Before the Department of Commerce
National Telecommunications and Information Administration
Washington, D.C.

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

COMMENTS OF CTIA

Thomas C. Power
Senior Vice President and General Counsel

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

November 9, 2018

Table of Contents

I. INTRODUCTION

CTIA[1] welcomes the National Telecommunications and Information Administration's ("NTIA's") Request for Comments on *Developing the Administration's Approach to Consumer Privacy* ("RFC")[2] and commends NTIA's thoughtful examination of consumer privacy issues. As CTIA made clear when NTIA published the RFC: "The wireless industry is committed to safeguarding consumer privacy and supports the need to establish uniform privacy standards across the digital economy. [CTIA] appreciate[s] NTIA's leadership in proposing privacy principles to inform the legislative debate that will enable innovation to continue to flourish."[3]

CTIA members remain committed to protecting the privacy of their customers. For years, the wireless industry has embraced a leadership role, recognizing that the protection of consumer privacy does not stop at compliance with existing regimes, but that consumer trust is key for the continued growth of the mobile ecosystem. Communications networks, along with the emerging technologies that they support, depend on trust. This gives companies strong incentives to develop robust privacy programs and practices.

Examples of the industry's commitment to customer privacy abound, including the development of self-regulatory regimes. For example, CTIA and wireless carriers enshrined their commitment to protecting privacy online through a set of core privacy principles: the ISP

[1] CTIA® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st- century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] *Developing the Administration's Approach to Consumer Privacy*, NTIA, Request for Comments, Docket No. 180821780-8780-01 (Sept. 25, 2018) ("RFC").

[3] Melanie Tiano, *CTIA Statement on NTIA Seeking Comment on Privacy Proposal* (Sept. 25, 2018), https://www.ctia.org/news/ctia-statement-on-ntia-privacy-proposal.

Privacy Principles.[4] These principles show commitment to transparency, consumer choice, data security, and data breach notification.[5] Other commitments reflect the industry's view of transparency. Examples at CTIA alone include the *Consumer Code for Wireless Service*, which incorporates CTIA's Best Practices and Guidelines for Location-Based Services, among others.[6]

It is time for the United States to adopt a federal privacy law that establishes a comprehensive and uniform framework for consumer privacy. As AT&T testified before the U.S. Senate Committee on Commerce, Science, and Transportation,

> While we've all been talking about privacy for years, today we stand at a critical juncture in that discussion. Perhaps for the first time, there is widespread agreement among industry, policy makers and many consumer groups of the need for a new and comprehensive federal privacy law. This consensus is driven by a recognition that in today's data-driven world, it is more important than ever to maintain consumers' trust and give them control over their personal information. Consumers rightly expect that consistent privacy protections will apply regardless of which app, device, service or company is collecting and using their personal information.[7]

And as Verizon explained in a recent blog post calling for a new consumer privacy framework,

> [t]he U.S.'s ability to strike the right policy balance on privacy will determine the trajectory of U.S. innovation for years to come. This is too important to sit out. So let's roll up our sleeves, put aside our differences, and work across the policy community to develop consensus on a robust and rational consumer privacy framework. Our ability to realize the full potential of our bright digital future depends on it. The time is now.[8]

The private sector has been united in calling for a nationally unified approach. CTIA supports

---

[4] CTIA et al., *ISP Privacy Principles* (Jan. 27, 2017), https://api.ctia.org/docs/default-source/default-document-library/final---protecting-consumer-privacy-online.pdf.
[5] *Id.*
[6] *See* CTIA, *Consumer Code for Wireless Service*, *https://www.ctia.org/the-wireless-industry/industry-commitments/consumer-code-for-wireless-service* (last visited Nov. 6, 2018); *see* CTIA, *Wireless Industry Commitments*, https://www.ctia.org/the-wireless-industry/industry-commitments (last visited Nov. 6, 2018).
[7] *Examining Safeguards for Consumer Data Privacy Before the S. Comm. on Commerce, Sci., & Transp.*, 115th Cong. (2018) (statement of Leonard Cali, Senior Vice President Global Public Policy, AT&T), *available at* https://www.commerce.senate.gov/public/_cache/files/b42b3943-1409-44f4-9aa9-91ad21ffb43a/C1C79DF5A0936D0F6769AD106E17D3D3.09.24.18cali-testimony.pdf.
[8] Verizon, Kathy Grillo, *Privacy: It's time for Congress to do right by consumers* (Oct. 8, 2018), https://www.verizon.com/about/news/privacy-its-time-congress-do-right-consumers.

