Multicultural Media, Telecom & Internet Council

**1919 Pennsylvania Ave. NW, Suite 725**
**Washington, D.C. 20006**
**Phone: 202-332-0500**
**www.mmtconline.org**

December 12, 2018

David J. Redl
Assistant Secretary for Communications and Information
National Telecommunications and Information Administration
1401 Constitution Ave NW
Washington, D.C. 20230

Dear Assistant Secretary Redl:

RE: Request for Comments on *Developing the Administration's Approach to Consumer Privacy*, **Docket No. 180821780-8780-01**

The Multicultural Media, Telecom and Internet Council ("MMTC") respectfully submits this response to the request of the National Telecommunications and Information Administration ("NTIA") for comments on *Developing the Administration's Approach to Consumer Privacy* ("Privacy RFC" or "RFC").[1] In its RFC, NTIA outlines a broad framework that focuses on a set of high-level goals and user-centric privacy outcomes designed to balance consumer protection with organizational flexibility in achieving those goals and outcomes. As the nation continues to face a persistent digital divide, with profound disparities in broadband adoption based on race, location, and wealth, it is vital that NTIA and the Administration continue to develop this approach with these concerns in mind.

Broadband access is essential to full participation and access to opportunities for education, jobs, telemedicine, civic engagement, and enhanced quality of life. Communities of color, low-income individuals, and other marginalized populations historically have had limited opportunities to gain new skills, secure quality and high-wage jobs, obtain a valuable education, participate in civic dialogue, and benefit from advanced telemedicine and other technologies.

NTIA has reported that "nearly three-quarters of Internet-using households had significant concerns about online privacy and security risks in 2017, while a third said these worries caused them to hold back from some online activities. About 20 percent said they had experienced an

[1] *Developing the Administration's Approach to Consumer Privacy*, National Telecommunications and Information Administration, Docket No. 180821780-8780-01 ("NTIA Privacy RFC")

online security breach, identity theft, or a similar crime during the past year."[2] Low-income populations and other marginalized groups are more sensitive to the harms caused by serious data breaches, without the informational and financial resources to recover. As such, it is imperative that the Administration's approach to consumer privacy takes the unique needs of low-income and other marginalized groups into account.

**The Regulatory Landscape Must Be Harmonized with Privacy Protections That Are Technology Neutral**

Comprehensive Application

A federal privacy protection framework applied across all fifty states will provide the strongest protection for consumers, will promote broadband adoption, and is likely to help bridge the digital divide. As it currently stands, consumer privacy is governed by a patchwork of state and federal statutes that place duplicative or contradictory privacy-related obligations on organizations and only further confuse consumers. Where a consumer lives or works should not determine how the privacy of their information should be protected. A robust federal privacy framework would eliminate a patchwork of state privacy laws, minimize confusion for consumers, and provide consistency and certainty for the organizations seeking to comply with the laws.

Further, MMTC agrees with NTIA that "[a]ny action addressing consumer privacy should apply to all private sector organizations that collect, store, use, or share personal data in activities that are not covered by sectoral laws."[3] Currently, internet service providers ("ISPs" such as AT&T, Comcast, and Verizon) are regulated differently from online "edge" companies such as Facebook and Google under certain federal and state laws,[4] which contributes to increased consumer confusion and risk, depending on where and how the consumer is using the internet.

---

[2] Rafi Goldberg, *Most Americans Continue to Have Privacy and Security Concerns, NTIA Survey Finds*, NTIA Blog (August 1, 2018), https://www.ntia.doc.gov/blog/2018/most-americans-continue-have-privacy-and-security-concerns-ntia-survey-finds

[3] *NTIA Privacy RFC, supra* at 1.

[4] Notwithstanding the repeal of the FCC's 2015 Title II Order (*Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601 (2015) ("*2015 Order*"), which classified ISPs as common carriers, the FCC's new Restoring Internet Freedom Order still imposes additional written transparency disclosures on ISPs regarding network management, security, and privacy practices, amongst others. *Restoring Internet Freedom*, Declaratory Ruling, Report and Order, and Order, 33 FCC Rcd 311, ¶¶ 209-238 (2018). No such requirements are imposed on edge providers or other members of the internet ecosystem. *See also* Minn. Stat. §§ 325M.01 - .09 (prohibiting ISPs from knowing disclosure of consumer personally identifiable information) and Nevada Revised Stat. § 205.498 (requiring an ISP to keep all information concerning a consumer confidential unless under certain circumstances or with the consumer's permission).

