Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Lifeline and Link Up Reform and Modernization	)	WC Docket No. 11-42
	)	
Telecommunications Carriers Eligible for Universal Service Support	)	WC Docket No. 09-197
	)	
Connect America Fund	)	WC Docket No. 10-90
	)	

PETITION FOR PARTIAL RECONSIDERATION

Thomas C. Power
Senior Vice President, General Counsel

Debbie Matties
Vice President, Privacy

Scott K. Bergmann
Vice President, Regulatory Affairs

CTIA – THE WIRELESS ASSOCIATION®
1400 16th Street, NW, Suite 600
Washington, D.C. 20036
(202) 785-0081

August 13, 2015

TABLE OF CONTENTS

I. INTRODUCTION AND SUMMARY. 2

II. SECTION 222(a) DOES NOT GIVE THE COMMISSION AUTHORITY OVER CARRIERS' DATA SECURITY PRACTICES BEYOND THOSE RELATED TO CPNI. 3

A. The Language, Structure, and Purpose of Section 222 Make Clear that CPNI Is the *Only* Customer Data that Section 222 Protects. 3

B. Congress Chose to Address "Proprietary Information" and not "Personal Information" or "Personally Identifiable Information" in Section 222. 6

C. The *TerraCom/YourTel NAL* Does Not Support New Data Security Obligations. 8

III. SECTION 201(b) DOES NOT PROVIDE THE COMMISSION WITH AUTHORITY OVER CARRIERS' DATA SECURITY PRACTICES. 10

IV. THE COMMISSION'S IMPOSITION OF DATA SECURITY OBLIGATIONS BASED ON SECTIONS 222(a) AND 201(b) VIOLATES THE APA. 12

A. The Commission's Interpretations of Sections 222(a) and 201(b) Depart from Longstanding Precedent Without a Reasoned Explanation. 12

B. The Commission Has Imposed Substantive Data Security Obligations Without Notice and Comment. 16

V. CONCLUSION 18

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Lifeline and Link Up Reform and Modernization	)	WC Docket No. 11-42
	)	
Telecommunications Carriers Eligible for Universal Service Support	)	WC Docket No. 09-197
	)	
Connect America Fund	)	WC Docket No. 10-90
	)	

PETITION FOR PARTIAL RECONSIDERATION

Pursuant to Section 1.429 of the Commission's rules,[1] CTIA – The Wireless Association® hereby seeks reconsideration of a narrow, discrete aspect of the *Order on Reconsideration* in the above-captioned proceeding pertaining to data security obligations under the Communications Act.[2] Specifically, CTIA requests that the Commission reconsider its declarations that (1) Section 222(a) imposes a duty of confidentiality upon carriers, other than with respect to Customer Proprietary Network Information ("CPNI"), and (2) Section 201(b) imposes a duty upon carriers to implement data security measures.[3] To be clear, this petition seeks reconsideration solely with respect to the scope of the Commission's authority under those two subsections of the Communications Act. CTIA's petition does not address the *Order on Reconsideration*'s underlying obligation that carriers must retain certain documentation that verifies the eligibility of Lifeline subscribers.

---

[1] 47 C.F.R. § 1.429.

[2] *Lifeline and Link Up Reform and Modernization; Telecommunications Carriers Eligible for Universal Service Support; Connect America Fund*, Second Further Notice of Proposed Rulemaking, Order on Reconsideration, Second Report and Order, and Memorandum Opinion and Order, 30 FCC Rcd 7818 (2015) ("*Order on Reconsideration*").

[3] *Id*. at 7895-96 ¶¶ 234-35.

I. INTRODUCTION AND SUMMARY.

Wireless carriers take very seriously their obligations to protect the security of their customers' data. Indeed, carriers already are required by relevant state and federal laws to do so. To that end, CTIA member companies have established robust data security programs, and they have devoted substantial capital, resources, and personnel to preventing, detecting, deterring, and responding to data security threats. Beyond their legal obligations, CTIA member companies also recognize that safeguarding their customers' data is a good business practice. Thus, carriers have strong incentives to earn and maintain consumer trust and loyalty by protecting the security of their customers' data.

The object of this petition is to ensure that the Commission's data security requirements are rooted in, and conform to, the applicable statutory provisions enacted by Congress. In the *Order on Reconsideration*, the Commission claims that Sections 222(a) and 201(b) of the Communications Act[4] are the source of customer data security obligations. The Commission cites those provisions as imposing a duty to protect and secure all data obtained while verifying the eligibility of potential Lifeline subscribers, including data beyond CPNI.[5] However, the Commission's ability to regulate the security of carriers' customers' information is limited to the authority that Congress granted over CPNI as defined in Section 222(h). Congress gave the Commission no authority to impose customer data security regulations other than with respect to CPNI, and neither Section 222(a) nor Section 201(b) gives the Commission authority to impose customer data security requirements of any kind. In addition, the Commission's assertions that

---

[4] 47 U.S.C. §§ 222(a), 201(b).

