ncta
National Cable & Telecommunications Association
25 Massachusetts Avenue, NW – Suite 100
Washington, DC 20001
(202) 222-2300

www.ncta.com

Loretta Polk
Vice President and Associate General Counsel

(202) 222-2445
(202) 222-2446 Fax

August 29, 2016

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Re: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106

Dear Ms. Dortch:

In its notice of proposed rulemaking (NPRM) in this proceeding, the Commission proposes an aggressive reading of section 222 that would result in data that never before has been treated as customer proprietary network information (CPNI) being subject to radical use restrictions that historically have been reserved only for information that is considered "sensitive."[1] Faced with a record that confirms such an overly broad reading is contrary to the plain language of the statute, Congressional intent, good public policy, and consumer expectations and preferences, some parties have attempted to prop up the Commission's proposals with novel – but unsustainable – readings of the statute. The latest of these efforts – by Georgetown Law Professor Paul Ohm[2] – fails for many of the same reasons that previous, similar efforts failed.

- First, the Commission cannot read the statute to impose requirements on de-identified information, including de-identified information that is not aggregated. Congress chose to include the modifier "individually identifiable" in section 222(c)(1) when describing the subset of CPNI to which certain restrictions would attach, and no amount of linguistic gymnastics frees the Commission to ignore those words.

- Second, internet service providers (ISPs) take reasonable steps to de-identify data when it is used for purposes other than provision of the service – as the record reflects, there are a number of tools that allow ISPs to do just that. The Commission should not, however, adopt a de-identification standard that is so strict as to make it impossible for ISPs to comply. Such a standard would have the practical effect of reading "individually

---

[1] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, 31 FCC Rcd ¶¶ 41-47, 57, 61-62 (2016) (*NPRM*).

[2] Letter from Professor Paul Ohm, Georgetown Law, to Marlene H. Dortch, Secretary, Federal Communications Commission, WC Docket No. 16-106 (July 28, 2016) (Ohm *Ex Parte* Letter).

identifiable" out of the statute – a position that runs counter to basic principles of statutory construction and is bad public policy.

- Third, the Commission's proposal would impose a regime that is designed for sensitive information – i.e., opt-in consent as default – on information, including widely accessible device identifiers like IP addresses, that is and always has been considered non-sensitive by the FTC and others. There is neither a statutory mandate nor a body of factual or technical evidence that requires this result under the statute and no policy outcome that justifies it, especially in light of the well-established and highly successful FTC privacy framework and Administration Consumer Privacy Bill of Rights.

The net result of this analysis is that the record – and the law – continues to support a more focused approach, with respect to both the information that would be covered and the consent regime that would apply in a way that protects consumers and allows for innovation and competition.

I. THE STATUTE DISTINGUISHES BETWEEN INDIVIDUALLY IDENTIFIABLE CPNI (WHICH IS SUBJECT TO THE STATUTE'S RESTRICTIONS) AND NON-INDIVIDUALLY IDENTIFIABLE CPNI (WHICH IS NOT)

As numerous commenters in the record highlight,[3] in section 222(c)(1), Congress expressly directed that the constraints on the use and disclosure of CPNI were to be applied only to CPNI that is "individually identifiable."[4] In his letter, Professor Ohm strains to argue that, in adopting this language, Congress intended to subject CPNI that is *not* "individually identifiable" to the constraints of section 222(c)(1) unless such CPNI *also* qualifies as "aggregate customer information." But this reading is at odds with the plain language, structure, and purpose of section 222.