As it stands, consumers already do not differentiate between ISPs, edge companies, and other entities that impact multiple aspects of their online experiences, and they have an expectation that privacy rules are consistent and *apply broadly to all actors online*. MMTC, along with eight leading intergovernmental, consumer, business, and social justice organizations, has commented that "[e]ven if consumers fully understood the difference between [ISPs and edge providers], the system is far more complicated, with many intermediaries and partners working to ensure that services are delivered efficiently and to the correct consumers."[5] Further, leaving consumers reliant upon inconsistent sector-specific regulation will increase variability and contribute to complexity.

A uniform federal framework, applied across the entire internet ecosystem, will eliminate consumer confusion while minimizing multijurisdictional compliance burdens on companies that interface with consumers through the internet, creating stronger privacy and security protections overall.

**A Single Federal Framework with the FTC As the Enforcement Agency Using Section 5 of the FTC Act Is Preferable to a Patchwork of State Legislation, Empowering Small Businesses and Consumers**

Harmonize the Regulatory Landscape under FTC Authority

When it comes to consumer privacy, the simpler the better. Thus, in addition to the confusion resulting from different privacy protections based on technology, a fragmented enforcement approach to consumer privacy will have an adverse impact on many vulnerable consumers, who are particularly susceptible to long-term consequences resulting from harmful practices conducted online and offline. The Federal Trade Commission ("FTC") is uniquely positioned to regulate consumer privacy, with years of expertise, experience, and precedent through over 500 cases adjudicated under agency rules and regulations.[6] Specifically, the FTC has brought enforcement actions addressing a wide range of privacy issues, including spam, social networking, behavioral advertising, pretexting, spyware, peer-to-peer file sharing, and mobile.[7] The FTC's history and experience grants the agency the judgment to understand how consumers interpret, manage, and are affected by online influences.

---

[5] Comments of the Multicultural Media, Telecom and Internet Council and Eight Leading Intergovernmental, Consumer, Business and Social Justice Organizations, WC Docket No. 16-106 (filed May 27, 2016) ("MMTC, et al. Comments"), http://www.mmtconline.org/wp-content/uploads/2016/05/PARTNERPRIVACY-COMMENTS-52716.pdf.

[6] Lesley Fair, *FTC staff comments on FCC privacy proposal,* FTC Business Blog (June 1, 2016, 11:00 AM), https://www.ftc.gov/news-events/blogs/business-blog/2016/06/ftc-staff-comments-fcc-privacy-proposal.

[7] *Privacy & Data Security Update: 2017*, Federal Trade Commission, January 2017 – December 2017, 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

Additionally, Section 5 of the Federal Trade Commission Act ("FTC Act") prohibits "unfair or deceptive acts or practices in or affecting commerce" and grants the agency with enforcement authority.[8] The FTC also has authority to enforce a variety of sector-specific laws that provide significant protections to consumers, and particularly vulnerable consumers that have been historically marginalized. Such laws include the Truth in Lending Act, the Children's Online Privacy Protection Act, the Equal Credit Opportunity Act, the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, and the Telemarketing and Consumer Fraud and Abuse Prevention Act.[9]

While it has the authority to address a wide array of practices affecting consumers, including those that emerge with the development of new technologies and business models, careful consideration should be given as to whether additional tools are needed to ensure that the FTC is able to effectively protect the privacy of consumers. MMTC is open to working with NTIA and the FTC to examine whether additional enforcement authority, rulemaking authority, and/or more human and financial resources are needed to maximize the FTC's ability to serve as the privacy watchdog for the broad and complex internet ecosystem. This would include the repeal of certain FTC exemptions from enforcement under the FTC Act, where the FTC does not have authority to regulate certain industries, such as common carriers.[10]

Transparency

It is vital that any regulatory approach be as transparent as possible to consumers. Currently, entities that collect, store, use, and share personal data have lengthy and legalistic privacy policies that are difficult to understand and largely unread by consumers. Many websites provide statements that pop up when users visit, generally stating that "[b]y using this website, you agree to the use of tracking cookies." However, these statements largely used across the internet ecosystem are vague and simply require consumers to agree to the use of tracking cookies used by the website but provide little information on how the data is used.

