**Before the**
**Federal Communications Commission**
**Washington, D.C. 20554**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Verizon Communications | ) | File No.: EB-TCD-18-00027698 |
| | ) | NAL/Acct. No.: 202032170006 |
| | ) | FRN: 0003257094 |

**FORFEITURE ORDER**

**Adopted: April 17, 2024** **Released: April 29, 2024**

By the Commission: Chairwoman Rosenworcel issuing a statement; Commissioners Carr and Simington dissenting and issuing separate statements.

**TABLE OF CONTENTS**

Heading Paragraph #



## I. INTRODUCTION

1. On February 28, 2020, the Commission issued a Notice of Apparent Liability for Forfeiture and Admonishment (*NAL*) against Verizon Communications (Verizon or Company).[1] In the *NAL*, the Commission admonished Verizon for apparently disclosing its customers' location information, without their consent, to a third party who was not authorized to receive it, and proposed to fine Verizon

[1] *Verizon Communications*, Notice of Apparent Liability for Forfeiture and Admonishment, 35 FCC Rcd 1698 (2020) (*NAL*).

$48,318,750 for failing to take reasonable steps to protect its customers' location information. After reviewing the Company's response to the *NAL*,[2] we find no reason to cancel or withdraw the proposed penalty. However, pursuant to additional factual evidence provided in Verizon's NAL Response that is relevant to the forfeiture calculation, we reduce the proposed penalty by $1,417,500, and therefore impose a penalty of $46,901,250 against Verizon.

## II. BACKGROUND

### A. Legal Background

2. As set forth fully in the *NAL*,[3] carriers are required to protect the confidentiality of certain customer data related to the provision of telecommunications service. This includes location information, which is customer proprietary network information (CPNI) pursuant to section 222 of the Communications Act (Act).[4] The Commission has advised carriers that this duty requires them to take "every reasonable precaution" to safeguard their customers' information.[5] Section 222(a) of the Act imposes a general duty on telecommunications carriers to "protect the confidentiality of proprietary information" of "customers."[6] Section 222(c) establishes specific privacy requirements for "customer proprietary network information" or CPNI, namely information relating to the "quantity, technical configuration, type, destination, *location*, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier" and that is "made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[7] The Commission has promulgated regulations implementing section 222 (CPNI Rules), which require, among other things, that carriers employ "reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI."[8]

3. *Customer Consent to Disclose CPNI.* With limited exceptions, a carrier may only use, disclose, or permit access to CPNI with customer approval.[9] Generally, carriers must obtain a customer's "opt-in approval" before disclosing that customer's CPNI.[10] This means that a carrier must obtain the

[2] *Verizon Communications*, Response to Notice of Apparent Liability for Forfeiture and Admonishment (filed May 7, 2020) (on file in EB-TCD-18-00027698) (NAL Response or Response).

[3] *See generally NAL*.

[4] 47 U.S.C. § 222.

[5] *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, 6959, para. 64 (2007) (*2007 CPNI Order*).

[6] 47 U.S.C. § 222(a).

[7] 47 U.S.C. § 222(c), (h)(1)(A) (emphasis added). "Telecommunications service" is defined as "the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used." 47 U.S.C. § 153(53). The mobile voice services provided by Verizon are "telecommunications services." *See* 47 U.S.C. § 332(c)(1); H.R. Conf. Rep. No. 104-458 at 125 (1996) ("This definition [of 'telecommunications service'] is intended to include commercial mobile service.").

[8] *See* 47 CFR § 64.2001 *et seq*.; *id*. § 64.2010(a). The CPNI Rules are a subset of, and are thus included within, the Commission's rules.

[9] 47 U.S.C. § 222(c)(1) ("Except as required by law *or with the approval of the customer*, a telecommunications carrier that receives or obtains [CPNI] by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable [CPNI] in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.") (emphasis added).

[10] 47 CFR § 64.2007(b).

customer's "affirmative, express consent allowing the requested CPNI usage, disclosure, or access after the customer is provided appropriate notification of the carrier's request . . . ."[11]

4. This opt-in requirement has been in place since 2007, when the Commission amended its rules in the *2007 CPNI Order* after finding that once carriers disclosed CPNI to third parties, including joint venturers and independent contractors, that information was out of the control of the carrier and had a higher risk of being improperly disclosed.[12] Accordingly, among other things, this opt-in requirement was meant to allow individual consumers to determine if they wanted to bear the increased risk associated with sharing CPNI with such third parties.[13] In the Commission's view, obtaining a customer's express consent in these circumstances is particularly important, because a carrier cannot simply rectify the harms resulting from a breach by terminating its agreement with such a third party, "nor can the Commission completely alleviate a customer's concerns about the privacy invasion through an enforcement proceeding."[14] The Commission further concluded that contractual safeguards between a carrier and such a third party do not obviate the need for explicit customer consent, as such safeguards do not eliminate the increased risk of unauthorized CPNI disclosures that accompany information that is provided by a carrier to such a third party.[15] Thus, the Commission determined that, with limited exceptions, a carrier may only use, disclose, or permit access to CPNI with the customer's opt-in approval.[16]

5. *Reasonable Measures to Safeguard CPNI.* The Commission has also recognized that an opt-in requirement alone is not enough to protect customer CPNI, especially in light of tactics like "pretexting," where a party pretends to be a particular customer or other authorized person in order to illegally obtain access to that customer's information (thus circumventing opt-in requirements).[17] Therefore, the Commission adopted rules requiring carriers to "take reasonable measures to *discover* and *protect* against attempts to gain unauthorized access to CPNI."[18] To provide some direction on how carriers should protect against tactics like pretexting, the Commission included in its amended rules customer authentication requirements tailored to whether a customer is seeking in-person, online, or over-the-phone access to CPNI.[19] It also adopted password and account notification requirements.[20]

6. The Commission made clear that the specific customer authentication requirements it adopted were "minimum standards" and emphasized the Commission's commitment "to taking resolute enforcement action to ensure that the goals of section 222 [were] achieved."[21] Although carriers are not expected to eliminate every vulnerability to the security of CPNI, they must employ "reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI."[22] They must also take reasonable measures to protect the confidentiality of CPNI—a permanent and ongoing obligation to

---

[11] 47 CFR § 64.2003(k).

[12] *2007 CPNI Order*, 22 FCC Rcd at 6947-53, paras. 37-49. Prior to the *2007 CPNI Order* the Commission's rules had allowed carriers to share CPNI with joint venture partners and independent contractors on an opt-out basis for the purpose of marketing communications-related services to customers. *Id*. at 6931-32, para. 8.

[13] *2007 CPNI Order*, 22 FCC Rcd at 6950, para. 45.

[14] *2007 CPNI Order*, 22 FCC Rcd at 6949, para. 42.

[15] *2007 CPNI Order*, 22 FCC Rcd at 6952, para. 49.

[16] *See* 47 CFR § 64.2007(b).

[17] *See 2007 CPNI Order*, 22 FCC Rcd at 6928, para. 1 & n.1.

[18] 47 CFR § 64.2010(a) (emphasis added).

[19] *See* 47 CFR § 64.2010(b)-(d).

[20] *See* 47 CFR § 64.2010(e)-(f).

[21] *2007 CPNI Order*, 22 FCC Rcd at 6959-60, para. 65.

[22] 47 CFR § 64.2010(a).

police disclosures and ensure proper functioning of security measures.[23] As the Commission stated in the *NAL*, several government entities provide guidance and publish best practices that are intended to help companies evaluate the strength of their information security measures.[24]

7. *Section 217.* Finally, the Act makes clear that carriers cannot disclaim their statutory obligations to protect their customers' CPNI by delegating such obligations to third parties. Section 217 of the Act provides that "the act, omission, or failure of any officer, agent, or other person acting for or employed by any common carrier or user, acting within the scope of his employment, shall in every case be also deemed to be the act, omission, or failure of such carrier or user as well as that of the person."[25]

### B. Factual Background

8. *Customer Location Information and Verizon's Location-Based Services Business Model.* Verizon provides mobile voice and data services to consumers throughout the United States by enabling consumer mobile phones to make and receive calls or transmit data on Verizon's wireless network.[26] As part of its business, Verizon ran a Location-Based Services (LBS) program until March 2019. Through the LBS program, Verizon sold access to its customers' location information to companies known as "location information aggregators," who then resold access to such information to third-party location-based service providers or in some cases to intermediary companies who then resold access to such information to location-based service providers.[27] Verizon had arrangements with two location information aggregators: LocationSmart and Zumigo (the Aggregators). Each Aggregator, in turn, had arrangements with location-based service providers. In total, Verizon sold access to its customers' location information (directly or indirectly) to 67 third-party entities (including the two Aggregators).[28]

9. The Verizon LBS program was largely governed via contractual provisions that vested Verizon with oversight authority over the Aggregators. Verizon entered into contracts with the Aggregators, and the Aggregators then entered into their own contracts with various LBS providers. Verizon asserts that its LBS program was subject to a number of safeguards and that both the LBS providers and Aggregators had to satisfy various requirements, which were memorialized in and governed by contract

---

[23] *See 2007 CPNI Order*, 22 FCC Rcd at 6959, para. 64 ("We fully expect carriers to take every reasonable precaution to protect the confidentiality of proprietary or personal customer information.").

[24] For example, the National Institute of Standards and Technology (NIST) is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems. NIST publishes cybersecurity and privacy frameworks which feature instructive practices and guidelines for organizations to reference. The publications can be useful in determining whether particular cybersecurity or privacy practices are reasonable by comparison. The model practices identified in the NIST and other frameworks, however, are not legally binding rules, and we do not consider them as such here. The Federal Trade Commission (FTC), the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC), and the Cybersecurity & Infrastructure Security Agency (CISA) also offer guidance related to managing data security risks. *See* NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (NIST Cybersecurity Framework); NIST, The NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0 (Jan. 16, 2020), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf; FTC, Start with Security: A Guide for Business, Lessons Learned from FTC Cases (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Communications Security, Reliability and Interoperability Council, CSRIC Best Practices, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data; CISA, Cross-Sector Cybersecurity Performance Goals and Objectives (last visited Aug. 17, 2022), https://www.cisa.gov/cpgs.

