Before the
National Telecommunications and Information Administration

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

COMMENTS OF

CENTER ON PRIVACY & TECHNOLOGY AT GEORGETOWN LAW

Laura M. Moy
Gabrielle Rejouis
Center on Privacy & Technology at Georgetown Law
600 New Jersey Avenue, NW
Washington, DC 20001
(202) 662-9547

Filed November 9, 2018

Table of Contents

I. Introduction and Summary

The Center on Privacy & Technology at Georgetown Law is pleased to submit these comments in response to the National Telecommunications and Information Administration's (NTIA) request for public comments (RFC) on proposed user-centric privacy outcomes and high-level goals that should guide this Administration's approach to consumer privacy in the near future.[1]

The Center on Privacy & Technology generally supports NTIA's proposed privacy outcomes and proposed high level goals for federal action on privacy. In addition, however, the Center on Privacy & Technology urges NTIA to move further in the direction of strong consumer protection by recognizing additional important privacy outcomes and high-level goals for federal action, and by approaching calls for a risk-based approach and harmonization with caution. In particular, NTIA should:

- Assert explicitly and forcefully that transparency and control—or notice and consent—alone are insufficient to protect consumers in the 21st century.
- Include non-discrimination among its list of desired privacy outcomes.
- Include purpose specification and use limitation among its list of privacy outcomes.
- Recognize that privacy violations themselves are harmful, and not support a privacy framework that conditions privacy obligations on the outcome of an assessment of risk of tangible secondary harms to individual users.
- Not support regulatory "harmonization" at the expense of context-specific privacy.
- Not support regulatory "harmonization" at the expense of strong existing protections.
- Identify strong privacy enforcement authority as a goal for federal action.
- Identify regulatory agility as a goal for federal action.

[1] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600 (Sept. 26, 2018) [hereinafter RFC].

II. Notice and Consent, While Necessary, Are Not Sufficient to Protect Consumers in the 21st Century

The Center on Privacy & Technology agrees with NTIA that while transparency and control are important privacy outcomes for any federal action on privacy, more is needed. Consent today is less meaningful than it once was. It is increasingly difficult for consumers to understand the many ways in which their information might be collected, what that information might reveal about them, and how it might be used.

Even when they are given information about how companies will handle their data, Americans often lack sufficient choice to be able to exercise meaningful control over their data. As dominant providers of online services have grown, expanded partnerships with other services, and become integrated with everyday communications, they have become an unavoidable part of consumers' lives. In addition to rendering consent mechanisms illusory, this amplifies societal vulnerability to harms perpetrated by tech giants. Consumers now find that they effectively have no choice but to use services provided by—and share their data with—a handful of these large companies.

For example:

- The cost disparity between Apple and Android devices drives many low-income consumers to Android-powered devices, subjecting them to greater tracking by Google and less privacy-enhancing encryption defaults.[2]
- On the web, consumers cannot avoid being tracked by Google's pervasive analytics and advertising networks.[3]
- In some instances, employers require employees to have accounts through tech giants such as Facebook.[4]

---

[2] *See Christopher Soghoian: Your Smartphone Is a Civil Rights Issue*, Tiny Ted, https://en.tiny.ted.com/talks/christopher_soghoian_your_smartphone_is_a_civil_rights_issue.

[3] According to one report, Google Analytics is present on 56% of all websites. W3Techs, *Usage Statistics and Market Share of Google Analytics for Websites*, https://w3techs.com/technologies/details/ta-googleanalytics/all/all (last visited Aug. 19, 2018).

[4] Landan Hayes, CareerBuilder, *Not Getting Job Offers? Your Social media Could Be the Reason,* Aug. 9, 2018, https://www.careerbuilder.com/advice/not-getting-job-offers-your-social-media-could-be-the-reason ("Nearly half of employers (47 percent) say that if they can't find a job candidate online, they are less likely to call that person in for an interview"); *see* Laura Fosmire, *Senate Moves Forward on Social Media and Employment Bill*, Statesman J., Mar. 4, 2015, https://www.statesmanjournal.com/story/money/business/2015/03/04/senate-moves-forward-social-media-employment-bill/24359757/; Kashmir Hill, *Beware, Tech Abandoners. People Without Facebook Accounts Are 'Suspicious,'* Forbes, Aug. 6, 2012,

- Amazon is putting local retailers and booksellers out of business, limiting offline options for consumers to purchase certain goods. The platform is also positioning itself as the platform through which cities, counties, and schools purchase office and classroom supplies, leaving retailers with little choice other than to use Amazon to reach government buyers.[5]
- In order to get online, consumers have no choice but to share vast amounts of information about their online activities and associations with an Internet service provider—of which there may only be one or two possible options in any given location.