First, under the plain language of section 222(c)(1), information can only be subject to the use and disclosure restrictions established under the statute if it is both (i) CPNI and (ii) individually identifiable. Tellingly, Ohm concedes that his position is predicated upon the view that "information born as CPNI, even when de-identified" can nonetheless constitute "individually identifiable" information under section 222(c)(1) – unless it is aggregate customer information.[5] But the term "individually identifiable CPNI" cannot encompass CPNI which is "*not* individually identifiable." Stated another way, there is no plausible reading of the

---

[3] *See, e.g.*, NCTA Comments at 19-21 ("The [FCC's] proposed approach violates Section 222 by reading out of the statute the Congressional directive in subsection (c)(1) to impose use restrictions only on 'individually identifiable' data."); AT&T Comments at 61-62 (discussing how section 222 categorically exempts both aggregate and non-aggregate de-identified data from CPNI regulation); Comcast Comments at 84-86 (explaining how the Commission's proposed treatment of non-aggregate de-identified information is inconsistent with the terms of section 222).

[4] 47 U.S.C. § 222(c)(1).

[5] Ohm *Ex Parte* Letter at 2 ("'Individually identifiable CPNI'" consists only of "anything falling outside the defined term, aggregate customer information").

unambiguous words "individually identifiable" that could also encompass information that does *not* in fact identify an individual.

Ohm's convoluted interpretation of section 222(c) is at odds with basic canons of statutory construction. If, as Ohm suggests, Congress intended there to be only two categories of information – "aggregate customer information" and "individually identifiable CPNI" – there would have been no reason to confine the use and disclosure constraints established in section 222(c)(1) to "individually identifiable" CPNI.[6] Nor would there have been any reason for Congress to refer to "individually identifiable" CPNI only once in section 222, while referencing CPNI without the "individually identifiable" modifier multiple times in that section.[7] Indeed, Professor Ohm's letter fails to even address, much less explain, why Congress would have forged this distinction.[8]

Indeed, section 222(c)(1) references the term "individually identifiable" CPNI *in the same sentence* as it references CPNI *without* that qualifier.[9] Congress could have used "parallel construction" within section 222(c)(1) itself to indicate that all the CPNI it *just mentioned* would be covered by the constraints on use and disclosure in that provision. But Congress instead deliberately specified a *subset* of CPNI – that which is individually identifiable – as being covered by the Act's constraints on use and disclosure. Fundamental principles of statutory construction bar a conclusion that – as Ohm's position requires – Congress deliberately conflated the meaning of "CPNI" and "individually identifiable CPNI" in the same sentence and intended that the two terms should be read interchangeably.

Second, Ohm predicates his entire argument upon a supposed parallelism between subsections (c)(1) and (c)(3), which he contends shows that individually identifiable and aggregate are the sole binary choices set forth in the statute with regard to how to categorize CPNI.[10] But this contention is only coherent if "aggregate customer information" constitutes the exclusive, binary opposite of "individually identifiable" CPNI in all circumstances. That is not the case: a single customer record with *no* identifying information is manifestly *not* "individually identifiable," even though it may be CPNI. But this single record – which is not "individually identifiable" – could not meet the definition of "aggregate customer information," which Congress defined as "<u>collective</u> data that relates to a <u>group</u> or category of services or customers

---

[6] *Moskal v. United States*, 498 U. S. 103, 108 (1990); *Mountain States Tel. & Tel. Co. v. Pueblo of Santa Ana*, 472 U. S. 237 (1985); *Walter v. Metropolitan Educ. Enters.*, 117 S. Ct. 660, 664 (1997) ("[s]tatutes must be interpreted, if possible, to give each word some operative effect").

[7] *Russello v. United States*, 464 U.S. 16, 23 (1983) ("where Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion").

[8] *Recording Industry Ass'n of America, Inc. v. Verizon Internet Servs., Inc.*, 351 F.3d 1229, 1235 (D.C. Cir. 2003) ("[w]here different terms are used in a single piece of legislation, the court must presume that Congress intended the terms have different meanings") (internal quotation marks and brackets omitted).

[9] 47 U.S.C. § 222(c)(1).

