

**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

REPLY OF CTIA – THE WIRELESS ASSOCIATION®

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, DC 20036
(202) 783-0081

October 19, 2015

TABLE OF CONTENTS

I. INTRODUCTION AND SUMMARY.....1

II. THE PIOS’ PROCEDURAL ARGUMENTS FAIL AS A MATTER OF LAW AND ARE FACTUALLY INACCURATE.2

 A. CTIA Has Section 405 Standing to Petition for Reconsideration.....2

 B. The *Order*’s Confidentiality and Data Security Obligations Constitute “Agency Action” Subject to Reconsideration.....4

 C. The Confidentiality and Data Security Obligations Were Subject to APA Notice Requirements.5

III. SECTION 222(a) DOES NOT GIVE THE COMMISSION AUTHORITY OVER CARRIERS’ DATA SECURITY PRACTICES BEYOND THOSE RELATED TO CPNI.6

IV. THE PIOS’ ARGUMENTS SUPPORTING THE COMMISSION’S ASSERTION OF UNPRECEDENTED AUTHORITY UNDER SECTION 201(b) ARE UNPERSUASIVE.....8

V. THE COMMISSION’S IMPOSITION OF DATA SECURITY OBLIGATIONS BASED ON SECTIONS 222(a) AND 201(b) VIOLATES THE APA.10

VI. CONCLUSION.....10

**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

REPLY OF CTIA – THE WIRELESS ASSOCIATION®

CTIA – The Wireless Association® (“CTIA”) hereby replies to the opposition filed by certain organizations (the “PIOs”)¹ to CTIA’s Petition for Partial Reconsideration² of the *Order*.³

I. INTRODUCTION AND SUMMARY.

The Petition seeks reconsideration of a discrete part of the *Order* pertaining to carriers’ data security obligations under the Communications Act (the “Act”). Contrary to the PIOs’ assertion, CTIA members already are subject to rigorous data security obligations with respect to this information under existing federal and state laws. Moreover, CTIA does not challenge the rule requiring Lifeline providers to retain customer eligibility documentation adopted in the *Order* pursuant to Section 254,⁴ but takes issue with the data security requirements imposed under jurisdiction the Commission purportedly found in Sections 222 and 201(b).

¹ See Opposition to Petition for Partial Reconsideration of Appalshop, *et al.*, Corrected Version, WC Docket Nos. 11-42 *et al.* (filed Oct. 9, 2015) (“Opposition”).

² Petition for Partial Reconsideration of CTIA – The Wireless Association®, WC Docket Nos. 11-42 *et al.* (filed Aug. 13, 2015) (“Petition”).

³ *Lifeline and Link Up Reform and Modernization, et al.*, WC Docket Nos. 11-42 *et al.*, Second Further Notice of Proposed Rulemaking, Order on Reconsideration, Second Report and Order, and Memorandum Opinion and Order, 30 FCC Rcd 7818 (2015) (“*Order*”).

⁴ See *Order* ¶ 298.

Specifically, Section 222(a) does not give the Commission authority over carriers' data security practices beyond those related to Customer Proprietary Network Information ("CPNI"), and Section 201(b) does not provide the Commission with authority over carriers' data security practices. Contrary to the PIOs' assertion in their Opposition, CTIA members do not contend that they have no obligation to protect this information, but rather acknowledge that they already are subject to rigorous data security obligations.⁵ Thus, if the Commission were to reconsider and vacate the *Order* with respect to this issue, carriers would continue to be legally obligated to protect this information, but not under the Act.

In response to the Petition, the PIOs have filed an unpersuasive Opposition that merely recites the statements that the Commission made in the *Order* and in the *TerraCom/YourTel NAL* and ultimately fails to refute the arguments made in the Petition. As shown below, all of the PIOs' arguments fail as a matter of law. The only other filing in the docket entirely supports CTIA's Petition.⁶ The Commission therefore should reconsider and vacate the *Order*'s confidentiality and data security obligations under Sections 222(a) and 201(b) of the Act to the extent that they impose obligations beyond those related to CPNI.

II. THE PIOS' PROCEDURAL ARGUMENTS FAIL AS A MATTER OF LAW AND ARE FACTUALLY INACCURATE.

A. CTIA Has Section 405 Standing to Petition for Reconsideration.

The PIOs' standing challenge, arguing CTIA's members were not injured or aggrieved by the *Order*,⁷ misses the point because any "party" to a proceeding may file a petition for

⁵ Petition at 2.

⁶ Comments of American Cable Association in Support of Petition for Partial Reconsideration, WC Docket Nos. 11-42 *et al.* (filed Oct. 8, 2015).

