guarantee that new privacy efforts don't have the unintended consequence of locking in current platforms' dominance by locking down their control over our data.

II. Tech Companies Have Made Progress Toward Basic Data Portability

When it comes to offering basic portability of data that users themselves have uploaded to a service, a great deal of progress has already been made. For example, since 2010 Facebook has offered users the ability to download a browse-able archive containing their profile information, a list of their friends, all of their wall posts, photos, videos, messages and more, via its "Download Your Information" tool.[5] Similarly, since 2011, Google has offered an even wider range of data to download, in a wider range of formats reflecting its wider range of service offerings, through its own "Download Your Data" tool (formerly "Google Takeout").[6] Twitter, too, offers a tool for users to download all of their past tweets and attached media.[7] And now, thanks to Article 20 of the General Data Protection Regulation (GDPR), Europeans have an

[2] For a simple technical introduction to data portability and interoperability, and basic definitions of some of the terms used here, see Ross Schulman, *A Tech Intro to Data Portability*, New America Weekly, https://www.newamerica.org/oti/blog/tech-intro-data-portability.
[3] *A Deep Dive Into Data Portability*, New America (June 6, 2018), https://www.newamerica.org/oti/events/deep-dive-data-portability-how-can-we-enable-platform-competition-and-protect-privacy-same-time.
[4] David N. Cicilline & Terrell McSweeny, *Competition Is at the Heart of Facebook's Privacy Problem*, Wired (Apr. 24, 2018), https://www.wired.com/story/competition-is-at-the-heart-of-facebooks-privacy-problem.
[5] Alexia Tsotis, *Facebook Now Allows You to Download Your Information*, TechCrunch (Oct. 6, 2010); https://techcrunch.com/2010/10/06/facebook-now-allows-you-to-download-your-information/; Accessing & Downloading Your Information, Facebook, https://www.facebook.com/help/1701730696756992.
[6] Erick Schonfeld, *Google Takeout, An Easier Way to Take Your Data With You*, TechCrunch (June 30, 2011), https://techcrunch.com/2011/06/30/google-takeout/; Download Your Data, Google Account Help, https://support.google.com/accounts/answer/3024190?hl=en.
[7] How to Download Your Twitter Archive, Twitter Help Center, https://help.twitter.com/en/managing-your-account/how-to-download-your-twitter-archive.

explicit legal right to such portability. Specifically, they have a right to receive the data they have previously provided to a data controller, in a commonly-used, machine-readable format, and to transmit that data to a different service without hindrance.[8]

Due in part to this new legal requirement, internet companies have recently been taking new steps to broaden their portability offerings, and better optimize them for providing data in formats suited to porting to another service.[9] For example, Facebook now allows users to download their data in the structured JSON data format instead of in unstructured HTML that was designed for personal archiving and viewing rather than portability, hopefully making it easier to move the data between different services.[10] Notably, that tool has gotten a lot of use since the Cambridge Analytica scandal, with countless news features pointing to it as a way to retrieve your data before quitting the service, or to simply get a better idea of how much data Facebook stores about you.[11]

While these tools have provided users the much-appreciated and increasingly popular ability to download and peruse archives of their data, they have not yet enabled a great deal of active porting of that data between services. The greatest obstacle to these download-your-data offerings serving the purpose of transitioning to another service is reflected in their very names: the simple requirement that users must first *download* their data, and then manually upload it into whatever service they want to move it to, is a serious barrier, because such a two-step process requires significant time, technical knowledge, and bandwidth. And, in a classic chicken-and-egg problem, most services have not created new and easy means for users to manually bulk-upload their data from other services.

Google and Microsoft have recently sought to address this problem by launching the Data Transfer Project, an open source software project that now counts Facebook and Twitter as contributors.[12] The goal of that project is to establish a common framework for easily moving data directly between services with just a few clicks and without having to download the data

---

[8] Right to Data Portability, GDPR Info, https://gdpr-info.eu/art-20-gdpr.

[9] *See, e.g.*, William Malcolm, *Our Preparations for Europe's New Data Protection Law*, Google Blog, https://blog.google/outreach-initiatives/public-policy/our-preparations-europes-new-data-protection-law (describing improvements to Google's portability offerings); Kate Conger, *How to Download Your Data with All the Fancy New GDPR Tools*, Gizmodo (May 25, 2018), https://gizmodo.com/how-to-download-your-data-with-all-the-fancy-new-gdpr-t-1826334079 (surveying post-GDPR portability offerings of multiple companies).