this call. Federal legislation is the only way to achieve a uniform national approach to privacy and to accomplish the goals identified by NTIA, which CTIA supports. NTIA should complete this process and produce a privacy framework that it can offer as the foundation for harmonized federal privacy activities, including federal legislation.

CTIA commends the agency's high-level goals for federal action, and applauds the proposed privacy outcomes. These comments also highlight a few areas that require particular care as NTIA seeks to encourage innovation and economic growth.

II. NTIA'S POLICY GOALS ARE CRITICAL TO PROMOTE A SENSIBLE LEGAL AND POLICY ENVIRONMENT, PARTICULARLY HARMONIZATION, COMPREHENSIVE APPLICATION, AND FLEXIBILITY.

CTIA supports comprehensive privacy legislation that will preempt state privacy laws and establish consistent protections that are technology-neutral and that apply uniformly. This is the only way to achieve the goals reflected throughout NTIA's RFC, including meaningful and consistent consumer protection.

A. Harmonization Is a Critical Goal.

CTIA agrees with NTIA that harmonization is a critical goal for federal privacy policy. The current ecosystem is characterized by increasing fragmentation. This risks confusing consumers, as well as straining private resources and burdening the private sector. The only way to promote harmonization and combat fragmentation is through preemptive federal legislation, which will provide clarity and certainty to consumers and businesses.

NTIA describes well the "need to avoid duplicative and contradictory privacy-related obligations placed on organizations."[9] As it rightly notes, "[w]e are actively witnessing the production of a patchwork of competing and contradictory baseline laws. This emerging

[9] RFC at 48602.

patchwork harms the American economy and fails to improve privacy outcomes for individuals . . . ."[10]

The United States has reached a turning point on privacy as other countries turn to prescriptive regulation and state and local governments threaten to fragment the U.S. digital market. U.S. industry is confronting privacy regulation from several sources. Global challenges stem from the European Union's General Data Protection Regulation ("GDPR")[11] and forced data localization requirements in several countries,[12] among others. Domestically, consumers and companies are seeing fragmentation as various agencies weigh in on privacy. Domestic fragmentation is compounded as some state governments increasingly regulate privacy, which is particularly problematic in light of the global and interstate nature of the Internet ecosystem.[13] There is a risk of even further fragmentation in the United States, as local governments join states in attempts to regulate privacy.[14] With fifty states and over 30,000 localities, the specter of balkanization is increasingly worrisome.

These divergent efforts do not benefit consumers. In fact, they lead to consumer confusion about how data will be treated and what their rights may be. Consumers may be unaware that the same data held by similar entities in different jurisdictions can be treated and regulated differently. Complexity also contributes to over-notification and warning fatigue. Not

---

[10] *Id.*

[11] *See*, European Commission, *2018 reform of EU data protection rules*, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en (last visited Nov. 7, 2018).

[12] *See* Sreenidhi Srinivasan, *The Emerging Trend of Data Localization* (Mar.1, 2018), http://stlr.org/2018/03/01/the-emerging-trend-of-data-localization/ (explaining that "very broad localization mandates could change the Internet as we know it, discourage innovation, and at the same time, not even achieve the intended goals").

[13] *See, e.g.*, California Online Privacy Protection Act; California Consumer Privacy Act of 2018; Illinois Biometric Information Privacy Act.

[14] *See, e.g.*, Chicago Personal Data Collection and Protection Ordinance, Record # 02018-3240 (introduced Apr. 18, 2018), *available at* https://chicago.legistar.com/LegislationDetail.aspx?ID=3480452&GUID=241F981B-94D6-43E8-AC73-D122DBECD413; Proposition B; City Privacy Guidelines, San Francisco Voter Information Pamphlet & Sample Ballot, Consolidated General Election (passed Nov. 6, 2018), *available at* https://voterguide.sfelections.org/en/city-privacy-guidelines.

only do these divergent efforts harm consumers, they have adverse economic consequences by straining resources and unnecessarily burdening the private sector.

