Before the
FEDERAL TRADE COMMISSION
Washington, D.C. 20580

Advance Notice of Proposed Rulemaking for Trade Regulation Rule on Commercial Surveillance and Data Security	)))	**Docket ID No. 2022-17752**

Comments of

NTCA–THE RURAL BROADBAND ASSOCIATION

To the Commission:

I. INTRODUCTION

NTCA–The Rural Broadband Association (NTCA) hereby files these comments on the Advance Notice of Proposed Rulemaking (ANPR) in the above-captioned proceeding.[1] NTCA represents approximately 850 small, locally operated rural broadband providers and is also the parent entity of Services Management Corporation (SMC), a subsidiary that provides administrative management including health and retirement benefits services to members of the not-for-profit NTCA. Accordingly, NTCA's interest in the instant proceeding arises from several perspectives, including its representation of small businesses, internet service providers, and its work in the financial and health services industries. NTCA has led the charge promoting broadband and IoT among its rural broadband provider members[2] and is accordingly sensitive to data gathering that may occur through connected devices, even though NTCA itself is not part of the app industry.

[1] "Trade Regulation Rule on Commercial Surveillance and Data Security," Federal Trade Commission, 87 Fed. Reg. 51273 (2022).

[2] NTCA has published extensively on the role of broadband in agriculture, education, healthcare, and other sectors. Papers on these and other topics can be found at www.smartruralcommunity.org.

NTCA has participated actively in privacy proceedings across a range of agencies, including the Federal Communications Commission,[3] National Telecommunications and Information Administration,[4] and National Institute of Standards and Technology.[5] In filed comments, NTCA has recommended a national approach, rather than state-by-state patchwork, that is consistent with national-scope markets and which offers consumers and industry a common set of expectations and standards. NTCA has also supported the Federal Trade Commission (Commission) as the proper agency of jurisdiction for consumer privacy issues. In these instant comments, NTCA acknowledges need for data security and the protection of data that consumers wish to keep private. At the same time, NTCA recommends the Commission to consider the broader scope of consumer welfare issues implicated by the instant proceeding and to avoid inhibiting market development or placing undue burdens on small businesses. Accordingly, NTCA demonstrates the usefulness of voluntary industry guidelines and recommends the Commission to incorporate by reference such standards that can evolve in a timely and ongoing fashion to meet developing market conditions while also providing certainty and guidance to consumers and the marketplace. This judicious balance can accommodate the interests of industry and consumer advocates alike while offering behavioral guardrails for information holders and users. Flexible yet enforceable protections emerging from such a

[3] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services: Comments of NTCA–The Rural Broadband Association,* Docket No. 16-106, Federal Communications Commission (May 27, 2016); *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services: Reply Comments of NTCA–The Rural Broadband Association,* Docket No. 16-106, Federal Communications Commission (Jul. 6, 2016).

[4] *Developing the Administration's Approach to Consumer Privacy: Comments of NTCA–The Rural Broadband Association,* Docket No. 180821780-8780-01, RIN 0660-XC043, National Telecommunications and Information Administration (Nov. 9, 2018).

[5] *Developing a Privacy Framework: Comments of NTCA–The Rural Broadband Association,* Docket No. 181101997-8897-01, National Institute of Standards and Technology (Jan. 15, 2019).

regime would be backed by the full force and authority of the Commission while avoiding gaps between promulgated rules and future marketplace realities that can be predicted to develop as technology and consumer interests progress.

II. DISCUSSION

A. THE FTC IS THE PROPER AGENCY OF JURISDICTION

1. An Established Body of Case Law Reflects the FTC Ability to Meet Evolving Market Conditions

NTCA has consistently identified the Commission as the agency of choice to address privacy and advocated for development and application of a uniform standard across all actors in the broadband and internet ecosystem.[6] The growth of online transactions and interstate internet commerce for a range of activities including, for example, retail purchasing and healthcare (which itself is addressed through regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA))[7] renders a state-by-state patchwork of regulatory policies at best inconvenient and at worst unworkable for firms that have an online presence in multiple states. Moreover, a disjointed approach to privacy that looks at arbitrarily siloed industries and distinct online interactions would be confusing to consumers, leaving them with differing expectations and protections depending upon locations of the user and the entity in question. A uniform national approach, by contrast, would provide industries and their customers with clearer guidance and understanding.