[10] Josh Constine, *A Flaw-by-Flaw Guide to Facebook's New GDPR Privacy Changes*, TechCrunch (Apr. 18, 2018), https://techcrunch.com/2018/04/17/facebook-gdpr-changes.

[11] *See, e.g.*, Jefferson Graham, *I Downloaded All My Facebook Data. This Is What I Learned*, USA Today (Mar. 30, 2018), https://www.usatoday.com/story/tech/talkingtech/2018/03/30/downloaded-all-my-facebook-data-what-learned/471787002/; Brian X. Chen, *I Downloaded All the Information that Facebook Has on Me. Yikes*, N.Y. Times (Apr. 11, 2018), https://www.nytimes.com/2018/04/11/technology/personaltech/i-downloaded-the-information-that-facebook-has-on-me-yikes.html; Abby Ohlheiser, *Here's How to Download All Your Data from Facebook. It Might Be a Wake-up Call*, Wash. Post (Mar. 27, 2018), https://www.washingtonpost.com/news/the-intersect/wp/2018/03/27/heres-how-to-download-all-your-data-from-facebook-it-might-be-a-wake-up-call.

[12] *Introducing the Data Transfer Project: An Open Source Platform Promoting Universal Data Portability*, Google Open Source Blog (July 20, 2018), https://opensource.googleblog.com/2018/07/introducing-data-transfer-project.html.

yourself, a framework that could accommodate both existing players and new entrants into the market. To start, that project will be focusing on what one might call the low-hanging fruit of data portability, where common data formats already exist and where there is less variation between services: e.g., enabling users to transfer their stored files between cloud storage services, emails between email providers, contact information between address books, photos between photo sites and social network services, etc.[13] These are the easier cases, where the files being moved clearly belong to the user, and the transfers are basically apples to apples transitions using mostly well-established common file formats, as opposed to trying to (e.g.) port long Facebook posts into the character-constrained Twitter format.

Merely addressing these less challenging use cases will likely be a major years-long project requiring a great deal of resources and dedication, but at least a fruitful path has been set, with GDPR as a strong spur to action. However, achieving meaningful portability that empowers users and ensures competition will also require grappling with much harder cases as well, most especially when it comes to the issue of privacy.

III. There Are Difficult Tensions Between Data Portability and Privacy That Must Be Balanced

In some cases, the question of whether I should be able to download a piece of data is clear. Is it my file or post? Did I create it? Did I upload it? Where the answers to these questions are yes, the answer of whether you can port it should also usually be yes. However, in the interactive sphere of the internet, there are many pieces of data that raise harder questions. I should probably be able to download my own photos, but what about tags to faces in those photos that other people added? Most services will now let you download your own social media posts, but what about other people's comments to those posts, or your comments and tags on other people's posts and photos? What about information from shared groups or message boards? What about shared documents and other collaboratively created content? These are just some of the examples of the unresolved tension between my right to portability and my friends' right to privacy, and nowhere is that tension greater than when it comes to the portability of information about your contacts on social networks, or your "social graph."

The need for social graph portability has been a common theme in the wealth of recent commentary on the importance of data portability, often with reference to cell phone number portability as a precedent. Policymakers,[14] tech journalists,[15] and digital rights groups[16] including

[13] Brian Willard *et al.*, *Data Transfer Project: From Theory to Practice*, Google (July 2018), https://services.google.com/fh/files/blogs/data-transfer-project-google-whitepaper-v4.pdf.
[14] David N. Cicilline & Terrell McSweeny, *Competition Is at the Heart of Facebook's Privacy Problem*, Wired (Apr. 24, 2018), https://www.wired.com/story/competition-is-at-the-heart-of-facebooks-privacy-problem.
[15] Josh Constine, *Facebook Shouldn't Block You from Finding Friends on Competitors*, TechCrunch (Apr. 13, 2018), https://techcrunch.com/2018/04/13/free-the-social-graph.
[16] Bennett Cyphers & Danny O'Brien, *Facing Facebook: Data Portability and Interoperability Are Anti-Monopoly Medicine*, EFF (July 24, 2018), https://www.eff.org/deeplinks/2018/07/facing-facebook-data-portability-and-interoperability-are-anti-monopoly-medicine.

