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.