[25] 47 U.S.C. § 217.

[26] *See* Verizon Communications, 2021 Annual Report, https://www.verizon.com/about/sites/default/files/2021-Annual-Report-on-Form-10-K.pdf.

[27] The *NAL* includes a more complete discussion of the facts and history of this case and is incorporated herein by reference. *See NAL*, 35 FCC Rcd at 1703-12, paras. 11-38.

[28] *See NAL*, 35 FCC Rcd at 1703-04, paras. 12-13.

provisions with the Aggregators.[29] According to Verizon, these provisions included various information security requirements, including implementing and maintaining multiple types of security controls, preventing unauthorized disclosures of Verizon's data, and compliance with consumer protection and data privacy laws and industry best practices.[30] Beyond these security provisions, which Verizon required the Aggregators to likewise hold the LBS providers to, the Aggregator-LBS provider contracts included provisions obligating the LBS providers to provide Verizon's customers with clear disclosure of the way their location information would be "accessed, used, copied, stored, or disclosed" by the location-based service provider and obtain "affirmative, opt-in consent" from Verizon customers or users "prior to accessing, using, storing or disclosing location information."[31] This arrangement meant that it was typically the LBS providers who were obligated "to provide notice and obtain consent" from consumers—not the Aggregators or Verizon.[32] Verizon had broad authority under its contracts to "terminate its relationship with each Aggregator for any material breach of contract terms, and it could terminate any arrangement that failed to meet Verizon's standards."[33]

10. While Verizon did not have contracts with the LBS providers, each provider was required to submit an application that described, among other things, the "Use Case" or purposes for which it would use the location information, as well as the process it would use for providing notice and obtaining opt-in consent from a Verizon customer for use and sharing of the customer's location information.[34] Verizon claims that it only approved applications for one of six specific types of Use Cases: "'call routing, roadside assistance, proximity marketing, transportation and logistics, fraud mitigation/identity management, and mobile gaming/lottery.'"[35]

11. Verizon's approval process and ongoing monitoring involved a third-party Auditor, Aegis Mobile, LLC (Aegis).[36] According to Verizon, Aegis would "perform background checks on companies seeking access to location information before those companies were allowed to obtain it," and also "validate and reconcile the records of consent events and the records of each access to a subscriber's location on a daily basis."[37] Validation and reconciliation of requests for customer location information with the corresponding record of consumer consent was not always successful in the initial processing of data, and could vary greatly depending on which LBS provider was being checked (e.g., in a five and a half month time period, more than 50% of one LBS provider's transaction could not be reconciled in the first instance).[38] Verizon claimed that this was only the initial step of the consent validation process and that Aegis would follow-up "with the Aggregators or their [LBS] provider customers" and correct "misalignments in the data or performing other data operations," resulting in matching "99.95% of all

[29] *See NAL*, 35 FCC Rcd at 1704-05, paras. 14-16.

[30] *See NAL*, 35 FCC Rcd at 1705, para. 15; NAL Response at 18.

[31] *See NAL*, 35 FCC Rcd at 1705, para. 14 (citing Response to Supplemental Letter of Inquiry from Verizon to Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, at 8, Response to Question 4 (June 5, 2019) (on file in EB-TCD-18-00027698) (Supplemental LOI Response)).

[32] *See NAL*, 35 FCC Rcd at 1704-05, para. 14 (citing Supplemental LOI Response at 8, Response to Question 4).

[33] *NAL*, 35 FCC Rcd at 1705, para. 16 (citations omitted).

[34] *See NAL*, 35 FCC Rcd at 1705-06, para. 17 (citing Response to Letter of Inquiry from Verizon to Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, at 2, Response to Question 1 (Oct. 15, 2018) (on file in EB-TCD-18-00027698) (LOI Response)).

[35] *NAL*, 35 FCC Rcd at 1706, para. 17 (quoting LOI Response at 2, Response to Question 1).

[36] *See NAL*, 35 FCC Rcd at 1706-08, paras. 18-24.

[37] *NAL*, 35 FCC Rcd at 1706, paras. 18 & 19 (citations omitted).

[38] *See NAL*, 35 FCC Rcd at 1707, para. 20 (citing LOI Response at VZ-0000873, Response to Request for Documents No. 6).

records of location requests to the corresponding consent record," followed by a spot-check of the remaining 0.05% records.[39]

12. Verizon also asserted that Aegis's "broader oversight program" had additional components, including looking at trends in data to identify larger areas of concern and using various methods "to ensure that the Aggregators (and their location-based service provider customers) were complying with their contractual obligations."[40] According to Verizon, Aegis "applied fraud analytics techniques to refine its ability to broadly identify potential issues going forward"—but Verizon offered no examples of issues identified and addressed via such data analysis.[41] Verizon also claims that Aegis reviewed LBS providers to make sure they were in compliance with their use case, notice, and consent requirements.[42] In addition, Verizon says it reviewed and/or addressed "'discrete issues as they were raised by Aegis or otherwise.'"[43] For example, Verizon described an investigation into an allegation that a bail bonds company had obtained unauthorized access to Verizon consumers' location data.[44] According to Verizon, the investigation concluded that the company was likely a rejected applicant to its LBS program and that the company was not receiving location information, but that "it is possible for [LBS] program companies with delegated consent to falsify consent records and obtain [Verizon] subscriber data without their consent."[45] As the *NAL* explained, the "report made no recommendations for adopting additional methods to mitigate the risk of approved location-based service providers falsifying consent records to obtain Verizon customer location information without their consent."[46]

13. *Unauthorized Access and Use of Customer Location Information*. On May 10, 2018, the *New York Times* published an article that detailed security breaches involving Verizon's (and other carriers') practice of selling access to customer location information.[47] The *NAL* includes a more detailed summary of the article and its findings, but essentially the breaches involved a location-based service provider (Securus Technologies, Inc., or Securus) that offered a location-finding service to law enforcement and corrections officials that allowed such officials to access customer mobile device location *without* that device owner's knowledge or consent.[48] Not only was Securus's location-finding service outside the scope of its approved "Use Case" or any agreement with either Aggregator (and thus had not been reviewed and approved by Verizon), but despite Securus's claims that the program required appropriate "legal authorization," it did not verify such authorizations and its program was used and abused by a (now former) Missouri Sheriff (Cory Hutcheson) for non-law enforcement purposes and in the absence of any such legal authorization.[49] Securus obtained location services from a company called

[39] *NAL*, 35 FCC Rcd at 1707, para. 21 (citing Declaration of John A. Bruner, Jr., Aegis Mobile, LLC, paras. 5-6 (Feb. 21, 2020) (on file in EB-TCD-18-00027698) (Bruner Decl.)).

[40] *NAL*, 35 FCC Rcd at 1707-08, paras. 22-23 (citing Supplemental LOI Response at 4, 22, Response to Questions 1, 13; Bruner Decl. at para. 7).

[41] *NAL*, 35 FCC Rcd at 1707-08, para. 22.

[42] *See NAL*, 35 FCC Rcd at 1708, para. 23 (citing Supplemental LOI Response at 22, Response to Question 13).

[43] *NAL*, 35 FCC Rcd at 1708, para. 24 (quoting Supplemental LOI Response at 12, Response to Question 5).

[44] *See NAL*, 35 FCC Rcd at 1708, para. 24 (citing Supplemental LOI Response at 13, Response to Question 5).

[45] *NAL*, 35 FCC Rcd at 1708, para. 24 (citations omitted).

[46] *NAL*, 35 FCC Rcd at 1708, para. 24.

[47] *See* Jennifer Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, N.Y. Times (May 10, 2018), https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html.

[48] *See NAL*, 35 FCC Rcd at 1708-09, paras. 25-26 (citing Jennifer Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, N.Y. Times (May 10, 2018) https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html).

[49] *See NAL*, 35 FCC Rcd at 1708-09, paras. 25-26 (citing Jennifer Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, N.Y. Times (May 10, 2018)
(continued….)

3Cinteractive, and 3Cinteractive obtained Verizon consumers' location information pursuant to a contract with the Aggregator LocationSmart.[50] Verizon conceded that its regular audits "did not reveal that Securus was using this data in ways that differed from its approved use case with LocationSmart."[51]

14. The Department of Justice's U.S. Attorney's Office for the Eastern District of Missouri charged Hutcheson with, among other things, wire fraud and illegally possessing and transferring the means of identification of others, and Hutcheson pleaded guilty on November 20, 2018.[52] The Department of Justice's investigation of Hutcheson's actions included an examination of how the Securus location-finding service operated. Once Hutcheson became an authorized user of Securus's LBS software, he was able to obtain the location of specific mobile telephone devices.[53] In order to do so, users (including Hutcheson) were required to input the telephone number of the device they wanted to locate, and then "upload a document manually checking a box, the text of which stated, '[b]y checking this box, I hereby certify the attached document is an official document giving permission to look up the location on this phone number requested.'"[54] As soon as Hutcheson (or any other authorized user) submitted his request and uploaded a document, the Securus LBS platform would *immediately* provide the requested location information (regardless of the adequacy of the uploaded document).[55] Rather than "uploading the required legal process," Hutcheson instead "routinely uploaded false and fraudulent documents . . ., each time representing that the uploaded documents were valid legal process authorizing the location requests the defendant made."[56] Those "false and fraudulent documents" included "his health insurance policy, his auto insurance policy, and pages selected from Sheriff training materials."[57] Hutcheson "submitted thousands of Securus LBS requests and obtained the location data of hundreds of individual phone subscribers without valid legal authorization."[58]

15. *Verizon's Response to the Securus Disclosures*. Verizon directed LocationSmart to terminate Securus's and 3Cinteractive's access to Verizon customer location information on May 11, 2018.[59] Following this termination, Verizon stated that it "undertook a review to better understand how [the Securus and Hutcheson breaches] could occur despite the contractual, auditing, and other protections" in had in place to protect customer location data."[60] Verizon says it determined that its auditing did not identify Securus's unauthorized program because Securus used the profile of its approved

---

https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html; Doyle Murphy, *Ex-Missouri Sheriff Cory Hutcheson Sentenced to 6 Months in Prison*, Riverfront Times (Apr. 29, 2019), https://www.riverfronttimes.com/newsblog/2019/04/29/ex-missouri-sheriff-cory-hutcheson-sentenced-to-6-months-in-prison).