OTI[17] have all called on Facebook, Twitter, and other social networks to "free the social graph" and make it easy to replicate our networks of friends and followers on other social services. However, meaningful social graph portability raises privacy issues that number portability did not. There, the issue was your own personal information, your telephone number, which—if you could keep it despite changing phone carriers—would maintain the social graph of people who knew to contact you there, rather than requiring you to recreate it by informing all of those people of your new number. Here, although the goal remains the same (reduce switching costs by maintaining your previous connections), portability of your social graph requires moving personal data about all of your friends that is sufficient to reliably re-identify and reconnect with them on another service. Your friends, however, may not want or expect you to move that data about them to another platform, or they may not have ever shared such contact details with you in the first place.

Take, for example, Facebook. The one thing you cannot download from Facebook is the one thing you would most need if you wanted to move to a competing social network: your friends' contact information, or any other unique information that would help you reconnect with them on another service. Instead, all you get is a list of their names, which is not very helpful for re-identifying specific individuals, considering how common many names are. This poses what might be the biggest switching cost of all: having to rebuild your network of hundreds or even thousands of contacts on another service, many of whom you may only be connected to online through Facebook and for whom you may lack any other contact information.

Indeed, this barrier to switching social networks may be why Facebook has long treated its possession of your friends' contact information as a key competitive advantage, making it difficult for users to collect or export it. For example, when users were first able to share an email address with friends on their profile page, it was displayed as a graphic rather than as text so that it could not be cut and pasted. Some users may also recall when Facebook, in 2012, temporarily replaced users' non-Facebook addresses with new "@facebook.com" addresses by default, making it harder to obtain off-Facebook contact information about your friends.[18] And although there is a hard-to-find setting where Facebook users can allow their friends to download their contact information, it is by default set not to allow such downloading—one of the rare Facebook settings that defaults away from, rather than toward, more sharing with friends.

Facebook has consistently justified its attempts to restrict sharing contact info as a privacy and security measure, but the alignment with its own business goals was always more than a little convenient. In addition, it is also rather ironic, considering that a huge part of Facebook's meteoric growth was driven by importing contact information from other services, especially Gmail (which led to a dispute between Google and Facebook back in 2010, when Google briefly cut off Facebook's ability to access Google contacts over its API because

[17] Kevin Bankston, *How We Can 'Free' Our Facebook Friends*, New America Weekly (June 28, 2018), https://www.newamerica.org/weekly/edition-211/how-we-can-free-our-facebook-friends.
[18] Josh Constine, *Facebook Hides Your Email Address Leaving Only @Facebook.com Visible. Undo This Poppycock Now*, TechCrunch (June 25, 2016), https://techcrunch.com/2012/06/25/facebook-email-address.

Facebook wasn't reciprocally allowing other services to access contact information on Facebook).[19]

Regardless of that history, Facebook's reticence to share contact information has only been bolstered by recent events: It was, of course, users' ability to export data about their friends to outside apps that was at the root of the Cambridge Analytica scandal that has put Facebook in the privacy hot-seat. Meanwhile, thanks to GDPR's privacy requirements, the representations Facebook has made through its privacy policies and privacy settings, and the requirements of its consent decree with the FTC, Facebook would now probably need to get affirmative consent from your friends before letting you export their email addresses, even if they arguably did not have to before.

Even if Facebook could allow you to export the contact data that your friends have shared with you, though, that still would not help mitigate the issue of friends who have chosen not to share their contact information on their profiles. Other social networks pose similar problems. For example, most Twitter bios do not contain enough contact information for you to reliably connect with the same person on another network. Furthermore, there is the question of whether that person wants to be re-identified on another network at all, especially if their anonymity on one network like Twitter might be compromised if their relationship with the moving user was revealed on another, non-anonymous network like Facebook.