And even if consumers later become dissatisfied with the practices of a provider, it can be extremely difficult to switch to another provider. Not only are there limited alternatives available, but once an individual establishes an account with a provider and uses that account to create and store information, it may not be possible for the consumer to take that information elsewhere.

Federal action on privacy—whether principles or legislation—should therefore recognize that a framework premised on notice and consent alone is insufficient to protect consumers. NTIA's proposed approach is consistent with this idea and includes additional privacy outcomes. The Center on Privacy & Technology urges NTIA to go one step further and to acknowledge explicitly and directly that notice and consent are not sufficient to protect consumers.

III. Privacy Outcomes Should Include Affirmative Obligations that Attach Whenever Consumer Data Is Collected or Used

Beyond the need for greater transparency and control, NTIA names reasonable minimization, security, access and correction, risk management, and accountability as important privacy outcomes. The Center on Privacy & Technology generally supports these additional outcomes, and urges the NTIA additionally to recognize that certain uses of consumer data, such as discrimination, simply should not be allowed. The Center on Privacy & Technology also encourages NTIA to include purpose specification and use limitation among its list of privacy outcomes.

---

https://www.forbes.com/sites/kashmirhill/2012/08/06/beware-tech-abandoners-people-without-facebook-accounts-are-suspicious/#2d7072ca8f95.

[5] Olivia LaVecchia & Stacy Mitchell, *Amazon's Next Frontier: Your City's Purchasing* (2018), https://ilsr.org/wp-content/uploads/2018/07/ILSR_AmazonsNextFrontier_Final.pdf; Abha Bhattarai, *How Amazon's contract to sell office supplies to cities could hurt local retail*, Wash. Post, July 10, 2018, https://www.washingtonpost.com/business/2018/07/10/amazon-now-sells-office-supplies-books-thousands-cities-other-local-organizations/.

A. NTIA Should Clearly Assert that Some Uses of Data Simply Should Not Be Allowed

Any list of privacy outcomes should include a recognition that some uses of data simply should not be allowed. Chief among these are discriminatory uses. The information that Americans share online should not be used to selectively deny them access to—or awareness of—critical opportunities, especially things like housing, education, finance, employment, and healthcare. It should not be used to amplify hate speech. It should not be used to enable data brokers to secretly build ever-more-detailed consumer profiles that they then turn around and sell, unrestricted, to the highest bidder. Privacy should actively protect Americans from the most harmful uses of their information.

NTIA should, specifically, enumerate non-discrimination among any list of desired privacy outcomes released by the agency. There is much work to do in this area; at present, discriminatory uses of information are widespread. For example, Facebook made assurances in 2017 to tackle discriminatory advertising on its platform after facing public outrage and pressure from advocates regarding its "ethnic affinity" advertising clusters, but the Washington State Attorney General found that it was still possible to exclude people from seeing advertisements based on protected class membership.[6] Civil rights organizations are also suing Facebook for enabling landlords and real estate brokers to exclude families with children, women, and other protected classes of people from receiving housing ads.[7]

Discrimination also occurs in the targeting of employment advertisements. Advertisers can use Facebook's algorithm to target job ads to certain genders, often along gender stereotypes.[8] The systematic targeting and exclusion of communities can also be a byproduct of algorithmic content and ad distribution that optimizes for cost-effectiveness and user "engagement," which can lead to distribution that is discriminatory in impact, if not intent.[9] For example, algorithms seeking the best returns

---

[6] Sam Machkovech, Facebook Bows to WA State to Remove "Discriminatory" Ad Filters, Ars Technica, July 25, 2018, https://arstechnica.com/information-technology/2018/07/facebook-bows-to-wa-state-pressure-to-remove-discriminatory-ad-filters/.

[7] Nat'l Fair Housing Alliance, *Facebook Sued by Civil Rights Groups for Discrimination in Online Housing Advertisements* (Mar. 27, 2018), https://nationalfairhousing.org/2018/03/27/facebook-sued-by-civil-rights-groups-for-discrimination-in-online-housing-advertisements/.

[8] Women were excluded from seeing Uber driver, truck driver, and state police positions but targeted for nurse openings. *See* Ariana Tobin and Jeremy B. Merrill, *Facebook Is Letting Job Advertisers Target Only Men*, ProPublica, Sept. 18, 2018 https://www.propublica.org/article/facebook-is-letting-job-advertisers-target-only-men.