[10] Ohm's reliance on this parallelism implicitly concedes that the plain language of the statute does not support his position.

from which individual identifiers and characteristics have been removed."[11] Ohm's formulation means this record must be either individually identifiable CPNI or aggregate customer information – but such a record's inherent nature proves that *it is neither*. In short, Ohm's interpretation could only work if one were to ignore key terms and Congressional decisions about what data would fall within the scope of the constraints imposed by the statute – something which clear canons of statutory construction and well-established precedent preclude.[12]

Third, Ohm's "parallel construction" argument ignores the purpose and history of the statute and its various provisions. Section 222 was enacted to advance interests in both privacy and competition.[13] While section 222(c)(1) was intended to promote privacy of individually identifiable CPNI, one of the principal purposes driving adoption of section 222(c)(3) was promotion of competition with the ILECs. Congress did this by being explicit that the requirements of (c)(1) do not apply when the information qualifies as aggregate customer information,[14] and by ensuring that competing voice providers could obtain non-discriminatory access to aggregate customer information possessed by local exchange carriers.[15] Thus,

---

[11] To be sure, section 222(c)(3) establishes that carriers may group together customer information without regard for the constraints of subsection (c)(1), so long as "individual customer identifiers and characteristics have been removed." But this by no means suggests that Congress intended that CPNI of an individual customer with all identifying information removed should be subject to the restrictions of section 222(c)(1), as Ohm's position maintains. Again, such a reading cannot be reconciled with the plain language of section 222(c)(1) and in particular its use of the "individually identifiable" modifier. Instead, section 222(c)(3) – and the definition of aggregate customer information – simply confirms that if carriers maintain databases of CPNI with identifying information, they cannot treat collective groupings of such data as "aggregate customer information" unless and until any identifying information is removed.

[12] For example, to consider this single record "aggregate customer information," one must read the word "collective" out of the statutory definition, while also disregarding the plural forms employed elsewhere in the definition – e.g., "a group . . . of . . . customers." It simply strains credulity to conclude that a data record that cannot be used to identify a specific person nonetheless must be considered "individually identifiable" unless and until it is grouped with other records.

[13] "The Conference Report states that, through section 222, Congress sought to 'balance both competitive and consumer privacy interests with respect to CPNI.'" *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, 8089, at ¶ 37 (1998) (*CPNI Second Report and Order*) (*quoting* Joint Statement of Managers, S. Conf. Rep. No. 104-230, 104th Cong., 2d Sess. 1, at 205 (1996)).

[14] *Implementation of Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended, 2000 Biennial Regulatory Review – Review of Policies and Rules Concerning Unauthorized Changes of Consumers' Long Distance Carriers*, Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14860, ¶ 9 (2002) (explaining that "under sections 222(c)(3) and 222(e), aggregate customer information and subscriber list information receive less protection from use and disclosure in order to promote competition").

[15] *CPNI Second Report and Order*, 13 FCC Rcd at 8171, ¶ 152 ("The aggregate rule rationally serves Congress' goal of encouraging competitive markets, through availability of aggregate customer information, while protecting CPNI from disclosure absent customer approval[.]"). *See also id.* ¶ 143 ("To promote the interests of fair competition, section 222 also establishes important carrier obligations regarding aggregate customer information that expressly work in tandem with the carrier requirements surrounding CPNI.").

subsections (c)(1) and (c)(3) were not intended to serve as a "binary" construct, but were in fact designed by Congress with materially different objectives in mind.

II. IMPOSING OVERLY STRICT DE-IDENTIFICATION REQUIREMENTS WOULD BE CONTRARY TO LAW, SOUND PUBLIC POLICY, AND CURRENT DE-IDENTIFICATION STANDARDS

Professor Ohm also argues that, even if the statute could be read to exclude "non-individually identifiable information that is not aggregate," this category only "encompasses the most rigorously de-identified information" that could not "as an absolute, technical matter" be reidentified.[16] This position is contrary to both law and sound public policy.[17]