[5] If the Commission reconsiders and vacates this narrow aspect of the *Order on Reconsideration*, carriers will continue to be subject to rigorous data security regulations with respect to this information. As stated above, carriers are obliged under existing federal and state laws to safeguard the security of this data.

Sections 222(a) and 201(b) require carriers to protect data that goes beyond CPNI runs counter to the Administrative Procedure Act ("APA") by (1) departing from longstanding precedent without reasoned explanation and (2) imposing such obligations without providing notice and seeking comment. The Commission therefore should reconsider and vacate the *Order on Reconsideration*'s confidentiality and data security obligations under Sections 222(a) and 201(b) of the Communications Act to the extent they apply to information broader than CPNI.[6]

II. SECTION 222(a) DOES NOT GIVE THE COMMISSION AUTHORITY OVER CARRIERS' DATA SECURITY PRACTICES BEYOND THOSE RELATED TO CPNI.

Citing Section 222(a), paragraph 234 of the *Order on Reconsideration* "remind[s] [eligible telecommunications carriers] that pursuant to section 222 of the Act, they have a duty to protect 'the confidentiality of proprietary information' of customers."[7] Section 222, however, does not impose obligations on carriers regarding customer information beyond CPNI. Any interpretation of Section 222(a) that expands the scope of customer data protected beyond CPNI conflicts with the language, structure, and purpose of Section 222 and contravenes Congress's intent in enacting Section 222.

A. The Language, Structure, and Purpose of Section 222 Make Clear that CPNI Is the *Only* Customer Data that Section 222 Protects.

The language and structure of Section 222 make clear that Section 222 does not protect customer information beyond CPNI. The Commission's reading of Section 222(a) as

---

[6] Prior to the *Order on Reconsideration*, the Commission had not addressed in this proceeding data security authority under Sections 222(a) and 201(b) of the Communications Act. Thus, the arguments herein "relate to … circumstances which have changed since the last opportunity to present such matters to the Commission." 47 C.F.R. § 1.429(b)(1).

[7] *Order on Reconsideration*, 30 FCC Rcd at 7895-96 ¶ 234 (citing 47 U.S.C. § 222(a); *TerraCom, Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325, 13331-35 (2014) ("*TerraCom/YourTel NAL*")).

establishing a broad data security obligation cannot be squared with the clear and more specific provisions of the statute and must be reconsidered.

Indeed, the statute is coherent and internally consistent only if it is read to limit customers' "proprietary information" to CPNI. Section 222(a) is nothing more than a general principle that has force and effect – with respect to customer information – only as specified in Section 222(c). Section 222(a) merely identifies the three categories of information to which the statute applies, *i.e.*, proprietary information relating to (1) carriers, (2) equipment manufacturers, and (3) customers. The definitions of these categories and the carriers' substantive obligations are spelled out in three corresponding subsections of the Communications Act. In the case of customer information, the operative subsection is Section 222(c).[8] Section 222(c) expressly limits the type of *customer* information to which the statute applies to CPNI, which Section 222(h) defines to mean *only* information related to the (1) quantity; (2) technical configuration; (3) type; (4) destination; (5) location; (6) amount of use of a telecommunications service; and (7) information contained in bills pertaining to telephone exchange service or telephone toll service.[9]

If Section 222(a) imposed a standalone requirement on carriers to protect customers' information beyond CPNI, other provisions of Section 222 would not make sense. Under such a reading, Section 222(a) would conflict with Section 222(e), which directs carriers to disclose "subscriber list information" (*i.e.*, subscribers' names, addresses, and phone numbers) to competing providers of phone directories, "[n]otwithstanding subsections (b), (c), and (d)" of

---

[8] In like fashion, Section 222(b) governs carriers' proprietary information, and Section 273(d)(2) governs equipment manufacturers' proprietary information.

[9] 47 U.S.C. §§ 222(c); 222(h). The definition of CPNI does not include customers' names, addresses, and phone numbers. *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information*, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, 14487 ¶ 146 (1999) ("*1999 CPNI Order*").

Section 222.[10] If Section 222(a) imposed a separate requirement on carriers to protect customers' personal information, then Congress would have added it to the list of subsections – (b), (c), and (d) – that are trumped by Section 222(e)'s disclosure requirement. Congress did not reference subsection (a), however, because Section 222(a) does not impose any such requirement.