Therefore, it is not sufficient to simply say "there should be social graph portability," because offering such portability will require answering the question of how best to provide such portability while also not violating privacy. There are no obvious or easy answers to that question. For example, social network providers could ask all users to give consent for their friends to export their contact information as part of their portability offering—or at least give friends the power to ask each other for that permission—but depending on how many choose to give that consent, it is likely to capture only a small portion of your contacts. Or, social network providers could allow users to download some other unique but less sensitive piece of a friend's data, like the URL of their Twitter profile, or their unique Facebook user ID number that is visible to anyone on Facebook who visits their profile. One could then upload that data to another service and automatically connect to others who have done the same and who have you in their list, and vice versa. However, even that may raise security concerns, making it trivially easy to "spoof" someone else's identity and automatically connect with that user's friends on another service, potentially revealing previously undisclosed relationships or identities.

Perhaps the most promising avenue for social graph portability would be for social network providers to allow the export of encrypted versions of your and your contacts' unique user IDs to obscure those IDs while also providing authentication, such that your relationships could only be automatically replicated on another service by your actual contacts, and only with consent from both you and them. However, offering such a privacy-protective social graph portability feature would require a major collaborative technical effort that could raise

[19] Jason Kincaid, *Google to Facebook: You Can't Import Our User Data Without Reciprocity*, TechCrunch (Nov. 4, 2010), https://techcrunch.com/2010/11/04/facebook-google-contacts

unanticipated privacy and security challenges as well as legal compliance questions, which is why companies and policymakers—including the FTC—need to start discussing and developing such approaches now.

Hopefully, if we can offer easy portability while striking the right balance on privacy, we will not only see more robust competition between existing tech giants but also more innovators rising to challenge their dominance. On the other hand, it may be that the incumbent platforms have so successfully leveraged their network effects (and successfully stifled competition by acquiring other fast-growing, potentially competitive services) that portability alone will not be enough. Allowing new entrants to leverage the existing platforms' networks of users through interoperability may be the only way to ensure that they can reach the critical mass of users that they would need to survive and compete.

IV. Interoperability Is Another Important Function That Would Help Promote Competition

Interoperability between different computer systems using common standards is at the heart of the Internet and has been a key enabler of its explosive growth and innovation. For example, both email and the world wide web are decentralized or "federated" technologies based on open standards. Thanks to open protocols like SMTP and IMAP, anyone can run an email server that talks to other email servers, send and receive emails between different email servers, and easily move archives of email between services. Similarly, thanks to HTML and HTTP, anyone can host a web server that serves content to any web browser and can link to content on any other site. In the recent past it was also very easy to chat across different instant messaging services and servers, such as Google Chat and AOL Instant Messenger or even your own personally hosted chat server, using the common XMPP standard.[20] However, those open and interoperable chat systems have now mostly been replaced with closed, non-interoperable IM products like Facebook Messenger, Whatsapp, and Google Hangouts.[21]

Social networking technology also has the capacity to be decentralized, open and interoperable, as demonstrated by the growing "fediverse" of decentralized services that rely on the W3C-developed protocol "ActivityPub," which in turn is based on the open "Activity Streams 2.0" standard.[22] For example, the Fediverse includes an open source Twitter replacement called Mastodon running on a decentralized network of servers around the world, as well as a YouTube replacement called PeerTube.[23] By using the same protocols, the different services in the Fediverse can interoperate in novel ways. For example, a user on Mastodon can

[20] Ben Parr, *Gmail Chat & AIM Are Now Interoperable*, Mashable (May 19, 2011), https://mashable.com/2011/05/19/gmail-aim.
[21] Steven J. Vaughan-Nichols, *The Great Instant-Messaging Foul-Up*, ZDNet (Mar. 14, 2017), https://www.zdnet.com/article/the-great-instant-messaging-foul-up
[22] *See* ActivityPub Homepage, W3C, https://www.w3.org/TR/activitypub, and James Snell, *Activity Streams 2.0*, Medium (Sept. 1, 2016), https://medium.com/@jasnell/activity-streams-2-0-70881f866935.
[23] *See* Fediverse Homepage, https://fediverse.party, and Fediverse Article, Wikipedia, https://en.wikipedia.org/wiki/Fediverse.

follow a user on PeerTube, and both watch and comment on that user's PeerTube videos, from the Mastodon software client. However, some researchers have concluded that these alternatives are unlikely to attract enough users to meaningfully compete with the large existing commercial networks unless those larger networks offer meaningful portability or even direct interoperability using the same open standards.[24] Some have even suggested that such direct, decentralized interoperability should be mandated by regulators to address the existing major platforms' concentration of power.[25] On the other hand, others have suggested that relying on open standards to allow federation may hinder the pace of innovation in features that consumers want to see.[26]

