Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of Lifeline and Link Up Reform and Modernization, Telecommunications Carriers Eligible for Universal Service Support, Connect America Fund	WC Docket Nos. 11–42, 09–197, and 10–90

OPPOSITION TO PETITION FOR PARTIAL RECONSIDERATION

Appalshop
Center for Democracy & Technology
Center for Digital Democracy
Center for Rural Strategies
Consumer Action
Consumer Federation of America
Consumer Watchdog
New America's Open Technology Institute
Public Knowledge
United Church of Christ, OC, Inc.,
World Privacy Forum

Filed October 8, 2015

TABLE OF CONTENTS

Summary 1

Argument 3

I. Lifeline Applicants' Sensitive Information Must Be Protected 3

II. The Petition Fails to Respond to an Agency Action that Can Be Challenged 4

A. CTIA Has Not Suffered Any Injury, Therefore It Lacks Standing to File this Petition 5

B. The Commission's Order Does Not Constitute an "Agency Action" Appealable Under Section 405 6

C. For the Same Reason, CTIA's Notice Arguments Also Fail 7

III. Sections 222(a) and 222(c) Contemplate Distinct, but Related, Obligations to Protect Consumer Privacy 9

A. The Specific Provisions of 222(c) Do Not Eliminate the General Duty Imposed by 222(a) 9

B. The Legislative History of Section 222 Is Consistent With a Reading that Protects Personal Information Other than CPNI 12

IV. Section 201(b) Grants the Commission Authority to Protect Consumers Against Unjust and Unreasonable Data Security Practices 13

A. Section 222 Does Not Limit the FCC's Data Security Authority Under Section 201(b) 14

B. The FCC's Interpretation of Section 201(b) Is Entitled to Deference 16

V. CTIA's Concerns Are Best Addressed Outside the Scope of the Current Proceeding 19

Conclusion 20

Appalshop, Center for Democracy & Technology, Center for Digital Democracy, Center for Rural Strategies, Consumer Action, Consumer Federation of America, Consumer Watchdog, New America's Open Technology Institute, Public Knowledge, United Church of Christ, OC, Inc., and World Privacy Forum (collectively, "Privacy PIOs") hereby file this timely Opposition to CTIA's Petition for Reconsideration.

SUMMARY

In the Commission's 2012 *Lifeline Reform Order*,[1] the Commission properly expressed concern for Lifeline applicants' privacy. That order prohibited Eligible Telecommunications Carriers ("ETCs") from retaining the information that Lifeline applicants submit to determine eligibility for support. The Commission at that time required ETCs to keep records of the type of information used to verify eligibility, and the steps taken by ETCs to verify the accuracy of that information, but prohibited retention of the eligibility documents themselves.[2]

TracFone, along with other ETCs, asked the Commission to reconsider that decision and instead permit ETCs to copy and store digitally this eligibility

---

[1] *See Lifeline and Link Up Reform and Modernization et al.*, WC Docket No. 11-42 et al., Report and Order and Further Notice of Proposed Rulemaking, 27 FCC Rcd 6656 (2012) ("*Lifeline Reform Order*").

[2] *See Lifeline and Link Up Reform and Modernization et al.*, WC Docket No. 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) at ¶¶ 224–25 ("*Order on Reconsideration*").

determination information.[3] TracFone and other ETCs detailed IT and access security measures that can be taken to minimize privacy and security risks.[4]

In the 2015 *Order on Reconsideration*, the Commission granted TracFone's request in part. As part of its analysis and explanation of its decision on reconsideration, the Commission recounted ETCs' commitments to privacy and security. The *Order on Reconsideration* reminded Lifeline providers that their obligation to protect this information in the manner recounted flows not merely from the Commission's authority for the Lifeline program in Section 254, but from Sections 222 and 201(b) as well. The *Order on Reconsideration* also provided guidance on precautions that ETCs might take to fulfill their obligations.