Ohm wrongly claims that a rigid standard of "not linked or linkable to an individual . . . follows the lead of the FTC."[18] Not only is that standard *not* the position of the FTC, it is directly contrary to guidance provided by the National Institute for Standards and Technology (NIST) and inconsistent with court precedent on the question of what data qualifies as individually identifiable:

- The FTC staff's own comments in this proceeding dispute this contention, recommending that any information governed by the FCC's proposed rules should "only include information that is 'reasonably' linkable to an individual" and stating that the type of unqualified "linkable" standard proposed in the *NPRM* "could unnecessarily limit the use of data that does not pose a risk to consumers. While almost any piece of data could be linked to a consumer, it is appropriate to consider whether such a link is practical or likely in light of current technology."[19]
- Ohm's assertion also is refuted by the FTC's 2012 Privacy Report, which states that a "company must take *reasonable* measures to ensure that the data is de-identified."[20] In addition, the FTC's recent Internet of Things report reaffirms that the efficacy of de-identification measures should turn on whether or not data "can be reasonably reidentified."[21]

---

[16] Ohm *Ex Parte* Letter at 3.

[17] In her well known work critiquing the approach to de-identification that Ohm espouses, Jane Yakowitz asserts that Ohm so exaggerates the risks of re-identification that the result is distorted policy mandates that are not in the public's best interest. Jane Yakowitz, Tragedy of the Data Commons, 25 HARV. J.L. & TECH. 1, 62 (2011).

[18] Ohm *Ex Parte* Letter at 3.

[19] FTC Staff Comments at 9.

[20] *Protecting Consumer Privacy in an Era of Rapid Change*, Federal Trade Commission, at 21 (2012) (*FTC 2012 Privacy Report*) (emphasis added). "This means that the company must achieve a reasonable level of justified confidence that the data cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, computer, or other device." *Id. See also id.* at 21 ("Depending on the circumstances, a variety of technical approaches to de-identification may be reasonable, such as deletion or modification of data fields, the addition of sufficient 'noise' to data, statistical sampling, or the use of aggregate or synthetic data.").

[21] *Internet of Things: Privacy and Security in a Connected World*, Federal Trade Commission Staff Report, at 37 (2015) (*FTC Internet of Things Report*).

- NIST's current standard for de-identification, which the FCC references in the NPRM, requires the removal of "enough PII such that the remaining information does not identify an individual and there is no *reasonable* basis to believe that the information can be used to identify an individual."[22] This "reasonableness" standard is incorporated into NIST's current draft containing its updated guidance on de-identification.[23]
- The FCC's proposed standard for determining whether information is "individually identifiable" would also be drastically out-of-step with court precedent that consistently has declined to treat information as identifiable based upon the theoretical, technical possibility that such information might be able to identify an individual.[24]

Professor Ohm argues that a strict de-identification standard is the "best result from a policy standpoint."[25] But as the FTC and numerous other parties have explained, this is decidedly *not* the case. Rather, it would lead to a result that imposes higher costs on consumers, impedes innovative uses of information that pose no threat of harm to consumers (and indeed may benefit them), and hamstrings competition.[26] These are not even good policy results, let alone the best policy results. As NCTA and numerous commenters in this proceeding explained, de-identification bolsters consumer welfare and fosters a wide range of social benefits by heightening privacy protections for consumers while enabling and promoting data-driven insights and benefits that are a major growth driver of the internet economy.[27] And the FTC in its recent Internet of Things Report agreed, concluding that "robust de-identification measures

---

[22] Erika McCallister, et al., U.S. Department of Commerce, National Institute of Standards and Technology, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," NIST Special Publication 800-122 at ES-3 (emphasis added) (April 2010).

[23] Simson L. Garfinkel, U.S. Department of Commerce, National Institute of Standards and Technology, "De-Identifying Government Datasets," Draft NIST Special Publication 800-188 at 50 (August 2016) (defining de-identified information as "records that have had enough PII removed or obscured such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual").