---

[6] *See, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services: Comments of NTCA–The Rural Broadband Association,* Docket No. 16-106, Federal Communications Commission (May 27, 2016); *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services: Reply Comments of NTCA–The Rural Broadband Association,* Docket No. 16-106, Federal Communications Commission (Jul. 6, 2016); *Developing the Administration's Approach to Consumer Privacy: Comments of NTCA–The Rural Broadband Association,* Docket No. 180821780-8780-01, RIN 0660-XC043, National Telecommunications and Information Administration (Nov. 9, 2018).

[7] Pub. Law 104-191, 110 Stat. 1936 (104th Cong. 1996). HIPAA privacy rules are codified at 42 U.S.C. § 160(A) and § 164(I).

This national method, however, need not be grounded in overly prescriptive regulation. Rather, to the extent the Commission determines that agency action is necessary even as bipartisan legislation currently moves forward,[8] the Commission can look to its successful enforcement of privacy violations as reflected in numerous administrative (and affirmed by many judicial) decisions and craft a targeted and surgical approach. This would build upon a growing body of case law that both demonstrates and *defines* the Commission's enforceable perspectives on privacy, while offering firm basis for the type of industry-developed standards discussed more fully below.

An introduction to a Columbia Law Review article is instructive:

> . . . in practice, FTC privacy jurisprudence has become the broadest and most influential regulating force on information privacy in the United States – more than nearly any privacy statue or any common law tort. . . . the FTC's privacy jurisprudence is functionally equivalent to a body of common law . . . a common view of the FTC's privacy jurisprudence is that it is thin, merely focusing on enforcing privacy promises. In contrast, a deeper look at the principles that emerge from FTC privacy 'common law' demonstrates the FTC's privacy jurisprudence is quite thick. The FTC has codified certain norms and best practices and has developed some baseline privacy protections. . . .[9]

Indeed, a substantial and growing library of administrative and judicial decisions paints a comprehensive portrait of best practices for industry.[10] Notably, these guardrails have emerged

---

[8] American Data Privacy and Protection Act, H.R. 8152 (117th Cong., 2021-2022).

[9] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Columbia Law Review 583 (2011) (Solove and Hartzog).

[10] *See, i.e., Federal Trade Commission v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015) (finding lax cybersecurity constituted unfair business practice); *Federal Trade Commission, et. al., v. Vizio, et. al.,* Case 2:17cv-00758 (Dist. N.J. 2017) (settlement following collection of smart TV user data without consent); *I/M/O Goal Financial, LLC,* FTC Docket No. C-4216 (2008) (finding violations of customer information and consumer financial information rules (Gramm-Leach-Bliley) as well as 15 U.S.C. § 45 *et seq.*); *I/M/O Guidance Software, Inc.,* FTC Docket No. C-4187 (2007) (finding liability for maintaining sensitive in information in clear readable text; not adequately assessing vulnerability of network and applications; not implementing readily-available defenses; failure to employ sufficient methods to detect breaches; *I/M/O Levono, Inc.,* Federal Trade Commission, Docket No. C-4636 (2018) (concerning laptops with pre-loaded "man in the middle" software that accessed user information without adequate notice); *I/M/O TaxSlayer, LLC,* Federal Trade Commission, Docket No. C-4626 (2017) (failure to adequately safeguard clients' financial information).

without prescriptive rules from the Commission other than the statutory language of Section 5 prohibiting unfair and deceptive trade practices or specific, targeted rules promulgated under Congressional directive, for example, the Children's Online Privacy Protection Act (COPPA) or Gram-Leach-Bliley Act.