In the absence of widespread decentralized interoperability based on open standards, the social network space is instead dominated by closed platforms like Facebook that have been built on top of the open system of the internet—what some have called "walled gardens"—where interoperability, when it exists, is typically accomplished through tightly controlled Application Programming Interfaces, or APIs.[27] For example, the Facebook Platform API has allowed a huge ecosystem of app developers to build services that can leverage Facebook users' data to provide them with services beyond Facebook's. Other services like Twitter and Gmail, and even operating systems like iOS and Android, offer similar platforms for third-party applications, with activity on those platforms essentially under the control of the platform providers by virtue of their control over the APIs.

This model of interoperability, which we'll call "centralized interoperability" in contrast with decentralized or federated interoperability, could potentially offer a solution to the data portability challenges outlined above. For example, a third-party social network or messaging app developer could provide a service that competes with the platform provider but that relies directly on the social graph that resides on the original service rather than requiring the user to move their social graph over to the new service. Similarly, different services could allow cross-posting of content on their services via APIs, if they chose to, similarly mitigating the need to fully relocate one's social network to another service, and allowing the smaller provider to benefit from the larger service's network effects.

There are two problems that currently limit the usefulness of centralized interoperability as a tool for competition and innovation. First and most simply, many providers will conclude that allowing competing services to leverage their APIs, or to cross-post content between their users, is not in their own business interest. For example, Facebook's policy for app developers

[24] *See generally* Chelsea Barabas, *The Decentralized Web*, MIT Digital Currency Initiative & Center for Civic Media (Aug. 2017), https://dci.mit.edu/decentralizedweb; see also Chelsea Barabas *et al.*, *Decentralized Social Networks Sound Great. Too Bad They'll Never Work*, Wired (Sept. 8, 2017), https://www.wired.com/story/decentralized-social-networks-sound-great-too-bad-theyll-never-work.
[25] *See generally* Joshua Gans, *Enhancing Competition with Data and Identify Portability*, Hamilton Project (June 2018), https://www.brookings.edu/wp-content/uploads/2018/06/ES_THP_20180611_Gans.pdf.
[26] moxie0, *Reflections: The Ecosystem Is Moving*, Signal Blog (May 10, 2016), https://signal.org/blog/the-ecosystem-is-moving.
[27] For a brief explanation of APIs, see Ross Schulman, *A Tech Intro to Data Portability*, New America Weekly, https://www.newamerica.org/oti/blog/tech-intro-data-portability.

has long required that apps "must not replicate core Facebook features or functionality, and must not promote [their] other apps that do so."[28] More specifically, "your app is not eligible… if it contains its own in-app chat functionality or its own user generated feed" akin to Facebook's messaging product or Facebook's newsfeed.[29] Under public pressure after the Cambridge Analytica scandal, Facebook had indicated that it is reevaluating this term of service,[30] but unless and until it takes action, consumers will not be able to directly use their Facebook data to benefit from competing services off of Facebook.

The second challenge to the continued utility of centralized interoperability is the risk to privacy. APIs are powerful tools for allowing users to leverage their data from one service on another service. However, as the Cambridge Analytica scandal demonstrated, it can also be a powerful tool for gaining access to unwitting users' personal information and using it in ways that do not conform with their privacy expectations. Now, in the post-Cambridge Analytica world, Facebook and other major companies like Google—which recently received similar criticism over the actions of app developers who have abused the API that allows Gmail to interoperate with non-Google services[31]—are under enormous pressure to lock down their APIs and only allow users to share data with the most trusted and vetted partners. As Facebook's Mark Zuckerberg himself put it, "I think the feedback that we've gotten from our community and from the world is that privacy and having the data locked down is more important to people than maybe making it easier to bring more data and have different kinds of experiences."[32] This pressure has led some commentators to publicly wonder, "Will third-party plugins survive the tech backlash?"[33]

The concern is legitimate. Third-party app ecosystems have been a critical engine of innovation and economic growth in the tech industry over the past decade. Although they certainly benefited the platforms themselves, they also enabled entirely new software markets supporting enormous ecosystems of small and mid-sized businesses that were able to take advantage of the platforms' massive networks of users. It would ultimately be a loss for consumers and competitors if, after the platforms have already reaped most of the benefits in terms of user growth and engagement that these app ecosystems provided, those same platforms were to suddenly re-concentrate their power over users' data in the name of privacy.