[24] *See e.g.*, *In Re. Nickelodeon Consumer Privacy Litigation*, 2016 U.S. App. Lexis 11700 (3rd Cir. 2016) (noting that most courts have concluded that "static digital identifiers that could, in theory, be combined with other information to identify a person do not count as 'personally identifiable information' under the" Video Privacy Protection Act and holding that PII "means the kind of information that would <u>readily permit</u> an <u>ordinary person</u> to identify a specific individual's video-watching behavior") (emphasis added).

[25] Ohm *Ex Parte* Letter at 3; *see also* Letter from Dallas Harris, Policy Fellow, Public Knowledge, to Marlene, H. Dortch, Secretary, Federal Communications Commission, WC Docket No. 16-106, at 2 (Aug. 3, 2016); Letter from Dallas Harris, Policy Fellow, Public Knowledge, to Marlene, H. Dortch, Secretary, Federal Communications Commission, WC Docket No. 16-106, at 1-3 (July 26, 2016) (Public Knowledge July 26 *Ex Parte* Letter).

[26] *See, e.g.*, FTC Comments at 9; NCTA Comments at 66.

[27] *See, e.g.*, NCTA Reply Comments at 41-42; NCTA Comments at 68-70; CTIA Comments at 40-41; Internet Commerce Coalition Comments at 14; IMS Health Comments at 5; Consumers Research Comments at 22-24.

can enable companies to analyze data they collect in order to innovate in a privacy-protective way."[28]

To be sure, none of this is to argue that ISPs should not use reasonable de-identification tools and procedures. There are a number of widely-used tools and procedures that ISPs (along with others in the internet ecosystem) can, do, and will continue to use to make it as difficult as possible for anybody who might try to re-identify the data to do so.[29] However, this does not mean that the standard for de-identifying information adopted by the Commission can or should be so strict as to make compliance impossible, or completely eradicate the consumer-enhancing uses of the remaining dataset, especially in light of the substantial legal and policy concerns noted above.

III. THE COMMISSION CAN AND SHOULD DIFFERENTIATE BETWEEN SENSITIVE AND NON-SENSITIVE INFORMATION IN ITS RULES

Professor Ohm's arguments against calibrating the restrictiveness of the Commission's proposed CPNI rules based upon the sensitivity of the data [30] are at odds with consumer preferences and expectations, as well as with the core tenets of the FTC and White House privacy frameworks.[31]

A survey placed into the record by the Progressive Policy Institute found that by a margin of 83 percent to 12 percent, customers agree that the protections afforded for broadband customer data should be predicated upon the sensitivity of the data.[32]

The FTC staff's comments emphasized that the FCC should follow "the FTC's longstanding approach, which calls for the level of choice to be tied to the sensitivity of data."[33] Specifically, the FTC recommends that the FCC adopt an approach under which only sensitive data should be subject to an opt-in regime, while opt-out choice should be deemed sufficient for use and disclosure of non-sensitive data.[34] This is the same approach taken in the FTC's 2012

---

[28] *FTC Internet of Things Report* at 43 ("robust de-identification measures can enable companies to analyze data they collect in order to innovate in a privacy-protective way").

[29] *See, e.g.*, IMS Health Comments at 10-14; FPF Comments at 6.

[30] Ohm *Ex Parte* Letter at 4-5; *see also* Public Knowledge July 26 *Ex Parte* Letter at 3.

[31] NCTA Comments at 6; NCTA Reply Comments at 26, 44-46; ITI Comments at 14-15; ITIF Comments at 17; T-Mobile Comments at 7; Internet Commerce Coalition Comments at 9-13; ICLE Comments at 2.

[32] Progressive Policy Institute, Internet User Survey at 3.

[33] FTC Staff Comments at 23.

[34] *Id.* at 20-23. The FTC also notes that "this approach is also consistent with existing international frameworks, such as the OECD Privacy Guidelines, which distinguish between sensitive and non-sensitive information." *Id.* at 23.