CTIA, on behalf of its members, filed the Petition for Partial Reconsideration ("Petition") at issue here.[5] CTIA stresses that it does not object to the outcome of the *Order on Reconsideration*. It simply objects to the Commission's explanation of the legal authority it would use to enforce the privacy obligations acknowledged by TracFone and other ETCs and recounted in the *Order on Reconsideration*.

As explained below, to the extent CTIA merely objects to the Commission's legal theory and not to substantive action undertaken in the *Order*, CTIA lacks

---

[3] *See* Petition for Reconsideration and Clarification by TracFone Wireless, Inc., WC Docket No. 11-42 et al. (filed Apr. 2, 2012); Supplement to Petition for Reconsideration and Emergency Petition to Require Retention of Program-Based Eligibility Documentation, WC Docket No. 11-42 et al. (filed May 30, 2012).

[4] *See Lifeline Reform Order* at ¶ 232 (citing comments filed by Nexus and Sprint, as well as provided by carriers to the Government Accountability Office).

[5] Petition for Partial Reconsideration by CTIA, WC Docket No. 11-42 et al. (filed Aug. 13, 2015).

standing because it suffers no injury in fact.[6] Even assuming CTIA had standing, the Petition is procedurally flawed because the Commission has not imposed new obligations on CTIA's members. The *Order on Reconsideration* simply explains the existing duties of ETCs to avoid confusion about whether protecting the privacy of Lifeline applicants is mandatory and enforceable, or voluntary and unenforceable.[7]

Even if CTIA could overcome these standing and procedural barriers, the Commission should nevertheless deny the Petition on its merits. There is no support for CTIA's argument that the presence of specific provisions applicable to CPNI in Section 222(c) eliminates the general duty imposed by 222(a). On the contrary, the legislative history of 222 is consistent with a reading that protects personal information other than CPNI. Nor does the existence of Section 222 limit the Commission's data security authority under its 201(b) authority to prohibit unjust and unreasonable practices, a reasonable interpretation of which is that the Commission can prohibit carriers from failing to adopt reasonable measures to protect sensitive customer information.

ARGUMENT

I. Lifeline Applicants' Sensitive Information Must Be Protected

CTIA's Petition rests on the remarkable contention that applicants for and participants in the Lifeline program are entitled to no protection whatsoever when

---

[6] *See Sprint Nextel Corp. and Clearwire Corp., Order on Reconsideration and Terminating Proceeding*, 27 FCC Rcd 16478 (2012) ("*Sprint/Clearwire Recon*").
[7] *See* Technology Transitions, GN Docket No. 13-5, *Report and Order, Order on Reconsideration, and Further Notice of Proposed Rulemaking* (released Aug. 7, 2015) at ¶¶ 187-88 ("*Tech Transitions Order*").

it comes to carriers' handling of personal information. As the Commission explained in its rationale for relying on Sections 222 and 201 of the Communications Act as authority to require protections for such information, it is essential that carriers live up to the assurances they already have made with respect to data security and privacy for the Lifeline program. The information contained in Lifeline eligibility applications must be protected. Lifeline applicants are required to share a range of information about themselves that is both highly sensitive and personally identifiable, such as name, address, date of birth, full or partial Social Security number, and driver's license number. Applicants also must provide information about their income and/or their status in public assistance programs. In the words of the Commission, "some of the data fields . . . constitute particularly sensitive information."[8] Breach of such sensitive information can lead to a host of significant harms to the individuals impacted by such breaches, ranging from financial fraud and identity theft to emotional harm stemming from the revelation of their financial status. Fortunately, the Commission articulated ample grounds for the authority to require that, in the digital era as electronic submission and storage of these records becomes widespread, Lifeline providers take reasonable steps to protect the security of this information.