[9] *See* Anja Lambrecht & Catherine E. Tucker, *Algorithmic Bias? An empirical Study into Apparent Gender-Based Discrimination in the Display of STEM Career Ads* (Mar. 9, 2018),

on optimized ads displayed more ads for science, technology, engineering and mathematics opportunities to men than women.[10]

Digital data and services should operate as tools to advance opportunities and equity, rather than to reinforce existing social disparities. Federal action on privacy therefore must seek to ensure that users' data is not used to exclude users from awareness of or opportunities in critical areas including education, jobs, healthcare, housing, and credit.

B. NTIA Should Include Purpose Specification and Use Limitation Among Its List of Privacy Outcomes

Federal action on privacy should recognize baseline obligations that automatically attach when Americans' information is collected or used. The privacy outcomes enumerated in the RFC appear to move in this direction, but the Center on Privacy & Technology urges NTIA to consider also adding additional outcomes based on the familiar Fair Information Practices (FIPs) of collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.[11] The FIPs framework creates meaningful obligations for companies that collect personal data, and rights for individuals whose personal data is collected.

In particular, NTIA should add purpose specification and use limitation to the list of desired privacy outcomes. Entities that collect, share, and use Americans' data should be required to articulate the purpose for which they are engaging in collection or use, and to limit their activities—and the activities of any downstream or third-party actors—to uses that are consistent with that purpose.

---

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852260 (finding that because younger women are an expensive demographic to show ads to, "An algorithm which simply optimizes cost-effectiveness in ad delivery will deliver ads that were intended to be gender-neutral in an apparently discriminatory way, due to crowding out."): Latanya Sweeney, *Discrimination in Online Ad Delivery,* Communications of the ACM, May 2013, at 44, https://cacm.acm.org/magazines/2013/5/163753-discrimination-in-online-ad-delivery/.

[10] Dina Fine Maron, *Science Career Ads Are Disproportionately Seen by Men*, Scientific American, July 25, 2018 https://www.scientificamerican.com/article/science-career-ads-are-disproportionately-seen-by-men/.

[11] *See* Int'l Ass'n Privacy Professionals, *Fair Information Practices,* https://iapp.org/resources/article/fair-infomation-practices/ (last visited Oct. 31, 2018); Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last visited Oct. 7, 2018).

IV. NTIA Should Recognize that Privacy Violations Themselves Are Harmful

In the RFC, NTIA notes the need to "minimiz[e] harm to individuals arising from the collection, storage, use, and sharing of their information."[12] In its description of the "reasonable minimization" privacy outcome, NTIA asserts that "data collection, storage length, use, and sharing by organizations should be minimized in a manner and to an extent that is reasonable and appropriate to the context and risk of privacy harm."[13] And in its list of high-level goals for federal action, NTIA supports an approach to privacy regulations that is "based on risk modeling."[14] Taken together, these portions of the RFC could indicate that NTIA considers some privacy violations to be less harmful or even altogether harmless, and perhaps even that privacy violations that do not cause secondary harm need not be protected against.

The Center on Privacy & Technology urges NTIA to recognize that even when secondary harms are not immediately apparent, privacy violations are themselves harmful. The use of people's information in a way that exceeds social norms or user expectations violates user rights, undermines user trust, and contributes to an atmosphere of growing privacy concerns that ultimately may interfere with adoption and use of online services. For example, in 2016 NTIA found, based on data collected by the Census Bureau in 2015,

> Forty-five percent of online households reported that [privacy and security] concerns stopped them from conducting financial transactions, buying goods or services, posting on social networks, or expressing opinions on controversial or political issues via the Internet, and 30 percent refrained from at least two of these activities.[15]

And in January 2016, the City of Portland, Oregon's Office for Community Technology reported that in focus groups conducted by the city to improve the city's understanding of adoption challenges, privacy concerns were raised in every group.[16]

---

[12] RFC at 48601.
[13] *Id.*
[14] *Id.* at 480602.
[15] Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, NTIA (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.
[16] Angela Siefer, *Signs On Letter Encouraging FCC Protect Privacy Of Broadband Consumers*, NDIA (Jan. 26, 2016), http://www.digitalinclusionalliance.org/blog/2016/1/26/ndia-signs-on-letter-encouraging-fcc-protect-privacy-of-broadband-consumers.

In addition, even when privacy violations do not result in tangible and measurable harm to specific individuals, they may result in harms to society. For example, beyond subjecting individual users to specific uses and transfers that they find objectionable, information uses and misuses may harm society by:

- Supporting the dissemination of propaganda, misinformation, and disinformation. Americans' data may be used to generate and target false information, including state-sponsored propaganda, careless or low-quality reporting, and false information designed and intended to undermine democracy.[17] As false information proliferates, Americans are rapidly losing trust in journalism.

