**Before the**
**NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION**
**Washington, DC 20230**

| | | |
|---|---|---|
| **Developing the Administration's Approach to Consumer Privacy** | **)** **)** | **Docket No. 180821780-8780-01** **RIN 0660-XC043** |

**Comments of**

**NTCA–THE RURAL BROADBAND ASSOCIATION**

## I. INTRODUCTION

NTCA–The Rural Broadband Association (NTCA) hereby submits comments in response to the Request for Public Comments issued by the National Telecommunications and Information Administration (NTIA) of the Department of Commerce (Department).[1] NTCA represents nearly 850 independent, community-based telecommunications companies and cooperatives and more than 400 other firms that support or are themselves engaged in the provision of communications services in the most rural portions of America. All NTCA service provider members are full service rural local exchange carriers (RLECs) and Internet service providers (ISPs). NTCA members are committed to protecting the privacy of their customers, and as telecommunications providers are subject to specialized rules pursuant to Section 222 of the Communications Act, as amended.[2] NTCA participates actively in Federal Communications

[1] *Developing the Administration's Approach to Consumer Privacy: Request for Public Comment,* Docket No. 180821780-8780-01, RIN 0660-XC043, National Telecommunications and Information Administration, Department of Commerce, 83 Fed. Reg. 48600 (Sep. 26, 2018).

[2] 47 U.S.C. § 222; *see also* 47 C.F.R. § 64.2001, *et. seq.*

Commission (FCC) proceedings that addressed broadband privacy issues;[3] appeared at Federal workshops;[4] and has included privacy and data security programming in continuing legal education (CLE) programming offered to its members.[5] NTCA's attention to these issues reflects its members' commitment to safeguarding consumer privacy while responding dynamically to evolving technology and consumer expectations.

## II. DISCUSSION

### A. FUNDAMENTAL INTEGRATION OF TECHNOLOGY IN CONSUMERS' LIVES WARRANTS A STUDIED EXAMINATON OF PRIVACY POLICY

Historic regulatory paradigms that govern privacy must be reevaluated as broadband-enabled applications and services become further intertwined with commercial and residential appliances and applications in an Internet of Things (IoT) environment. Policies that address consumer protection and privacy are ripe for examination as network, edge and application providers support healthcare, education, commerce and other vital functions, particularly as each actor in the ecosystem may have access to sensitive customer data. The rapid integration of advanced technology into ordinary life can be discerned from the changing roster of firms with highest market values. The highest valued companies in 2006 were ExxonMobil, GE,

[3] *See, e.g.., Protecting the Privacy of Customers of Broadband and Other Telecommunications Services: Comments of NTCA–The Rural Broadband Association,* Federal Communications Commission, Docket No. 16-106 (May 27, 2016).

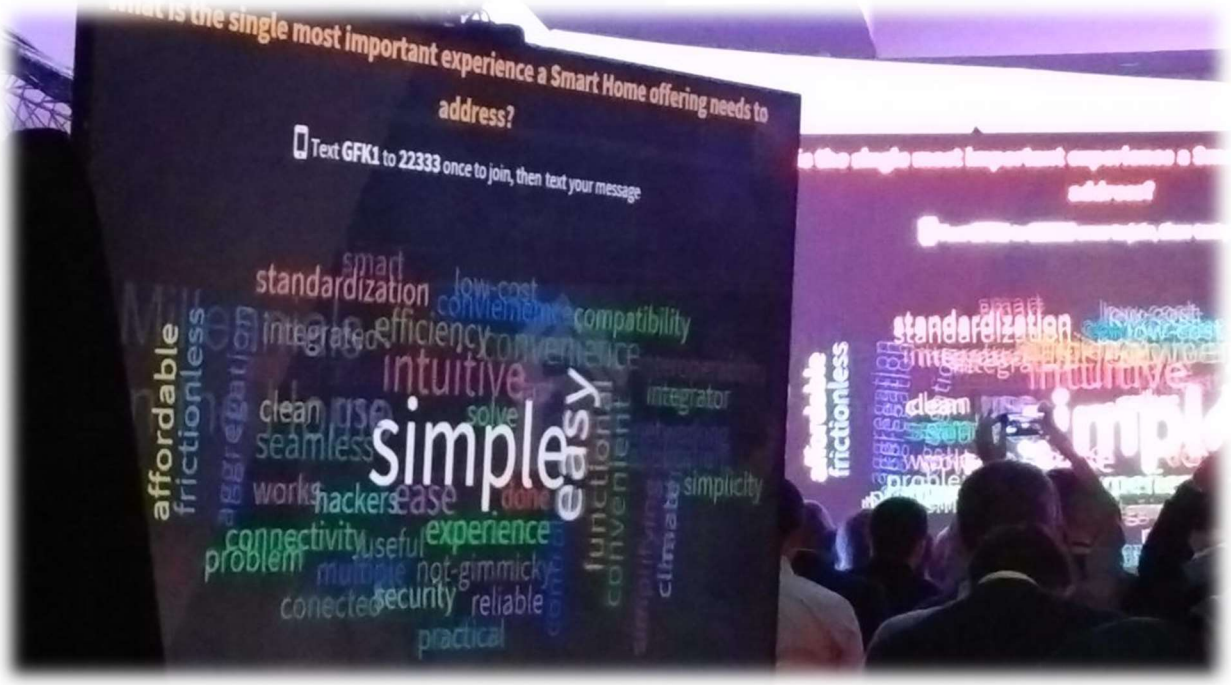
[4] *See,* "FCC Staff Announce Agenda for Public Workshop on Broadband Consumer Policy," FCC News (Apr. 22, 2015) (FCC Public Workshop on Broadband Consumer Policy (Apr. 28, 2015) (https://apps.fcc.gov/edocs_public/attachment/DOC-333155A1.pdf) (announcing appearance of NTCA VP Policy).