In addition, if Section 222(a) were read to impose an independent duty on carriers to protect customer information other than CPNI, the exceptions Congress set forth in Section 222(d) would not make sense. Section 222(d) provides exceptions to the general prohibition on the disclosure of *CPNI*, allowing carriers to use CPNI to do billing, deter fraud, and assist emergency health, law enforcement, and fire personnel. These exceptions apply only to CPNI and do not extend to any other customer information, such as the broader category of customer "proprietary information" that the Commission believes must be protected under Section 222(a). In the Commission's view, then, the statute permits a carrier to share CPNI with first responders in the event of a threat to life or property, but in those same potentially life-or-death circumstances the carrier must refrain from sharing some broader category of customers' "proprietary information" that is apparently too sensitive to be shared even with first responders but that Congress did not bother to define.[11] It is not rational to assume that in Section 222(a) Congress established a separate category of customer information that carriers must withhold from first responders; the only reasonable interpretation is that Section 222(a) does not establish a separate category of protected information at all.

The legislative history also confirms that with respect to *customers'* information, Congress intended that Section 222 apply only to CPNI as defined in Section 222(h)(1) and not

---

[10] 47 U.S.C. § 222(e).

[11] *See* 47 U.S.C. § 222(d).

to some broader category of customer "proprietary" information. For instance, the Conference Report described Section 222 as "striv[ing] to balance both competitive and consumer privacy interests with respect to *CPNI*."[12] In conference, Congress eliminated catch-all provisions in the House and Senate bills that would have given the Commission broader authority to regulate customer information more generally.[13] The final bill circumscribed the customer information that the statute would cover by limiting such information to the precise categories listed in Section 222(h)(1).

In light of the foregoing, there is no way to read Section 222(a) as a standalone grant of authority. The Commission's broader conclusion in the *Order on Reconsideration* is an error that the Commission must correct.

B. Congress Chose to Address "Proprietary Information" and not "Personal Information" or "Personally Identifiable Information" in Section 222.

Congress chose to draft Section 222 in a different manner from privacy laws that Congress passed to protect "personal information" or "personally identifiable information,"[14] *including privacy laws that amended the Communications Act*.[15] Indeed, Congress chose to use

---

[12] H.R. REP. NO. 104-458, at 205 (1996) (Conf. Rep.) (Joint Explanatory Statement of the Committee of Conference) (emphasis added).

[13] The House version of the bill defined CPNI to include the information currently listed in Section 222(h) as well as "such other information concerning the customer as is available to the local exchange carrier by virtue of the customer's use of the carrier's telephone exchange service or telephone toll services, and specified as within the definition of such term by such rules as the Commission shall prescribe consistent with the public interest." H.R. REP. NO. 104-204, at 22-23, 89-91 (1995). The Senate version of the bill defined the customer information covered broadly as "customer-specific proprietary information," with no limiting language. S. REP. NO. 104-32, at 23-24 (1995).

[14] "Personal information" and "personally identifiable information" are terms of art in privacy statutes, and they generally mean information that identifies an individual or that, when linked to other information, can be used to identify an individual. These terms typically include information such as Social Security Numbers, financial information, and other identifiable or identifying information.

[15] In addition to the privacy laws that amended the Communications Act, Congress also passed a number of other privacy laws that protect "personal information" or "personally identifiable information" (but not "proprietary information") around the same time that it passed Section 222. These privacy statutes include the Children's Online Privacy Protection Act, the Gramm-Leach-Bliley Act, and the

the term "personally identifiable information" elsewhere in the Communications Act, both before and after Congress drafted Section 222 in 1996. For example, in 1984, Congress imposed certain duties on cable operators to protect the privacy of "personally identifiable information concerning any subscriber."[16] Likewise, in 2004, Congress imposed similar duties on satellite operators to protect the privacy of "personally identifiable information" of satellite subscribers.[17] If Congress similarly had wanted Section 222 to cover "personally identifiable information" and not just CPNI, it would have said so.[18]

Instead, Congress used the term "proprietary information" in Section 222, not "personal information" or "personally identifiable information," because it intended Section 222 to serve a different purpose. Specifically, because CPNI was available only to carriers and their customers, Congress was concerned that "[i]ncumbent carriers already in possession of CPNI could leverage

---

Video Privacy Protection Act, to name a few. Children's Online Privacy Protection Act, Pub. L. No. 105-277 (1998) (codifying definition of children's "personal information" at 15 U.S.C. § 6501(8)); Gramm-Leach-Bliley Act, Pub. L. No. 106-102 (1999) (codifying definition of "nonpublic personal information" at 15 U.S.C. § 6809(4)); Video Privacy Protection Act, Pub. L. No. 100-618 (1988) (codifying definition of "personally identifiable information" at 18 U.S.C. § 2710); *see also, e.g.*, Family Educational Rights and Privacy Act, Pub. L. No. 93-389 § 513 (1974) (codifying at 20 U.S.C. § 1232g(b)(2) certain protections for students' "personally identifiable information").

[16] Cable Communications Policy Act of 1984, Pub. L. No. 98-549 (1984) (establishing Section 631 of the Communications Act, codified at 47 U.S.C. § 551, to protect the privacy of cable subscribers' "personally identifiable information").