As part of the effort to promote a harmonized privacy regime, sectoral laws should be examined in the context of any national privacy framework, to ensure consistent treatment of data and avoid dual jurisdiction. In the RFC, NTIA presumes that sectoral laws—namely, the Health Insurance Portability and Accountability Act ("HIPAA"), the Gramm-Leach-Bliley Act ("GLBA"), the Fair Credit Reporting Act ("FCRA"), and the Children's Online Privacy and Protection Act ("COPPA")—should be excepted from any national framework. Certain sectoral laws may reasonably be excepted from a national framework because they are examples of Congress's judgment about specific risks in particular sectors. However, NTIA and others should carefully examine (1) how a privacy framework would intersect with existing sectoral laws and (2) to what extent those sectoral laws will remain in effect following the adoption of a national framework.

NTIA and others should promote consistent treatment of similar information and consider how to harmonize existing regimes that treat identical information differently based solely on who collects or holds it. One example of a sector approach that should be reconsidered is the Communications Act and FCC regulation of specific information when handled by telecommunications carriers but not by other companies. Consumers do not expect their communications data to be subject to different privacy protections when they use an online communication service versus a service that is covered by the Communications Act. A bifurcated privacy regime also creates inconsistencies that distort competition. Therefore, provisions of the Communications Act and FCC regulation should be reviewed and potentially superseded by a national framework that applies universally to consumer data and prevents dual

jurisdiction. This uniform framework should be enforced by a single regulator at the federal level, acknowledging the possibility of State Attorneys General being authorized to enforce the federal law. For the reasons discussed below, and notwithstanding broader Federal Trade Commission ("FTC") jurisdictional issues, the FTC should enforce a uniform national framework across all sectors.

B. Comprehensive Application Is Laudable and Promoted by Technological-Neutrality.

NTIA proposes that "[a]ny action addressing consumer privacy should apply to all private sector organizations that collect, store, use, or share personal data . . . ."[15] Ideally, privacy protections should be technology-neutral and apply uniformly. CTIA has urged government to avoid regulatory classifications or technology choices that dictate outcomes.[16] Consumers do not expect privacy rights to differ based on regulatory arcana or platform characteristics.

Fitting with the concept of comprehensive application, NTIA rightly identifies the FTC as the agency to enforce consumer privacy. Identifying a single agency to enforce a national privacy framework will avoid duplication and inconsistent outcomes. The FTC is the appropriate agency to fill this role as it has the right enforcement tools and capabilities to address privacy and consumer protection. With decades of experience in consumer privacy,[17] it has brought more than 500 privacy-related enforcement actions, including actions against a range of

[15] RFC at 48602.
[16] CTIA, *Positions: Privacy*, https://www.ctia.org/positions/privacy ("Policymakers should seek a privacy framework that ensures consistent treatment of consumer information across platforms and applications. Such an approach would minimize consumer confusion and ensure all players in the mobile ecosystem can compete on a level playing field.") (last visited Nov. 6, 2018).
[17] FTC, *Protecting Consumer Privacy and Security*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security ("The FTC has been the chief federal agency on privacy policy and enforcement since the 1970s . . . .") (last visited Nov. 6, 2018).

Internet companies.[18] At the heart of the FTC's approach to protecting privacy is a balancing of benefits and harms.[19] The FTC generally offers a consistent regulatory approach, embodied by its flexible, notice-and-choice framework. As the ISP Privacy Principles make clear: "[T]he highly respected FTC framework . . . has protected internet users for years and provided the flexibility necessary to innovate new product solutions to enhance consumers' online experiences."[20]

Finally, CTIA agrees with NTIA that it is important to ensure that the FTC has the resources, authority, and direction to enforce consumer privacy in a way that balances strong consumer protection, legal clarity, and flexibility to innovate.[21]