[5] Joshua Seidemann, YOUR FACE IS NOT A TESTIMONIAL ACT*,* NTCA Legal Seminar, Nashville (2017); Joshua Seidemann, PLEASE DON'T EMBARRASS THE FUTURE, NTCA Legal Seminar, Seattle (2018).

Microsoft, and Citigroup; by 2016, those companies had been replaced by Apple, Amazon, Alphabet and Microsoft (those companies remain the top four in 2018).[6] In fact, Microsoft's active promotion of White Spaces is consistent with its interest is in building a greater market base for connected devices. The import of the overall market transition is less about seismic change than it is about an almost imperceptible change – a quiet creeping of technology into more and more aspects of daily consumer and industrial life, and in a way that is intended specifically to be non-intrusive.

In a session devoted to millennials' use of technology at the 2017 Consumer Electronics Show, a panelist took a spot poll and asked members of the capacity audience to text the most important criterion they would s eek in a smart home system. As a word cloud refreshed several times over the next minute, one word emerged and remained the largest: simple.

[6] *See,* Felix Richter, "The Age of Tech," Statista (Aug. 2, 2016) https://www.statista.com/chart/5403/most-valuable-companies-2006-vs-2016/; *see, also,* "The 100 Largest Companies in the World by Market Value in 2018," Statista (https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-value/) (viewed Nov. 8, 2018, 12:35).




A revolution that is forecast to hit $4.6 billion in annual revenues and reach 41.2 million connected smart-home units (increases of 36 percent and 43 percent, respectively)[7] is at its core desired by users -- and accordingly formulated by designers -- only to make things easier. And to make things easier, more easily. Strides toward standardization, efficiency, intuitiveness and simplicity, however, can pave a path toward greater unnoticed risk as devices (and not just networks) gather increasing amounts and broader of types of data both actively *and* passively.[8] This can be particularly concerning since, unlike the types of safeguards enacted by software vendors and ISPs, many IoT devices are not built with anti-virus capabilities; do not require

[7] "Total Consumer Tech Revenue to Reach Record $377 Billion in 2018, Says CTA Mid-Year Report," Consumer Technology Association, Arlington, VA (Jul. 31, 2018) (https://cta.tech/News/Press-Releases/2018/July/Total-Consumer-Tech-Revenue-to-Reach-Record-$377-B.aspx) (viewed Nov. 8, 2018, 12:19).

[8] *See, e.g.,* Lily Hay Newman, "Don't Freak Out About that Amazon Alexa Eavesdropping Situation," Wired (May 24, 2018).

users to change default log-in and password information; and, do not update to respond to changing threats.[9] Cisco predicts overall connected devices in the United States will increase from 2.3 billion to 4.1 billion, implicating applications ranging from healthcare to connected vehicles and pitting innovation against consumer trust and safety.