> Critics of the FTC call it weak and ineffective – '[l]ow-[t]ech, [d]efensive, [and] [t]oothless' in the words of one critic. But many privacy lawyers and companies view the FTC as a formidable enforcement power, and they closely scrutinize FTC actions in order to guide their decisions.[11]

Accordingly, NTCA submits that the Commission's current processes and capabilities provide a foundational bulwark against bad behavior, and that surgical steps taken collaboratively with industry and consumer interests will enable sound guidance for industry and consumers.[12]

B. REGULATORY CAUTION IS APPROPRIATE WHEN ADDRESSING ISSUES THAT AFFECT AN EXPANDING RANGE OF INDUSTRY SECTORS THAT ARE THEMSELVES AFFECTED BY RAPID TECHNOLOGICAL EVOLUTION

As the Commission may contemplate the promulgation of requirements, it is important to consider the potential negative impact that overly prescriptive requirements can have on the market and, by extension, innovation. At the outset, NTCA notes the very language of the ANPR signals the potential for a pervasive prescriptive approach that could impose far more than necessary requirements on numerous industries, including small businesses such as the members of NTCA. Stating that consumers "surrender" their data, or that companies "surveil" consumers, the ANPR sets a tone that suggests industries act with adversarial intent rather than in the normal and ordinary course of business across many sectors. Health insurance providers collect sensitive

---

[11] Solove & Hartzog at 600.

[12] To some extent, the FTC currently provides such guidance. *See, i.e.,* "Consumer Privacy," Federal Trade Commission (https://www.ftc.gov/business-guidance/privacy-security/consumer-privacy) (visited Oct. 13, 2022).

data in order to administer claims and assist members with treatment and wellbeing; this is hardly the equivalent of "surveil," which means to "closely monitor or observe." Similarly, "surrender" means to "cease resistance to an enemy or opponent." The ANPR seems to suggest, however subtly, that industry is a foe and consumers are compelled under duress to provide data they would prefer to hold private. The reflective tone of this language paints a skewed narrative of American commerce, particularly in light of numerous studies finding that many consumers will willingly share personal information in exchange for good or services they may characterize as only nominally valuable. This "privacy paradox," namely, the difference between perceived privacy concerns and actual privacy behaviors, is a known and studied phenomenon. And while there may be an observed dichotomy in the level of protection that many people profess to desire and the actual protection they choose to exercise in the face of incentives, it cannot be presumed that consumers are misled wholesale toward hazard. Studies have found that "consumers state a strong preference for privacy but are willing to give their personal information for small incentives."[13] Accordingly, while the language of the ANPR suggests an ongoing tension between consumers and industry, a more balanced inquiry on the way to proposed new oversight should seek out the determinative points at which customers choose to share their data, and address regulatory intervention toward those intersections on an as-needed basis.

[13] Guy Aridor, Yeon-Koo Che, Tobias Salz, *The Economic Consequences of Data Privacy Regulation: Empirical Evidence from the GDPR,* at 6 (2020) (Aridor, *et al.*), *citing* Bettina Berendt, Oliver Gunther, Sarah Spiekermann, *Privacy in E-commerce: Stated Preferences v. Actual Behavior,* 4 Communications of the ACM 101-106 (2005); Patricia A. Norberg, Daniel R. Horne, David A. Horne, *The Privacy Paradox: Personal Information Disclosure Intentions versus Behavior,* 41 Journal of Consumer Affairs 100-126 (2007); Susan Athey, Christian Catalini, Catherine Tucker, *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk,* National Bureau of Economic Research (2017).

Indeed, the scope of the ANPR argues for a cautious approach. The ANPR presumes to cover all fields that are not regulated by specific, targeted laws such as the Children's Online Privacy Protection Act (COPPA); Gram-Leach-Bliley Act; Health Breach Notification Rule; and others as enumerated by the Commission.[14] The ANPR sets a tone with such questions as, "To what extent do commercial surveillance or lax security measures harm consumers?" staking a presumption that information acquisition *de facto* is harmful and contrary to consumer interests. The ANPR defines "commercial surveillance," as the "collection, aggregation, analysis, retention, transfer, or monetization of consumer data."[15] As observed by a filing in the instant proceeding, "The ANPR's reimagination of the concept of consumer privacy as 'consumer surveillance' underscores the dystopian slant, rhetorically stacking the deck in favor of draconian (and *ultra vires*) regulations."[16]