---

[28] Facebook Platform Policy as of Apr. 16, 2018 as cached at the Internet Archive, https://web.archive.org/web/20180415090010/https://developers.facebook.com/policy. In mid-April, this prohibition on replicating Facebook's functionality was slightly shortened and softened to read "Add something unique to the community. Don't replicate core functionality that Facebook already provides." Facebook Platform Policy, Facebook, https://developers.facebook.com/policy.

[29] *Id.*

[30] *A Deep Dive Into Data Portability*, New America (June 6, 2018), https://www.newamerica.org/oti/events/deep-dive-data-portability-how-can-we-enable-platform-competition-and-protect-privacy-same-time.

[31] Douglas MacMillan, *Tech's 'Dirty Secret': The App Developers Sifting through Your Gmail*, Wall St. J. (July 2, 2018), https://www.wsj.com/articles/techs-dirty-secret-the-app-developers-sifting-through-your-gmail-1530544442.

[32] Nicholas Thompson, Mark Zuckerberg Talks to Wired about Facebook's Privacy Problem, Wired (Mar. 21, 2018), https://www.wired.com/story/mark-zuckerberg-talks-to-wired-about-facebooks-privacy-problem.

[33] Russell Brandom, *Will Third-Party Plugins Survive the Tech Backlash?*, Verge (Jul 6, 2018), https://www.theverge.com/2018/7/6/17538400/gmail-plugin-privacy-app-developers-google-facebook.

Yet that is certainly the direction the market is going in, under direct pressure from policymakers and the public in response to serious privacy concerns. For instance, Facebook has seriously narrowed the range of data available over its APIs and the range of parties that can access that data in the months since Cambridge Analytica.[34] Some of those changes have led to a direct diminishing of interoperability with other popular services, like eliminating the ability to cross-post content from Twitter to Facebook.[35] Indeed, hundreds of thousands of apps have been cut off from the Facebook API for failure to submit to the platform's new enhanced app review process, with more to come.[36]

Certainly, action to better secure users data is welcome, and several of these steps will enhance privacy and security in much-needed ways. There is, however, a growing fear amongst even the most pro-privacy consumer advocates that in rushing to lock down our data, we may be throwing the competition baby out with the privacy bathwater, unwittingly undermining the data portability and interoperability that would likely be necessary for new entrants into the social networking space to effectively compete with the big incumbents.[37] Put another way, in seeking to address the privacy mistakes of the existing players, we ironically may be helping lock in their dominance by making it harder for new—and perhaps more privacy-protective—services to compete with them. As former FTC Commissioner Terrell McSweeny has warned,

> [I]t's tempting to presume that privacy can only be protected by severely restricting the flow of data – by closing off one provider's data from another's. Such an approach, however, could limit the ability of users to easily move their data around and reduce the potential for innovative new entrants to markets and all the benefits that may flow to consumers from them. Privacy is a crucial aspect of consumer rights in the digital age – and openness is another. The right balance will be found in policies that give users meaningful control over their digital identities but that also foster competition and innovation.[38]

---

[34] Mike Schroepfer, *An Update on Our Plans to Restrict Data Access on Facebook*, Facebook Newsroom (Apr. 4, 2018), https://newsroom.fb.com/news/2018/04/restricting-data-access.

[35] Mark Wycislik-Wilson, Facebook API Changes Mean You Can No Longer Cross-Post from Twitter, Betanews (Aug. 2, 2018), https://betanews.com/2018/08/02/twitter-facebook-crossposts-stop.

[36] Konstantinos Papamiltiadis, *Enhanced Developer App Review and Graph API 3.0 Now Live*, Facebook for Developers (May 1, 2018), https://developers.facebook.com/blog/post/2018/05/01/enhanced-developer-app-review-and-graph-api-3.0-now-live/; Ime Archibong, *An Update on Facebook App Review*, Facebook Newsroom (July 31, 2018), https://newsroom.fb.com/news/2018/07/update-on-app-review (100s of thousands of inactive sites shut off for failing to meet deadline).