The Department's investigation is, therefore, timely. Ninety-percent (90%) of IoT devices collect at least one piece of personal information.[10] By way of example, the smart clothing industry is growing rapidly.[11] Sensors embedded in fabric can monitor metrics such as heart rate, respiration, body temperature and other data. Many consumers may not be overly concerned about the privacy of this data. However, implications of who owns and may share these types of data may be triggered if that information, by way of example, were to be shared with actuaries from health and life insurance companies to create tailored coverage and premiums.

With these evolving concerns in mind, NTCA has identified the hallmarks of "notice, choice and security" to address these issues.[12] To be sure, these guideposts mark broad

[9] *See,* Timothy W. Martin, "Smart Devices Draw New Defenses," Wall Street Journal, p.B1 (Oct. 18, 2018).

[10] Michael Roppolo, "Internet of Things Devices Full of Security Gaps, Study Shows," CBS News (Jul. 30, 2014 (https://www.cbsnews.com/news/internet-of-things-devices-full-of-security-gaps-study-shows/) (viewed Nov. 8, 2018, 12:50).

[11] Genevieve Scarano, "Report: Smart Clothing Shipments to Reach 26.9M Units by 2022," Sourcing Journal (Aug. 29, 2017) (https://sourcingjournal.com/topics/technology/report-smart-clothing-shipments-to-reach-26-9m-by-2022-71209/) (viewed Nov. 8, 2018, 12:52).

[12] Statement of Joshua Seidemann, NTCA Vice President of Policy, FCC Public Workshop on Broadband Consumer Policy (Apr. 28, 2015) (*see,* "FCC Staff Announce Agenda for Public Workshop on Broadband Consumer Policy," FCC News (Apr. 22, 2015) (https://apps.fcc.gov/edocs_public/attachmatch/DOC-333155A1.pdf) (viewed May 10, 2016, 13:44)).

categories of multi-layered, multi-faceted issues. Ultimately, however, they are tied directly to consumer interests, and therefore interlock neatly with existing legal standards that guide commercial practices of entities throughout the ecosystem who can access and amass consumer data. These touchstones should serve as guiding principles in the development of strong, technology-flexible, self-regulating standards that will be best suited to ensure privacy protections that are reasonably designed to keep pace with the dynamic field, regardless of industry silos and self-declared lines of business.

### B. THE FEDERAL TRADE COMMISSION IS THE MOST SUITABLE AGENCY OF JURISDICTION FOR BROADBAND PRIVACY.

The Federal Trade Commission (FTC) is the most suitable agency of jurisdiction for broadband privacy, since it is the agency of jurisdiction for consumer privacy, generally. The primary source for FTC authority is Section 5 of the FTC Act, which prohibits "unfair or deceptive or practices in or affecting commerce."[13] "Unfair or deceptive" is a material representation, omission, or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment. "Practice" is an action that (a) causes or is likely to cause substantial injury to the consumer which is not (b) reasonably avoided by the consumer or (c) outweighed by countervailing benefits to the consumer or competition.[14] These standards are rooted in a company's effective promise of how it will protect a customer's

[13] 15 U.S.C. §45(a)(1).

[14] *See,* 15 U.S.C. § 45(n). This standard is also incorporated in the Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. 111-203, 124 Stat. 1376, *codified at* 12 U.S.C. § 5511 (2011). This three-prong approach was first articulated in the FTC's "Policy Statement on Unfairness," and later incorporated into the FTC Act. *See,* https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness (viewed May 26, 2016, 12:27).

information, regardless of industry or vertical sector. The specific acts that are embraced by these standards are not defined. Congress deliberately, and presciently, crafted general terms, finding that if it "were to adopt the method of definition, it would undertake an endless task."[15] As explained by the FTC, "The statute was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion."[16] This can be a guiding principle for the Department's instant inquiry.

Rapidly evolving technology and the implications it bears upon privacy validate Congressional intent of more than a century ago. Current applications of these standards must address the impact of deceitful data collection and improper use of data; other considerations may include device design and unfair information security practices. In the vein of “notice, choice and security,” the FTC umbrella can cover obligations of edge, app, device and communications providers to maintain confidentiality; to collect data only in a manner consistent with stated policies; and, to protect that data.[17] NTCA submits that FTC guidelines as

[15] H.R. Cong. Rep. No 1142, 63rd Cong., 2d. Sess. at 19 (1941).