C. A Flexible, Risk- and Outcome-Based Approach Is Critical to Ensure Continued Innovation and Protect Consumer Privacy.

Flexibility is another critical goal for federal privacy policy. A flexible national framework will ensure that privacy protections do not stifle or disrupt innovation. NTIA rightfully highlights the virtue of flexibility in privacy approaches throughout the RFC, noting that (1) organizations must have flexibility in protecting consumer privacy[22] and (2) the U.S. regulatory framework needs to remain flexible in order to, among other things, allow for innovation and accommodate "novel business models and technologies."[23]

---

[18] *See* FTC, *Privacy & Data Security Update: 2017*, at 2 (Jan. 2018), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf.

[19] *See, e.g.*, FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, at 47-48 (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (in discussing consent, FTC discussed importance of sensitive data, while observing that "on the other hand, the risks to consumers may not justify the potential burdens on general audience businesses that incidentally collect and use sensitive information.").

[20] CTIA et al., *ISP Privacy Principles* (Jan. 27, 2017), https://api.ctia.org/docs/default-source/default-document-library/final---protecting-consumer-privacy-online.pdf.

[21] *See* RFC at 48602.

[22] *See, e.g., id.*

[23] *Id.*

Additionally, CTIA applauds the risk- and outcome-based approach that NTIA promotes in the RFC: "Risk management is the core of this Administration's approach, as it provides the flexibility to encourage innovation in business models and privacy tools, while focusing on potential consumer harm and maximizing privacy outcomes."[24] Such an approach is the best way to have comprehensive application across the diversity of U.S. organizations. NTIA proposes modeling its approach on the risk- and outcome-based model used to date in cybersecurity, suggesting that "instead of creating a compliance model that creates cumbersome red tape—without necessarily achieving measurable privacy protections—the approach to privacy regulations should be based on risk modeling and focused on creating user-centric outcomes."[25] CTIA agrees. A risk- and outcome-based approach is the best way to develop expectations and approaches that can be useful to varied industries, companies, and abilities. Indeed, CTIA members have been honing and employing risk management concepts and practices for decades. Risk management is at the heart of FTC's approach to privacy and security,[26] and it is encouraging that it is a guiding principle for NTIA, as well.

Critical to a risk-based approach to privacy is an appropriate understanding of a privacy risk. CTIA urges NTIA to work with stakeholders to guide efforts to define "risk" as part of this proceeding. What constitutes privacy risk or harm is currently being examined through several agency efforts, including at the National Institute of Standards and Technology ("NIST")[27] and

---

[24] *Id.*
[25] *Id.*
[26] *See* FTC, *Start with Security: A Guide for Business* 1 (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (advising companies to "assess their options and make reasonable choices based on the nature of their business and the sensitivity of the information involved.").
[27] *See* NIST, *Privacy Framework*, https://www.nist.gov/privacy-framework (last visited Nov. 6, 2018) ("The NIST Privacy Framework is currently under development. NIST envisions that it will be a voluntary tool for organizations to better identify, assess, manage, and communicate about privacy risks so that individuals can enjoy the benefits of innovative technologies with greater confidence and trust.").

the FTC.[28] NTIA should use this current process to help steer those determinations and avoid conflicting definitions. Divergent approaches to defining the scope of privacy risks or harms—just like divergent privacy regimes as a whole—will risk confusing consumers and overburdening businesses.

III. NTIA'S PROPOSED PRIVACY OUTCOMES PROPERLY IDENTIFY IMPORTANT AREAS FOR FURTHER CONSIDERATION.

In addition to its goals for federal action, NTIA identifies "user-centric privacy outcomes that underpin the protections that should be produced by any Federal actions on consumer-privacy policy." NTIA wisely is not proposing a specific legal standard; its proposed outcomes are "inputs for building better privacy protections."[29] As highlighted below, CTIA suggests that some issues identified by NTIA require particular care and consideration as NTIA seeks to encourage innovation and economic growth while balancing interests in privacy.