II. The Petition Fails to Respond to an Agency Action that Can Be Challenged

The Petition is procedurally flawed because it does not respond to an agency action that can be challenged. CTIA challenges the Commission's assertion of its

[8] *Lifeline Reform Order* at ¶ 207; *Order on Reconsideration* at ¶ 19.

authority under Sections 201(b) and 222(a), as well as the Commission's reminder that it has relied on this authority to require providers to adopt measures to protect the security and privacy of Lifeline eligibility applications. But neither the Commission's assertion of its authority, nor its reminder of the precedential effect of data security duties it has enforced in adjudicatory actions that fall outside the context of notice-and-comment rulemaking, amounts to an agency action in a rulemaking proceeding that could be subject to a viable petition for reconsideration.

A. CTIA Has Not Suffered Any Injury, Therefore It Lacks Standing to File this Petition

CTIA "seeks reconsideration solely with respect to the scope of the Commission's authority under [Sections 201(b) and 222(a)] 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."[9] Indeed, CTIA does not challenge any substantial portion of the *Order on Reconsideration*. On the contrary, CTIA accepts without objection the obligations laid out by the *Order on Reconsideration*.[10]

As the Commission has elsewhere explained, a party that does not object to the outcome of a proceeding but merely objects to the underlying rationale, does not suffer an injury in fact and is therefore not "aggrieved" within the meaning of Section 405.[11] In the *Sprint/Clearwire Recon Order*, the Commission found that the

---

[9] Petition at 1–2.
[10] *See id.*
[11] 47 U.S.C. §405(a).

Public Interest Spectrum Coalition (PISC) could not meet the statutory standing under Section 405 because it did not object to the Commission's decision to approve the merger, but because of it objected to the related Commission decision to modify the spectrum screen.[12] CTIA does not object to the basic duty imposed by the Commission, and its concerns about possible future enforcement cannot give rise to Section 405 standing.[13]

B. The Commission's Order Does Not Constitute an "Agency Action" Appealable Under Section 405

Even if CTIA were a "party aggrieved" within the meaning of Section 405, CTIA does not seek reconsideration of any agency "order, decision, report, or action" as required by Section 405. As CTIA makes clear in its Petition for *Partial* Reconsideration (emphasis added), CTIA does not object to the Commission's *Order on Reconsideration*. Rather, CTIA takes umbrage at what it considers the Commission's overly expansive view of Section 222 and Section 201(b). To the extent this would constitute a Commission "action," this action lies in the comfortably far off and hypothetical future.

CTIA therefore does not face a situation where the challenged statements "require [its members] to do anything, nor does it expose them to additional penalties in a future enforcement proceeding, or impact their ability" to participate

---

[12] *Sprint/Clearwire Recon,* 27 FCC Rcd at 16480-81.

[13] *See id. See also Clapper v. Amnesty International USA*, 132 S. Ct. 2431 (2012) (plaintiff's decision to incur expenses to avoid hypothetical phone monitoring does not give rise to injury in fact).

in the program.[14] The challenged text simply "remind[s]" ETCs that the Commission has *already* interpreted these statutory provisions as imposing an enforceable duty on ETCs and "[a]ccordingly, we expect ETCs to live up to their assurances." As clarification of *which* assurances, the *Order* recites a set of expectations based on the record.[15]

Each of these statements is a recitation of existing duties, followed by a warning as to the scope of these duties moving forward. These paragraphs do not constitute an agency action subject to review. Agency statements "that merely warn regulated entities are not considered to be final agency actions, as they do not 'determin[e] rights or obligations' nor do 'legal consequences flow' from them."[16] The fact that CTIA disputes that Section 222 and Section 201(b) are the legal source of these duties does not convert a reminder into a rulemaking—especially where, as here, CTIA explicitly acknowledges that it has a duty (presumably under some other source of statutory authority more to CTIA's liking).