[16] FTC Policy Statement on Unfairness, *appended to, In re: International Harvester Co.,*104 F.T.C. 949, 1070 (1984), *citing FTC v. R.F. Keppel & Bro.,* 291 U.S. 304, 310 (1934) ("Neither the language nor the history of the Act suggests Congress intended to confine the forbidden methods to fixed and unyielding categories").

[17] *See, FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015) (failure to use readily available technology such as firewalls; storage of information in plain text; failure to implement adequate policies; failure to remedy known vulnerabilities; failure to use adequate protocols and passwords; failure to restrict access to network; and failure to follow incident response procedures, taken together, constitute unreasonable behavior).

illustrated by an evolving body of case law provide a substantial, relevant analytical construct.[18] NTCA submits, as well, that the broad scope of firms that participate in the edge, app, device and ISP market (and other markets supported by those technologies) argues for relying on the general standards of Section 5 of the Act, as opposed to creating new classes of technology-specific or sector-specific law. By way of illustration, HIPPA covers health care data,[19] while other regulations address children's online privacy protection.[20] Those laws address discrete data sets or audiences, and special provisions address special concerns. By contrast, consumer data, whether gathered by an ISP, an app provider, and on-line publisher or an on-line seller is governed by comprehensive principles that address the *type* of information without reference to the *holder* of that information. A single standard across the "connected ecosphere" would prevent a patchwork of differing standards for different players. Indeed, former FCC Chairman Tom Wheeler succinctly articulated this principle before the House Subcommittee on Communications and Technology, stating consumers deserve a "uniform expectation of privacy."[21]

---

[18] For a review of FTC privacy jurisprudence, *see*, Daniel H. Solove and Woodrow Hartzog, *The FTC and the New Common Law of Privacy,* 114 COLUMBIA L. REV. 583 (2014).

[19] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936, *codified at* 42 U.S.C. § 300(gg), 29 U.S.C. § 1181 *et seq. and* 42 U.S.C. 1320(d) *et seq.*

[20] Children's Online Privacy Protection Act of 1998, Pub. L. 105-277, 112 Stat. 2681, *codified at* 15 U.S.C. § 6501, *et seq.*

[21] Hearing before the U.S. House of Representatives Subcommittee on Communications and Technology, "Oversight of the Federal Communications Commission," Preliminary Transcript at 141 (Nov. 17, 2015). Chairman Wheeler further asserted in that testimony that the FCC "will not be regulating the edge providers differently" than ISPs. Although NTCA opposed FCC actions that imposed prescriptive privacy regulations singularly on ISPs (and which were eventually removed by invocation of the Congressional Review Act, *see,* S.J. Res. 34, 115th Cong. (2017-2018)), NTCA offers former Chairman Wheeler's articulation as applicable to the larger market of Internet-connected interactions and transactions.

On-line retailers process substantially the same information as their brick and mortar counterparts, which may be include certain information that is substantively similar to that obtained by app providers or social media sites. Consistent data privacy protections should apply to all parties that hold characteristically-similar information. Websites such as Facebook, Amazon, and others gather information about user habits and preferences, but there is no formal body of "Internet law" whose specific regulations address those practices. Rather, an evolving body of case law applies proven principles to the industry as it evolves to meet changing consumer perceptions, technology and market demands. This approach is sensible and creates a level playing field for all actors on the broadband stage. NTCA emphasizes that it does not advocate *disregard* for privacy; rather, NTCA advocates a *consistent regard* for privacy that addresses *all* players in the market who gather, store and use customer data.

ISPs such as NTCA members have been described as "in a position to develop highly detailed and comprehensive profiles of their customers – and to do so in a manner that may be completely invisible."[22] NTCA members do not, as a practice, engage in the brokering of customer data. Accordingly, NTCA submits that a level playing field administered beneath FTC oversight will provide consistent and comprehensive consumer protection while promoting parity among market players. Neither an NTCA member nor other ISP should be prevented from nor held liable for actions that if undertaken by another party would be permitted.

---

[22] *Protecting the Privacy of Broadband and Other Telecommunications Services: Notice of Proposed Rulemaking,* Federal Communications Commission, Docket No. 16-106, FCC 16-39, at para. 4 (2016).