[50] *See NAL*, 35 FCC Rcd at 1709, para 27 (citing Supplemental LOI Response at 15, Response to Question 7).

[51] *NAL*, 35 FCC Rcd at 1709, para. 29 (citing LOI Response at 12, Response to Question 8).

[52] *See* Press Release, U.S. Attorney's Office Eastern District of Missouri, *Mississippi County Sheriff Pleads Guilty to Fraud and Identity Theft, Agrees to Resign* (Nov. 20, 2018), https://www.justice.gov/usao-edmo/pr/mississippi-county-sheriff-pleads-guilty-fraud-and-identity-theft-agrees-resign.

[53] *See* Government's Sentencing Memorandum at 3, *United States v. Corey Hutcheson*, Case No. 1:18-CR-00041 JAR, Doc. No. 65 (E.D. Mo. Apr. 23, 2019) (Hutcheson Sentencing Memo), https://storage.courtlistener.com/recap/gov.uscourts.moed.160663/gov.uscourts.moed.160663.65.0.pdf. ; *see also NAL*, 35 FCC Rcd at 1708-09, paras. 25-26.

[54] Hutcheson Sentencing Memo at 3; *see also NAL*, 35 FCC Rcd at 1708-09, para. 25.

[55] *See* Hutcheson Sentencing Memo at 3-4; *see also NAL*, 35 FCC Rcd at 1708-09, para. 25.

[56] Hutcheson Sentencing Memo at 4; *see also NAL*, 35 FCC Rcd at 1709, para. 26.

[57] Hutcheson Sentencing Memo at 4; *see also NAL*, 35 FCC Rcd at 1709, para. 26.

[58] Hutcheson Sentencing Memo at 4; *see also NAL*, 35 FCC Rcd at 1709, para. 26.

[59] *See NAL*, 35 FCC Rcd at 1709, para. 28 (citing Supplemental LOI Response at 16, Response to Question 7).

[60] *NAL*, 35 FCC Rcd at 1709, para. 29 (citing LOI Response at 12, Response to Question 8).

Use Case, the number of Securus requests appeared normal, and nothing in Securus's background check changed such that the auditor would question Securus's credibility.[61] Verizon also claimed to conduct a broader investigation, which the Company said "did not uncover any new incidents in which a Location Aggregator (or its customer) mispresented that it had customer consent."[62] However, through this investigation Verizon learned of a vulnerability whereby a cybersecurity researcher gained access "to Verizon customer data through LocationSmart's website via a demonstration page for prospective [LocationSmart] customers."[63] Though Verizon claims that the cybersecurity research only attempted location queries for individuals who had consented, it nonetheless suggested "that it was not aware of LocationSmart's use of Verizon customer location information for this purpose before the investigation and state[d] that it 'directed both LocationSmart and Zumigo to not use Verizon customer data in any demonstration site going forward.'"[64]

16. On June 12, 2018, Verizon notified the two Aggregators that it intended to terminate their contracts under the LBS program as soon as possible.[65] However, it was not until November 30, 2018, that Verizon terminated all arrangements with Zumigo, and terminated all but four arrangements with LocationSmart (the four exceptions being arrangements with companies that provided location-based roadside assistance).[66] Per Verizon, during the more than five intervening months it had "(1) stopped authorizing any new uses of location information by the Aggregators or the sharing of such information with any new customers of the Aggregators, and (2) strengthened its transaction verification process to identify anomalies in consent requests that might be indicative of a problem (e.g., multiple location requests in a 24-hour period or an increase in location requests that are out of the ordinary).[67]

17. While Verizon was phasing out its relationships with the Aggregators, it started a "Direct Location Services" program as an alternative, under which Verizon itself would obtain consent from its customers to share their location information with particular LBS providers.[68] Verizon obtained affirmative consent by sending its customer a text message and only sharing location information with an LBS provider if the Verizon customer responded affirmatively to the text message request.[69]

18. Eventually, Verizon completely exited the location-based services business. On April 5, 2019, Verizon announced it would terminate its in-house Direct Location Services program by the end of July 2019.[70] As far as its LBS Aggregator program, Verizon stopped providing LocationSmart and its four remaining LBS providers access to Verizon customer location information on March 30, 2019.[71] In other words, Verizon did not finally terminate its location-based service program until March 30, 2019, or 324 days from when the *New York Times* first reported on the Securus location-finding service, as well as the abuse of that service by Hutcheson.

19. *Notice of Apparent Liability*. On February 28, 2020, the Commission issued the *Verizon NAL* proposing a $48,318,750 fine against Verizon for its apparent willful and repeated violation of

[61] *See NAL*, 35 FCC Rcd at 1710, para. 29 (citing LOI Response at 12, Response to Question 8).

[62] *NAL*, 35 FCC Rcd at 1710, para. 30 (citing LOI Response at 12, Response to Question 8).

[63] *NAL*, 35 FCC Rcd at 1710, para. 31 (citing LOI Response at 13, Response to Question 10).

[64] *NAL*, 35 FCC Rcd at 1710, para. 31 (citing LOI Response at 13, Response to Question 10).

[65] *NAL*, 35 FCC Rcd at 1710, para 32 (citing LOI Response at 9, Response to Question 6).

[66] *See NAL*, 35 FCC Rcd at 1710, para. 34 (citing Supplemental LOI Response at 2, Response to Question 1).

[67] *NAL*, 35 FCC Rcd at 1710, para 32 (citing LOI Response at 10, Response to Question 6).

[68] *See NAL*, 35 FCC Rcd at 1710-11, para. 33 (citing LOI Response at 9, Response to Question 6; Supplemental LOI Response at 3, Response to Question 1).

[69] *See NAL*, 35 FCC Rcd at 1711, para. 33 (citing Supplemental LOI Response at 3, 9, Response to Questions 1, 4).

[70] *See NAL*, 35 FCC Rcd at 1711, para. 36 (citing Supplemental LOI Response at 5, Response to Question 1).

[71] *See NAL*, 35 FCC Rcd at 1711, para. 35 (Supplemental LOI Response at 2, Response to Question 1).

section 222 of the Act and section 64.2010 of the Commission's CPNI Rules for failing to have reasonable protections in place to prevent unauthorized access to customer location information. In the *Verizon NAL*, the Commission also admonished Verizon for apparently disclosing its customers' location information, without their consent, to a third party who was not authorized to receive it.

20. On May 7, 2020, Verizon filed a response to the *NAL*.[72] Verizon makes a number of arguments as to why the *NAL* should be withdrawn and cancelled. Verizon argues that location information is not CPNI and thus is not subject to the Act and the Commission's CPNI Rules, and that even if it was, the Company did not have fair notice that it would be classified as CPNI.[73] Verizon also argues that it acted reasonably both pre- and post-publication of the *New York Times* article. The Company claims that the LBS program had reasonable protections in place before the *New York Times* article, and that the Company's response to the article, including its months-long continuation of the LBS program, was likewise reasonable.[74] Verizon argues that the forfeiture amount is arbitrary and capricious.[75] Finally, Verizon contends that the forfeiture amount is incorrect insofar as the *NAL* miscounts the number of LBS providers and the number of days in the forfeiture calculation.[76]

## III. DISCUSSION

21. The Commission proposed a forfeiture in this case in accordance with section 503(b) of the Communications Act of 1934, as amended (Act),[77] section 1.80 of the Commission's rules,[78] and the Commission's *Forfeiture Policy Statement*.[79] When we assess forfeitures, section 503(b)(2)(E) requires that the Commission take into account the "nature, circumstances, extent, and gravity of the violation and, with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other matters as justice may require."[80] We have fully considered Verizon's NAL Response, which includes a variety of legal and factual arguments. With one exception, we find none of Verizon's arguments persuasive. Upon review of Verizon's NAL Response and a further review of the evidence in the record, we will adjust the forfeiture calculation to account for updated evidence related to the non-participation of two entities in Verizon's LBS program that had been included in the original forfeiture calculation. We therefore reduce the $48,318,750 forfeiture proposed in the *NAL* by $1,417,500, and impose a penalty of $46,901,250.

### A. Location Information is CPNI

22. As the *NAL* explained in more detail, the customer location information disclosed in Verizon's LBS program is CPNI under the Act and our rules.[81] Section 222 defines CPNI as "information that relates to the quantity, technical configuration, type, destination, *location*, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier,

[72] *Verizon Communications*, Response to Notice of Apparent Liability for Forfeiture and Admonishment (filed May 7, 2020) (on file in EB-TCD-18-00027698) (NAL Response or Response).

[73] NAL Response at 5-6, 9-11, 32-39.

[74] NAL Response at 39-40, 44-54.

[75] NAL Response at 8-9, 56-59.

[76] NAL Response at 58, Exh. A (Supplemental Declaration of John A. Bruner, Aegis Mobile, LLC, para. 12 (May 6, 2020)), Exh D.

[77] 47 U.S.C. § 503(b).

[78] 47 CFR § 1.80.

[79] *The Commission's Forfeiture Policy Statement and Amendment of Section 1.80 of the Rules to Incorporate the Forfeiture Guidelines*, Report and Order, 12 FCC Rcd 17087 (1997) (*Forfeiture Policy Statement*), *recons. denied*, Memorandum Opinion and Order, 15 FCC Rcd 303 (1999).

[80] 47 U.S.C. § 503(b)(2)(E).