C. For the Same Reason, CTIA's Notice Arguments Also Fail

To the extent the Commission took any action to expand its jurisdiction, as CTIA contends, that action took place in context of the *TerraCom, Inc. and YourTel*

---

[14] *Nat'l Ass'n of Home Builders v. U.S. E.P.A.*, 956 F. Supp. 2d 198, 212 (D.D.C. 2013) *aff'd sub nom. Nat'l Ass'n of Home Builders v. E.P.A.*, 786 F.3d 34 (D.C. Cir. 2015) (assertion by EPA that Santa Cruz River constituted navigable water not subject to challenge as agency action and did not create Article III standing, even if it made it more likely that members of association would need to apply for Clean Water Act permits in the future).

[15] *Order on Reconsideration* at ¶¶ 234–235.

[16] *Nat'l Ass'n of Home Builders*, 956 F. Supp. 2d at 212 (quoting *Holistic Candlers*, 664 F.3d 940, 945 (D.C. Cir. 2012)).

America, Inc. enforcement.[17] That CTIA does not like the outcome or the implications of *TerraCom* does not transform a mere reminder of the Commission's previous determination into an independent rulemaking subject to challenge. Nor does the Commission restating the duties it identified in *TerraCom* transform this proceeding into an opportunity for CTIA to retroactively petition for reversal of *TerraCom*.[18]

To the extent anything the Commission did in the *Order on Reconsideration* at issue here constitutes an agency action, it would clearly be an interpretive ruling and not subject to notice and comment requirement.[19] As the Commission recently noted, an interpretive ruling will not require notice and comment unless it contradicts previous Commission determinations.[20] Although CTIA attempts to characterize the language in the *Order* as a "radical departure," its actual complaint is that the *Order* precisely follows the Commission's previous determination in *TerraCom*. Accordingly, even if CTIA had suffered a cognizable injury, and even if the FCC's recitation of its pre-existing determination could

---

[17] *TerraCom, Inc. and YourTel America, Inc.,* Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325 (2014). CTIA's argument that it lacked "constructive notice" because *TerraCom* remained unresolved is meritless and only serves to illustrate that CTIA's Petition has nothing to do with this proceeding and everything to do with its efforts to challenge the Commission's holding in *TerraCom*.

[18] Even if CTIA could somehow transform this proceeding into an opportunity to challenge the *TerraCom NAL*, its notice arguments would be without merit. "The fact that an order rendered in an adjudication may affect agency policy and have general prospective application, does not make it rulemaking subject to APA section 553 notice and comment." *Conference Group, LLC v. FCC*, 720 F.3d 420, 428-29 (D.C. Cir. 2013).

[19] *See Perez v. Mortgage Bankers Ass'n*, 135 S. Ct. 1199 (2015).

[20] *Tech Transitions Order* at ¶¶ 192-95.

constitute an "agency action," the action would constitute an interpretive rule thus expressly exempted from the notice requirement of the APA.[21]

III. Sections 222(a) and 222(c) Contemplate Distinct, but Related, Obligations to Protect Consumer Privacy

The Petition proposes an interpretation of Section 222 under which Section 222(a) has no independent operative meaning and, therefore, carriers have no obligation under the statute to take any steps to protect sensitive personal information submitted by Lifeline applicants or customers. Both the text of Section 222 and its legislative history are inconsistent with such a cramped reading of the statute.

A. The Specific Provisions of 222(c) Do Not Eliminate the General Duty Imposed by 222(a)

CTIA is correct that Section 222(a)'s instruction to protect the proprietary information of carriers, equipment manufacturers, and customers is less specific than Section 222(c)'s provisions regarding the privacy of customer proprietary network information ("CPNI"). But the broader wording of Section 222(a) does not mean the provision is without "force and effect" with respect to customers'

---

[21] CTIA's argument that it could not have had notice that the FCC would rely on *TerraCom* is not merely irrelevant, it borders on the frivolous. CTIA had clear knowledge of the *TerraCom* decision, *see* Comments of CTIA, In the Matter of Guide to Cyber Threat Information Sharing (Draft), NIST Special Publication 800-150 (Draft) (Nov. 28, 2014), a*vailable at* http://www.ctia.org/docs/default-source/fcc-filings/ctia-comments-on-nist-800-150.pdf?sfvrsn=0 and CTIA knew that the entire subject of the TracFone Petition for Reconsideration was the duty and ability of ETCs to protect the privacy of information submitted by Lifeline applicants.

personal information other than that specified in Section 222(c).[22] General provisions should not be read to supersede specific ones where the two contradict. But where they do not, "effect shall be given to every clause and part of a statute."[23] Here, that result is accomplished by reading 222(a) to govern customer proprietary information other than CPNI, rather than reading 222(a) out of the statute entirely.