Other firms have, and exercise, substantial use of customer data. By way of example, unless disabled, mobile Google maps can track a user's physical location and store that information over a period of years.[23] And, even disabling the function will not erase past history; one periodical declared, "Google's Location History Browser is a Minute-By-Minute Map of Your Life."[24] The extent to which technology is enabling firms to utilize data is expanding: Google AI not only predicts what people will write, but also when people will die. (Google's "Smart Compose" suggests words and phrases to help writers conclude sentences;[25] in trials, Google's Medical Brain team achieved accuracy rates over 90 percent predicting the deaths of hospital patients).[26] Amazon, Facebook, WhatsApp, and Apple offer competing technologies that rely on deep data collections and increasingly capable analytics.[27] The Washington Post uses cookies, web beacons and "other technologies" for online tracking and

[23] Matt Elliott, "Where to Find the Map that Shows Google is Tracking Your Location," c|net (Nov. 5, 2015) (http://www.cnet.com/how-to/how-to-delete-and-disable-your-google-location-history) (viewed May 19, 2016, 17:49).

[24] Greg Kumparak, "Google's Location History Browser is a Minute-By-Minute Map of Your Life," TechCrunch (Dec. 18, 2013) (http://techcrunch.com/2013/12/18/google-location-history) (viewed May 19, 2016, 18:05).

[25] Bryan Clark, "Gmail Adds a Predictive Type Feature Called Smart Compose (May 8, 2018) (https://thenextweb.com/google/2018/05/09/gmail-adds-a-predictive-type-feature-called-smart-compose/); *see, also,* Stephanie Merry, "Here's Why That's So [Disconcerting]," Washington Post, C1 (Oct. 27, 2018).

[26] Anthony Cuthbertson, "Google AI Can Predict When People Will Die with 95 Percent Accuracy," Independent (Jun. 19, 2018) (https://www.independent.co.uk/life-style/gadgets-and-tech/news/google-ai-predict-when-die-death-date-medical-brain-deepmind-a8405826.html).

[27] DJ Pangburn, "How - and Why - Apple, Google, and Facebook Follow You Around in Real Life," Fast Company (Dec. 22, 2017) (https://www.fastcompany.com/40477441/facebook-google-apple-know-where-you-are)

advertising.[28] NTCA does not decry these technologies; Google's ability to review "big data" enables its software to now recognize eye disease in scanned images. [29] However, NTCA proposes that the security and use of data sets should be addressed based upon the data, and not upon the holder.

Proper prosecution of these protections resides within the FTC. The primary function of the FTC is to protect mass-market consumers. The FTC has pursued hundreds of cases to protect the privacy and security of consumer information.[30] The FTC has not only the legal jurisdiction, but also the subject matter expertise. The FTC is the proper agency of jurisdiction to administer a level playing field.[31]

### C. A LEVEL PLAYING FIELD THROUGHOUT THE DATA ECOSYSTEM WILL ENSURE A CONSISTENT AND PROTECTED CONSUMER EXPERIENCE.

NTCA submits that, with regard to privacy issues, customers do not distinguish between the various parties whose collective roles create the online user experience; indeed, in some cases, consumers may not even be fully aware of all the actors that combine to provide access

[28] Privacy Policy, Washington Post (https://www.washingtonpost.com/privacy-policy/2011/11/18/gIQASIiaiN_story.html) (viewed May 25, 2016, 10:50). The Post explains further that in addition to itself, "third-parties may collect or receive certain information about your use of Services, including through the use of cookies, beacons, and similar technologies, and this information may be combined in information collected across different websites and online services."

[29] "Google Touts New AI-Powered Tools," Jack Nikas, Wall Street Journal, p.B1 (May 19, 2016).

[30] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services: Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission,* Federal Communications Commission, Docket No. 16-106, at 4 (May 27, 2016) (FTC Staff).

[31] In 2007, the FTC issued a 167-page review that delved into both the technical and legal bases of the internet and how the law approaches it. *See,* "Broadband Connectivity Competition Policy," Federal Trade Commission (June 2007).

to and use of an app, service, or other product or commercial interaction. Consumers therefore need and benefit from a uniform expectation of privacy and security for their online activities, and risk harm if disparate consumer protection obligations exist among broadband, app, device and edge providers with whom they interact in their online experience. Similar to the even-handed approach embraced by the *Browser Act*,[32] the framework that emerges from the Department's instant investigation should ultimately promote a single set of standards for data privacy without regard to the perceived regulatory status or line of business of a particular holder of data. Although as noted above Congress has addressed specific market segments with tailored rules, the universe of "on-line" data embraces everything from sensitive health data to who needs another quart of milk (smart scales set in a refrigerator can alert users when the weight of the carton indicates that the milk is "running low").[33] The FTC explained the interlocked nature of the marketplace in comments to the FCC:

> . . . it makes little sense to exclude only BIAS [broadband internet access service] providers from the FTC's privacy and data security jurisdiction, which covers virtually all other entities in the Internet ecosystem, including some of the largest and most powerful companies using consumer data. Indeed, the FTC has actively applied its authority across the Internet, including bringing action against social media companies, Original Equipment Manufacturers, operating systems, software providers, content providers, app developers, IoT companies

[32] *See,* FTC Staff at 23-29. *See, also,* Balancing the Rights of Web Surfers Equally and Responsibly Act of 2017, H.R. 2520, 115the Cong. (2017). *See also*, Press Release, Communications and Technology Subcommittee Chairman Marsha Blackburn, Blackburn Introduces Bill to Protect Online Privacy (May 19, 2017) (stating that the Browser Act "creates a level and fair privacy playing field by bringing all entities that collect and sell the personal data of individuals under the same rules.").

[33] *See,* Paula Petcu, "Got Milk? Building a Smart Fridge Weight Scale," MonoHelix Labs Blog (Oct. 29, 2016) (http://www.monohelixlabs.com/building-smart-fridge-weight-scale.html) (viewed Nov. 8, 2018, 18:05).

and ad networks. It has issued specific guidance to app stores, app developers, ad networks, and others.[34]

Rather than enact a bewildering web of prescriptive regulations, NTCA suggests that a single set of standards, with guidance that differentiates between the respective sensitivity of various data, be implemented.

### D. SOUND POLICY WILL RECOGNIZE THE INTERESTS OF CONSUMERS AND DIFFERENCES AMONG DIFFERENT DATA SETS.

As NTCA articulated above, sound policy and ultimate enforcement by the FTC rests upon three principles:

> **Notice:** This principle contemplates clear notice to consumers that explains the privacy practices of the firm. In these regards, a balance must be struck between language that is clear and comprehensible and which also defines the rights and obligations of all parties. Moreover, the notice must be readily available and conspicuous in a commercially reasonable manner.
>
> **Choice:** This principle defines the customer's choice to determine information that can be shared and the types of parties with whom the information may be shared. This principle contemplates the various levels of sensitivity of different data sets, from personally identifiable information which may be available from public sources to confidential health or similarly sensitive personal data. In addition to assessing layers of sensitivity, the different sets of entities with which those various layers of data could be shared would be identified. These may include but not necessarily be limited to: (a) within the company for purposes of providing the service; (b) within the company for purposes of offering new services; (c) among corporate affiliates; and (d) among third-parties with which there are contractual or other relationships. Customers would exercise choice to determine which entities can access particular sets of data.
>
> **Security:** This principle defines the obligation of the data holder to protect customer data consistent with industry standards. In these regards, industry standards are anticipated to contemplate best-practices; flexible and scalable methodologies to protect data; and recognition of size and position of the firm in the marketplace. This principle also contemplates practices that speak to maintaining, securing and purging data. Flexibility is necessary in order to respond to changing marketplace demands and evolving technological capabilities, as well as cyber-based threats. In juxtaposition, a

[34] FTC Staff at 18.

prescriptive approach would eliminate innate agility necessary for market development and security advantages inherent through the use of risk management.

## III. CONCLUSION

Consumer privacy in a connected environment contemplates the participation of many types of firms and entities. A uniform approach to consumer privacy that encompasses all actors in the on-line marketplace will ensure consumers enjoy a consistent expectation of privacy, while regulatory parity among market players will promote innovation and competition. The FTC, pursuant to its statutory authority and the principles of Section 5 of the FTC Act, is best positioned to oversee this market. A collaborative approach to regulation that balances consumers interests in both privacy protection *and* a flourishing market will recognize various layers of data sensitivity and differences in the categories of affiliates and third-parties with which it may be shared.

Respectfully submitted,

s/*Joshua Seidemann*
Joshua Seidemann
Vice President, Policy
NTCA–The Rural Broadband Association
4121 Wilson Blvd., Suite 1000
Arlington, VA 22203
703-351-2035
www.ntca.org

DATED: November 9, 2018