[37] See, e.g., Caroline Holland, *We Hope the Facebook Cambridge Analytica Scandal Will Improve Privacy Protections – But Could the Fallout Harm Competition?*, Medium (May 3, 2018), https://medium.com/read-write-participate/we-hope-the-facebook-cambridge-analytica-scandal-will-improve-privacy-protections-but-could-the-a1ef9a246afb.

[38] Terrell McSweeny, *How Should Facebook and Other Companies Protect Privacy While Letting People Share Their Information Between Apps and Services?*, Facebook Newsroom (Aug. 6, 2018), https://newsroom.fb.com/news/2018/08/guest-post-terrell-mcsweeny.

This discussion leads to the question, what is the right balance? How can we ensure enough access over APIs to allow users to leverage their data to benefit from more innovation and competition, while also protecting those same users against their own bad decisions or the bad acts of unsavory app developers?

There are no easy answers here, but it helps to clearly distinguish between the two separate but related issues around privacy expectations raised by the Cambridge Analytica scandal. First, although Facebook would argue that they had consented, it is clear that many Facebook users did not expect their personal data to be disclosed to apps that their friends used but that they did not. Second, users did not expect app developers (in that case, Aleksandr Kogan who developed the "This is Your Digital Life" quiz) to violate Facebook's rules and hand their data over to third parties (like Cambridge Analytica). Aggressively addressing this first problem—ensuring that users are well-informed of the risks before they are allowed to share data with an outside app, and that there is clear notice and consent for such transfers—will have minimal impact on competition and innovation but will help to protect users' privacy and give them more control over their data. On the other hand, aggressively addressing the second problem in the wrong way could easily diminish competition, innovation, and users' own freedom to choose which services they want to share their data with.

In the wake of the Cambridge Analytica scandal and the recent reporting around Gmail apps, the pressure is on platforms to take full responsibility for every app that is on their platform, and only allow users to export data to them if they have been individually approved. This requirement is a tall order when talking about an app ecosystem that may involve millions of players.[39] Such pressure to vet data recipients will also inevitably extend to data portability efforts like the Data Transfer Project, where the major companies will rightly fear that they may be held responsible if they allow their users to choose to export their data to a newer, smaller, less well-known service provider that then behaves badly with that data. Yet pushing the already-dominant companies to sharply constrain with whom you can choose to share your data, and giving them the power to pick and choose who will get to be in the shrinking population of third-party apps that you are allowed to use, is a recipe for anti-competitive conditions.

The public wants and needs vetting that will keep internet users safe from bad actors, yet it also wants and needs an open and competitive internet ecosystem where people are not locked into their current services. How do we reconcile these equally important goals? One approach may be to push companies toward a sliding scale of consent and risk. This approach would allow sharing of data with a small white-listed population of heavily-vetted, trusted app partners with a very simple notice and consent interface, while sharing with a similarly small black-listed population of suspect or wholly unverified apps would be allowed only if the user consented after having clicked through multiple serious warnings about the risks involved, and sharing with a much larger universe of apps—not heavily vetted but also with no apparent red flags—would

[39] There were 9 *million* apps/connected web sites on the FB platform in 2012 according to IPO filing*:* Brittany Darwell, *Facebook Platform Supports More than 42 Million Pages and 9 Million Apps*, AdWeek (Apr. 27, 2012), https://www.adweek.com/digital/facebook-platform-supports-more-than-42-million-pages-and-9-million-apps.

require some level of warning and user convenience in between the two extremes. Such an approach would recognize and honor the fact that the seemingly opposed values of privacy and portability basically boil down to the same thing: providing users with well-informed control over their own data.

Of course, this sliding scale approach is just one idea, and we offer it only as an example of a possible approach toward finding the policy balance that former Commissioner McSweeny was imagining. What we need most right now are even better ideas from even more stakeholders, based on a recognition that any approach to addressing internet privacy must also seek to preserve data portability and interoperability. The FTC should take the lead role in ensuring that dialogue.

V. The FTC Should Take Several Steps to Encourage Data Portability and Interoperability

The FTC can promote data portability and interoperability norms and better ensure online competition by continuing to play the role of fact-finder, provide strong and clear guidance to online companies, and require companies that are part of mergers and acquisitions to adopt certain data practices. While adopting these approaches and others, the FTC should be careful that whatever steps it takes toward improving privacy protections do not undermine the ability of companies to implement robust data portability and interoperability functions.

