Before the
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
DEPARTMENT OF COMMERCE
Gaithersburg, MD 20899

Developing a Privacy Framework	**)**	**Docket No. 181101997-8897-01**

I. INTRODUCTION

NTCA-The Rural Broadband Association (NTCA) hereby submits comments in the above-captioned proceeding.[1] NTCA represents nearly 850 independent, community-based telecommunications companies and cooperatives and more than 400 other firms that support the provision of communications in the most rural portions of the United States. NTCA members and small operators like them serve fewer than five-percent of the U.S. population, yet their collective service territories cover 37 percent of the U.S. landmass. All NTCA service provider members are rural local exchange carriers as defined by the Communications Act, as amended,[2] and Internet service providers.[3] In delivering such services to users within communities in which they live and serve, NTCA members are committed to protecting the privacy of these customers. NTCA submits that, for purposes of the instant RFI, *what* "privacy"

[1] *Developing a Privacy Framework: Request for Information* National Institute of Standards and Technology, Department of Commerce, Docket No. 181101997-8997-01, 83 Fed. Reg. 56824 (Nov. 14, 2018) (RFI).

[2] *See,* 47 U.S.C. § 153(44).

[3] According to the most recent survey data, nearly 50 percent of NTCA members' customer base can receive maximum download speeds of greater than/equal to 10 Mbps. For these and other data, *see,* Broadband/Internet Availability Survey Report, NTCA-The Rural Broadband Association, Arlington, VA (Dec. 2018).

is has been largely defined by various statutes and case law. In contrast, *how* privacy should be ensured is best approached through voluntary, dynamic, market-driven standards. These are the best tools because they are flexible, scalable and able to respond more rapidly to evolving threats than regulatory rulemaking.

II. DISCUSSION

In certain cases, NTCA members are currently bound by regulations to protect proprietary customer information. As telecommunications providers, NTCA members are subject to specialized rules pursuant to Section 222 of the Communications Act.[4] NTCA members also adhere to the "Red Flags Rule," which requires the implementation of a program to detect identity theft.[5] NTCA has staked an active role in emerging privacy proceedings undertaken by a variety of Federal agencies, including the Federal Communications Commission[6] and National Telecommunications and Information Administration (NTIA).[7] NTCA has been featured at Federal workshops[8] and included privacy and data security programming

[4] 47 U.S.C. § 222; *see, also,* 47 C.F.R. § 64.2001, *et. seq.*

[5] *See,* 16 C.F.R. § 681.1.

[6] *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).

[7] *Developing the Administration's Approach to Consumer Privacy: Comments of NTCA-The Rural Broadband Association,* Docket No. 1808217180-8780-01, RIN 0660-XC043, National Telecommunications and Information Administration (Nov. 9, 2018).

[8] *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).

in continuing legal education (CLE) programming offered to its members.[9] NTCA also offers Cyber-Wise, a complete suite of cyber-security educational programming and hosts annual cyber-security conferences.[10] NTCA's attention to these issues reflects its members' commitment to safeguarding consumer privacy while responding dynamically to evolving technology and consumer expectations.

These actions are predicated on the understanding that NTCA members are on the front-lines of data security in their communities and that their networks enable the use of IoT and other devices that commonly implicate considerations of user privacy. The proliferation of devices underlies what NIST notes as the challenge of meeting "diverse privacy needs in an increasingly connected and complex environment."[11] NTCA agrees: devices gather increasing amounts and broader of types of data both actively *and* passively.[12] Ninety-percent (90%) of IoT devices collect at least one piece of personal information.[13] And, unlike the types of safeguards enacted by software vendors and ISPs, many IoT devices are not built with anti-virus capabilities; do not require users to change default log-in and password information; and, do

[9] 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).

[10] *See,* https://www.ntca.org/events-education/education/cyber-wise, describing NTCA's cyber-security conferences and programming.

[11] RFI at 83 Fed. Reg. 56824.

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

[13] 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).

not update to respond to changing threats.[14] 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 NIST investigation is, therefore, timely.

Privacy, or, more specifically, information that is considered private, is defined already today by numerous administrative and judicial decisions grounded in Section 5 of the Federal Trade Commission (FTC) Act and other sector-specific statutes. The FTC umbrella covers 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.[15] The specific acts (and protected information) that are embraced by these standards are not defined in a static or fixed form: Congress deliberately, and presciently, crafted general terms, finding that if it "were to adopt the method of definition, it would undertake an endless task."[16] Congress complemented general FTC standards with sector-specific laws such as HIPPA, which covers health care data;[17] regulations that address children's online privacy protection;[18] and

---

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

[15] *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).

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

[17] 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.*

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

financial data.[19] In remarks to the Consumer Electronics Show last week, former FTC Commissioner Maureen K. Ohlhausen noted the FTC has prosecuted more than 500 cases involving both online and "offline" privacy breaches.[20]

Therefore, there is relative clarity to understanding that private data must be protected, paired with a general recognition of *which* data must be protected. The instant inquiry, then, is ostensibly aimed at defining *how* that data must be protected. By way of analogy, privacy is a castle on the hill whose identity and presence has been confirmed the FTC and other statutes; the instant inquiry, in contrast, is aimed at defining the best defense of that castle, whether by high walls, a moat or other defensive structures.