[17] Satellite Home Viewer and Reauthorization Act of 2004, Pub. L. No. 108-447 (2004) (establishing Section 338(i) of the Communications Act, codified at 47 U.S.C. § 338(i), to protect the privacy of satellite subscribers' "personally identifiable information").

[18] Just as it did in the Communications Act, Congress has distinguished the terms "proprietary information" and "personally identifiable information" from one another elsewhere when they appeared together in the same statutes. For example, Congress directed the Director of the Federal Housing Finance Agency, which is required to collect and make public certain mortgage-related information from Federal Home Loan Banks, to protect information "that the Director determines is proprietary *or* that would provide personally identifiable information…." 12 U.S.C. § 1430(k)(2)(B) (emphasis added). The Commission also has distinguished "personal" from "proprietary" information. *See Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601, 5821 ¶ 463 (2015) (asserting that broadband providers are in a position to obtain "personal *and* proprietary information about their customers") (emphasis added).

their control of CPNI in one market to perpetuate their dominance as they enter other service markets."[19]

The *Order on Reconsideration* assumes that the Commission used "proprietary information" in a way that was intended to be synonymous with "personally identifiable information," yet Congress's careful use of the latter term in other statutes shows the error of the Commission's conclusion.

C. The *TerraCom/YourTel NAL* Does Not Support New Data Security Obligations.

The *Order on Reconsideration* favorably cites the *TerraCom/YourTel NAL*,[20] but to the extent that this "tentative" Commission conclusion found a substantive obligation under Section 222(a), it too was erroneous.[21]

The *TerraCom/YourTel NAL* does not address the arguments set out above regarding the internal consistency of Section 222 as a whole, the legislative history of the statute, or Congress's otherwise careful use of "personally identifiable information" as a term of art in statutory drafting. Rather, the *TerraCom/YourTel NAL* simply states that it is "clear that the scope of 'proprietary information' protected by Section 222(a) is broader than the statutorily defined term" CPNI, and that Section 222(a) provides protection not just for proprietary information, but also for *personal* information.[22] To support this proposition, the Commission asserted that "[h]ad Congress wanted to limit the protections of subsection (a) to CPNI, it could

---

[19] *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, 8064 ¶ 2 (1998) ("*1998 CPNI Order*").

[20] *TerraCom/YourTel NAL*, *supra*, note 7.

[21] Notices of apparent liability for forfeiture represent only "tentative conclusions" of the Commission and are insufficient to put parties on notice of official agency policy, particularly in light of other contrary authority. *See, e.g.*, *CBS Corp. v. FCC*, 663 F.3d 122, 130 (3d Cir. 2011), *cert. denied*, 132 S. Ct. 2677 (2012).

[22] *See TerraCom/YourTel NAL*, 29 FCC Rcd at 13330-31 ¶¶ 15-18.

have done so."[23] In fact, it did, by drafting Section 222 in a manner that *necessarily limits the protection of customer proprietary information in Section 222(a) to CPNI*. Otherwise, as discussed above, other provisions of the statute would not make sense.

The Commission also cites to the headings of Section 222 ("Privacy of customer information") and Section 222(c)(1) ("Privacy requirements for telecommunications carriers") to support its conclusion that it is "clear" that "proprietary information" is broader than CPNI.[24] It is telling that the Commission cites to these headings as its primary support for its interpretation given the minimal interpretive value ascribed to them by courts. Titles or headings of statutes cannot limit the plain meaning of the statue or "undo that which the text makes plain."[25] Nor can a title "enlarge or confer powers."[26] Even assuming the headings are relevant to the analysis, Section 222's heading ("Privacy of customer information") has no bearing on the scope of Section 222, given that Section 222 clearly governs the privacy of carriers' and equipment manufacturers' proprietary information, in addition to customers' information. The reference to "privacy" in the heading therefore does not mean that customer "proprietary information" referenced in Section 222(a) is broader than CPNI referenced in Section 222(c). Moreover, Section 222(c)(1)'s heading ("Privacy requirements for telecommunications carriers") is subsidiary to the heading of Section 222(c) itself ("Confidentiality of customer proprietary network information"), which suggests that the "privacy" at issue relates only to CPNI.

---

[23] *Id.* at 13330 ¶ 15.

[24] *Id*. at 13330 ¶ 14.

[25] Norman J. Singer, Sutherland Statutory Construction § 47:03 (6th ed. 2000) (citing *Bhd. of RR Trainmen v. Baltimore & Ohio RR*, 331 U.S. 519, 528-29 (1947) ("[T]he title of a statute and the heading of a section cannot limit the plain meaning of the text.").

[26] *Pennhurst State Sch. & Hosp. v. Halderman*, 451 U.S. 1, 19 n.14 (1981) (quoting *U.S. v. Oregon & California R.R. Co.*, 164 U.S. 526, 541 (1896) and *Cornell v. Coyne*, 192 U.S. 418, 430 (1904)).