- Amplifying hate speech. Americans' data may also be used to make the distribution of hateful and racist rhetoric and calls to violence more efficient.[18]

- Driving political polarization. Americans' data may also be used to drive content distribution platforms that are more likely to promote hyper-partisan content, which in turn may exacerbate political polarization. As one prominent legal scholar has written, "Self-insulation and personalization are solutions to some genuine problems, but they also spread falsehoods, and promote polarization and fragmentation."[19]

- Damaging public health. Digital sites and services often use users' data to inform design choices that will increase user engagement, including by intentionally

[17] David McCabe, *Facebook Finds New Coordinated Political Disinformation Campaign*, Axios, July 31, 2018, https://www.axios.com/facebook-finds-misinformation-campaign-4c5910b3-021a-45b7-b75c-b1ac80cbce49.html; Dipayan Ghosh & Ben Scott, *Disinformation Is Becoming Unstoppable*, Time, Jan. 24, 2018; April Glaser & Will Oremus, *The Shape of Mis- and Disinformation*, Slate, July 26, 2018, https://slate.com/technology/2018/07/claire-wardle-speaks-to-if-then-about-how-disinformation-spreads-on-social-media.html; Alice Marwick & Rebecca Lewis, *Media Manipulation and Disinformation Online* (2017), https://datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf.

[18] *See* Ariana Tobin, Madeleine Varner, & Julia Angwin, *Facebook's Uneven Enforcement of Hate Speech Rules Allows Vile Posts to Stay Up*, ProPublica, Dec. 28, 2017, https://www.propublica.org/article/facebook-enforcement-hate-speech-rules-mistakes; Swathi Shanmugasundaram, Southern Poverty Law Center, *The Persistence of Anti-Muslim Hate on Facebook* (May 5, 2018), https://www.splcenter.org/hatewatch/2018/05/05/persistence-anti-muslim-hate-facebook.

[19] Cass R. Sunstein, #*Republic: Divided Democracy in the Age of Social Media* at 5 (2017).

designing products to be addictive and inescapable.[20] This can lead to a cascade of other problems, including heightened rates of depression, suicide, and sleep deprivation among young people.[21]

NTIA therefore should recognize that privacy violations must always be protected against, and should adopt caution as it considers any approach to privacy that conditions privacy obligations on the outcome of an assessment of risk of tangible secondary harms that individual users may suffer.

V. NTIA Should Not Support Regulatory "Harmonization" at the Expense of Context-Specific Privacy or of Strong Existing Protections

NTIA indicates that this Administration supports an approach to federal action on privacy that prioritizes "harmoniz[ing] the regulatory landscape." The Center on Privacy & Technology urges NTIA not to support harmonization that comes at the expense either of context-specific privacy norms or of strong existing protections.

A. Protections for Americans' Private Information Should Take into Account the Context in Which Information Is Shared

There is no one-size-fits-all approach for privacy. Rather, privacy standards often must be context-specific, carefully tailored based on the avoidability of the information sharing, the sensitivity of the information share, and the expectations of consumers. As this Administration considers establishing comprehensive baseline privacy standards, existing laws should not be simultaneously eliminated. Many of those existing narrower privacy laws have already been appropriately tailored to establish heightened privacy standards under specific circumstances. These laws protect consumer information in

[20] Center for Humane Technology, The Problem, http://humanetech.com/problem/ (last visited Oct. 7, 2018) (explaining that operators of online services competing for users' attention are constantly learning how better to "hook" their users, and designing products intentionally to addict users).

[21] Recent studies have linked the use of platforms like Facebook, Snapchat, and Instagram to depressive symptoms in young adults caused by negatively comparing oneself to others on social media platforms. Brian A. Feinstein, et al., *Negative Social Comparison on Facebook and Depressive Symptoms: Rumination as a Mechanism*, 2 Psych. Pop. Media Culture 161 (2013). http://psycnet.apa.org/record/2013-25137-002. Experts have also found that teens who spend three hours a day or more on electronic devices are 35 percent more likely to have a risk factor for suicide and 28 percent more likely to get less than seven hours of sleep. Jean M. Twenge, *Have Smartphones Destroyed a Generation?*, The Atlantic, Sept. 2017, https://www.theatlantic.com/magazine/archive/2017/09/has-the-smartphone-destroyed-a-generation/534198/.

specific contexts in which sharing is unavoidable—such as the information shared by students in an educational context,[22] by consumers in a financial context,[23] by customers in a telecommunications context,[24] and by patients in a medical context.[25] This is also consistent with the FTC's evaluation of potentially problematic data-related practices under its Section 5 authority to prohibit unfair practices.[26]