⁷ Petition at 5-6.

reconsideration of an FCC order.⁸ CTIA, as a party to this proceeding, is statutorily entitled to file a petition for reconsideration.

Even though other state and federal laws apply to personal data, CTIA members *are* injured or aggrieved by the *Order*'s imposition of particularized data security obligations detailing specific technical measures like “protective naming conventions.”⁹ As the *TerraCom/YourTel NAL* and subsequent settlement show, when carriers fail to implement the Commission's preferred security safeguards, the Commission may seek exorbitant and seemingly unbounded fines with no connection to any actual consumer injury.¹⁰ The *Order* will constrain carriers with the risk of huge fines if they implement new data security solutions that depart from the *Order*, even if those new solutions better protect consumers. For all these reasons, CTIA and its members are unquestionably aggrieved by the data security obligations that the Commission found in the *Order*.

The PIOs attempt to make much of the fact that CTIA does not challenge the obligation to retain customer eligibility data,¹¹ but the Petition *does* challenge and request vacatur of the

⁸ 47 U.S.C. § 405(a) (“any party . . . may petition for reconsideration”).

⁹ The order requires eligible telecommunications carriers (“ETCs”), among other things, to protect the confidentiality of “all documentation submitted by a consumer or collected by an ETC to determine a customer’s eligibility for Lifeline service, as well as all personally identifiable information contained therein,” and the Commission indicated that “it expects, that, at a minimum, ETCs must employ the following practices to serve any subscriber information that is stored on a computer connected to a network: firewalls and boundary protections; protective naming conventions; user authentication requirements; and usage restrictions, to protect the confidentiality of consumers’ proprietary information retained for this or allowable purposes.” *Order* ¶¶ 234-235. The Commission also indicated that these obligations apply “at the application stage . . . as well as after the consumer becomes a subscriber.” *Id.* at n.456.

¹⁰ The Commission sought a forfeiture of \$10 million for defendants’ apparent failing, among other things, to implement reasonable data security practices to protect customers’ information. *TerraCom, Inc. and YourTel America, Inc.*, Notice of Apparent Liability, 29 FCC Rcd 13325 (2014) (“*TerraCom/YourTel NAL*”). Despite the absence of evidence of actual consumer harm, the Commission initially used a rigid formula to estimate that a *conservative* forfeiture for TerraCom and YourTel would amount to \$9 billion. *Id.* ¶ 52. Given the choice of proceeding with the *NAL* and risking a forfeiture of \$10 million, or settling the matter, *TerraCom* and *YourTel* ultimately agreed to settle for \$3.5 million.

¹¹ Opposition at 5, *passim*.

Order's confidentiality and data security protection.¹² As a result, this case is unlike *Sprint Nextel Corp. and Clearwire Corp.* cited by the PIOs.¹³ In that case, a petitioner for reconsideration objected solely to the reasoning of a Commission decision. Here, CTIA objects to the substantive and specific confidentiality and data security obligations in the *Order*, representing the Commission's first articulation of those obligations in an order of general applicability. These obligations unquestionably injure CTIA's members.

B. The *Order*'s Confidentiality and Data Security Obligations Constitute "Agency Action" Subject to Reconsideration.

The claim that the data security obligations in the *Order* do not "require" CTIA members to "do anything" and thus do not constitute any agency order, decision, or action is off the mark.¹⁴ The *Order*'s detailed data security obligations belie any such conclusion.¹⁵

The PIOs' assertion that imposition of data security requirements is not an "action" because the Commission "simply remind[ed]" ETCs of their existing obligations is similarly erroneous.¹⁶ The only underlying basis that the Commission cited for purporting to be "remind[ing]" carriers of pre-existing data security obligations is the Commission's non-precedential Notice of Apparent Liability ("NAL") in the *TerraCom* case.¹⁷ An NAL provides only the FCC's "tentative conclusions," and "provides insufficient notice of the FCC's official policy..."¹⁸ Moreover, the Enforcement Bureau settled *TerraCom* before the Commission ever ruled on the defendants' jurisdictional challenges to the FCC's tentative interpretation of

¹² Petition at 3. CTIA does not suggest that providers should retain eligibility documentation without data security protections. As noted above, Lifeline providers are subject to such requirements under other provisions of law.

¹³ See Opposition at 3, 6; *Sprint Nextel Corp. and Clearwire Corp.*, Order on Reconsideration, 27 FCC Rcd 16478 (2012).

¹⁴ Opposition at 6 (citation omitted).

¹⁵ See *supra* Section I.A. & n.9.

¹⁶ Opposition at 7.

¹⁷ See generally *TerraCom/YourTel NAL*.