NTCA accordingly urges the Commission to exercise restraint and caution when considering rules that would affect an overwhelming proportion of the national economy and its businesses. Moreover, overly prescriptive regulations can find themselves relegated to irrelevance and inconsistency as technology, marketplace norms, and consumer expectations change. The need for flexible and responsive privacy regulation must reflect the evolving marketplace. For example, a 2012 study found not only that older people were more reluctant than younger people to share information, but that the differences between preferences among those groups widened over the course of a seven-year period.[17] Other market dynamics similarly

[14] *See,* 87 Fed. Reg. at 51268.

[15] 87 Fed. Reg. at 51277.

[16] Comments of Americans for Prosperity Foundation (Sep. 30, 2022).

[17] Yosuke Uno, Akira Sonoda, Masaki Bessho, "*The Economics of Privacy: A Primer Especially for Policymakers*, Bank of Japan Working Paper Series (Aug. 2021), *citing* Avi Goldfarb & Catherine E. Tucker, *Shifts in Privacy Concerns*, 102 American Economic Review 3, at 349-353 (2012).

demonstrate fluid consumer privacy preferences and accordingly support processes that favor the ability of regulators and industry to adapt to rapidly changing technological advancements and their anticipated impact on privacy concerns. These concerns are particularly relevant inasmuch as the ANPR supposes to cast a large net into which nearly every sector of the national economy could be captured. In its research and advocacy, NTCA has highlighted the ever-expanding role of broadband in sectors that include, but are not limited to, agriculture, economic development, education, and healthcare.[18] In addition to its analyses of use-cases for these technologies, NTCA administers a leading industry cybersecurity program.[19] Finally, NTCA-subsidiary SMC administers health and financial services. NTCA has participated actively in a diverse array of both government and industry efforts addressing these issues and is innately aware of and sensitive to the issues surrounding data collection and security.

The 95 questions of the ANPR contemplate a broad range of issues, many of which are broad and themselves contemplate numerous unenumerated sub-questions. Commissioner Noah Philips cautioned the ANPR "addresses too many topics to be coherent."[20] NTCA's experience in the health, financial, broadband, and small businesses sectors informs its concern that the scope and tone of the ANPR will not favor a balanced result that balances effectively the numerous elements of consumer welfare, including not only consumer privacy but also such factors as efficiencies and innovation. Instructive guidance can be drawn from Europe's

[18] *See,* Rick Schadelbauer, *Anticipating Economic Returns of Rural Telehealth*, NTCA–The Rural Broadband Association (2017); Joshua Seidemann *From Fiber to Field: The Role of Rural Broadband in Emerging Agricultural Technology*, NTCA–The Rural Broadband Association (2021); Joshua Seidemann, *Rural Broadband and the Next Generation of American Jobs*, NTCA–The Rural Broadband Association (2019).

[19] CyberShare is a small broadband provider ISAC that collects and disseminates threat information, indicators, and mitigation strategies from a variety of public and private sources and facilitates communications among participations. *See,* www.ntca.org/member-services/cybershare (visited Nov. 15, 2022).

[20] Dissent of Commissioner Noah Phillips (citations omitted), 87 Fed. Reg. at 51924.

implementation of the General Data Protection Regulation (GDPR). As compliance costs and liabilities increased, some firms reportedly ceased to offer services in the European Union, including the Los Angeles Times and Pottery Barn.[21] Consumer welfare also contemplates the inherent costs of compliance. Regulations along the lines of GDPR or the California Consumer Privacy Act (CCPA) could generate costs of approximately $122B.[22] These would include outlays to appoint data protection officers; conduct privacy audits; deploy infrastructure; and manage data deletion. These costs, in addition to decreases in efficiencies or innovation, must be part of the overall consumer welfare analysis. Consumer privacy is critical but cannot be isolated as the *sine qua non* of consumer welfare and benefits to the exclusion of all other factors. The questions of the ANPR warrant, *inter alia,* factual investigation of current practices; modeling of potential alternatives; cost/benefit analyses; impact projections; and identification of potential or actual harms that Commission action endeavors to forestall, including anticipated economic impacts as well as the potential effect of regulation on industry innovation. Only this type of comprehensive investigation and cost-benefit analysis will illuminate the proper path forward, and that effort can be served by the collaborative interaction in an industry-led standards forum.