Whether or not information sharing is avoidable by a consumer is often tied to the question of whether or not a service or transaction is essential. When a service is essential, information sharing may be considered unavoidable because the consumer cannot reasonably decline the service altogether. This, too, helps explain why heightened privacy protections apply in the educational,[27] financial,[28] telecommunications,[29] and medical contexts—all of these contexts involve essential services.[30]

B. New Protections for Americans' Privacy Should Not Eliminate Existing Protections

NTIA also should not support regulatory "harmonization" at the expense of existing protections that already benefit Americans under state or federal laws. Americans are asking for *more* protections for their private information, not less. This is why Americans were outraged when Congress voted last year to eliminate strong privacy regulations that had been passed by the FCC.[31]

State laws play an important role in filling gaps that exist in federal legislation. Consider, for example, the ways that states have expanded data security and breach notification laws over time to cover additional market sectors. Connecticut's data security and breach notification statute now covers entities operating at multiple nodes

---

[22] Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.
[23] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338, (1999).
[24] 47 U.S.C. § 222.
[25] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (1996).
[26] FTC, *FTC Policy Statement on Unfairness* (Dec. 17, 1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.
[27] Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.
[28] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338, (1999).
[29] 47 U.S.C. § 222.
[30] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (1996).
[31] *See* Matthew Yglesias, *Republicans' Rollback of Broadband Privacy Is Hideously Unpopular*, Vox, Apr. 4, 2017, https://www.vox.com/policy-and-politics/2017/4/4/15167544/broadband-privacy-poll.

of the health care pipeline.[32] California adopted a data security statute—the Student Online Personal Information Protection Act (SOPIPA)—that is tailored to online educational platforms, and that prompted twenty-one other states to adopt student data security laws modeled on California's example.[33] Minnesota adopted a law requiring Internet Service Providers (ISPs) to maintain the security and privacy of consumers' private information.[34] And Texas now requires any nonprofit athletic or sports association to protect sensitive personal information.[35]

Some states have also expanded the types of information that data holders are responsible for protecting from unauthorized access, or for notifying consumers of when breached. For example, ten states have expanded breach notification laws so that companies are now required to notify consumers of unauthorized access to their biometric data—unique measurements of a person's body that can be used to determine a person's identity.[36] A large number of states also now require companies to notify consumers about breaches of medical or health data—information that can be used in aid of medical identity theft, potentially resulting in fraudulent healthcare charges and even introduction of false information into one's medical record.[37]

And states are doing other important work on privacy as well. In addition to the California Consumer Privacy Act,[38] California also has a law requiring notification about breaches of information collected through an automated license plate recognition

---

[32] C.G.S.A. § 38a-999b(a)(2) ("health insurer, health care center or other entity licensed to do health insurance business in this state, pharmacy benefits manager . . . third-party administrator . . . that administers health benefits, and utilization review company.").

[33] West's Ann.Cal.Bus. & Prof.Code § 22584(d)(1) (schools must "[i]mplement and maintain reasonable security procedures and practices . . . and protect that information from unauthorized access, destruction, use, modification, or disclosure."); Rachel Anderson, *Last Year's Education Data Privacy Legislation Trends*, iKeepSafe, Jan. 17, 2018, https://ikeepsafe.org/last-years-education-data-privacy-legislation-trends/.

[34] M.S.A. § 325M.05 (must "take reasonable steps to maintain the security and privacy of a consumer's personally identifiable information.").

[35] V.T.C.A., Bus. & C. § 521.052 ("implement and maintain reasonable procedures . . . to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.").

[36] States that have done this include Delaware, Illinois, Iowa, Maryland, Nebraska, New Mexico, North Carolina, Oregon, Wisconsin, and Wyoming.

[37] See Joshua Cohen, *Medical Identity Theft – The Crime that Can Kill You*, MLMIC Dateline (Spring 2015), available at https://www.mlmic.com/wp-content/uploads/2014/04/Dateline-SE_Spring15.pdf ("A patient receiving medical care fraudulently can lead to the real patient receiving the wrong blood type, prescription, or even being misdiagnosed at a later time."). Medical or health data is covered by breach notification laws in Alabama, Arkansas, California, Delaware, Florida, Illinois, Kentucky, Maryland, Montana, Nevada, North Dakota, Oregon, Puerto Rico, Nevada, Rhode Island, Texas, Virginia, and Wyoming.

[38] California Consumer Privacy Act, https://www.caprivacy.org/ (last visited October 7, 2018).

system.[39] Vermont has the Data Broker Act[40] and Illinois has the Biometric Information Protection Act.[41]

To avoid doing harm to consumers benefiting from these existing consumer protections, any federal action on privacy or data security must preserve strong state standards. NTIA should, accordingly, approach calls for "harmonization" with caution.