Finally, the *TerraCom/YourTel NAL* erroneously expands Section 222(a) to impose an obligation to protect information that Lifeline "*applicants*" submit to carriers.[27] Section 222(a), however, applies only to "*customers*," which the Commission's rules define to mean "person[s] or entit[ies] to which the telecommunications carrier *is currently providing service*."[28] "Applicants" are not subscribers to whom the carrier is providing service; therefore, they are not "customers." Thus, the Commission does not have authority under Section 222(a) to impose obligations regarding information submitted by "applicants" to the Lifeline program. Indeed, it cannot ignore the definition of "customer" in its own rules and invent a new, more expansive definition for the same term in the same statute simply to "give effect to the broader duty and privacy protections" that it now states Section 222(a) imposes.[29]

III. SECTION 201(b) DOES NOT PROVIDE THE COMMISSION WITH AUTHORITY OVER CARRIERS' DATA SECURITY PRACTICES.

The *Order on Reconsideration* asserts that Section 201(b)'s requirement that practices be just and reasonable "imposes a duty on [carriers] related to document retention security practices."[30] But Section 201(b) neither imposes such requirement nor gives the Commission authority to impose such a requirement.

Congress necessarily assumed that the Commission lacked authority over carriers' data privacy and security practices when it adopted what the Commission called a "comprehensive

---

[27] *TerraCom/YourTel NAL*, 29 FCC Rcd at 13334 ¶ 27. Again, as explained above, existing federal and state laws already require carriers to safeguard the security of personal information that Lifeline applicants submit to them.

[28] 47 C.F.R. § 64.2003 (emphasis added).

[29] *TerraCom/YourTel NAL*, 29 FCC Rcd at 13334 ¶ 27.

[30] *Order on Reconsideration*, 30 FCC Rcd at 7896 ¶ 235. The *Order on Reconsideration* also directs ETCs to implement minimum security protections to protect the confidentiality of a category of information that the Commission calls "consumers' proprietary personal information." *Id*. The Commission does not explain what "consumer proprietary personal information" means. Indeed, it is a term that does not appear anywhere in Section 222 or in previous Commission orders.

new framework" to address such practices in Section 222.[31] If the Commission already had privacy and data security authority under Section 201(b), the adoption of Section 222 would have been superfluous. Understanding that the Commission lacked – and still lacks – such authority under Section 201(b), Congress acted to define the Commission's privacy and data security authority in Section 222.[32] Even after enacting Section 222, Congress again made clear that it believed the Commission lacked broad data privacy and security authority: when Congress added "location" to the definition of CPNI through the Wireless Communications and Public Safety Act of 1999, it did so because "[u]nless [the] legislation [was] enacted, there [would have been] no protection for a customer's location information."[33] If the Commission already had authority to address the protection of location information under Section 201(b), congressional action would have been unnecessary and superfluous.

The Commission cannot read Section 201(b) in a way that upsets the balance that Section 222 establishes. The Commission itself recognized this balance when it stated shortly after Congress passed Section 222 that it was "persuaded that Congress established a comprehensive new framework in Section 222, which balances principles of privacy and competition in connection with the use and disclosure of *CPNI* and other customer information [*i.e.*, subscriber list information and aggregate customer information]."[34] Congress established protections for CPNI and the other categories of customer information described in Section 222, but declined to

---

[31] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, 8073-74 ¶ 14 (1998).

[32] *See* 139 Cong. Rec. E 2745 (Nov. 3, 1993) (statement of Congressman Markey) ("The legislation I am introducing today will ensure that the fundamental privacy rights of each American will be protected even as this new era of communications becomes ever more sophisticated and ubiquitously deployed.").

[33] 145 Cong. Rec. H 9858 (Oct. 12, 1999) (statement of Rep. John Shimkus).

[34] *1998 CPNI Order*, 13 FCC Rcd at 8073-74 ¶ 14 (emphasis added).

set forth protections for a broader set of customer information, including "personally identifiable information." Therefore, it follows that Congress intended the Commission's data security authority over common carriers to be limited to the categories of information set forth in Section 222. Thus, the Commission cannot assert broader authority under Section 201(b).

IV. THE COMMISSION'S IMPOSITION OF DATA SECURITY OBLIGATIONS BASED ON SECTIONS 222(a) AND 201(b) VIOLATES THE APA.

Even if the Commission had authority under Section 222(a) and Section 201(b) to impose obligations regarding customer information beyond CPNI, which it does not, the Commission's reliance on Sections 222(a) and 201(b) is a departure from longstanding Commission precedent and does not comply with requirements under the APA to provide notice and the opportunity to comment.