[21] *See,* Danica Kirka, "Amid Confusion, EU Enacts a New Data Privacy Law," PBS News Hour (May 25, 2018) (https://www.pbs.org/newshour/world/amid-confusion-eu-enacts-new-data-privacy-law) (visited Nov. 21, 2022); Jennifer Huddelston, "The Price of Privacy: The Impact of Strict Data Regulations on Innovation and More," American Action Forum (Jun. 3, 2021).

[22] Alan McQuin & Daniel Castro, "The Costs of an Unnecessarily Stringent Federal Data Privacy Law," Information Technology & Innovation Foundation, at 1 (Aug. 2019).

C. THE FTC CAN INCORPORATE BY REFERENCE VOLUNTARY INDUSTRY-LED STANDARDS

1. Industry-Led Standards Can Address Certain of the Underlying Challenges of the Current Proceeding

NTCA recommends the Commission to consider the usefulness of voluntary industry standards, incorporated into Commission rules by reference, rather than prescriptive rules issued under the carve-out provisions of the FTC Act. Unlike many other agencies (for example, the Federal Communications Commission or the Federal Energy Regulatory Commission) the Commission does not have broad rulemaking authority. Rather, the Commission operates generally as an enforcement agency acting upon specific complaints alleging violations of statutory standards. The Commission may "prosecute any inquiry necessary to its duties" and is authorized to "gather and compile information concerning, and to investigate from time to time the organization, business, conduct, practices, and management of any person, partnership, or corporation . . ,"[23] but it is not by nature a regulatory compliance agency. The Commission's limited rulemaking authority for the instant proceeding is rooted in Section 18 of the FTC Act, which is the exclusive authority for rules addressing unfair or deceptive practices. The Commission "must have reason to believe that the practices to be addressed by the rulemaking are 'prevalent.'"[24]

Even if the Commission possesses authority to promulgate far-reaching privacy rules, NTCA submits that the instant proceeding risks an exceedingly broad outcome that could result in unnecessary as well as duplicative and burdensome regulations.[25] It is

[23] FTC Act Sec 3, 15 U.S.C. § 43; FTC Act Sec. 6(a), 15 U.S.C. § 46(a).

[24] "A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority," Federal Trade Commission (May 2021).

[25] Certain of these concerns have been cited in filed comments as well as industry briefing papers. *See, i.e.,* Lawrence J., Spiwak, *Biting Off More Than It Can Chew? Some Thoughts on the FTC's Advance Notice of*

precisely the broad nature of the 95 questions that invites pause to consider alternative avenues to the balanced goals of protecting consumer privacy while not inhibiting the market, and to whether the broad net cast in this proceeding meets the spirit of the limited rulemaking authority granted to the Commission. Toward these ends, NTCA recommends the Commission to consider voluntary industry standards, incorporated by reference, as the basis for regulatory activity. Industry-led standards and guidelines balance market and consumer protection interests while enabling timely responses to marketplace changes and developments. Voluntary standards can emerge from collaborative negotiations among industry representatives, consumer interest groups, and standards-setting bodies; government representatives may also participate in the role of facilitators or to elucidate regulatory intersections. Voluntary standards that are created by collaborative efforts among industry and public interest groups can strike a reasonable balance that earns "buy-in" from all parties. The Commission incorporation of an industry standard basis for regulation here would coalesce competing opinions and provide grounds for future flexibility and refinement.