VI. NTIA Should Identify Strong Privacy Enforcement Authority as a High-Level Goal for Federal Action

NTIA acknowledges that "[i]t is important to take steps to ensure that the FTC has the necessary resources" to enforce privacy. But more broadly, NTIA should clarify that what is needed is *strong* enforcement authority. Legislation should empower an expert agency or agencies to vigorously enforce the law—including the ability to fine companies for privacy and data security violations. The Federal Trade Commission does not have the ability to levy fines for privacy and data security.[42] This is widely viewed as a challenge by agency officials; indeed, civil penalty authority has been explicitly requested by multiple FTC officials, including Chairman Simons, Commissioner Slaughter, former commissioner Ohlhausen, former Commissioner Terrell McSweeny, and former director of the Bureau of Consumer Protection, Jessica Rich.[43] To improve privacy and data security for consumers, the FTC—or another

[39] West's Ann.Cal.Civ.Code § 1798.82(h).

[40] Devin Coldewey, *Vermont Passes First Law to Crack Down on Data Brokers*, TechCruch, May 27, 2018, https://techcrunch.com/2018/05/27/vermont-passes-first-first-law-to-crack-down-on-data-brokers/.

[41] 740 ILCS 14/1 et seq.

[42] There are exceptions to this rule. As the FTC explains, "If a company violates an FTC order, the FTC can seek civil monetary penalties for the violations. The FTC can also obtain civil monetary penalties for violations of certain privacy statutes and rules, including the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, and the Telemarketing Sales Rule." FTC, *Privacy & Security Update 2016,* https://www.ftc.gov/reports/privacy-data-security-update-2016.

[43] *See, e.g., Oversight of the Federal Trade Commission: Hearing Before the Subcomm. On Digital Commerce and Consumer Protection of the H. Comm. on Energy & Commerce* (2018) (statement of Joseph J. Simons, Chairman, Fed. Trade Commission) (calling for civil penalty authority, arguing that monetary penalties "would actually...cause the business to think through how it's conducting...its business and what it's doing in terms of security and privacy."); *id.* (statement of Rebecca Kelly Slaughter, Commissioner, Fed. Trade Comm'n) (calling for civil penalty authority); Maureen Ohlhausen, Commissioner, Fed. Trade Commission, Remarks Before the Congressional Bipartisan Privacy Caucus (Feb. 3, 2014), transcript *available at* https://www.ftc.gov/system/files/documents/public_statements/remarks-commissioner-maureen-k.ohlhausen/140203datasecurityohlhausen.pdf; Terrell McSweeny, *Psychographics, Predictive Analytics, Artificial Intelligence, & Bots: Is the FTC Keeping Pace?*, 2 Geo. L. Tech. Rev.

agency or agencies—must be given more powerful regulatory tools and stronger enforcement authority.

The Center on Privacy & Technology agrees with NTIA that agencies also need resources to do their jobs well. The FTC is a relatively small agency, and should be given additional staff and resources if it is to be expected to step up its work on privacy. The agency would benefit from a larger Bureau of Technology equipped to fully grapple with the challenges of advancing technology—an idea supported by numerous current and former FTC officials.[44]

Even with additional staff and resources, however, enforcement agencies may, for a variety of reasons, sometimes fail to strongly enforce privacy standards.[45] To provide an additional backstop for consumers in the event that agencies lack the

514, 529 (2018), https://www.georgetownlawtechreview.org/wp-content/uploads/2018/07/2.2-McSweeny-pp-514-30.pdf; *Opportunities and Challenges in Advancing Health Information Technology: Hearing Before the Subcomms. On Info. Tech. and Health, Benefits, and Admin. Rules of the H. Oversight and Gov't Reform Comm.* (2016) (statement of Jessica Rich, Director of the Bureau of Consumer Protection, Fed. Trade Commission).

[44] A Bureau of Technology is an idea that has been cited by Chairman Joseph Simons, Commissioner Rebecca Kelly Slaughter, former Commissioner Terrell McSweeny, and Professor David Vladeck, former Director of the Bureau of Consumer Protection. *See, e.g.*, *Oversight of the Federal Trade Commission: Hearing Before the Subcomm. On Digital Commerce and Consumer Protection of the H. Comm. on Energy & Commerce* (2018) (statement that the Commission is "affirmatively evaluating whether to create a bureau of technology"); McSweeny, *supra* note 4, at 530; U.S. Fed. Trade Comm'n, *Remarks of Commissioner Rebecca Kelly Slaughter on Raising the Standard: Bringing Security and Transparency to the Internet of Things?* at 5 (July 26, 2018), https://www.ftc.gov/system/files/documents/public_statements/1395854/slaughter_-_raising_the_standard_-_bringing_security_and_transparency_to_the_internet_of_things_7-26.pdf; Aaron Fluitt, Institute for Technology Law & Policy at Georgetown Law, *Georgetown's David Vladeck Outlines Challenges and Opportunities for Incoming FTC Commissioners,* Apr. 6, 2018, https://www.georgetowntech.org/news-fullposts/2018/4/7/april-6-2018-georgetowns-david-vladeck-outlines-challenges-opportunities-for-incoming-ftc-commissioners.