The Commission's approach to construing 222(a) is similar to that of its approach to construing Section 628 of the Act to reach exclusive inside wiring contracts between cable operators and multiple dwelling units. As in the Petition here, petitioners challenged the Commission's authority to ban such arrangements under 628(b)'s general prohibition against unfair methods of competition because the specific regulations required under Section 628(c)(1) dealt only with satellite broadcast programming.[24] Petitioners in that proceeding also cited the structure of the statute, which contains specific regulations and remedies, and legislative history that, in their view, reflected the limited intent of the statute.

These arguments did not persuade the D.C Circuit. The court noted that if Congress intended to limit 628 to satellite broadcast programming, the broad language of 628(b) was a peculiar way to effectuate that limitation.[25] Similarly, the court found that the structure of 628 showed that "Congress had a particular manifestation of a problem in mind, but in no way expressed an unambiguous intent to limit the Commission's power solely to that version of the problem."[26] The

---

[22] Petition at 4.
[23] *RadLAX Gateway Hotel, LLC v. Amalgamated Bank*, 132 S. Ct. 2065, 2070-72 (2012) (quoting *D. Ginsberg & Sons, Inc. v. Popkin*, 285 U.S. 204, 208 (1932)).
[24] *Nat'l Cable & Telecomms. Ass'n v. FCC*, 567 F.3d 659, 663 (D.C. Cir. 2009).
[25] *Id*. at 664.
[26] *Id*. at 665.

legislative history likewise evinced no clear intent to limit the statute to the specific problem of satellite programming, the statements of individual legislators notwithstanding.[27]

Here, too, the general obligation to protect the confidentiality in Section 222(a) is not mere decoration for the specific obligations provided elsewhere in the statute. Indeed, beyond the general duty of 222(a), Section 222 does not even have a specific provision regarding the proprietary information of equipment manufacturers.[28] While Section 222(c) may reflect a "particular manifestation" of privacy protection Congress had in mind, it does not leave the sensitive personal information of customers and prospective customers wholly unprotected. Such a reading would lead to asymmetrical and absurd results. For example, a carrier that received the personal information of a rival carrier's customers in the course of providing telecommunications services could not use that information for any other purpose but would have no parallel restriction—or, for that matter, any obligation—to protect the confidentiality of proprietary information it received

---

[27] *See id*. (noting that the legislative history was not one-sided and that "[e]ven if legislative history could carry petitioners all the way from statutory language that literally authorized the Commission's action to the proposition that the statute unambiguously forecloses the agency's view, *this* legislative history cannot").

[28] CTIA attempts to cover equipment manufacturers by citing Section 273(d)(2). Petition at 4 n.8. However, that provision prohibits "[a]ny entity which established standards for telecommunications equipment or customer premises equipment, or generic network requirements for such equipment, or certifies telecommunications equipment or customer premises equipment" from releasing or using proprietary information for unauthorized purposes. This is not a carrier-specific obligation and if it represented the sum total of a carrier's obligations with respect to equipment manufacturers, a carrier not involved in standards setting or certification would have no obligation whatsoever to protect the confidentiality of an equipment manufacturer's proprietary information.

from its own customers.[29] Nothing in the text or legislative history of Section 222 suggests Congress intended such a result.