[81] *See NAL*, 35 FCC Rcd at 1712-14, paras. 41-48.

and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[82] The customer location information used in Verizon's LBS program falls squarely within this definition. Verizon's arguments to the contrary[83] are largely reiterations of arguments the Commission considered and found unpersuasive in the *NAL*. Consistent with the analysis of location data found in the *NAL*, we remain persuaded that the location data at issue here constitute CPNI.

23. *First*, the customer location information at issue here relates to the location of a telecommunications service—i.e., Verizon's commercial mobile service.[84] As fully explained in the *NAL*:

> A wireless mobile device undergoes an authentication and attachment process to the carrier's network, via the closest towers. After a mobile device is authenticated and logically attached to a wireless network, it may be (1) connected (sending/receiving data/voice) or (2) idle. In either state, the carrier must be aware of and use the device's location in order for it to enable customers to send and receive calls. Verizon is therefore providing telecommunications service to these customers whenever it is enabling the customer's device to send and receive calls—regardless of whether the device is actively in use for a call.[85]

24. We conclude that the location information at issue here meets the first prong of the CPNI definition under either of two alternative interpretations. For one, we believe that the relevant statutory language is best read as referring to "information that relates to the . . . location, . . . of a telecommunications service . . . ."[86] That interpretation accords with the "rule of the last antecedent," which suggests that the term "of use" in section 222(h)(1)(A) modifies only "amount," as opposed to the preceding terms such as "location."[87] Our interpretation also better squares with the broader operation of section 222. If the language "of use" modified every term in the preceding list, it would lead to apparently anomalous results. For instance, although the phrase "amount of use of a telecommunications service" plainly refers at least to the number and length of telephone calls, it is not clear what "technical configuration of use" would mean. And our interpretation squares more readily with section 222(d)(1), which preserves carriers' ability to use CPNI to "initiate" service[88]—an event that, aspects of which, ordinarily occur before the service is in "use."

25. The location information at issue here readily fits within that interpretation of the first prong of the CPNI definition. Verizon's customers can access the commercial mobile service to which they subscribe over a broad geographic area, and their location at a given point in time—and the fact of Verizon's ability to use its network to determinate that location—is reasonably understood as associated with or a reference to the location of the Verizon telecommunications service.[89] Consequently, consistent

---

[82] 47 U.S.C. § 222(h)(1)(A) (emphasis added).

[83] *See* NAL Response at 5-6, 9-11, 32-39.

[84] *See* 47 U.S.C. § 332(c)(1) (providing that "a person engaged in the provision of a service that is a commercial mobile service shall, insofar as such person is so engaged, be treated as a common carrier for purposes of this chapter"), (d)(1) (defining "commercial mobile service").

[85] *See NAL*, 35 FCC Rcd at 1712, para. 43.

[86] 47 U.S.C. § 222(h)(1)(A).

[87] *See, e.g.*, *Lockhart v. United States*, 577 U.S. 347, 351 (2016) (the rule of the last antecedent "provides that 'a limiting clause or phrase . . . should ordinarily be read as modifying only the noun or phrase that it immediately follows'").

[88] 47 U.S.C. § 222(d)(1).

[89] *See, e.g.*, *NAL*, 35 FCC Rcd at 1703, para. 11 ("Verizon provides mobile voice and data services to consumers throughout the United States by enabling consumer mobile phones to make and receive calls or transmit data on Verizon's wireless network.").

with our assessment in the *NAL*,[90] we find this to be information that "relates to" the location of Verizon's telecommunications service within the meaning of the first prong of the CPNI definition.[91]

26. In the alternative, even if the term "of use" modified "location," we still conclude the information at issue fits within the first prong of the definition of CPNI. Verizon does not dispute the *NAL*'s explanation that customers' devices and Verizon's network regularly exchange information as necessary for customers to send and receive calls.[92] To the extent that Verizon contends that this does not represent use of the telecommunications service because it merely enables the provision of that service, Verizon does not demonstrate why that is a fair characterization or why it would represent a meaningful distinction in any case. Consistent with the reasoning of the *NAL*,[93] we believe that Verizon's customers subscribe to its commercial mobile service to enable them to receive and transmit calls. When customers' devices are exchanging communications with Verizon's network, and thereby ensuring that they can receive incoming calls and place outgoing calls, we think that is a clear case of using the service to which they have subscribed, even outside the moments in time when they are engaged in calls.[94]

27. Nor do Verizon's arguments about the source and intended purpose of the location data at issue here persuade us to reach a contrary result. Verizon contends that the location data at issue here, while generated using "the same network functionality as the normal-course operational pinging that occurs between cell sites and customer devices to facilitate Verizon services," nonetheless "occurred separately from that normal-course operation—and was done specifically for the purpose of facilitating the third-party location-based services."[95] Thus, Verizon says, it obtained such location data with the intent of using it for purposes of its LBS initiative, rather than Verizon's provision of commercial mobile service.[96] But nothing in the text of the first prong of the CPNI definition turns on the carriers' stated intent in collecting it. So long as the information "relates to" one or more of the specified criteria, the other factors raised by Verizon do not matter. And as noted above, the information at issue here "relates to" the location of the telecommunications service (or to the location of use of that service), regardless of how Verizon obtained the information and how it planned to use the information.

28. We also are unpersuaded by Verizon's arguments that the location information covered by the first prong of the definition of CPNI is limited to call location information for voice calls based on

---

[90] *See, e.g.*, *NAL*, 35 FCC Rcd at 1712-14, paras. 43, 46.

[91] *See, e.g.*, *Collins Concise Dictionary*, Third Ed., at 1129 (HarperCollins Pub. 1995) (defining "relate" as, among other things, "establishing association (between two or more things) or (of something) to have relation or reference (to something else)"); *American Heritage Dictionary*, Third Ed., at 695 (Dell Pub. 1994) (defining "relate" as, among other things, "To bring into logical or natural association," "To establish or demonstrate a connection between," or "To have connection, relation, or reference"); *Merriam-Webster's Collegiate Dictionary*, Tenth Ed., at 987 (Merriam-Webster Pub. 1994) (defining "relate" as, among other things, "to show or establish logical or causal connection between"); *The Oxford Paperback Dictionary & Thesaurus*, at 636 (Oxford Univ. Press 1997) (defining "relate" as, among other things, "connect in thought or meaning" or "have reference to").

[92] *NAL*, 35 FCC Rcd at 1712-13, para. 43.

[93] *See, e.g.*, *NAL*, 35 FCC Rcd at 1712-14, paras. 43, 46.

[94] Definitions of "use" appear sufficiently broad to encompass our understanding of the term in this scenario. *See, e.g.*, *Collins Concise Dictionary*, Third Ed., at 1483 (HarperCollins Pub. 1995) (defining "use," among other things, to mean "to put into service or action; employ for a given purpose"); *American Heritage Dictionary*, Third Ed., at 884 (Dell Pub. 1994) (defining "use," among other things, to mean "To put into service; employ" and "To avail oneself of; practice"); *Merriam-Webster's Collegiate Dictionary*, Tenth Ed., at 1301 (Merriam-Webster Pub. 1994) (defining "use," among other things, to mean "to put into action or service: avail oneself of"); *The Oxford Paperback Dictionary & Thesaurus*, at 853 (Oxford Univ. Press 1997) (defining "use," among other things, to mean "cause to act or serve for purpose; bring into service" and "exploit for one's own ends").

[95] NAL Response at 34.

[96] NAL Response at 34-35.

what Verizon gleans from other language in section 222.[97] In addition to the *NAL*'s responses in this regard,[98] we conclude that the use of "location" in (h)(1)(A) as opposed to "call location information" in (d)(4) and (f)(1) must be given some significance:[99] All *location* information is protected as CPNI under (h)(1)(A). But carriers can disclose *call location* information for 911 purposes under (d)(4), which makes sense because 911 calls are *calls*. Nor would it have been irrational for Congress to expressly require opt-in consent for call location information in section 222(f)(1) if the definition of CPNI encompasses other forms of location information, as well. At the time the provision was enacted in 1999, Congress might reasonably have viewed call location information as obviously sufficiently sensitive to necessitate opt-in approval requirements while leaving it to the Commission's discretion whether to require opt-in approval for other location information, just as for other information falling within the definition of CPNI more generally. In addition, the Commission's references to "calls" in a prior order that was focused in significant part on data regarding customers' calls—and which did not purport to exhaustively address the application of section 222 to mobile wireless service—cannot reasonably be read as setting forth the outer bounds of the Commission's understanding of section 222.[100]

29. *Second*, the location information at issue was obtained by Verizon solely by virtue of its customer-carrier relationship. The *NAL* explains this in more detail, but the crux of the matter is that:

> Verizon provides wireless telephony services to the affected customers because they have chosen Verizon to be their provider of telecommunications service—in other words, they have a carrier-customer relationship. . . . Verizon's customers provided their wireless location data to Verizon because of their customer-carrier relationship with Verizon, . . . .[101]

In sum, although Verizon might also provide non-common-carrier services to the same customer, the customer provided the relevant data "solely by virtue of the carrier-customer relationship."[102]

30. The *NAL* did not specify with precision the standard for applying the second prong of the CPNI definition, and although we elaborate further on some of its contours here, we likewise need not resolve that question with specificity because we find that prong met here under a range of possible approaches. We begin by observing that the second prong of the CPNI definition is focused on a "relationship"—namely, the "carrier-customer relationship."[103] A relationship presumes associations involving at least two parties, and we conclude that it must be understood with that context in mind, rather than focused single-mindedly on one side of the relationship. Our accounting for the customer's viewpoint is also supported by the statutory text's focus on whether the information "is made available to the carrier by the customer"—rather than "obtained by the carrier"—"solely by virtue of the carrier-

---

[97] *See, e.g.*, NAL Response at 5, 32-34.

[98] *NAL*, 35 FCC Rcd at 1714, para. 47.