2. The NIST Privacy Framework is a Cogent Example of Consensus-Built Standards

The NIST Privacy Framework (Framework) offers a cogent example of how competing interests can craft a reliable framework. As the Commission is aware, NIST is a non-regulatory agency housed in the Department of Commerce. Its mandate is to promote American innovation and industrial competitiveness. The Framework "is a voluntary tool developed in collaboration

Proposed Rulemaking on "Commercial Surveillance and Data Security," Phoenix Center Policy Bulletin No. 59 (Sep. 2022).

with stakeholders intended to help organizations identify and manage privacy risk to build innovative products and services while protecting individuals' privacy."[26] NIST explains,

> Cutting-edge technologies such as the Internet of Things and artificial intelligence are raising further concerns about their impacts on individuals' privacy. Inside and outside the U.S., there are multiplying visions for how to address these challenges. Deriving benefits from data while simultaneously managing risks to individuals' privacy is not well-suited to one-size-fits-all solutions. Accordingly, the National Institute of Standards and Technology (NIST) is developing a voluntary privacy framework, in collaboration with private and public sector stakeholders, to help organizations with:
>
> - Building customer trust by supporting ethical decision-making in product and service design or deployment that optimizes beneficial uses of data while minimizing adverse consequences for individuals' privacy and society as a whole;
>
> - Fulfilling current compliance obligations, as well as future-proofing products and services to meet these obligations in a changing technological and policy environment; and
>
> - Facilitating communication about privacy practices with customers, assessors, and regulators.[27]

NTCA submits that these same principles, and the approach of a collaborative privacy framework, can be applied to the instant investigation of privacy regulations.

The Framework recognizes evolving expectations of privacy held by consumers and the differing reasons for and changing ways in which companies obtain and/or use

[26] *See,* NIST Privacy Framework (https://www.nist.gov/privacy-framework#:~:text=The%20NIST%20Privacy%20Framework%20is,services%20while%20protecting%20individuals'%20privacy) (visited Nov. 15, 2022).

[27] *See,* NIST Privacy Framework: Frequently Asked Questions (https://www.nist.gov/privacy-framework/frequently-asked-questions) (visited Nov. 16, 2022) (NIST FAQs).

information.[28] New technology and applications offer evolving ways to obtain and use customer information. These rapidly changing market conditions are not ripe for formal rulemaking proceedings but can be addressed more efficiently through flexible industry standard groups. The Framework creates a general, industry-wide umbrella of standards that offers a uniform approach for industry and customers. The Framework does not prescribe action but rather defines the bounds of reasonable behavior within which companies can operate. Because it is a voluntary framework, it does not offer a *per se* safe harbor but companies operating pursuant to the Framework can claim validly that they are operating pursuant to generally accepted industry standards. And, as described below, industry standards can play a significant role in agency enforcement actions.

Standards and frameworks create trust and reliability by adopting commonly known and accepted best practices. These qualities are enhanced when the standards are crafted by a broad swath of stakeholders that represent competing interests yet find compromise in solutions that balance the opposite positions. NIST explains the Framework "enables finding the right balance between building innovative systems, products, and services while protecting individuals' privacy."[29] And, while the Framework is voluntary, it nevertheless recognizes the intersection of related laws. The Framework features "regulatory crosswalks" that link Framework standards to enacted privacy laws.[30]

---

[28] The NIST Privacy Framework is a set of voluntary, industry-developed guidelines that are divided into five columns: Identify; Govern; Control; Communicate; and Protect. These same pillars are employed for the voluntary NIST Cybersecurity Framework. Each of the five guidelines is divided into categories and sub-categories that identify various levels of risks, actions, and other factors that guide companies to formulate standards for company practices.

[29] NIST FAQs.

[30] *See,* Crosswalks: NIST Privacy Framework (https://www.nist.gov/privacy-framework/resource-repository/browse/crosswalks) (visited Nov. 16, 2022).

3. The Consumer Products Safety Commission Offers Instructive Example for Regulatory Reliance on Industry-Led Standards.

NTCA suggests the for purposes of privacy regulation and the instant proceeding, the Commission can be guided by the Consumer Products Safety Commission (CPSC), which by design demurs from rulemaking and instead relies on industry-led standards for the prosecution of its consumer protection mandate. The Consumer Product Safety Act (CPSA)

> requires the [CPSC] to defer to 'voluntary consumer product safety standards' that are predominantly drafted and developed by private industry. In light of this mandate, the CPSC provides technical assistance and otherwise helps industry groups develop voluntary standards more frequently than it issues mandatory safety standards through rulemakings.[31]