Nor does the absence of references to subsection (a) in other subsections of the statute that permit the sharing of information under certain circumstances imply that Section 222(a) has no meaning apart from CPNI. For example, a carve-out for Section 222(a) from Section 222(e)'s provision on sharing subscriber information is not necessary and possibly confusing. Subscriber information is defined as information that has *already been published*.[30] Given that the subscriber list information is already public, Congress may have very reasonably determined that an express carve-out for Section 222(a) was not required.

B. The Legislative History of Section 222 Is Consistent With a Reading that Protects Personal Information Other than CPNI

The legislative history does not foreclose an interpretation of Section 222(a) that includes, but is not limited to, CPNI and requires basic protections for customers' personal information. Congress may have looked to Section 222 to "balance both competitive and consumer privacy interests with respect to CPNI,"[31] but this does not mean that Congress threw consumer privacy interests with respect to other personal information out the window. Congress may have been signaling that the balance between competition and privacy interests may be different or even less appropriate when it comes to certain sensitive personal information other than CPNI.

---

[29] *See* 47 U.S.C § 222(b).
[30] 47 U.S.C § 222(f)(3)(B).
[31] *See* Petition at 6 (quoting H.R. Rep. No. 104-458, at 205 (1996)).

In any event, Congress certainly did not characterize 222(a) as window dressing. According to the Conference Report, the subsection "stipulates that it is the duty of every telecommunications carrier to protect the confidentiality of proprietary information of and relating to other carriers, equipment manufacturers and customers."[32] Regardless of the words used to describe similar duties in other statutes, it did not use language in Section 222(a) suggesting that the duty was optional or limited to CPNI. CTIA's attempt to rely on prior drafts of the legislation as evidence of this intent is likewise unpersuasive.[33] As a general matter, "attempting to divine legislative intent on the basis of 'Congress's unexplained modification of language in earlier drafts of legislation' can be problematic."[34] Here, where the conference report of the legislation that actually was enacted speaks directly to the duty contemplated by 222(a), resort to earlier committee reports is unnecessary.

IV. Section 201(b) Grants the Commission Authority to Protect Consumers Against Unjust and Unreasonable Data Security Practices

The *Order on Reconsideration* echoes *TerraCom*'s entirely reasonable interpretation of Section 201 to require minimal data security practices. CTIA seeks to muddy that interpretation by arguing that Section 201(b) "neither imposes" a requirement related to document retention security practices "nor gives the

---

[32] H.R. Rep. No. 104-458 at 205.
[33] *See* Petition at 6 & n.13 (discussing the text of House and Senate bills that did not appear in the enacted legislation).
[34] *In re First Merchs. Acceptance Corp.*, 198 F.3d 394, 401 (3d Cir. 1999) (quoting *Appalachian Power Co. v. EPA*, 135 F.3d 791, 810 (D.C. Cir. 1998)).

Commission authority to impose such a requirement."[35] In CTIA's view, the existence of Section 222 negates the Commission's authority to interpret Section 201(b) to require reasonable data security measures. CTIA also argues that the Commission's interpretation of Section 201(b) to require carriers to implement minimal data security that they already claim to have implemented was unreasonable. Neither argument requires nor justifies disturbing the Commission's interpretation of Section 201.

A. Section 222 Does Not Limit the FCC's Data Security Authority Under Section 201(b)

CTIA points to no persuasive evidence that by enacting Section 222 or the 1996 Telecommunications of Act generally, Congress was either amending or interpreting Section 201 to be wholly irrelevant to the privacy or security of consumers' personal information. The arguments here closely resemble those brought in Wyndham Hotels and Resorts, LLC's challenge of the Federal Trade Commission's authority under Section 5 to require business entities to adopt reasonable security measures. In that case, Wyndham argued that, in the words of the Court, "d § 45(a) as initially enacted, three legislative acts since the subsection was amended in 1938 have reshaped the provision's meaning to exclude cybersecurity."[36] Because the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, and the Children's Online Privacy Protection Act were all passed after the FTC's Section 5 authority was established and all include data security provisions,

---

[35] Petition at 11.