[99] This interpretive approach is consistent with how the Commission has approached the interpretation of section 222 in other contexts in the past. *See, e.g.*, *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, 8084-85, para. 32 (1998) (distinguishing the interpretation of different language in section 222(a), (c)(1), and (d)(1), given that, "[u]nder well-established principles of statutory construction, 'where Congress has chosen different language in proximate subsections of the same statute,' we are 'obligated to give that choice effect'").

[100] *See generally 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 (2013) (*2013 CPNI Declaratory Ruling*).

[101] *NAL*, 35 FCC Rcd at 1713, para. 44.

[102] *NAL*, 35 FCC Rcd at 1714, para. 46.

[103] 47 U.S.C. § 222(h)(1)(A).

customer relationship."[104] Thus, although Verizon suggests that its acquisition of the location information at issue here is in some sense distinct from, or does not depend exclusively on, the carrier-customer relationship,[105] we find that belied by the technical and marketplace realities here, as experienced by Verizon customers.

31. As the *NAL* explains, when a customer subscribes to Verizon's commercial mobile service, Verizon "enables the connection of a customer's device to its network for the purpose of sending and receiving calls, and the customer has no choice but to reveal that location to the carrier."[106] Verizon does not dispute that the carrier-customer relationship fully enables Verizon to obtain the location data at issue here. Verizon contends that while it obtained location data for its LBS program using the same mechanism as it did to provide other services, its acquisition of location information nonetheless "occurred separately from that normal-course operation—and was done specifically for the purpose of facilitating the third-party location-based services."[107] However, Verizon does not claim that a customer, having subscribed to its commercial mobile service, entered a separate agreement with Verizon for the provision of that location information—or that Verizon's voice customers had any way to avoid providing that information if they wanted to subscribe to Verizon's commercial mobile service. Under circumstances such as these, we conclude that the location information at issue from Verizon's commercial mobile service customers was "made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[108]

32. Although we find that reasoning sufficient to resolve the application of the second prong of the CPNI definition, we independently conclude that the same decision is warranted even if we parse the matter more finely. For example, in its NAL Response, Verizon has argued that the location information as issue in this matter should not be considered CPNI because the "same equipment-to-device communication occurs for customers using data services . . . as it does for customers making phone calls" and that the "vast majority of traffic on Verizon's network . . . is data traffic."[109] But we are not persuaded that Verizon's provision of multiple services to its telecommunications customers (including SMS text messaging and internet service) takes the resulting *relationship* outside the scope of the "carrier-customer" relationship for the specific purposes of the CPNI definition. Nothing dissuades us that the purchase of telecommunications service alone was sufficient to obligate Verizon's customers to make their location information available to Verizon,[110] and in evaluating the second prong of the CPNI

[104] 47 U.S.C. § 222(h)(1)(A). Insofar as Verizon disputes whether "the location information that Verizon obtains" is "obtained solely by virtue of Verizon's provision of telecommunications service," *see, e.g.*, NAL Response at 36, the focus on Verizon's "telecommunications service" neither reflects the statutory text regarding prong two of the CPNI definition nor does it appropriately account for these concepts underlying the statutory focus on a customer-carrier "relationship." To be sure, section 222(c)(1) is limited in scope to "a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service." 47 U.S.C. § 222(c)(1). But in that provision, the required nexus is just that the carrier receive or obtain the CPNI "by virtue" (not "solely by virtue") of its provision of a telecommunications service. In its NAL Response, Verizon disputes whether the location information at issue meets the statutory definition of CPNI in section 222(h)(1)(A), *see* NAL Response at 34-36, but does not contend that, if it does meet that definition, section 222(c)(1) nonetheless should not be interpreted to apply here.

[105] *See, e.g.*, NAL Response at 9, 34-36.

[106] *NAL*, 35 FCC Rcd at 1713, para. 45.

[107] NAL Response at 34.

[108] 47 U.S.C. § 222(h)(1)(A).

[109] NAL Response at 9.

[110] Consequently, this is not a situation where we are relying on a theory that the carrier-customer relationship was merely one of a "confluence of multiple factors"—including relationships beyond the carrier-customer relationship itself—that collectively were required for Verizon to obtain the location information at issue here. *Bostock v. Clayton Cty.*, 140 S. Ct. 1731, 1739 (2019) (In contrast to the statute at issue there, Congress "could have added (continued….)

definition in the past, the Commission has noted that a carrier's "unique position with respect to its customers" when the carrier pre-configures a mobile device to collect information can satisfy "the 'carrier-customer relationship' element of the definition of CPNI."[111] Verizon points out[112] that section 153(51) of the Act provides that "[a] telecommunications carrier shall be treated as a common carrier under [the Act] only to the extent that it is engaged in providing telecommunications services."[113] But we are far from that scenario here, given the many necessary links to Verizon's telecommunications services for the CPNI definition to apply.[114] For one, the protections of section 222(c) only apply with respect to "information that relates to" certain characteristics of "a telecommunications service subscribed to by any customer of" Verizon.[115] And the information must have been provided by consumers in a manner that reflects the statutorily required nexus to Verizon's telecommunications service.[116] Our interpretation and application of section 222 thus accords with the text of both section 222 and section 153 of the Act, even if it does not reflect the policy that Verizon would prefer.

33. Finally, we reject Verizon's argument that because it also gathered location information from consumers who only subscribed to information services (e.g., tablets) and did not partake of telecommunications services, *none* of the location information has been gathered solely by virtue of the customer-carrier relationship.[117] Against the backdrop of the analysis above, that only bears on the status of the information from those specific, non-voice, customers. The *NAL*'s proposed forfeitures turn not on specific effects on specific customers individually but on Verizon's corporate practices as a whole with respect to the entities that received LBS data.[118] Verizon does not contend that the LBS data that it provided, directly or indirectly, to any of the entities associated with the proposed forfeitures in the *NAL* was limited exclusively to data from non-voice customers. Thus, the Verizon practices that formed the basis of the proposed forfeitures in the *NAL* included information from voice customers, which falls within the definition of CPNI for the reasons explained above.

34. The Commission therefore affirms its finding from the *NAL* that the location information at issue in the LBS program is CPNI.

---

'solely' to indicate that actions taken 'because of ' the confluence of multiple factors do not violate the law."); *cf. id*. (observing that "[o]ften, events have multiple but-for causes"). By contrast, information that carriers obtain independently from public records, for example, would not be information that the customer provided to the carrier solely by virtue of the carrier-customer relationship.

[111] *2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9616, para 23.

[112] *See* NAL Response at 36 n.28.

[113] 47 U.S.C. § 153(51).

[114] For similar reasons, we reject the suggestion that our approach regulates Verizon under section 222 based on the mere fact that it has the status of a telecommunications carrier, rather than being linked to its specific offering of telecommunications services. *See* NAL Response at 32-36.

[115] 47 U.S.C. § 222(h)(1)(A).

[116] 47 U.S.C. § 222(h)(1)(A).

[117] *See* NAL Response at 35-36.

[118] In particular, the *NAL* did not propose forfeitures based on unauthorized disclosure of CPNI associated with particular customers—it proposed forfeitures based on allegations that Verizon failed to take reasonable steps to protect its customers' location information, with forfeitures proposed not on a per-customer basis but on the basis of the days in which Verizon allegedly did not have a reasonable policy in place for particular entities that received LBS data. *See, e.g.*, *NAL*, 35 FCC Rcd at 1726-27, para. 87. And while *FTC v. AT&T Mobility LLC*, 883 F.3d 848 (9th Cir. 2018) (en banc), concluded that the common-carrier limitation on the FTC's authority is activities-based, rather than status-based, it also recognized that "there may be some overlap between the agencies' jurisdiction when the FCC's regulations of common carriers affect the non-common-carrier activities of those entities," observing that "[i]n the administrative context, two cops on the beat is nothing unusual." *Id*. at 862. Thus, our interpretation of section 222 is not at odds with the court's decision in *FTC v. AT&T Mobility*.

### B. Verizon Had Fair Notice That its LBS Practices Were Subject to Enforcement Under the Communications Act

35. We reject Verizon's claim that it lacked fair notice that its practices involving customer location information were subject to the Communications Act and potential penalties thereunder.[119] The language of section 222 makes clear that customer location information is CPNI; Verizon's practices involving CPNI, including customer location information, unquestionably are regulated under the Act and the Commission's CPNI Rules; and Verizon's failure to comply with the requirements of the Act and our rules, including the "reasonable measures" mandate of section 64.2010, foreseeably makes the Company liable for a forfeiture penalty under section 503 of the Act.

36. Verizon argues that if the Commission wishes to classify location information as CPNI, "it must do so on a prospective basis through a rulemaking or declaratory ruling."[120] But the Commission is not limited to these options. When, as in this case, a carrier's conduct falls within an area subject to regulation by the Commission, it is well established that enforcement action is also a proper vehicle to adjudicate the specific bounds of what is lawful and what is not, subject to principles of fair notice.[121]

37. Contrary to Verizon's assertion, the Commission is not "impos[ing] retroactive liability on a carrier that did not have adequate notice . . . ."[122] As the D.C. Circuit has explained, "[t]he fair notice doctrine, which is couched in terms of due process, provides redress only if an agency's interpretation is 'so far from a reasonable person's understanding of the regulations that they could not have fairly informed the regulated party of the agency's perspective.'"[123] And, in general, fair notice principles require that a regulated party be able to identify, with ascertainable certainty, the standards with which the agency expects parties to conform.[124]

38. Here, the Commission previously explained in the *2013 Declaratory Ruling* that it would not "set out a comprehensive list of data elements that pertain to a telecommunications service and satisfy the definition of CPNI and those data elements that do not."[125] Thus, Verizon cannot reasonably have assumed that the fact a given scenario had not been expressly addressed by Commission rules and precedent meant it fell outside the scope of CPNI and the associated protections of section 222 and the

[119] *See* NAL Response at 38-39.

[120] NAL Response at 38. As discussed more fully in this section, contrary to Verizon's argument, Verizon could have reasonably ascertained that the location information at issue here would be found to meet the definition of CPNI and Verizon would be subject to forfeiture penalties for failing to protect that customer location information as required under section 222 and the CPNI Rules.