The definition of defensive structures depends upon the threat environment, as well as the targeted entity. As the RFI cautions, there are potential challenges in developing a cross-sector standards-based framework for privacy.[21] Accordingly, and as NTIA notes, a "prioritized, flexible, risk-based, outcome-based, and cost-effective approach" that is consistent with legal and regulatory standards offers the most useful path forward.[22] NTCA agrees.

As small, community-based providers that live among and work alongside their subscribers, NTCA members are committed to protecting the private information of their

---

[19] Gramm-Leach-Bliley Act, Pub. L. 106-102, 113 Stat. 1338 (1999), 12 U.S.C. § 24(a), *et. seq.,* 15 U.S.C. § 80(b) *et. seq.*

[20] Maureen K. Ohlhausen, "American Privacy Regulations in a Post-GDPR World," Consumer Electronics Show, Las Vegas (Jan. 10, 2019).

[21] RFI at 83 Fed. Reg. 56826.

[22] RFI at 83 Fed. Reg. 56824.

customers in a manner consistent with industry practices. As a general matter, NTCA members do not broker their customers' information, and generally accord their broadband Internet access service (BIAS) customers the same treatment as their voice customers whose accounts are governed by customer proprietary network information (CPNI) rules.[23] These practices are vastly different than those engaged by many app and edge providers whose actions have earned the recent attention of policymakers. 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.[24] 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."[25] 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;[26] in trials, Google's Medical Brain team achieved accuracy rates over 90

[23] 47 C.F.R. § 64.2001, *et seq.*

[24] 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) (last viewed May 19, 2016, 17:49).

[25] 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) (last viewed May 19, 2016, 18:05).

[26] 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).

percent predicting the deaths of hospital patients).[27] Amazon, Facebook, WhatsApp, and Apple offer competing technologies that rely on deep data collections and increasingly capable analytics.[28] The Washington Post uses cookies, web beacons and "other technologies" for online tracking and advertising.[29] NTCA does not decry these technologies; Google's ability to review "big data" enables its software to now recognize eye disease in scanned images.[30] However, these varying practices among various firms underscores why an outcome-based, scalable and flexible framework is the correct approach as firms are charged with protecting the privacy of their users' data.

The NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework) produced a method by which entities of all sizes can utilize risk-based best practices tailored to their circumstances to address cyber-security issues dynamically and comprehensively. This is fully consistent with NIST's request to explore what an outcome-based approach to privacy would look like.[31] In that vein, the RFI offers sound

---

[27] 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).

[28] 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)

[29] Privacy Policy, Washington Post (https://www.washingtonpost.com/privacy-policy/2011/11/18/gIQASIiaiN_story.html) (last 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."

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

[31] RFI at 83 Fed. Reg. 56826.

starting points for the industry to consider, including objectives of predictability, manageability and disassociability.[32] However, the specific execution of various practices, such as de-identification, how information is collected, stored, used and shared, enabling user preferences, and default privacy configurations[33] should be left to voluntary industry standards.

In a 2016 Green Paper addressing the development of the IoT market, NTIA recognized the "risk of premature and excessive regulation."[34] NTCA submits these same concerns attend the instant inquiry. Organizations and devices will continue to collect, store and use data in an evolving manner. The threats to the security of that data will similarly evolve. Industry ability to respond must remain flexible, scalable and rapid. Accordingly, a voluntary, industry-driven approach is more suitable than a prescriptive approach grounded (if not inflexibly anchored) in regulatory rulemaking processes.

As described above, the universe of protected data and the duty to protect it is already largely defined by statute and a growing body of case law. How organizations protect that data will be best accomplished through industry-drawn practices that can respond rapidly to evolving threats.

III. CONCLUSION

NTCA supports the guiding principles articulated by NTIA in the RFI, specifically, to develop a consensus driven framework that is adaptable to many organizations across different

[32] RFI at 83 Fed. Reg. 56826.

[33] RFI at 83 Fed. Reg. 56826.

[34] *Fostering the Advancement of the Internet of Things: Request for Comments,* NTIA Docket No. 17010523-7023-01, 82 Fed. Reg. 4313 (Jan. 13, 2017).

sectors; which is risk-based, outcome-based, voluntary and non-prescriptive; compatible with other standards; and flexible to respond to evolving technology and threats. NTCA submits that this approach will best enable industry to meet the privacy standards formed by statue and defined by an evolving body of law.

Respectfully submitted,

s/Joshua Seidemann
Joshua Seidemann
Vice President, Policy
NTCA-The Rural Broadband Association
4121 Wilson Blvd., Suite 1000
Arlington, VA 22203
703-351-2000
www.ntca.org

DATED: January 15, 2019