[36] *Wyndham Hotels and Resorts, LLC v. Fed. Trade Comm'n*, No. 14-3514, slip op. at 21, (3d Cir. Aug. 24, 2015).

Wyndham contended that these "tailored grants of substantive authority to the FTC in the cybersecurity field would be inexplicable if the Commission already had general substantive authority over this field."[37]

The Third Circuit Court of Appeals rejected this theory. The court explained that the Fair Credit Reporting Act and Gramm-Leach-Bliley Act both required (rather than merely authorizing, as the FTC's Section 5 authority would do) the FTC to create cybersecurity regulations to apply to particular contexts.[38] In addition, the Gramm-Leach-Bliley Act relieved some of the requirements for declaring acts unfair under Section 5, and the Children's Online Privacy Protection Act relieved some of the requirements that normally apply to FTC rulemakings.[39] Therefore, "none of the recent legislation was 'inexplicable' if the FTC already had some authority to regulate corporate cybersecurity through § 45(a)."[40]

The same reasoning should prevail here. Like the Fair Credit Reporting Act and Gramm-Leach-Bliley Act, Section 222 creates a *statutory obligation* that carriers protect certain categories of information. The creation of particular statutory obligations, however, does not limit the Commission's authority to enforce other data security practices necessary to ensure that "charges, practices, classifications, and regulations for and in connection with such communication service, shall be just and reasonable" under Section 201(b)—a provision that Congress designed and has consistently intended to be flexible.

---

[37] *See id.* at 22.
[38] *Id.* at 23.
[39] *Id.*
[40] *Id.*

B. The FCC's Interpretation of Section 201(b) Is Entitled to Deference

The Commission has used its Section 201(b) authority to require telecommunications carriers to follow minimum data security practices if they want to participate in a federally subsidized program to help low-income Americans access telecommunications services. That interpretation is reasonable and entitled to deference.[41] Section 201(b) of the Communications Act delegates to the Commission the authority to define what constitutes "just and reasonable" practices, and what, conversely, is "unjust and unreasonable."

The FCC has relied on Section 201(b), *inter alia*, to require carriers to compensate payphone operators for completed calls,[42] to prohibit unjust and unreasonable telemarketing practices,[43] and to cap rates for inmate calling services in correctional facilities.[44] Courts, as well, have recognized that Section 201(b) is broad and flexible grant of authority.[45] As the Supreme Court has noted, the fact that Congress amended the Communications Act but left 201(b) intact over the

---

[41] *See generally Chevron v. Natural Resources Defense Council*, 467 U.S. 837 (1984); *City of Arlington, Tex. v. FCC*, 133 S. Ct. 1863 (2013).

[42] 2003 Payphone Order, 18 FCC Rcd 19975; *see Global Crossing Telecom. v. Metrophones*, 127 S. Ct. 1513 (2007).

[43] *Business Discount Plan*, https://transition.fcc.gov/eb/Orders/fcc00239.html

[44] Rates for Interstate Inmate Calling Services, *Report and Order and Further Notice of Proposed Rulemaking*, WC Docket No. 12-375, FCC 13-113 (rel. Sept. 26, 2013).

[45] *Global Crossing Telecom. v. Metrophones Telecom.*, 550 U.S. 45, 57 (2007) (explaining that Congress' decision to leave Section 201(b) intact even while radically changing the regulatory environment through other statutory changes suggests that Congress intended the Commission to interpret 201(b) flexibly).

years "indicates that the statute permits, indeed it suggests that Congress likely expected, the FCC to pour new substantive wine into its old regulatory bottles."[46]

Given the sensitivity of personal information and the likelihood of harm that could result from a data breach, it would be unjust and unreasonable for ETCs to fail to adopt basic security measures to protect consumers' personal information. The Commission's declaration to that effect is wholly reasonable. The Commission has relied on that declaration only when taking action in the most egregious of cases, where carriers failed to adopt even the most basic data security protections to protect consumers' personal information, there was an unreasonable risk of unauthorized access to that information, and the information was of such sensitivity that misuse of it could lead to great harm of the consumers in question.[47]

