**DISSENTING STATEMENT OF COMMISSIONER MICHAEL O'RIELLY**

Re: TerraCom, Inc. and YourTel America, Inc., Apparent Liability for Forfeiture, File No.: EB-TCD-13-00009175

Companies that collect personal information about their customers have a responsibility to take reasonable measures to protect that information. Most companies take that obligation extremely seriously because it's in their best interests. So I was disturbed to learn that YourTel and TerraCom had allowed sensitive information about their universal service Lifeline subscribers to be stored in such a way that it could be accessed over the Internet through simple queries. I am also troubled that the companies did not appear to do anything to monitor the activities of their vendor to ensure that it was taking all necessary steps to protect this information. This is unacceptable for many reasons.

As unfortunate as this case may be, however, I find major flaws with the item proposed. First, I'm not convinced that the FCC has authority to act. In my previous employment, I worked extensively on privacy matters, and I am familiar with privacy laws across federal agencies. I also was there for the creation of section 222 of the Act, and it is my firm belief that it was never intended to address the security of data on the Internet. I also do not believe that section 201(b) covers this conduct. Second, even if the FCC did have authority to act, I am not persuaded that it is appropriate for the agency to proceed, in this first instance, through an enforcement action because the agency has not provided fair notice that there could be liability for such conduct. The Commission should have sought comment on these issues to determine the authority for and scope of any data security rules for common carriers. Therefore, I must respectfully dissent from this Notice of Apparent Liability for Forfeiture.

I am noticing a disturbing trend at the Commission where, in the absence of clear statutory authority, the Commission suddenly imbues an innocuous provision of the Act with tremendous significance in order to meet its policy outcome. Section 706 was one such example. Today it's section 222(a).

Section 222(a), however, cannot be interpreted in a vacuum. There is a history here, and it is worth retelling because it is relevant not only to the Commission's authority to act, but also to whether parties would have fair notice of what conduct is barred by the provision.

Those that have been following common carrier law long enough will recall that CPNI rules pre-date the Telecommunications Act of 1996. In the *Computer II*, *Computer III*, *GTE ONA*, and *BOC CPE Relief* proceedings, the Commission established rules concerning the use of CPNI in the enhanced services operations of AT&T, the BOCs, and GTE, and the CPE operations of AT&T and the BOCs. The Commission adopted these rules (along with other nonstructural safeguards) because the Commission was concerned that the carriers could use CPNI obtained from their provision of regulated services to gain an anticompetitive advantage in the unregulated CPE and enhanced services markets.[1] It also determined that the CPNI requirements were necessary to protect legitimate customer expectations of confidentiality regarding individually identifiable information.[2]

With this history in mind, and with the further understanding that one of the goals of the 1996 Act was to open local markets to competition from new telecommunications carriers, the structure and purpose of section 222 becomes evident.

Section 222(a) begins with a duty on every telecommunications carrier to protect the confidentiality of proprietary information. That is, the purpose of section 222(a) was to extend CPNI

[1] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information,* CC Docket No. 96-115, Notice of Proposed Rulemaking, 11 FCC Rcd 12513, 12515, para. 4 (1996) (*CPNI NPRM*).

[2] *Id*.

rules to *all* telecommunications carriers, not just AT&T, the BOCs, and GTE. This was understood by the Commission at the time it was implementing the 1996 Act.[3] Then, sections 222(b) and (c) go on to codify certain restrictions to address the two concerns that led the Commission to adopt CPNI rules in the first place: to protect other carriers from anticompetitive practices; and to protect the privacy expectations of consumers.

Critically, the general duty in section 222(a) was intended to be read in conjunction with, not separate from, the specific limitations in sections 222(b) and (c). And that is how the Commission viewed the provisions.[4] Namely, section 222(a) sets forth who has the basic duty to protect the proprietary information of other telecommunications carriers, equipment manufacturers, and customers, while sections 222(b) and (c) detail when and how that duty is to be exercised. Section 222(b) requires that carriers may only use proprietary information of other carriers for the purpose of providing telecommunications and may not use it for their own marketing efforts. Section 222(c) specifies under what circumstances the proprietary information of customers (also known as CPNI) may be disclosed.