A. The Commission's Interpretations of Sections 222(a) and 201(b) Depart from Longstanding Precedent Without a Reasoned Explanation.

The Commission's reliance on Section 222(a) departs from longstanding Commission precedent, yet the Commission has failed to explain this change in policy to date, let alone provide notice and the opportunity to comment. Until the recent *TerraCom/YourTel NAL*, the Commission had long recognized that Section 222 covered limited types of customer information, asserting in multiple Commission orders that Section 222 covers just three categories of "customer information": (1) individually identifiable CPNI; (2) aggregate customer information; and (3) subscriber list information.[35] The Commission also correctly recognized that the reference to customer proprietary information in Section 222(a) is

[35] *See, e.g.*, *1998 CPNI Order*, 13 FCC Rcd at 8064 ¶ 2; *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended*, Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14860, 14864 ¶ 6 (2002); *see also U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1228 n.1 (10th Cir. 1999).

coextensive with the reference to CPNI in Section 222(c): "Section 222(a) imposes a general duty on telecommunications carriers to protect the confidentiality of proprietary information – a duty owed to other carriers, equipment manufacturers, and customers. . . . Section 222(c) outlines the confidentiality protections applicable to *customer information*."[36] Put another way, "[e]very telecommunications carrier has a general duty pursuant to section 222(a) to protect the confidentiality of CPNI."[37] Indeed, the Commission specifically denied a "request that the Commission hold that section 222 controls all issues involving customer information, rather than pertaining to CPNI."[38]

Even in this proceeding, until the *Order on Reconsideration*, the Commission's citations to Section 222 only referred to the protection of CPNI, not other customer information. In the *Notice of Proposed Rulemaking* that preceded the *Order on Reconsideration*, the Commission asked "[t]o the extent that use of customer proprietary network information (CPNI) is needed to ensure that a subscriber at a single residential address is not receiving multiple subsidized subscriptions, how do commenters suggest we ensure compliance with *section 222* of the Communications Act and our implementing rules?"[39] The Commission did not ask how it could ensure compliance with Section 222 with respect to the use of customer proprietary information

---

36 *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6930 ¶ 4 n.6 (2007) ("*2007 CPNI Order*") (emphasis added).

37 *2007 CPNI Order*, 22 FCC Rcd at 6930 ¶ 6; *see also Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Declaratory Ruling, 28 FCC Rcd 9609, 9619 ¶ 29 (2013) (*"2013 Mobile Device CPNI Ruling*").

38 *1999 CPNI Order*, 14 FCC Rcd at 14888 ¶ 147.

39 *Lifeline and Link Up Reform and Modernization*, Notice of Proposed Rulemaking, 26 FCC Rcd 2770, 2790 ¶ 57 (2011) ("*Notice of Proposed Rulemaking*") (italics in original); *see also Lifeline and Link Up Reform and Modernization*, Report and Order, 26 FCC Rcd 9022, 9029 ¶ 13 n.48 (2011) (noting that ETCs can disclose CPNI necessary to identify duplicative Lifeline claims pursuant to the exceptions in Section 222(d), but making no mention of production of other customer information).

or personal information beyond CPNI. The Commission did not do so presumably because it assumed – correctly – that Section 222 did not apply to any broader set of customer data.

Notwithstanding the Commission's past statements indicating that Section 222(a) does not cover customer proprietary information broader than CPNI, the Commission in the *TerraCom/YourTel NAL* relied on two sentences from Commission orders to assert that Section 222(a) imposes a broader obligation.

First, the *TerraCom/YourTel NAL* cited the *2007 CPNI Order*'s reference to Section 222(a) for the proposition that it "expect[s] carriers to take every reasonable precaution to protect the confidentiality of proprietary or personal customer information."[40] But the next two sentences of the *2007 CPNI Order* make clear that the Commission was talking about CPNI, not some broader category of proprietary information: "Of course, we require carriers to implement the specific minimum requirements set forth in the Commission's rules. We further expect carriers to take additional steps to protect the privacy of CPNI to the extent such additional measures are feasible for a particular carrier."[41] The preceding reference to "personal customer information" necessarily reflects Section 222's requirement that carriers protect "individually identifiable" *CPNI* (*i.e.*, the personal information that renders CPNI "individually identifiable").

Second, the Commission relied on a sentence in the *2013 Mobile Device CPNI Ruling* that said: "We also note that subsection (a)'s obligation to protect customer information is not

---

[40] *2007 CPNI Order*, 22 FCC Rcd at 6959 ¶ 64 (citation omitted); *TerraCom/YourTel NAL*, 29 FCC Rcd at 13330 ¶ 13 n.30.