[121] *See, e.g.*, *City of Arlington, Texas v. FCC*, 569 U.S. 290, 307 (2013) (affirmatively stating that "Congress has unambiguously vested the FCC with general authority to administer the Communications Act through rulemaking and adjudication"); *Neustar, Inc. v. FCC*, 857 F.3d 886, 894 (D.C. Cir. 2017); *Chisholm v. FCC*, 538 F.2d 349, 365 (D.C. Cir. 1976) (reiterating that "the choice whether to proceed by rulemaking or adjudication is primarily one for the agency regardless of whether the decision may affect agency policy and have general prospective application") (citing *N.L.R.B. v. Bell Aerospace Co*., 416 U.S. 267, 291-95 (1974); *SEC v. Chenery Corp*., 332 U.S. 194, 203 (1947) (stating that "the choice made between proceeding by general rule or by individual, ad hoc litigation is one that lies primarily in the informed discretion of the administrative agency").

[122] NAL Response at 38.

[123] *Mississippi Comm'n on Envtl. Quality v. EPA*, 790 F.3d 138, 186 (D.C. Cir. 2015) (quoting *United States v. Chrysler Corp.*, 158 F.3d 1350, 1354 (D.C. Cir. 1998)); *see also United States v. Thomas*, 864 F.2d 188, 195 (D.C. Cir. 1988) ("statutes cannot, in reason, define proscribed behavior exhaustively or with consummate precision").

[124] *Star Wireless, LLC v. FCC*, 522 F.3d 469, 473 (D.C. Cir. 2008) ("In assessing forfeitures against regulated entities, the Commission is required to provide adequate notice of the substance of the rule. . . . The court must consider whether by reviewing the regulation 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.") (internal quotations and citations omitted).

[125] *2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9617, para. 24 n.54.

Commission's implementing rules. To the contrary, the Commission has stated that "implicit in section 222 is a rebuttable presumption that information that fits the definition of CPNI contained in section 222([h])(1) is in fact CPNI."[126] Moreover, even while declining to comprehensively identify CPNI, including in the case of location information, the Commission emphasized that "location information in particular can be very sensitive customer information."[127] In addition, notwithstanding the fair notice claims it makes now, Verizon asserted to the Commission that it treated customer location information in an essentially equivalent manner to CPNI.[128]

39. Further, our conclusion that the location data at issue here fall within the definition of CPNI flows from the text of section 222 is consistent with the Commission's approach to interpreting that provision as laid out in prior precedent. As noted, CPNI is defined by statute, in relevant part, to include "information that relates to . . . the location . . . of a telecommunications service."[129] That definition further directs us to evaluate whether the relevant information "is made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[130] Our interpretation of those provisions above relies on the statutory text, interpreted consistent with ordinary tools of statutory interpretation, and is consistent with prior Commission precedent.

40. Finally, Verizon had fair notice of its obligations with respect to CPNI under section 64.2010 of the Commission's rules. In pertinent part, that rule provides that "[t]elecommunications carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI."[131] Beyond "requir[ing] carriers to implement the specific minimum requirements set forth in the Commission's rules," to comply with section 64.2010, the Commission "further expect[s] carriers to take additional steps to protect the privacy of CPNI to the extent such additional measures are feasible for a particular carrier."[132] The Commission granted carriers flexibility to incorporate the specific measures and practices that are consistent with their otherwise-existing "technological choices."[133] In the *2007 CPNI Order*, the Commission also explained, for example, that "a carrier that practices willful blindness" regarding unauthorized disclosure of CPNI likely "would not be able to demonstrate that it has taken sufficient measures" to discover and protect against such conduct.[134] And in the same order, the

---

[126] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, et al.*, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, 14495-96, para. 167 (1999). Although the Commission was responding, in part, to a request for clarification from MCI regarding ''laundering"' of CPNI by virtue of transfers to affiliated or unaffiliated entities, it was not limited just to that scenario alone. *See, e.g.*, *id*. at 14495, para. 166 (describing the MCI request for clarification being addressed as, among other things, "seek[ing] clarification that there is a rebuttable presumption that customer-specific information in a carrier's files was received on a confidential basis or through a service relationship governed by section 222").

[127] *2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9617, para. 24 n.54.

[128] *See* NAL Response at 40. Verizon concedes that "…even if the information used in Verizon's aggregator program were CPNI or even 'call location information,' Verizon would have satisfied either of Section 222's consent requirements because Verizon required affirmative, opt-in customer consent — the highest level of consent that Section 222 contemplates — before third parties were permitted to access customer location information." *Id*.

[129] 47 U.S.C. § 222(h)(1)(A); *see also, e.g.*, *2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9616, para. 22 n.48 (citing section 222(h)(1)(A) as "defining CPNI to include 'information that relates to the . . . location . . . of a telecommunications service subscribed to by any customer of a telecommunications carrier'").

[130] 47 U.S.C. § 222(h)(1)(A).

[131] 47 CFR § 64.2010(a).

[132] *2007 CPNI Order*, 22 FCC Rcd at 6959, para. 64.

[133] *Id.* at 6959-60, para. 65; *see also, e.g.*, *id*. at 6945-46, para. 34 ("we permit carriers to weigh the benefits and burdens of particular methods of possibly detecting pretexting," which "will allow carriers to improve the security of CPNI in the most efficient manner").

[134] *Id.* at 6946, para. 35.

Commission likewise identified the limitations of relying on "contractual safeguards" to address risks once CPNI has been disclosed outside the covered carrier.[135] Ultimately, while providing guidance regarding compliance with section 64.2010, the Commission also recognized that it was necessary to guard against providing bad actors "a 'roadmap' of how to obtain CPNI without authorization."[136] This provides sufficient direction for Verizon to understand its obligations under the rule as relevant here.

41. Thus, Verizon could reasonably have ascertained that (1) any enumeration of CPNI data elements set out by the agency was not exhaustive; (2) the customer location information at issue would be found to meet the definition of CPNI; and (3) Verizon would be subject to forfeiture penalties for failing to protect that customer location information as required under section 222 and the Commission's rules.[137]

### C. Verizon Failed to Take Reasonable Steps to Protect CPNI

42. Verizon violated section 222 of the Act and section 64.2010 of our rules by failing to take reasonable measures to discover and protect against attempts to gain unauthorized access to its customers' location information.[138] While our rules recognize that companies cannot prevent all data breaches, the rules require carriers to take reasonable steps to safeguard their customers' CPNI and discover attempts to gain access to their customers' CPNI. Further, as noted below, where an unauthorized disclosure has occurred—as here—the burden of production shifts to the carrier to offer evidence that it did have reasonable measures in place. Once the carrier offers some evidence of those safeguards, the rebuttable presumption falls away, and the Commission bears the burden of persuasion and must find by a preponderance of the evidence that the carrier's safeguards were unreasonable in order to find a violation of 47 CFR § 64.2010(a). Verizon contends that the Securus disclosures to Hutcheson did not constitute legal violations of section 222, disputes the timing and scope of those disclosures, and contends that finding a violation of section 222 and the Commission's rules otherwise is unjustified with regard to those disclosures.[139] Verizon then claims that it acted reasonably to protect its customers' location information both before and after the Securus disclosure came to light.[140] Verizon also argues that the Commission improperly shifted the burden of proving that such protections were reasonable to Verizon.[141] We find Verizon's arguments unpersuasive.

#### 1. Verizon's Customer Location Disclosures to Securus Were Unauthorized and Violated Section 222

43. As an initial matter, we conclude that it was not just disclosures to Hutcheson that were unauthorized. Rather, Securus's entire location-finding service[142] (as detailed in paragraphs 13-14, above) was predicated on unauthorized disclosures.[143] Consistent with Verizon's own description of

---

[135] *Id.* at 6952-53, para. 49.

[136] *Id.* at 6959-60, para. 65.

[137] Accordingly, we reject Verizon's argument that "[n]o carrier "acting in good faith" could have identified "with 'ascertainable certainty'" the NAL's expansive view of CPNI." NAL Response at 38.

[138] 47 CFR § 64.2010(a); *see also 2007 CPNI Order*, 22 FCC Rcd at 6959, para. 64 ("We fully expect carriers to take every reasonable precaution to protect the confidentiality of proprietary or personal customer information.").

[139] *See* NAL Response at 19-22, 28-30.

[140] *See* NAL Response at 39-40, 44-56.

[141] *See* NAL Response at 40-44.

[142] *See NAL*, 35 FCC Rcd at 1708-09, paras. 25-26 (citing Jennifer Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, N.Y. Times (May 10, 2018) https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html).

[143] Verizon states that "the NAL does not claim that Verizon disclosed information to Hutcheson—it claims that Securus did." NAL Response at 28. But it was Verizon CPNI that was disclosed, and as the *NAL* explained, (continued….)

events, the program was outside the scope of not only its approved use case, but also beyond any agreement with either Aggregator (and thus had not been reviewed by Verizon).[144] Verizon conceded that it was unable to distinguish location requests unrelated to the authorized use case (which involved an inmate collect-calling service) and that the practice did not trigger any review by Aegis.[145] And, to be clear, none of the records submitted in connection with the location-finding service evinced a consumer's actual opt-in consent. Therefore, every time Securus submitted a request for location information under the guise of its approved use case (a use case that required consumer consent) and Verizon provided the requested location information, a separate, unauthorized disclosure occurred.

44. Verizon attempts to avoid this conclusion by: (1) concentrating only on the disclosures made to Hutcheson, not on the overall Securus location-finding program;[146] and (2) trying to use section 222(c)(1)'s exception for disclosures that are required by law to shield itself.[147] This misses the larger point. Whether or not there was a legitimate law enforcement request for the information is irrelevant if Verizon did not satisfy its own obligations under section 222. Verizon provided the location information to Securus under Securus's false pretenses, and Verizon only did so because it took Securus at its word that Securus had obtained opt-in consumer consent.[148] This means that Verizon did not review any law enforcement requests and likewise did not provide the information pursuant to a law enforcement request because Verizon did not know there *were* any law enforcement requests in the first place – legitimate or otherwise.[149] Separately and independently, there is no indication that the law enforcement requests were properly reviewed by Securus, as evidenced by the ready success of Hutcheson's thinly veiled ruse.[150]

---

"Verizon is not absolved from liability simply because it was not directly responsible for operating the programs under which unauthorized disclosures occurred." *NAL*, 35 FCC Rcd at 1715, para. 52.