I do not see persuasive evidence that section 222(a) was intended to confer authority that was independent of the carrier information and CPNI provisions. Indeed, on multiple occasions, the Commission has made statements like "[e]very telecommunications carrier has a general duty pursuant to section 222(a) to protect the confidentiality of CPNI."[5] That is because the Commission viewed them as co-extensive.[6] In fact, it is very telling that the Commission has never before attempted to interpret 222(a) independent of CPNI. What is more, the House Conference Report on the 1996 Act notes, "[i]n

---

[3] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as amended*, CC Docket Nos. 96-115 and 96-149, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, para. 194 (1998) (*CPNI Second Order and FNPRM*) ("We recognize, however, that our new CPNI scheme will impose some additional burdens on carriers, particularly carriers not previously subject to our *Computer III* CPNI requirements. We believe, however, that these requirements are not unduly burdensome. All carriers must expend some resources to protect certain information of their customers. Indeed, section 222(a) specifically imposes a protection duty; '[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunications carries, equipment manufacturers, and customers.'" (quoting 47 U.S.C. §222(a)).

[4] *Id*. paras. 204-207 (reading section 222(a) in conjunction with 222(b) and 222(c)).

[5] *See, e.g.*, *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6931, para. 3 (2007); *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Notice of Proposed Rulemaking, 21 FCC Rcd 1782, 1784, para. 4 (2006) (same); *CPNI Second Order and FNPRM*, 13 FCC Rcd, 8061, para. 208 ("In particular, we seek comment on whether the duty in section 222(a) upon all telecommunications carriers to protect the confidentiality of customers' CPNI, or any other provision, permits and/or requires [the Commission] to prohibit the foreign storage or access to domestic CPNI.").

[6] *See, e.g.*, *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information,* CC Docket No. 96-115, Declaratory Ruling, 28 FCC Rcd 9609, 9617, para. 24 (2013) ("Although it is certainly true that *some* of the information that carriers have collected and stored on mobile devices is not CPNI, it is equally clear that some of it is. In any event, if the information a carrier collects in the future does not meet the statutory definition, then section 222 will not apply. To reiterate, the Commission is clarifying only that information that meets the definition of CPNI is subject to section 222, just as the same information would be subject to section 222 if it were stored elsewhere on a carrier's network.") (internal citations omitted); *see id*. at 9618, para. 27 (section 222(a) helps define where but not what is covered).

general, the new section 222 strives to balance both competitive and consumer privacy interests *with respect to CPNI*."[7]

Moreover, the fact that section 222(a) uses a broader term "proprietary information" is not dispositive in this instance. Separate from my working experiences with this provision, given the three-part structure of section 222, the statute includes a term in 222(a) that encompasses both the carrier information at issue in 222(b) and the customer information at issue in 222(c).

Furthermore, I find the reliance on the section heading in this case as a source of authority just plain laughable. If the Commission can invent new authority based on the "Privacy of Customer Information" heading of section 222, I can only imagine what it could do with the heading of section 215: "Transactions Relating to Services, Equipment, *And So Forth*".[8] I suspect that those in the Commission that are asked to defend the Commission's work would also agree that section headings are of little to no value.

I do not agree that section 201(b), which dates even further back to 1934, can be read to cover data protection, and I strongly disagree with the assertion in footnote 79 that the Commission has authority to enforce unlawful practices related to cybersecurity. Moreover, if data protection falls within the ambit of 201(b), then I can only imagine what else might be a practice "in connection with" a communications service. What is the limiting principle? Perhaps recognizing that it is on shaky legal ground, the NAL at least declines to propose a forfeiture for the failure to employ just or reasonable data security practices or to notify all consumers affected by the breach.

Yet even if the Commission did have authority under section 222(a) and/or section 201(b), and I do not believe that it does, I would still have serious concerns that the Commission did not provide fair notice that the companies could be liable under those sections for this conduct. In other words, it appears the Commission is short circuiting the procedural requirements of law.