A. Transparency Is a Core Privacy Principle that the Communications Sector Has Long Advanced.

CTIA agrees with NTIA that "users should be able to easily understand how an organization collects, stores, uses, and shares their personal information."[30] Transparency is a core principle of the current FTC approach to consumer privacy.[31] As the FTC explains, "[c]ompanies should disclose details about their collection and use of consumers' information."[32]

---

[28] *See* FTC, BE & BCP Staff Perspective, *FTC Informational Injury Workshop* (Oct. 2018), https://www.ftc.gov/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective; *see also* FTC, *FTC Hearing on Competition and Consumer Protection in the 21st Century - February 2019*, https://www.ftc.gov/news-events/events-calendar/ftc-hearing-competition-consumer-protection-21st-century-february-2019 (last visited Nov. 6, 2018).

[29] RFC at 48601.

[30] *Id.*

[31] *See* FTC, Staff Report, *Mobile Privacy Disclosures: Building Trust Through Transparency*, at 5-6 (Feb. 2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf (explaining that the FTC's seminal 2012 Privacy Report identified three core principles, one of which was "Greater Transparency").

[32] *Id.* at 6.

Transparency is also important under the current FTC approach to privacy, as it enables the agency to hold companies accountable to the commitments companies make to the public.

Transparency is a value long embraced by the Communications Sector. As part of the ISP Privacy Principles, CTIA and others committed to "continue to provide their broadband customers with a clear, comprehensible, accurate, and continuously available privacy notice that describes the customer information we collect, how we will use that information, and when we will share that information with third parties."[33] Verizon has urged that "[c]ompanies must provide clear and easy to understand information about their practices with respect to the collection, use, and sharing of personal information. As part of transparency, companies should have a mechanism that provides consumers with reasonable access to what information the company has about that consumer."[34] AT&T has similarly urged for transparency to be part of a national privacy law that builds on the FTC's framework: "Legislation should require companies to have a privacy policy that gives consumers clear and comprehensible information about the categories of data that are being collected, how consumer data is used and the types of third parties with whom data may be shared. Customers should have easy-to-understand privacy choices." Carriers and others have policies on their websites, which state their consumer data practices. While companies take varied approaches that evolve over time, the sector has continued to innovate in their communications about privacy with consumers and the public.

CTIA supports federal legislation that expects companies to provide consumers clear and comprehensible information about the categories of data that are being collected, used, or shared, and the types of third parties with whom that information may be shared.

---

[33] CTIA et al., *ISP Privacy Principles* (Jan. 27, 2017), https://api.ctia.org/docs/default-source/default-document-library/final---protecting-consumer-privacy-online.pdf.

[34] Verizon, Kathy Grillo, *Privacy: It's time for Congress to do right by consumers* (Oct. 8, 2018), https://www.verizon.com/about/news/privacy-its-time-congress-do-right-consumers.

B. Reasonable Consumer Control Over Data Is an Important Principle.

CTIA supports reasonable consumer control of data and agrees with NTIA that consumers "should be able to exercise reasonable control over the collection, use, storage, and disclosure of the personal information they provide to organizations."[35] This includes consumer choice, which is a principle that CTIA and others have committed to:

> ISPs will continue to give broadband customers easy-to-understand privacy choices based on the sensitivity of their personal data and how it will be used or disclosed, consistent with the FTC's privacy framework. In particular, ISPs will continue to: (i) follow the FTC's guidance regarding opt-in consent for the use and sharing of sensitive information as defined by the FTC; (ii) offer an opt-out choice to use non-sensitive customer information for personalized third-party marketing; and (iii) rely on implied consent to use customer information in activities like service fulfillment and support, fraud prevention, market research, product development, network management and security, compliance with law, and first-party marketing. This is the same flexible choice approach used across the Internet ecosystem and is very familiar to consumers.[36]

CTIA applauds NTIA's recognition of the importance of "reasonableness" in any evaluation of how to manage consumer control. NTIA rightly explains that "which controls to offer, when to offer them, and how they are offered should depend on context, taking into consideration factors such as a user's expectations and the sensitivity of the information."[37]

CTIA supports federal legislation that provides consumers with easy-to-understand privacy choices based upon the sensitivity of the information and how it is being collected, used, or shared.