¹⁸ *CBS Corp. v. FCC*, 663 F.3d 122, 130 (3d Cir. 2011), *cert. denied*, 132 S. Ct. 2677 (2012).

Sections 201(b) and 222(a).¹⁹ Thus, there is no *TerraCom* “precedent” on which the Commission may rely, and the Commission’s imposition of data security obligations in the *Order* must stand on its own and is properly subject to challenge in this proceeding.

The PIOs err in asserting that CTIA is seeking “an opportunity . . . to retroactively petition for reversal of *TerraCom*” because CTIA and its members could not have sought reconsideration of *TerraCom*.²⁰ NALs are not final actions and thus are not subject to reconsideration.²¹ Moreover, there is no basis in the Commission’s rules for non-parties to participate in restricted enforcement proceedings such as *TerraCom*.

The public interest demands that the Commission fully address the jurisdictional challenges raised by CTIA. For the Commission to impose such obligations for the first time in an enforcement settlement that cannot be challenged by anyone, and then rely on the non-reviewable settlement as binding precedent for purposes of a generally applicable rulemaking, would permit the Commission to engage in an “administrative law shell game” to avoid having to address legal challenges to an expansion of its data privacy and security jurisdiction.²² If the Commission believes its assertion of expanded jurisdiction is legally correct, it must lay out its legal reasoning *somewhere* and allow interested parties to challenge it.

C. The Confidentiality and Data Security Obligations Were Subject to APA Notice Requirements.

For the same reasons, the PIOs’ suggestion that the *TerraCom/YourTel NAL* vitiates any need for Administrative Procedure Act (“APA”) notice and comment also fails.²³ As noted

¹⁹ *TerraCom, Inc., and YourTel America, Inc.*, Order and Consent Decree, 30 FCC Rcd 7075 (EB 2015).

²⁰ Opposition at 8.

²¹ See, e.g., *T-Mobile USA, Inc.*, Forfeiture Order, 29 FCC Rcd 10752, 10763 n.79 (2014) (“A Notice of Apparent Liability is not a ‘final Commission action,’ which is a predicate for filing a petition for reconsideration.”).

²² See *AT&T v. FCC*, 978 F.2d 727, 732 (D.C. Cir. 1992).

²³ See Opposition at 7-9.

above, an NAL has no precedential value and is not subject to reconsideration.²⁴ As also discussed above, the Commission should not be permitted to evade review of its assertion of these new obligations through procedural sleight of hand.

Moreover, the suggestion that the *Order* was simply an interpretive ruling²⁵ is belied by the detailed obligations (firewalls and boundary protections, protective naming conventions, user authentication requirements, and usage restrictions) imposed by the Commission.²⁶ The FCC cannot use the interpretive rule exception to the APA notice and comment requirement to “bind[]” ETCs “to a strict and specific set of obligations.”²⁷

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

The PIOs fail to show that Section 222(a) imposes data security obligations on carriers with respect to customer information other than CPNI. The PIOs ignore entirely CTIA’s core argument regarding the difference between “proprietary information,” which Section 222 protects, and “personally identifiable information” and “personal information,” which data privacy and security statutes protect.²⁸ As CTIA explained, Congress typically uses the terms “personal information” or “personally identifiable information” in data privacy and security laws, including privacy laws that amended the Act. In Section 222, however, Congress instead deliberately used the term “proprietary information” because it intended Section 222 to serve a different purpose. Specifically, Section 222 was designed to ensure that incumbent carriers that

²⁴ See *supra* Section II.B.

²⁵ Opposition at 8-9.

²⁶ See *supra* Section I.A. & n.9.

²⁷ *Elec. Privacy Info. Ctr. v. United States Dep’t of Homeland Sec.*, 653 F.3d 1, 7 (D.C. Cir. 2011).

²⁸ Petition at 6-8.

held CPNI, which was available only to carriers and their customers, could not use CPNI for competitive advantage.²⁹

Moreover, the very cases that they cite to support their expansive and incorrect interpretation of Section 222(a) actually undermine their position:

RadLAX Gateway Hotel. The PIOs claim that the bedrock principle of statutory construction – that the “specific governs the general” – does not apply here.³⁰ Therefore, they argue, the statement of general principle regarding customers’ “proprietary information” in Section 222(a) should be read to expand the scope of the specific statutory obligation related to CPNI that is articulated in Section 222(c).³¹ But, as the Petition makes clear, if Section 222(a) imposed obligations with respect to customer information *beyond* CPNI, then the rest of Section 222 would be both incomprehensible and lead to absurd results that defy logic.³² This is *precisely* when the court in *RadLAX Gateway Hotel* stated that a specific statutory provision should supersede a general provision.³³

NCTA. The PIOs cite this case for the proposition that a specific statutory provision does not circumscribe a general provision.³⁴ In this case, the court based its expansive interpretation

²⁹ *Id.*

³⁰ Opposition at 10; *RadLAX Gateway Hotel, LLC v. Amalgamated Bank*, 132 S. Ct. 2065, 2070-71 (2012) (“*RadLax Gateway Hotel*”), citing *Moralas v. Trans World Airlines*, 504 U.S. 374, 384 (1992).