[45] The FTC has come under criticism for not doing enough to enforce its consent decrees. *See* Marc Rotenberg, *The Facebook-WhatsApp Lesson: Privacy Protection Necessary for Innovation,* Techonomy, May 4, 2018 https://techonomy.com/2018/05/facebook-whatsapp-lesson-privacy-protection-necessary-innovation/. And the FCC has been widely criticized for not doing enough to protect security and privacy of phone users. *See* Craig Timberg, *How Spies Can Use Your Cellphone to Find You–and Eavesdrop on Your Calls and Texts, Too,* Wash. Post, May 30, 2018, https://www.washingtonpost.com/business/technology/how-spies-can-use-your-cellphone-to-find-you--and-eavesdrop-on-your-calls-and-texts-too/2018/05/30/246bb794-5ec2-11e8-a4a4-c070ef53f315_story.html; *Wyden Demand FCC Investigate Unauthorized Tracking of Americans' Cell Phones*, May 11, 2018, https://www.wyden.senate.gov/news/press-releases/wyden-demands-fcc-investigate-unauthorized-location-tracking-of-americans-cell-phones; Violet Blue, *FCC Shrugs at Fake Cell Towers Around the White House,* Endgaget, June 8, 2018, https://www.engadget.com/2018/06/08/fcc-shrugs-at-fake-cell-towers-around-the-white-house/.

capacity or motivation to effectively enforce, Congress may also need to grant individual consumers themselves the right to bring civil actions against companies for violating privacy regulations.

State attorneys general should also be empowered to enforce privacy. A single agency cannot hope to police the entire digital ecosystem. State attorneys general do a large volume of important work in this area, both enforcing privacy laws and providing valuable guidance to companies trying to comply with the law. The guidance provided by state attorneys general is vitally important. Attorneys general frequently provide companies with ongoing guidance to help business understand, adapt to, and comply with legal requirements and best practices.[46]

State attorneys general will provide crucial complementary consumer protection support in thousands of small cases every year.[47] To ensure that consumers receive the best protection they possibly can, state attorneys general must be given the ability to help enforce any new federal standard. This type of authority exists—and has been successful—under the Children's Online Privacy Protection Act.[48]

VII. NTIA Should Also Include Regulatory Agility Among Its High-Level Goals for Federal Action

Any new privacy and data security protection must also be designed to be forward-looking and flexible, with built-in mechanisms for updating standards in accordance with shifting threats. NTIA should acknowledge the importance of ensuring

[46] Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General,* 92 Notre Dame L. Rev. 747, 759 (2016); Paul Shukovsky, *State Attorneys General Are Crucial Force in Enforcement of Data Breach Statutes,* Bloomberg Law: Privacy & Data Security, Oct. 7, 2013, https://www.bna.com/state-attorneys-general-n17179877665/.

[47] For example, according to the Massachusetts State Attorney General's Office, Massachusetts alone saw 2,314 data breaches reported in 2013, 97% of which involved fewer than 10,000 affected individuals. *Discussion Draft of H.R. __, Data Security and Breach Notification Act of 2015: Hearing Before the Subcomm. On Commerce, Manufacturing, and Trade of the H. Energy & Commerce Comm.* (2015) (statement of Sara Cable, Assistant Att'y Gen. Office of Mass. State Att'y Gen.). Each data breach affected, on average, 74 individuals. *Id.*

[48] The Children's Online Privacy Protection Act enables state attorneys general to bring actions on behalf of residents of their states against operators of online sites or services that they believe have violated children's privacy regulations. 15 U.S.C. §6504. State attorneys general use this authority; indeed, just weeks ago, the State Attorney General of New Mexico filed a suit against several companies for alleged children's privacy violations. *See AG Balderas Announces Lawsuit Against Tech Giants Who Illegally Monitor Child Location, Personal Data* (Sept. 12, 2018), https://www.nmag.gov/uploads/PressRelease/48737699ae174b30ac51a7eb286e661f/AG_Balderas_Announces_Lawsuit_Against_Tech_Giants_Who_Illegally_Monitor_Child_Location__Personal_Data_1.pdf.

that digital era privacy protections are designed to express regulatory agility by including regulatory agility among its high-level goals for federal action.