C. Robust Security Is Fundamental to Privacy.

CTIA agrees with NTIA that "[o]rganizations that collect, store, use, or share personal information should employ security safeguards to secure data," and that such "organizations

---

[35] RFC at 48601.
[36] CTIA et al., *ISP Privacy Principles* (Jan. 27, 2017), https://api.ctia.org/docs/default-source/default-document-library/final---protecting-consumer-privacy-online.pdf.
[37] RFC at 48601.

should take reasonable security measures appropriate to the level of risk associated with the improper loss of, or improper access to, the collected personal data."[38]

CTIA and its members support robust data security principles that are risk based, flexible, and scalable. CTIA, through its Cybersecurity Working Group,[39] is actively engaged in the security discussion at the national level and regularly collaborates with NIST on its cybersecurity efforts and guidance, including the *Framework for Improving Critical Infrastructure Cybersecurity*.[40] Data security is also one of the ISP Privacy Principles that CTIA and others have committed to:

> ISPs will continue to take reasonable measures to protect customer information we collect from unauthorized use, disclosure, or access. Consistent with the FTC's framework, precedent, and guidance, these measures will take into account the nature and scope of the ISP's activities, the sensitivity of the data, the size of the ISP, and technical feasibility.[41]

The commitment of the wireless industry to security is seen in the daily actions of carriers and others on the front lines of cyberattacks. The wireless industry is innovating to make the networks of the future even more secure. In addition to the enhanced privacy protections — like encryption of each device's international mobile subscriber identity, or IMSI — 5G will boast cutting edge security enhancements as well.[42]

CTIA supports federal legislation that requires companies to take reasonable technical, administrative, and physical measures to secure consumers' personal information. Federal

---

[38] *Id*. at 48601-02.
[39] CTIA, *Cybersecurity Working Group*, https://www.ctia.org/about-ctia/membership/cybersecurity-working-group (last visited Nov. 6, 2018) ("CTIA leads a forum that brings together all sectors of wireless communications—including service providers, manufacturers and wireless data, internet and applications companies—to advise on policy and best practices.").
[40] *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, NIST (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
[41] CTIA et al., *ISP Privacy Principles* (Jan. 27, 2017), https://api.ctia.org/docs/default-source/default-document-library/final---protecting-consumer-privacy-online.pdf.
[42] *See* CTIA, White Paper, *Protecting America's Next Generation Networks* (July 2018), *available at* https://www.ctia.org/news/protecting-americas-next-generation-networks.

legislation should also include a data breach notification standard based upon a reasonable risk that the breach will result in actual harm, such as identity theft or other financial harm, to the consumer. Further, federal legislation should preempt existing state laws to avoid the patchwork approach to current data breach notification requirements.

D. Access and Correction Rights Should Be Considered Under a Flexible, Risk-Management Framework.

CTIA understands why NTIA is considering advancing the outcome of providing consumers "qualified access to personal data that [consumers] have provided, and [the ability] to rectify, complete, amend, or delete this data" and commends NTIA's thoughtful approach. CTIA supports providing consumers reasonable control over their data. However, NTIA should be sure to consider the challenges that uniform access and correction rights may present, especially for small businesses.

NTIA should be cautious when making recommendations or determinations on access and correction rights. This is an area for risk management and flexibility. NTIA rightfully acknowledges the need to consider impacts, such as privacy risks.[43] All users, for example, may not need access to or the right to amend data in many circumstances, particularly where data is not being used in access decisions like employment or credit. Organizations, especially small organizations, will have different abilities to allow consumers to access and correct data. Access and correction rights also raise security considerations. Requiring companies to provide access, especially along with correction rights, will present challenges for companies, including those related to authentication of users and the burden to appropriately verify the accuracy of "corrected" information being provided.

[43] RFC at 48601.

E. Reasonable and Appropriate Data Minimization Should Be Approached Carefully.

NTIA suggests that "[d]ata 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."[44] NTIA should be careful to balance recommendations in a way that does not stifle innovative uses.

Specifically, while data minimization is an important concept in many scenarios, NTIA should be careful not to embrace the underlying assumption that collection of data is inherently negative, or that less data is always or generally better. Quite the contrary, the federal government has studied and touted the benefits of "big data" on multiple occasions.