[41] *2007 CPNI Order*, 22 FCC Rcd at 6959 ¶ 64. The references to CPNI are also pervasive in the surrounding paragraphs. *See generally id.* at 6959-60 ¶¶ 63, 65. The Commission went on in the same paragraph to mention its expectation that carriers take "reasonable measures" to prevent pretexting, *see id.* at 6959 ¶ 64, referring back to an earlier section of the *2007 CPNI Order* that indicated that, under Section 222(a), the Commission was codifying a requirement to take "reasonable measures" against pretexting. *Id.* at 6945-46 ¶¶ 33-34, n.106. Notably, the rule the Commission adopted to codify this "reasonable measures" requirement under Section 222(a) applies only to CPNI: "Telecommunications carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI." 47 C.F.R. § 64.2010(a).

limited to CPNI that the carrier has obtained or received."[42] But read in context, it is clear that this sentence was not suggesting that Section 222(a) covered customer information beyond CPNI (or aggregate customer information or subscriber list information). Rather, the Commission was explaining that Section 222(a) obliged carriers to protect CPNI that they have not yet "obtained or received": "[t]he fact that *CPNI* is on a device and *has not yet been transmitted to the carrier's own servers* also does not remove the data from the definition of CPNI."[43] Thus, this sentence actually confirms that Section 222(a) applies only to CPNI, not a broader category of information.

Similarly, until the *TerraCom/YourTel NAL*, the Commission had never before in the 80 year history of Section 201(b) asserted that 201(b) gave it authority to regulate data security.[44] Indeed, such a requirement would be – and is – inconsistent with congressional intent. Rather than address these fundamental challenges to its interpretation of Section 201(b), the Commission in the *TerraCom/YourTel NAL* did not provide any statutory analysis regarding Section 201(b) or cite any Commission or judicial precedent for its reading of Section 201(b).[45]

---

[42] *2013 Mobile Device CPNI Ruling*, 28 FCC Rcd at 9618 ¶ 27.

[43] *Id*. (emphasis added).

[44] The Commission's failure to find such authority to regulate data security practices under Section 201(b) previously is itself evidence that such authority does not exist. *See Util. Air. Regulatory Grp. v. EPA*, 134 S. Ct., 2427, 2444 (2014) ("When an agency claims to discover in a long-extant statute an unheralded power to regulate 'a significant portion of the American economy,' we typically greet its announcement with a measure of skepticism. We expect Congress to speak clearly if it wishes to assign to an agency decisions of vast 'economic and political significance.").

[45] The *TerraCom/YourTel NAL* provides a source for only one aspect of its novel interpretations of Section 201(b): its finding that misrepresentations of data security practices in privacy policies violate Section 201(b). *See TerraCom/YourTel NAL*, 29 FCC Rcd at 13339 ¶ 38 n.83 (citing *Joint FCC/FTC Policy Statement for the Advertising of Dial-Around and Other Long-Distance Services to Consumers*, 15 FCC Rcd 8654, 8654 ¶ 4 (FCC/FTC 2000)). But even that precedent supports at most only a finding that carriers' *misrepresentations* about their practices regarding data security *or some other activity*, and not the underlying practices or activities themselves, can violate Section 201(b). The precedent is otherwise inapposite: it neither provides justification to create a new data security regime under Section 201(b) from whole cloth, nor does it answer questions regarding how Commission regulation of carriers' data security practices under Section 201(b) is consistent with Section 222.

It did not, and could not, because there is no such support for the Commission's novel approach. Indeed, any analysis or citation to precedent necessarily would confirm that the Commission's assertion of data security authority under Section 201(b) ignores and upsets the balance Congress intended to establish under Section 222.

Even if the Commission did have authority to impose requirements on carriers with respect to customer data beyond CPNI, which it does not, the Commission still has failed to provide a reasoned explanation for this change in policy. An agency "may not … depart from a prior policy *sub silentio*" but instead must provide a "reasoned explanation for its action [which] would ordinarily demand that it display awareness that it *is* changing position."[46] The Commission, however, has failed to acknowledge that it has changed its position with respect to Section 222(a), and as noted above, it has incorrectly described prior Commission statements as interpreting Section 222(a) to apply to customer data broader than CPNI.[47] Likewise, the Commission has failed to explain why it now, after 80 years of silence, finds broad data security authority under Section 201(b) where Congress assumed it had none. Thus, the Commission has failed to provide a reasoned explanation for its new interpretations of Sections 222(a) and 201(b), as it must do.

B. The Commission Has Imposed Substantive Data Security Obligations Without Notice and Comment.

In addition, the Commission failed to provide notice and the opportunity to comment on the data security requirements in the *Order on Reconsideration*. Beyond just articulating a new duty under Sections 222(a) and 201(b), the *Order on Reconsideration* articulated stunningly

---

[46] *FCC v. Fox Television Stations, Inc.*, 556 U.S. 502, 515 (2009).