³¹ Opposition at 10.

³² See Petition at 4-6 (demonstrating that Section 222 is coherent and internally consistent *only if* it is read to limit customers’ “proprietary information” to CPNI).

³³ *RadLAX Gateway Hotel, LLC*, 132 S. Ct. at 2072. The PIOs seek to avoid this issue by asserting that Congress “may have” decided that clarifying the statute (and making it internally consistent) was not necessary. Opposition at 12. The PIOs also assert that limiting Section 222(a) to CPNI would lead to “asymmetrical and absurd results” with respect to carriers’ obligations to protect the “proprietary information” of other *carriers*. *Id.* at 11. The PIOs’ reading of the statute is incorrect. To the extent that carriers receive customer information related to customers of *another carrier*, such information is treated as the other carrier’s proprietary information and is governed by Section 222(b), while carriers’ obligations related to customer information from *their own customers* are covered under Section 222(c).

³⁴ *Id.* at 10-11; *Nat’l Cable & Telecomms. Ass’n v. FCC*, 567 F.3d 659 (D.C. Cir. 2009) (“*NCTA*”) (holding that a statute’s general provision designed to promote cable competition by limiting anti-competitive practices should be read expansively and was not curtailed by a more specific provision).

of the law on the statutory language that described the prohibited anti-competitive activities listed as the “*minimum* contents of regulations,” as well as on the statute’s legislative history.³⁵ Not only did the statute itself expressly state that the activities it was meant to circumscribe were not limited to those listed in the statute, but the legislative history also supported this expansive reading.³⁶ The court’s reasoning supports CTIA’s argument that the specific language of Section 222(c) limits the scope of customer information in Section 222(a) to CPNI.³⁷ Thus, based on the rules of statutory construction that the court applied in *NCTA*, Congress evidenced a clear intent to limit the scope of Section 222 to CPNI.³⁸

IV. THE PIOS’ ARGUMENTS SUPPORTING THE COMMISSION’S ASSERTION OF UNPRECEDENTED AUTHORITY UNDER SECTION 201(b) ARE UNPERSUASIVE.

Citing *Wyndham*, the PIOS argue that Congress’s enactment of Section 222 to regulate carriers’ data security practices does not preclude a finding that the previously-enacted Section 201(b) also authorizes the Commission to regulate the security of customers’ “proprietary information.”³⁹ The PIOS base their argument on the *Wyndham* court’s finding that Congress’s enactment of several statutes giving the Federal Trade Commission (“FTC”) authority to regulate data security long after Congress already had enacted Section 45(a) of the Federal Trade

³⁵ *NCTA*, 567 F.3d at 665 (emphasis added).

³⁶ *Id.*

³⁷ See Petition at 5-6 (noting that when the full Congress passed Section 222, rather than include language that would have broadened the scope of customers’ “proprietary information,” Congress chose instead to pass a bill that *limited* the scope of Section 222 to CPNI).

³⁸ Unable to overcome the evidence to the contrary, the PIOS assert that the legislative history “does not foreclose” the possibility that Section 222(a) covers customer “proprietary information” beyond CPNI. Opposition at 12. But a reading of Section 222(a) that captures customers’ information beyond CPNI would lead to absurd results. See Petition at 4-5. It is precisely in such a case that one must turn to legislative history to divine Congress’s intent, which makes clear that with respect to *customers’* information, Congress intended that Section 222 apply only to CPNI. *United States v. Granderson*, 511 U.S. 39, 47 n.5 (1994) (dismissing an interpretation said to lead to an absurd result); *Public Citizen v. Department of Justice*, 491 U.S. 440,454 (1989) (looking to congressional intent to “lend the term its proper scope” “[w]here the literal reading of a statutory term would compel ‘an odd result’”).

³⁹ Opposition at 14-16 (citing *Wyndham Hotels and Resorts, LLC v. Fed. Trade Comm’n*, No. 14-3514, slip op. at 21 (3d Cir. Aug. 24, 2015) (“*Wyndham*”)).