Privacy Report[35] and its 2013 Staff Report on Mobile Privacy Disclosures.[36] In addition, the White House Consumer Privacy Bill of Rights recommends that companies offer consumers choices "that reflect the scale, scope, and *sensitivity* of the personal data" they collect, use, or disclose.[37]

While Ohm claims that other privacy statutes support his position, he is incorrect. For example, the constraints of the Wiretap Act he cites distinguish between the content of communications and non-content metadata.[38] Sections 338 and 631 of the Cable Act vary their safeguards for cable and DBS subscriber personally identifiable information based on the nature of the information, allowing opt-out consent for the use and disclosure of name and address information, but requiring opt-in consent (with certain exceptions) for individually identifiable viewing data.[39] The Family Educational Rights and Privacy Act (FERPA) distinguishes between "education records,"[40] for which disclosure is prohibited without prior written consent, and "directory information,"[41] for which only opt-out consent is required.[42] Professor Ohm also refrains from mentioning the Gramm-Leach-Bliley Act, where Congress allowed financial institutions to share their customers' financial data with unaffiliated third parties for their own uses, including marketing, pursuant to notice and opt-*out* consent,[43] or the CAN-SPAM Act, which allows *any* third party to send marketing emails to *any* U.S. resident also pursuant to opt-

---

[35] *FTC 2012 Privacy Report* at 15-16 ("The Commission agrees that the first-party collection and use of non-sensitive data (e.g., data that is not a Social Security number or financial, health, children's, or geolocation information) creates fewer privacy concerns than practices that involve sensitive data or sharing with third parties."); *id.* at 36-54 (describing uses and disclosures that generally require either no consent (because consent is implied) or opt-out consent).

[36] Staff Report, *Mobile Privacy Disclosures: Building Trust Through Transparency*, Federal Trade Commission, at 23 (2013).

[37] *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, The White House, at 47 (2012) (emphasis added).

[38] *See e.g., Graf v. Zynga Game Network*, 750 F.3d 1098, 1107 (9th Cir. 2014) ("[U]nder ECPA, the term 'contents' refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication."); *United States v. Reed*, 575 F.3d 900, 916 (9th Cir. 2009) (data automatically generated about a telephone call, such as the call's time of origination and its duration, do not constitute "content" for purposes of ECPA); *Gilday v. Dubois*, 124 F.3d 277, 296 n.27 (1st Cir. 1997) (call "detailing" – "recording such billing-related matters as the number called and the duration of the call"– is not prohibited interception of content under ECPA because "it simply captures electronic signals relating to the PIN of the caller, the number called, and the date, time, and length of the call").

[39] 47 U.S.C. § 551; 47 U.S.C. § 338(h).

[40] Defined as records containing information directly related to a student that are maintained by a school. 20 U.S.C. § 1232g(a)(4).

[41] Defined to include the information one might find in a yearbook or school directory, such as "the student's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received…" 20 U.S.C. § 1232g(a)(5)(A).

[42] 20 U.S.C. § 1232g.

[43] 15 U.S.C. § 6802 (b)(2).

out consent.[44]

Here, the Commission has flexibility to replicate the sensitivity-based approach that has been so successful on the internet and is consistent with consumer expectations and preferences.[45] This is particularly prudent in light of the fact that, unlike the closed telephone network (which was the basis for Congress' enactment of section 222), on the open internet many entities across the internet ecosystem have access to the information that the Commission proposes to treat as CPNI and customer PI.[46] Moreover, as Professor Tribe explains, "whereas the FTC's privacy framework is based primarily on an *opt-out* regime, the FCC's proposal flips this on its head, proposing an unprecedented and far-reaching *opt-in* regime targeted solely at ISPs and covering *all* data, not just sensitive data[;] technological and market developments since the *U.S. West* decision in 1999 make the proposed rules even *more constitutionally problematic* than the CPNI regulations invalidated by the Tenth Circuit. The proposed rules would impose a *much larger* burden on speech and are far *less* tailored to any substantial government interest."[47]