The need for regulatory agility is currently being met by state legislatures. In recent years, California passed the California Consumer Privacy Act[49] and Vermont passed the Data Broker Act.[50] Between 2015 and 2018 at least 23 states—from all regions of the country—passed data security or breach notification legislation.[51]

Given the high level of legislative activity currently taking place at the state level on these issues, the most straightforward way that federal action on privacy can preserve regulatory agility in privacy and data security would be simply by leaving state legislative authority intact. In the event, however, that federal action on privacy seeks to resolve differences between state laws by establishing a uniform federal standard, it must ensure that robust mechanisms for regulatory agility are built in. One such mechanism would be robust rulemaking authority for any agency or agencies that are to be tasked with protecting the privacy and security of Americans' information. Indeed, FTC commissioners have directly asked Congress for rulemaking authority.[52]

---

[49] California Consumer Privacy Act, https://www.caprivacy.org/ (last visited November 1, 2018).

[50] Devin Coldeway, *Vermont Passes First Law to Crack down on Data Brokers,* TechCrunch, May 27, 2018, https://techcrunch.com/2018/05/27/vermont-passes-first-first-law-to-crack-down-on-data-brokers/.

[51] Since 2015, data security or breach notification legislation has been enacted in Alabama, Arizona, California, Connecticut, Delaware, Florida, Illinois, Iowa, Maryland, Montana, Nebraska, New Hampshire, New Mexico, North Dakota, Oregon, Rhode Island, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, and Wyoming. *See* Nat'l Conf. State Legislatures, *2015 Security Breach Legislation* (Dec. 31, 2015), http://www.ncsl.org/research/telecommunicatons-and-information-technology/2015-security-breach-legislation.aspx; Nat'l Conf. State Legislatures, *2016 Security Breach Legislation* (Nov. 29, 2016), http://www.ncsl.org/research/telecommunicatons-and-information-technology/2016-security-breach-legislation.aspx; Nat'l Conf. State Legislatures, *2017 Security Breach Legislation* (Dec. 29, 2017), http://www.ncsl.org/research/telecommunicatons-and-information-technology/2017-security-breach-legislation.aspx; Nat'l Conf. State Legislatures, *2018 Security Breach Legislation*, http://www.ncsl.org/research/telecommunicatons-and-information-technology/2016-security-breach-legislation.aspx (last visited Nov. 1, 2018).

[52] Maureen K. Ohlhausen, FTC Commissioner, Remarks Before the Congressional Bipartisan Privacy Caucus (Feb. 3, 2014), available at https://www.ftc.gov/system/files/documents/public_statements/remarks-commissioner-maureen-k.ohlhausen/140203datasecurityohlhausen.pdf ("Legislation in both areas – data security and breach notification – should give the FTC… rulemaking authority under the Administrative Procedure Act"); *Oversight of the Federal Trade Commission: Hearing Before the Subcomm. On Digital Commerce and Consumer Protection of the H. Comm. on Energy & Commerce* (2018) (statement of Joseph J. Simons, Chairman, Fed. Trade Commission) (stating he "support[s] data security legislation that would give the authority to issue implementing rules under the Administrative Procedure Act"); *id.* (statement of Rebecca Kelly Slaughter, Comm'r)

Rulemaking enables agencies to adjust regulations as technology changes, as the FTC did just a few years ago with the COPPA Rule.[53]

VIII. Conclusion

NTIA's proposed approach to consumer privacy offers a number of positive elements. The Center on Privacy & Technology urges NTIA to move further in the direction of strong consumer protection by recognizing additional important privacy outcomes and high-level goals for federal action, and by approaching calls for a risk-based approach and harmonization with caution.

Respectfully submitted,

Center on Privacy & Technology at
Georgetown Law

By:

/s/

Laura M. Moy
Gabrielle Rejouis
Center on Privacy & Technology
Georgetown Law
600 New Jersey Avenue, NW
Washington, DC 20001
(202) 662-9547

Filed November 9, 2018

(calling for APA rulemaking authority); *id.* (statement of Rohit Chopra, Comm'r) (also supporting rulemaking authority, stating, "the development of rules is a much more participatory process than individual enforcement actions and it also gives clear notice to the marketplace rather than being surprised, and I think it would be a good idea.").

[53] Federal Trade Commission, *FTC Strengthens Kids' Privacy, Gives Parents Greater Control over Their Information by Amending Children's Online Privacy Protection Rule*, Dec. 19, 2012, https://www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over.