In addition, it is well established that it is an unjust and unreasonable practice under Section 201(b) to misrepresent business practices, especially in circumstances where consumers are likely to rely on the misrepresentation to their detriment. For example, in 1998 the Commission found that Business Discount Plan "violated section 201(b) of the Act by using unjust and unreasonable telemarketing practices in connection with its slamming violations, such as misrepresenting the nature of BDP's service offering."[48]

This approach is also consistent with parallel provisions in other statutes interpreted by other agencies—specifically, Section 5 of the Federal Trade Commission Act, which declares unlawful "unfair or deceptive acts or practices in

---

[46] *Id.*

[47] *YourTel & TerraCom* at ¶¶ 31–35.

[48] *Business Discount Plan, Inc.* 14 FCC Rcd 340 (rel. Dec. 17, 1998).

or affecting commerce."[49] The agencies have long noted the similar purpose, function, and application of the two provisions, particularly when it comes to businesses' own representations regarding their practices.[50] On the issue of data security more broadly, the FTC has relied on its Section 5 authority to state that "a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities."[51]

At the minimum, Section 201 requires carriers to have *some* basic data security practices in place, particularly when they have already stated that they do. Even if CTIA is procedurally allowed to challenge that unremarkable observation, it easily withstands that challenge.

---

[49] 15 U.S.C. § 45. The FTC has broad authority to enforce Section 5 under a range of entities that operate in commerce; however, due to a statutory exception, this authority does not extend to entities designated as common carriers under Title II of the Communications Act.

[50] For example, in 2000, in a Joint Policy Statement on truthful advertising, the FTC and FCC declared, "Principles of truth-in-advertising law developed by the FTC under Section 5 of the FTC Act provide helpful guidance to carriers regarding how to comply with section 201(b) of the Communications Act in this context." *Joint FCC/FTC Policy Statement for the Advertising of Dial-Around and Other Long-Distance Services to Consumers*, 15 FCC Rcd 8654, 8655 (rel. Mar. 1, 2000).

[51] FTC, *Commission Statement Marking the FTC's 50th Data Security Settlement* 1 (Jan. 31, 2014), https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

V. CTIA's Concerns Are Best Addressed Outside the Scope of the Current Proceeding

To the extent that CTIA wishes to challenge or otherwise debate the outlines of its Section 222 obligations, that is best done in a separate proceeding. The depth and sensitivity of personal information involved in the provision of Lifeline raise unique challenges, and the Commission's statements have been appropriately cabined to the proceeding at hand. CTIA's concerns, however, address substantially broader issues of carrier obligations in a Title II regulatory landscape. As a result, they should be filed outside of the current proceeding. This proceeding concerns only the reminder of a limited set of data security requirements relevant to Lifeline ETC's. Moreover, there is every possibility that those obligations will be modified once the Commission decides the larger issues driving the *Lifeline* proceeding and currently subject to the *Second Further Notice of Proposed Rulemaking*. That proceeding will examine transferring eligibility verification duties to a third party other than the ETCs and the possibility of coordinated enrollment with other federal assistance program. Privacy PIOs would welcome the Commission opening a proceeding to fully explore emerging issues with Section 222 consumer privacy protections, particularly their application to broadband Internet access service. But this is not that proceeding.

CONCLUSION

For the foregoing reasons, the Petition should be denied.

Respectfully submitted,

Appalshop
Center for Democracy & Technology
Center for Digital Democracy
Center for Rural Strategies
Consumer Action
Consumer Federation of America
Consumer Watchdog
New America's Open Technology Institute
Public Knowledge
United Church of Christ, OC, Inc.,
World Privacy Forum

By:

/s/

Laura M. Moy
New America's Open Technology Institute
Washington, DC 20036
(202) 596-3346

Filed: October 8, 2015