[144] *See* LOI Response at 11-12, Response to Question 8; *NAL*, 35 FCC Rcd at 1709, para. 27; *see also, e.g.*, NAL Response at 19-21.

[145] *See NAL*, 35 FCC Rcd at 1709-10, 1715, paras. 27-29, 51.

[146] *See* NAL Response at 19-22 (raising arguments based on the number of identified disclosures to Hutcheson and the time periods at issue in those identified disclosures); *id*. at 48 (disputing "that the fact that Securus was able to share with Hutcheson the information for a small number of Verizon customers without authorization is evidence that Verizon's program safeguards were inadequate").

[147] *See* NAL Response at 20 n.17 (relying on 47 U.S.C. § 222(c)(1), which allows disclosure of CPNI "as required by law").

[148] As the *NAL* explained, "[t]o the extent that the third parties were *not* acting on behalf of the carrier, the carrier itself would have provided those third parties with access to its customers' CPNI without obtaining for themselves the approval required by section 222(c)(1)—thus violating federal law." *NAL*, 35 FCC Rcd at 1716, para. 54 n.145. Although the *NAL* noted that "Verizon does not appear to argue that situation is present here," *id*., the totality of the record persuades us that this is, in fact, the import of the facts and Verizon's arguments here.

[149] *See* LOI Response at 11-12, Response to Question 8; *NAL*, 35 FCC Rcd at 1709, para. 27; NAL Response at 19-21. *See also NAL*, 35 FCC Rcd at 1708-09, paras. 25-26 (citing Jennifer Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, N.Y. Times (May 10, 2018) https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html; Doyle Murphy, *Ex-Missouri Sheriff Cory Hutcheson Sentenced to 6 Months in Prison*, Riverfront Times (Apr. 29, 2019), https://www.riverfronttimes.com/newsblog/2019/04/29/ex-missouri-sheriff-cory-hutcheson-sentenced-to-6-months-in-prison). It is not reasonable to interpret Verizon as having been relying on a third party to disclose information as required by law where Verizon neither knew nor approved of the third party doing so.

[150] *See* Hutcheson Sentencing Memo at 3-4 (explaining that after uploading documents that were blatantly not legal authorizations, location information was immediately transmitted with no intervening time for any documents to be reviewed for validity); *NAL*, 35 FCC Rcd at 1709, para. 26 (describing Hutcheson's uploading of documents that were blatantly not legal authorizations in order to obtain location information). As the *NAL* explained, "Verizon does not deny the existence of the Securus location-finding service nor the abuse of that system by Hutcheson." *NAL*, 35 FCC Rcd at 1709, para. 27. Verizon likewise does not dispute here that Hutcheson was, as a general matter, able to access location data by providing documents that were blatantly not legal authorizations as described (continued….)

Thus, the disclosures made to Hutcheson were doubly unauthorized under section 222(c)(1). First, Securus used the façade of their approved use case to hide the true purpose and destination of the request, resulting in Verizon's unauthorized disclosure of location information to Securus. Second, Hutcheson likewise submitted blatantly fake requests to Securus under the guise of law enforcement, resulting in Securus's unauthorized disclosure of location information to Hutcheson.[151] Despite Verizon's arguments, the Company is clearly not "required by law" to disclose location information based on any and every pretense or unsupported request. Therefore, consistent with the *NAL*, we find that the Securus disclosures, including those made to Hutcheson, were unauthorized.

45. We thus conclude that Verizon was appropriately admonished in relation to such disclosures.[152] In objecting to the admonishment, Verizon criticizes the approach of finding a violation of section 222 when there is an unauthorized disclosure of CPNI as inconsistent with the limits of carriers' practical ability to prevent all unauthorized disclosures,[153] and as "contrary to the current CPNI rules, which enshrine a reasonableness approach to CPNI issues."[154] But Verizon fails to grapple with the text of the restriction on unauthorized use or disclosure in section 222(c)(1) of the Act and section 64.2007(b) of the Commission's rules.[155] Rather than incorporating some kind of *de minimis* exception or reasonableness standard, section 222(c)(1)'s statutory restriction on use and disclosure is unequivocal, as likewise reflected in section 64.2007(b) of the Commission's rules.[156] Against that backdrop, we also are not persuaded that the admonishment causes unfair surprise to Verizon, even assuming *arguendo* that such a standard applied to an admonishment here.

### 2. Verizon's Protection of Customer Location Information Was Unreasonable Both Before and After the Securus/Hutcheson Disclosures

46. The Commission affirms the *NAL* and finds that Verizon failed to take reasonable measures to discover and protect against attempts to gain unauthorized access to its customers' location information. As fully laid out in the *NAL*, the record not only shows that Verizon did not have reasonable protections in place prior to 2018 *New York Times* article detailing the Securus/Hutcheson breaches,[157] but also that Verizon failed to promptly address its demonstrably inadequate CPNI safeguards after Securus/Hutcheson disclosure.[158]

---

in the *NAL* and confirmed in the Hutcheson Sentencing Memo. It at most asserts that there conceivably might have been legal authorizations associated with the specifically-identified Verizon customers, *see* NAL Response at 20 n.17, but does provide any reason to believe that Securus (let alone Verizon) could have or would have made that assessment before providing the location data.

[151] *See* Hutcheson Sentencing Memo at 3-4 (Hutcheson "uploaded legally defective search warrants that either did not authorize the acquisition of location data, were unsigned, or had no connection to the targeted phone user" and in "most of these instances . . . even notarized his own signature."); *see also NAL*, 35 FCC Rcd at 1709, para. 26.

[152] Among other things, Verizon argues that it would not have satisfied the willfulness requirement that is a prerequisite for a forfeiture under section 503(b) of the Act. *See* NAL Response at 28-29. Given that we do not impose a forfeiture for that conduct here, we need not address Verizon's arguments in that regard.

[153] *See* NAL Response at 29.

[154] NAL Response at 29-30 (citing 47 CFR § 64.2010(a)).

[155] 47 U.S.C. § 222(c)(1); 47 CFR § 64.2007(b).

[156] We note that Verizon does not contend that it literally would not have been possible to avoid the disclosures, so our interpretation does not demand the impossible of Verizon or any other carrier.

[157] *See NAL*, 35 FCC Rcd at 1717-21, paras. 58-73. Verizon disputes the relevance of the reasonableness of Verizon's procedures prior to the Securus and Hutcheson breaches, *see* NAL Response at 45 n.37, but Verizon neglects the fact that its post-breach procedures largely consist of those very same procedures, with only limited changes of potential relevance here.

[158] *See NAL*, 35 FCC Rcd at 1721-24, paras.74-82.

47. Verizon attempts to excuse its unreasonable practices by cataloging the steps it did take before and after the *New York Times* article. Verizon argues that, prior to the Securus disclosure, its efforts conformed to the CTIA Guidelines for ensuring customer consent to the use of location data.[159] Specifically, Verizon states that its safeguards included: "vetting and conducting ongoing monitoring of third-party program participants; limiting the sharing of information to certain, preapproved use cases; imposing information security requirements and adherence to industry best practices; reviewing notice and consent language; requiring production of consent records on a daily basis; and retaining Aegis to review those consent records, analyze program data to find any potential issues, and otherwise monitor the program."[160]

48. The safeguards that Verizon had in place before the Securus disclosure were not reasonable. The CTIA guidelines focus on best practices for notice and consent by location-based service providers—but they do not include best practices recommendations for carriers that sell access to their customers' location information to location-based service providers.[161] For example, they do not offer guidance to carriers on how to assure that location-based service providers comply with a contractual obligation to access location information only after furnishing proper notice and receiving customer consent (which was at issue here). Further, to enforce the safeguards Verizon did use, the Company's efforts "apparently mainly consisted of analysis of unverified vendor-created consent records,"[162] and we agree with the *NAL* regarding those efforts' shortcomings.[163] Although Verizon criticizes aspects of the analysis in the *NAL* and states that it also "used methods for discovering and addressing falsified transaction and consent records in connection with the location aggregator program that were *not* reliant only on the accuracy of what third parties submitted,"[164] we nonetheless conclude that the resulting measures employed were not reasonable. Critically, as explained in the *NAL*:

> The unauthorized service did not collect consents from Verizon's customers—just the opposite. When working as intended, Securus's unauthorized program collected electronic copies of legal process asserting a right to obtain location information *without the knowledge or consent of the Verizon customer*. A system allegedly designed to monitor customer consents but that is incapable of detecting its opposite is not a "reasonable measure" to detect unauthorized uses of or access to CPNI.[165]

Whatever risks Verizon's measures might have guarded against in other respects,[166] we conclude that measures with such a significant loophole are unreasonable under section 64.2010(a).

49. Given our finding of significant shortcomings in the measures Verizon employed, we reject Verizon's other criticisms of the analysis in the *NAL*. For one, Verizon seeks to characterize the

---

[159] *See* NAL Response at 54. To the extent that Verizon seeks to defend its actions by claiming that it attempted to ensure consumers provided opt-in consent, *see* NAL Response at 39-40, that aspiration is meaningful here only insofar as Verizon employed reasonable procedures to carry that out. Consistent with the *NAL*, and for the reasons explained below, we conclude that it did not.

[160] NAL Response at 46. The *NAL* also explained that the fact that Verizon provided access to "coarse" location data does not render its procedures reasonable. *NAL*, 35 FCC Rcd at 1720-21, para. 71. We agree with that assessment, which Verizon does not appear to dispute here.