Most products that fall beneath the CPSC's jurisdiction are governed by voluntary industry standards. Congress has expressly directed the CPSC to promulgate mandatory consumer safety rules in some instances, but the CPSC is generally required to "defer to industry-developed voluntary safety standards." To be clear, and to emphasize the continued role that the FTC would have in privacy enforcement, *voluntary standards do not equate to a lack of agency involvement:* The CPSC issues regular reports on industry standards. And, while the CPSC cannot *per se* enforce a voluntary standard, a party's failure to comply with a standard can play a dispositive role in CPSC enforcement proceedings.[32] NTCA suggests that even if Congress has not directed the Commission to rely on industry-developed standards, neither does the FTC Act prohibit such reliance.

[31] David Carpenter, "The Consumer Product Safety Act: A Legal Analysis," Congressional Research Service, at 1 (Apr. 24, 2018) (CRS).

[32] CRS at 13.

Moreover, the limited scope of FTC rulemaking authority would tend to support limited regulatory rulemaking that instead defers to non-promulgated industry standards.

As noted above, the CPSC relies voluntary standards more often than promulgated rules. The standards are usually developed by industry groups such as American National Standards Institute (ANSI), Underwriters Laboratory (UL), or other bodies that combine trade organizations, researchers, and consumer advocates.[33] This design does not run afoul of limits on the Federal Government's authority to delegate its powers to private actors.[34] In similar vein, the FTC could defer to the Framework (which itself is crafted under Federal authority) or other industry-led standards. This approach would be eminently consistent with the FTC mandate to prosecute "unfair and deceptive" practices precisely what is "unfair and deceptive" is an evolving perspective informed by the collaborative work of a standards-setting body. The Framework or a similar industry-led initiative would balance the interests of industry and consumer protection and enable flexible evolutions more rapidly than APA-administered rulemaking.[35]

---

[33] CRS at 12.

[34] *See, Texas et al. v. Commissioner of Internal Revenue Service,* 596 U.S. _____ (2022), *citing Department of Transportation v. Association of American Railroads,* 575 U.S. 43 (2015).

[35] This approach would nevertheless benefit from processes intended to encourage timely action by relevant industry bodies. Certain cost-benefit analyses undertaken by the CPSC have resulted in what observers have defined as "paralysis by analysis." CRS at 9, fn. 94. The CPSC worked with the window covering industry for more than 20 years to develop voluntary standards for window blind cords. GAO report at 9, fn.96; *see also* "Updated Voluntary Window Covering Safety Standard Takes Effect: Go Cordless," Consumer Product Safety Commission (Dec. 18, 2018) (https://www.cpsc.gov/Newsroom/News-Releases/2019/Updated-Voluntary-Window-Covering-Safety-Standard-Takes-Effect-Go-Cordless) (visited Nov. 16, 2022). But that does not mean that in the intervening years industry was not culpable for death or injury. Rather, cases were in fact litigated and a body of case law provided instructive direction for manufacturers. But a uniform, industry-accepted standard did not exist.

III. CONCLUSION

As described above, the instant ANPR is a broad and unspecific inquiry that appears to presage overly prescriptive regulation. Initial critiques, internally and externally, of the scope of proposed rulemaking vis-à-vis the Commission's rulemaking authority suggest that an alternative route premised on stakeholder-developed standards may be result in more broadly accepted and ultimately more effective outcomes. Specifically, NTCA recommends the Commission to consider the design of the CPSC and to premise its privacy regulation on deferral to voluntary standards. These standards, whose development would include the participation of industry, consumer protection interests, and the FTC, would provide reasonable guidance to consumers and firms. This approach would enable timely responses to marketplace changes and ensure the Commission's growing capabilities to address adequately the needs of an evolving marketplace.

Respectfully submitted,

s*Joshua Seidemann*
Joshua Seidemann
VP Policy and Industry Innovation
NTCA–The Rural Broadband Association
4121 Wilson Blvd., Suite 1000
Arlington, VA 22203
703-351-2000
www.ntca.org

DATED: November 21, 2022