Ohm's suggestion that "it is very difficult to define whether information is sensitive" is belied by the numerous statutes that in fact make such distinctions, and by the FTC's well-established and successful track record of administering a comprehensive privacy and data security framework whose constraints vary according to the sensitivity of the data. Further, self-regulatory codes of conduct from the Digital Advertising Alliance (DAA) and the Network Advertising Initiative (NAI) – which are complied with and operationalized by thousands of member companies – vary privacy protections and choice mechanisms depending upon the sensitivity of the data, thereby underscoring the prevalence of the types of distinctions Ohm erroneously claims cannot readily be forged, implemented, or enforced.[48]

---

[44] 15 U.S.C. § 7701 *et seq*.

[45] *See* Comcast Comments at 23.

[46] *See, e.g.*, Peter Swire, Justin Hemmings, & Alana Kirkland, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others*, Working Paper of The Institute for Information Security & Privacy at Georgia Tech, at 51-57 (Feb. 29, 2016), http://peterswire.net/wp-content/uploads/Online-Privacy-and-ISPs.pdf ("[B]ased on a factual analysis of today's Internet ecosystem in the United States, ISPs have neither comprehensive nor unique access to information about users' online activity.").

[47] Laurence H. Tribe & Jonathan S. Massey, *The Federal Communications Commission's Proposed Broadband Privacy Rules Would Violate the First Amendment*, at 16, 34 (May 27, 2016) (emphasis added), *attached to* Letter from CTIA, NCTA, & USTelecom Association, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 (filed May 27, 2016).

[48] *See* Network Advertising Initiative, *2013 NAI Code of Conduct*, at 3 (2013), https://www.networkadvertising.org/2013_Principles.pdf; Digital Advertising Alliance, *Self-Regulatory Principles for Online Behavioral Advertising*, at 16-17 (2009) http://www.aboutads.info/obaprinciples.

IV. CONCLUSION

Numerous commenters explain how the Commission's proposed rule will make it harder for providers to reach consumers with innovative offerings and lower-priced bundles, will raise costs for consumers, and will erect barriers that would impede efforts by ISPs to bring new competition to the highly concentrated marketplace for online advertising.[49] Professor Ohm's assertion that all of these experienced and highly-credentialed businesspeople, regulators, economists, and even behavioral psychologists are wrong reflects either a misunderstanding of the breadth and scope of the proposed rule, or unfamiliarity with the practical realities of operating in today's internet ecosystem.

As the Commission moves forward with its rulemaking, we anticipate additional, creative efforts to justify the Commission's unreasonably expansive interpretation of its authority. Ultimately, however, the best approach that comports with the plain language of the statute, sound public policy, and well-established marketplace standards is one that:

(1) Limits the applicability of any rules to *individually identifiable* CPNI, regardless of whether the information is also aggregated with other information;

(2) Establishes a "reasonableness" standard for what information is not individually identifiable, as recommended by the FTC and many others in the record; and

(3) Adopts a sensitivity-based consent regime that follows the FTC's recommendation to (i) apply opt-in consent to the use and disclosure of sensitive information (i.e., social security numbers; health, financial, and children's information; and precise geolocation data) for marketing or advertising purposes, and (ii) apply opt-out consent for most other uses and disclosures (with specific common industry uses and disclosures permitted based on implied consent).

This approach will protect consumers, is consistent with consumer expectations and preferences (as well as the well-established and highly successful FTC and Administration approach), and will allow companies in this space to innovate, invest, and compete – all of which is to the benefit of the public interest.

Respectfully submitted,

/s/ Loretta Polk

Loretta Polk

---

[49] *See* NCTA Comments at 4; AT&T Comments at 54-56; ANA Comments at 23-24.