The FTC in particular continually examines the implications of big data, including both concerns and benefits. The FTC's 2016 *Big Data Report* explained that "big data" can make possible "numerous opportunities for improvements in society. In addition to more effectively matching products and services to consumers, big data can create opportunities for low-income and underserved communities. For example, . . . big data is helping target educational, credit, healthcare, and employment opportunities to low-income and underserved populations."[45] And just this week, the FTC held hearings to explore the role of big data in competition and innovation.[46] As the federal government moves forward with privacy policy, it is imperative to focus on the benefits of "big data."

Just one example of innovation that will be fueled by data is Artificial Intelligence ("AI"). For AI to reach its full potential, it will require access to quality data, including data that

---

[44] *Id.*
[45] FTC, *Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues*, at *i* (Jan. 2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.
[46] *See* FTC Hearings on Competition and Consumer Protection in the 21st Century, Hearing #6, Nov. 6-8, 2018.

is collected in the future and data that has already been collected. NTIA should acknowledge these future beneficial innovations and the need to enable robust collection and use of data.

Additionally, NTIA should make clear that any national privacy framework should encourage organizations to engage in de-identification and aggregation, which are critical, privacy-enhancing, and consumer-friendly activities that can enable innovative uses of data while respecting consumer privacy. De-identification and aggregation have many benefits, including security benefits such as facilitating information sharing and turning useful data into a less attractive target to bad actors. Other benefits include improving medical research, improving traffic flow and transportation infrastructure, analyzing disaster recovery efforts, monitoring socio-economic conditions, allocating police resources, and improving the dissemination of useful information to consumers in a manner that increases competition and innovation and reduces prices.[47] Fortunately, the FTC has put forth a three-part test for using and sharing de-identified data, a test that is tied to the concept of reasonableness.[48] The FTC's test is designed to provide strong consumer protection even as technology evolves to enable new methods of data re-identification. Further, it is outcome-based, which allows companies to adopt new and innovative de-identification methods, tools, and technology to achieve the reasonable

[47] *See id.* at 20-21; Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data*, 64 Stan. L. Rev. Online 63 (2012), https://www.stanfordlawreview.org/online/privacy-paradox-privacy-and-big-data/ (discussing manifold public interest benefits from big data analytics and arguing that sophisticated re-identification should underscore, rather than undermine, importance of de-identification); Ann Cavoukian & Khaled El Emam, *Dispelling the Myths Surrounding De-Identification* (2011), https://www.ipc.on.ca/images/Resources/anonymization.pdf; *see also* Reply Comments of T-Mobile USA, Inc., WC Docket No. 13-306, at 3-7 (Mar. 4, 2014) (addressing studies and concluding that "the risk of privacy harm from re-identification is significantly lower than many risks we take without concern" (internal quotation marks omitted)); *id.* at 7-8 (recounting various uses of de-identified data in the public interest).

[48] FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, at 22 (Mar. 2012) (holding that as long as (1) a given data set is not reasonably identifiable, (2) the company publicly commits not to re-identify it, and (3) the company requires any downstream users of the data to keep it in de-identified form, that data will fall outside the scope of the framework" that otherwise "applies to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consume, computer, or other device, unless the entity collects only non-sensitive data from fewer than 5,000 consumers per year and does not share the data with third parties."), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

standards.

In short, de-identification and aggregation allow for the benefits of "big data" while reducing the associated privacy and security risks. These benefits, and the many others, are at risk under any regime that does not treat de-identified or aggregated data as distinct from sensitive data.

IV. CONCLUSION.

CTIA appreciates the opportunity to participate in NTIA's consumer privacy proceeding at this critical juncture. CTIA largely supports NTIA's proposal and urges NTIA to complete this process and produce a privacy framework that it can offer as the groundwork for federal privacy legislation and other harmonized federal privacy activities.

Respectfully submitted,

/s/ Melanie K. Tiano
Melanie K. Tiano
Director, Cybersecurity and Privacy

Thomas C. Power
Senior Vice President and General Counsel

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org