Commission Act (“FTC Act”) did not preclude the FTC from using Section 45(a) to regulate companies’ data security practices.⁴⁰ The circumstances surrounding the passage of Section 222 are readily distinguished from the statutes cited in *Wyndham*, however.

Unlike in the present case, the plaintiffs in *Wyndham* did not point to any evidence that Congress had passed the Gramm-Leach-Bliley Act and other data security statutes in an effort to give the FTC authority that it did not think the FTC already had under Section 45(a).⁴¹ Here, however, Congress enacted Section 222 precisely because the Act did not otherwise give the Commission authority to regulate the security of certain customer information.⁴²

Moreover, the court in *Wyndham* found that the plaintiffs in that case had received adequate notice that Section 45(a) governed companies’ data security practices. Specifically, because the FTC had long enforced Section 45(a) against companies that had inadequate data security practices, the court held that plaintiffs in *Wyndham* had “fair notice” that Section 45(a) would reach the plaintiffs’ conduct in that case.⁴³ Carriers here, however, did not have adequate notice that the Commission would regulate carriers’ data security practices under Section 201(b). As explained above, the *TerraCom/YourTel NAL* cannot serve as notice of the Commission’s

⁴⁰ The PIOs also cite *Global Crossing Telecom. v. Metrophones Telecom.*, 550 U.S. 45 (2007), to support the Commission’s alleged authority under Section 201(b) to regulate carriers’ data security practices. That case, which held that a carrier violated Section 201(b) when it violated a regulation requiring carriers to reimburse payphone operators for charges associated with long-distance calls, has no bearing here. Critical to the Court’s holding in *Global Crossing* was its finding that the “underlying regulated activity at issue [in that case] resembles activity that . . . communications agencies have long regulated. . . .” *Id.* at 55 (emphasis in original). Here, however, Congress and the Commission long have known that for decades, to provide services, carriers have collected personal information from their customers that is not CPNI, and yet the Commission has *no* history whatsoever of regulating carriers’ data security practices related to customers’ personal information.

⁴¹ See *Wyndham* at 21-23 (discussing legislation passed long after the FTC Act that directed the FTC to promulgate data security regulations, without citing any evidence that Congress had viewed the FTC to otherwise lack such authority under Section 45(a)).

⁴² See Petition at 10-11 (explaining that Congress enacted Section 222 as a “comprehensive *new* framework” to address the security of certain customer information and noting that Members of Congress stated that, without such legislation, certain customer information would not have been protected) (emphasis added).

⁴³ *Wyndham* at 38-40 (stating that “[f]air notice is satisfied here as long as the company can reasonably foresee that a court could construe its conduct as falling within the meaning of the statute”).

“official policy,”⁴⁴ and the Commission cannot overcome its failure to provide proper notice by “reminding” carriers of an obligation under Sections 222(a) and 201(b) that they do not have.⁴⁵

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

Finally, the PIOs argue that the scope of Sections 222(a) and 201(b) is an issue best addressed outside of the scope of the current proceeding.⁴⁶ CTIA agrees, and taking this argument to its logical conclusion, urges the Commission to grant the Petition, vacate its statements imposing data security obligations under Sections 222(a) and 201(b), and consider the data security issues as part of a broader notice and comment rulemaking.⁴⁷ Such a proceeding is not only appropriate, it is required. As CTIA argued in its Petition – an argument that the PIOs fail to address – the Commission’s interpretation of both Section 222 and Section 201(b) departs from longstanding precedent without a reasoned explanation.⁴⁸

VI. CONCLUSION.

For the reasons above and for the reasons stated in the Petition, CTIA requests that the Commission reconsider and vacate the *Order*’s confidentiality and data security obligations under Section 222(a) and 201(b) of the Act to the extent that they impose obligations with respect to customer information other than CPNI.

⁴⁴ See *supra* Section II.B.

⁴⁵ The PIOs also assert that it is “well-established that it is an unjust and unreasonable practice under Section 201(b) to misrepresent business practices.” Opposition at 17. That is different, however, from requiring ETCs to have particular data security safeguards in place. See Petition at 15, n.45.

⁴⁶ Opposition at 19.

⁴⁷ Petition at 12-18.

⁴⁸ See *id.*

Respectfully submitted,

/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, DC 20036
(202) 783-0081

October 19, 2015

CERTIFICATE OF SERVICE

I hereby certify that the foregoing REPLY OF CTIA – THE WIRELESS ASSOCIATION® was served on October 19, 2015, by placing a true and correct copy thereof in U.S. Mail, postage prepaid, addressed to:

Privacy PIOs
c/o Laura M. Moy
New America's Open Technology Institute
1899 L Street, NW, Suite 400
Washington, DC 20036



L. Charles Keller