I acknowledge that the Commission has asserted in the past that it may announce new interpretations or policies in the context of an adjudication. However, "[a] fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required."[9] Accordingly, "[a] conviction or punishment fails to comply with due process if the statute or regulation under which it is obtained 'fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement.'"[10] Moreover, "[i]n the absence of notice—for example, where the regulation is not sufficiently clear to warn a party about what is expected of it—an agency may not deprive a party of property by imposing civil or criminal liability."[11]

As the FCC itself has explained, "fair notice of the obligation being imposed on a regulatee" means that "'by reviewing the regulations and other public statements issued by the agency a regulated party acting in good faith would be able to identify, with ascertainable certainty, the standards with which the agency expects parties to conform before imposing civil liability.'"[12] However, there are no regulations *at all* on section 222(a), and I am not aware of any statements that say or even hint that 222(a)

---

[7] H.R. REP. NO. 104-458, at 205 (1996) (CONF. REP.) (emphasis added).

[8] 47 U.S.C. § 215 (emphasis added).

[9] *F.C.C. v. Fox Television Stations, Inc*., 132 S.Ct. 2307, 2317 (2012) (citing *Connally v. General Constr. Co.,* 269 U.S. 385, 391 (1926)).

[10] *Id*. (quoting *United States v. Williams*, 553 U.S. 285, 304 (2008)).

[11] *Trinity Broadcasting of Florida, Inc., v. FCC*, 211 F.3d 618, 628 (D.C. Cir. 2000) (quoting *General Elec. Co. v. EPA,* 53 F.3d 1324, 1328-29 (D.C. Cir. 1995)).

[12] *Infinity Broadcasting Corporation of Florida*, File No. EB-04-TP-478, Order on Review, 24 FCC Rcd 4270, 4275, para. 17 (2009) (*quoting Trinity*, 211 F.3d at 628).

and/or 201(b) covers this conduct. If there were, I would have expected them to be cited in this NAL. At most, and this is being more than generous, a very creative practitioner might have been able to imagine a scenario under which misrepresenting data security practices could fall within section 201(b). But that's it. For these reasons, and for the reasons discussed above, I do not think that the companies had fair notice and, therefore, the Commission should not propose a forfeiture. I would not be surprised to see this issue litigated at some point.

In fact, a series of agency actions (and inaction) made it *less likely* that the companies would have had fair notice. In 2007, the Commission sought comment on, among other things, requiring carriers to physically safeguard the security and confidentiality of CPNI.[13] This included questions on whether to adopt rules governing the physical transfer of CPNI among companies or to any other third party authorized to access or maintain CPNI, including a carrier's joint venture partners and independent contractors. Since the Commission included reference to this proceeding in the NAL, it certainly knows that it never acted on that part of the further notice.[14] In fact, commenters generally opposed further requirements and noted that the chief concern was access to CPNI by pretexters over the phone, not hackers seeking to gain unlawful access to carriers' CPNI databases.[15] So the issue appeared to have died. Moreover, when the Commission did act on another part of the 2007 further notice regarding data on mobile devices, it did so only after the relevant Bureaus sought further comment to refresh the record, including on whether the Commission should act by declaratory ruling, which it ultimately did. Therefore, it would have been reasonable for a regulated entity acting in good faith to believe that, at most, the Commission might act on physical safeguards, but only with respect to CPNI, and only after seeking further comment.

In sum, while I am troubled that sensitive information about Lifeline subscribers was exposed to the public, I cannot support an NAL that exceeds our authority and comes without fair notice to the companies involved. I respectfully dissent.

---

[13] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6961, para. 70 (2007).

[14] While the Commission has previously pursued enforcement actions despite having open rulemaking proceedings, I am concerned that open proceedings may provide companies with a false sense of security. This makes it all the more important that the Commission close open rulemaking proceedings by a date certain or as soon as it determines that it will not act on the open issues.

[15] *See, e.g.*, Comments of Verizon, CC Docket No. 96-115, WC Docket No. 04-36, at 15-17 (filed July 9, 2007); Comments of the Rural Cellular Association, CC Docket No. 96-115, WC Docket No. 04-36, at 4-5 (filed July 9, 2007); Comments of the National Cable & Telecommunications Association, CC Docket No. 96-115, WC Docket No. 04-36, at 2 (filed July 9, 2007); Comments of COMPTEL, CC Docket No. 96-115, WC Docket No. 04-36, at 2-3 (filed July 9, 2007); *but see* Consumer Coalition Comments, CC Docket No. 96-115, WC Docket No. 04-36, at 9-12 (filed July 9, 2007) (requesting that the FCC require carriers to encrypt stored CPNI and limit employee access to CPNI).