Privacy terms should be simple to understand and clearly outline what data is collected; how it is used; how long it is stored; and what data is shared with other entities, for what purpose, and with whom.

Moreover, in providing consumers with understandable privacy policies, it is important that these policies be translated into other languages. The FTC previously has commented that "if a subscriber transacts business with the Broadband Internet Access Service ('BIAS') provider in a language other than English, the BIAS provider should translate the privacy notice into that

---

[8] 15 USC § 45

[9] *Privacy & Data Security Update: 2017*, *supra* at 1.

[10] 15 USC 45(a)(2); *see generally FTC v AT&T Mobility LLC*, 888 F.3d 848 (9th Cir. 2018)(clarifying in an *en banc* decision that the FTC's authority to regulate a common carrier is activity-based, not status-based). Common carriers engaged in non-common carrier activity are under FTC enforcement, but common carrier activity is not.

language" and that "if a company advertises or offers a product for sale in a language other than English, the company should also translate any material disclosures into that language."[11] This approach is in alignment with the FTC's existing Business Opportunity Rule and policy statement on foreign language advertising.[12]

MMTC agrees with the FTC's approach, and we believe that these requirements must extend to all BIAS and edge providers to ensure non-English-speaking and limited-English-proficient consumers are not left without access to vital information on how their data is handled.

Scalability

In its RFC, NTIA states that "[the] Administration should ensure that the proverbial sticks used to incentivize strong consumer privacy outcomes are deployed in proportion to the scale and scope of the information an organization is handling."[13]

For our entire 32-year existence, MMTC has advocated for policies that promote and encourage small business development and success by creating opportunities for diverse businesses to thrive, thereby enabling diverse communities to close economic gaps. The internet has provided unprecedented pathways to success for small, minority, and women-owned businesses to succeed. Thus, MMTC agrees that the FTC should ensure it does not place undue compliance burdens on "small businesses that collect little personal information and do not maintain sensitive information about their customers […] so long as they make good-faith efforts to utilize privacy protections."[14] Notwithstanding, any considerations about undue burdens on small businesses must be appropriately balanced with consumer privacy protection goals and outcomes, and particularly when it comes to protecting vulnerable communities as we continue to work toward closing the digital divide.

Ensure Privacy Outcomes and Goals Encompass Key Privacy Principles

In a May 2018 letter, a diverse civil rights coalition of 51 national organizations, including MMTC, asserted that several key privacy principles be the cornerstone of any legislation designed to protect the Internet and extend its promise to all Americans.[15] To ensure the

---

[11] *Comments of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission*, WC Docket No. 16-106 (filed May 27, 2016), available at https://ecfsapi.fcc.gov/file/60002078443.pdf

[12] *See* Business Opportunity Rule, 16 C.F.R. § 437.3(a); Requirements concerning clear and conspicuous disclosures in foreign language advertising and sales materials, 16 C.F.R. § 14.9.

[13] *NTIA Privacy RFC, supra*.

[14] *Id.*

[15] Letter to Sen. John Thune, Sen. Bill Nelson, Rep. Greg Walden, and Rep. Frank Pallone from MANA, A National Latina Organization, National Urban League, OCA - Asian Pacific American Advocates National Center, *et al*, May 10, 2018, available at http://www.mmtconline.org/wp-content/uploads/2018/05/Data-Privacy_Access_Civil-Rights-Groups_5_10_18_FINAL.pdf

protection of vulnerable communities, NTIA should work with these principles in mind as it continues to shape its privacy framework.

Key principles that are echoed throughout this letter include strong protections for privacy and individual control of personal information, consistent rules and equal treatment across the country and in the internet ecosystem, and a renewed commitment to closing the digital divide.[16] Referring to the opportunities afforded by internet access, the letter holds that the principles are vital for ensuring that "this remarkable engine for civic, cultural, economic, and social engagement remain open, safe, and secure for all Americans."[17]

**Conclusion**

Our nation's leadership has a duty to protect all Americans. In light of the persistent digital divide, distrust, and confusion among consumers and our nation's most vulnerable communities, it is necessary that NTIA and the Administration shape privacy policies and legislation with their unique concerns in mind. In doing so, all of our nation's consumers can enjoy a secure experience when they engage online.

Respectfully submitted,

Maurita K. Coley

Maurita K. Coley
President and CEO
MMTC

[16] *Id.*
[17] *Id.*