[47] *See TerraCom/YourTel NAL*, 29 FCC Rcd at 13352 (dissenting statement of Commissioner O'Rielly) (noting that the Commission had viewed Section 222(a) as a general duty to be read in conjunction with Sections 222(b) and (c) and that the Commission had viewed the customer proprietary information in Section 222(a) as co-extensive with CPNI).

specific data security safeguards that it requires carriers to adopt and implement.[48] The APA, however, requires agencies to follow notice-and-comment procedures when they adopt "legislative rules," *i.e.*, rules that have the "force and effect of law."[49] The Commission did not propose these specific, substantive data security requirements for carriers in any notice of proposed rulemaking, yet it intends them to have the "force and effect of law." Even if these security safeguards reflect "assurances" that some commenters made about "appropriate measures" they take to protect data,[50] carriers could not have anticipated that the Commission would adopt these new data security requirements for carriers. Had the Commission provided notice, commenters would have had the opportunity to raise the concerns discussed above regarding the limits of the Commission's authority to promulgate data privacy or security rules under Sections 222(a) and 201(b).

---

[48] *Order on Reconsideration*, 30 FCC Rcd at 7896 ¶ 235.

[49] *Nat'l Mining Ass'n v. McCarthy*, 758 F.3d 243, 250 (D.C. Cir. 2014) (quoting *INS v. Chadha*, 462 U.S. 919, 986 n.19 (1983)); *see also* 5 U.S.C. § 553 (setting forth three-step procedure for notice-and-comment rulemaking).

[50] *Order on Reconsideration*, 30 FCC Rcd at 7895 ¶ 235. In the *Notice of Proposed Rulemaking* and 2012 Report and Order in this proceeding, the Commission discussed the sensitivity of certain data that it wanted ETCs to collect. The Commission did *not* seek comment on specific ways *ETCs* should be required to protect the security of such data, however. Rather, it focused on data security in the context of a proposal to establish a centralized database that the Universal Service Administrative Company ("USAC") would use to store this information. *See Notice of Proposed Rulemaking*, 26 FCC Rcd at 2790 ¶ 57 (discussing proposal to require ETCs to provide *USAC* with certain data about subscribers and seeking comment on "[w]hat measures…*USAC* could put in place to ensure compliance with ECPA or other applicable laws…") (emphasis added); *Lifeline and Link Up Reform and Modernization; Lifeline and Link Up; Federal-State Joint Board on Universal Service; Advancing Broadband Availability Through Digital Literacy Training*, Report and Order and Further Notice of Proposed Rulemaking, 27 FCC Rcd 6656, 6745 ¶ 207 (2012) (explaining that the *Notice of Proposed Rulemaking* sought comment on what security safeguards *USAC* should be required to implement to protect the security of data in the centralized database) (emphasis added). The mere reference to compliance with CPNI requirements under Section 222 is insufficient to provide notice that the Commission was considering specific security protections applying to non-CPNI information.

For the foregoing reasons, these new data security safeguards are neither part of, nor a logical outgrowth from, anything that the Commission noticed in the docket.[51] Thus, these requirements do not satisfy the Commission's obligations under the APA to provide notice and the opportunity to comment before adopting new rules. Accordingly, the Commission should reconsider these obligations.

V. CONCLUSION.

CTIA members understand the importance of protecting the security of their customers' personal information. They spend substantial resources to implement and maintain strong data security programs, both to comply with their existing data security obligations under federal and state laws and because they consider protecting customers' data security to be a critically important business practice. While CTIA members are committed to protecting the security of their customers' data, the Communications Act does not give the Commission authority to police carriers' practices with regard to customer data that is not CPNI. Accordingly, the Commission should reconsider its declarations that, under Sections 222 and 201(b), carriers must (1) keep subscriber eligibility information confidential, to the extent that this information is broader than CPNI, and (2) implement data security measures to protect this information.

---

[51] *See Pub. Serv. Comm'n of D.C. v. FCC*, 906 F.2d 713, 717 (D.C. Cir. 1990) ("It is well established that ... the final rule must be 'a logical outgrowth' of the rule proposed."). The focus of the logical outgrowth test is whether commenting parties "should have anticipated" that the Commission might adopt the requirement at issue. *Aeronautical Radio, Inc., v. FCC*, 928 F.2d 428, 445-46 (D.C. Cir. 1991) (internal quotation marks omitted). Where parties could not have anticipated that the rule ultimately adopted was possible, the final rule is not a "logical outgrowth" of the original proposal and the APA's notice requirements are violated. *See id.*

Respectfully submitted,

CTIA – THE WIRELESS ASSOCIATION®

By: */s/ Thomas C. Power*

Thomas C. Power
Senior Vice President, General Counsel

Debbie Matties
Vice President, Privacy

Scott K. Bergmann
Vice President, Regulatory Affairs

CTIA – THE WIRELESS ASSOCIATION®
1400 16th Street, NW, Suite 600
Washington, D.C. 20036
(202) 785-0081

August 13, 2015