As an initial step, the FTC should continue to play its role as a fact-finder. By seeking comment on data portability and interoperability in these proceedings, hosting hearings, and synthesizing that information in comprehensive reports, it can arm itself and the public with the information it needs to make positive change. As the FTC learns more about online competition between tech companies, and the complex relationship between competition, big data, and privacy online, it can develop and share much-needed expertise in how to address the relevant technical and policy problems.

The FTC should apply that expertise to the development of strong, clear guidance to companies on portability and interoperability, including the hard questions raised in these comments. The FTC should use its bully pulpit to push companies to offer robust portability features and enhance their interoperability with other services, including by encouraging collaborative standard-setting efforts such as the Data Transfer Project and encouraging the adoption of existing open standards like Activity Streams 2.0. It should also seek to provide guidance on how to address outstanding challenges such as how to provide social graph portability while preserving privacy, and outstanding questions such as the extent to which platforms should (or should not) vet third-party providers before allowing users to move or share their data with those providers. Much as it helped set the norm that all websites should secure

connections with HTTPS encryption by default,[40] the FTC's ability to set norms is critically needed in this emerging area of technology and competition.

In its review of mergers and acquisitions, the FTC should examine the new company's policies and practices on data portability and interoperability, with pro-competitive policies viewed favorably. The internet sector has already seen a worrisome level of market concentration through aggressive M&As, whether considering the increasing number of mergers of telecommunications service providers with each other and with content providers, Microsoft's merger with LinkedIn, AOL's merger with Yahoo, Facebook's acquisition of Instagram and Whatsapp just as their user growth was beginning to explode, or Google's 200+ acquisitions over its relatively short history.[41] In the future, as it critically evaluates similar acquisitions by already-dominant tech giants,[42] the FTC should include a review of the acquiring company's policies and practices on data portability and interoperability. Acquisitions by companies that offer users little in the way of portability tools or interoperable service offerings, and especially by those that take affirmative steps to block portability or interoperability including through anti-competitive terms of service, should be disfavored. Alternatively, the implementation of meaningful portability and/or interoperability offerings should be a condition of approval. There is precedent for such conditions in regard to online services: in 2001, one condition of the AOL/Time-Warner merger was that AOL could not offer video chat as a feature of its instant messaging client, AIM, unless and until it implemented an industry-wide standard for interoperable instant messaging or entered into contracts enabling interoperability with three other major instant messaging providers.[43]

Finally, the FTC should work to ensure that whatever steps it or Congress takes to better protect online privacy should also support rather than undermine data portability and interoperability. In particular, the FTC should work closely with Congress to ensure that any potential future privacy legislation includes a grant to the FTC of rulemaking authority over data portability and interoperability as well as privacy. The FTC has long sought comprehensive privacy legislation and enhanced rulemaking authority from Congress, and this FTC should continue that tradition.

In sum, the FTC must ensure that the importance of portability and interoperability is part of any policy conversation about privacy because they are so closely intertwined. The wrong approach to one may easily undermine the other, yet for consumers to truly exercise control over their own data and how it used, they need—and deserve—both.

---

[40] The FTC should play a role here similar to that which it played in promoting the adoption of HTTPS by default, to better protect the privacy and security of web users. *See Getting Internet Companies To Do the Right Thing*, New America (https://www.newamerica.org/in-depth/getting-internet-companies-do-right-thing/case-study-1-using-transit-encryption-default (recounting the critical role played by the FTC and others in achieving the widespread adoption of transit encryption).

[41] *See* List of Mergers and Acquisitions by Alphabet, Wikipedia, https://en.wikipedia.org/wiki/List_of_mergers_and_acquisitions_by_Alphabet.

[42] Caroline Holland, Taking on Big Tech Through Merger Enforcement, Medium (Jan 26, 2018), https://medium.com/read-write-participate/taking-on-big-tech-through-merger-enforcement-f15b7973e37.

[43] Fact Sheet: FCC's Conditioned Approval of AOL-Time Warner Merger, FCC (Jan. 2001), https://transition.fcc.gov/Bureaus/Cable/Public_Notices/2001/fcc01011_fact.pdf.