[161] *See* CTIA, Best Practices and Guidelines for Location Based Services, https://www.ctia.org/the-wireless-industry/industry-commitments/best-practices-and-guidelines-for-location-based-services.

[162] *See NAL*, 35 FCC Rcd at 1721, para.72.

[163] *NAL*, 35 FCC Rcd at 1718-20, paras. 64-67.

[164] NAL Response at 47.

[165] *NAL*, 35 FCC Rcd at 1720, para. 70.

[166] *See* NAL Response at 48 (observing that "the NAL also expressly acknowledges instances in which Verizon's program safeguards identified and addressed other potential issues.").

Securus and Hutcheson breaches as outliers,[167] contending "[t]he fact that Verizon's safeguards evidently prevented any unauthorized access by any other program participant or any impact on any other customer demonstrates that those safeguards were both reasonable and effective."[168] Verizon also criticizes the Commission's consideration of an internal Verizon analysis of its safeguards in the *NAL*,[169] characterizing that internal analysis as having identified a merely theoretical risk "that program participants . . . could have submitted falsified location requests or consent records" while seeking to rely on the report's assertion that "'[i]t is unlikely any current program companies are performing fraudulent activities to obtain [Verizon] subscriber information without their consent due to the program management processes and oversight that is in place today.'"[170] Notably, however, Verizon's measures were not what identified the unauthorized disclosures in the case of Securus and Hutcheson. Thus, in the face of what we see as the failing in a fundamental aspect of Verizon's safeguards, we reject the theory that the reasonableness of those measures can be inferred from the fact that even more unauthorized disclosures have not been publicly identified.

50. Verizon also contends that the *NAL* misinterpreted information about what were merely preliminary results of the Aegis record reconciliation program, and that this misinterpretation led the Commission to question what those results signified for the effectiveness of Verizon's measures.[171] But the *NAL* made clear that it understood the relevant results flowed just from Aegis' "initial attempts to match the consent and access records," and recognized that, as an effort 'to track down how well the Location Aggregators were fulfilling their record-keeping obligations,'" it provided reason for concern.[172] Verizon's contention that Aegis ultimately could, with enough time and additional investigation, identify supporting consent records where it looked for them,[173] does not undermine the questions about the reliability of the LBS providers in following the contractual requirement—or of the strength of those contractual requirements—for ensuring that prior customer notice and consent was provided and obtained.[174] While Verizon's explanation makes the case that its measures did provide some protection as to some potential risks, viewed in its totality we nonetheless find Verizon's measures unreasonable for the reasons described here.

51. And to the extent that Verizon raises broader objections to the process for developing the record, particularly before the issuance of the *NAL*, those claims do not alter our analysis either.[175] Verizon had ample opportunity to present evidence and arguments in response to the *NAL*, and our conclusions here are based on what we know about the measures Verizon employed—not based on questions or uncertainty about how those safeguards operated.

52. Likewise, Verizon's safeguards after the Securus disclosure were also unreasonable. Verizon should have been keenly aware of the inadequacy of its safeguards after the May 2018 *New York Times* article. Nonetheless, Verizon did not and cannot demonstrate that its safeguards were made reasonable in the months that followed the 2018 *New York Times* article. In fact, rather than promptly

[167] *See* NAL Response at 48-50.

[168] NAL Response at 50.

[169] *See* NAL Response at 46-47.

[170] NAL Response at 47.

[171] *See* NAL Response at 48 n.39.

[172] *NAL*, 35 FCC Rcd at 1719-20, para. 68.

[173] *See* NAL Response at 15-16. In a small number of cases, Aegis relied on sampling rather than comprehensively looking for supporting consent records. *See* NAL Response at 16.

[174] *See, e.g.*, *NAL*, 35 FCC Rcd at 1719-20, para. 68 (noting that there could be significant variation in the initial results among different LBS providers and that Verizon itself looked to the results of Aegis' initial attempts to verify consent to identify whether there was cause for concern).

[175] *See* NAL Response at 26, 48 n.39.

implementing reasonable safeguards, Verizon continued to sell access to its customers' location information under (for all intents and purposes) the *same system* that was exploited by Securus and Hutcheson.[176]

53. We reject Verizon's attempt to dispute that the reports of the Securus and Hutcheson breaches should have made Verizon aware of the need for greater safeguards beyond cutting off Securus.[177] In particular, Verizon cites its theory that the location information is not CPNI and its view that the Securus/Hutcheson disclosures was a limited, outlier situation that did not raise broader questions about the efficacy of its safeguards.[178] As explained above, however, the location information is, in fact, CPNI.[179] And as explained earlier in this section, the Securus and Hutcheson breaches revealed fundamental shortcomings in Verizon's safeguards, rather than only demonstrating the sort of narrow, limited problems that Verizon claims. We therefore conclude that Verizon should have known of the inadequacies in its safeguards and the need for significant changes after the May 2018 *New York Times* article. Indeed, notwithstanding its arguments here, Verizon itself did, in fact, recognize the need to take steps in the wake of that article, ultimately including ending its location-based services initiative.[180]

54. Although Verizon explored implementing an enhanced direct notice and consent mechanism, this approach did not extend beyond the exploratory stage.[181] Likewise, Verizon touts the fact that after the May 2018 *New York Times* article "Verizon actually did decide within 30 days to terminate the program entirely," although it took a longer period of time to effectuate that decision.[182] But the mere fact that Verizon was working on possible alternative processes or had not-yet-implemented plans to end its location aggregator initiative is not sufficient to satisfy its obligation to "take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI."[183] Until the new measures actually are in place, or the initiative actually terminated, they cannot enable a carrier to "discover and protect against" the harms that are the target of that rule—and thus, they cannot be relied upon to satisfy that rule. Nor does the time and effort involved in Verizon's work on the exploratory processes or on terminating the location aggregator initiative render the procedures that remained in place in the meantime "reasonable" under that rule, given their glaring weaknesses.

55. We also are unpersuaded that the steps Verizon did take were reasonable. Verizon cut off 3CI and Securus and declined to allow access to location information for additional LBS providers and use cases,[184] but those actions did not improve the safeguards for consumers whose location information could be disclosed under the location data sharing arrangements that remained in place. Verizon also

[176] *See NAL*, 35 FCC Rcd at 1721, para.74.

[177] *See* NAL Response at 50-52.

[178] *See* NAL Response at 50-52.

[179] *See supra* section III.A.

[180] *See* NAL Response at 21-25.

[181] *See* NAL Response at 53.

[182] NAL Response at 51. Verizon argues that "the Commission never before set out specific requirements that a carrier must take in response to a third party's unauthorized access to location data, much less announced a hard-and-fast 30-day deadline by which any specific action must be taken." *Id*. at 8. The 30-day period cited in *NAL* was not a deadline but a grace period during which the Commission used its discretion and did not assess a fine. However, Verizon's existing data security practices were unreasonable both before and after the May 2018 article—the article merely exposed those unreasonable practices. As such, the Commission could have assessed a fine *for every single day* such unreasonable practices were in place (both before and after the Securus/Hutcheson disclosures)—the 30 days provided Verizon with a grace period to either end the program or reform its practices.

[183] 47 CFR § 64.2010(a).

[184] *See, e.g.*, NAL Response at 21, 24, 51.

contends that it had Aegis review the vetting procedures and data analytics used.[185] But the only changes Verizon claims actually were implemented were having Aegis "strengthen the transaction verification process to identify any anomalies in the data relating to consent requests that could indicate a potential issue, such as multiple location requests within a 24-hour period or an increase in location requests that were out of the ordinary for a particular LBS provider."[186] But nothing Verizon has said, nor anything in the record, gives the Commission any reason to believe that those particular measures were likely to have identified the problem that enabled the Securus and Hutcheson breaches in the first place. In particular, Verizon identified reasons why Aegis' regular auditing did not identify the Securus and Hutcheson breaches,[187] and we are not persuaded that the newly implemented measures would have remedied those shortcomings. Further, Verizon does not identify the timing of when those measures were implemented, and while other steps were considered the record does not reveal whether or when they ultimately were implemented at all. Thus after considering all of the data security measures that Verizon implemented in response to the Securus disclosure[188] we conclude that these measures were inadequate.

56. Verizon further argues that the Commission fails to appropriately account for the fact that many location-based services are "beneficial services that Verizon's customers affirmatively wanted."[189] We disagree. The issue here is not whether there are any beneficial services offered by LBS providers, but whether Verizon reasonably protected its customers' location information. In any event, because of the sensitive personal information involved, the benefits of LBS must be weighed against the risks; here, the risks were grave, particularly because Verizon did not have a reliable way of confirming customer consent. The Commission considered Verizon's arguments, but finds they are outweighed by these risks.

57. The *NAL* listed numerous steps that could have been taken to squarely address the proven vulnerability, up to and including deploying enhanced measures to verify consumer consent (even directly verifying consumer consent) and shutting down the LBS program.[190] Rather than taking definitive steps to remedy the obvious LBS program issues, Verizon instead took piecemeal steps. Moreover, the steps Verizon took did not rectify the systemic vulnerabilities at the heart of its LBS program—including relying on third parties to obtain customer consent for the disclosure of location information and failing to verify the validity of that consent.

58. Verizon's attempts to characterize the Commission as relying on an extreme strict liability-type approach fall short, as well.[191] We agree with Verizon that section 64.2010 of the Commission's rules requires only reasonable measures—not perfect ones—but that is not enough to help Verizon here.[192] Contrary to Verizon's suggestion, this is not a situation where the Commission is relying on 20/20 hindsight after a breach to find a violation of section 64.2010(a) of the rules based on any shortcoming in a carrier's measures, no matter how small, that results in a strict liability approach that is

[185] *See* NAL Response at 52-53; NAL Response, Exh. A, Brunner Supplemental Decl. at para. 11.

[186] NAL Response at 52.

[187] Verizon explained, for example, that Aegis' regular auditing "likely did not alert Aegis to a potential problem because: (i) Securus was using its profile for the approved use case to access location information for unauthorized purposes; (ii) nothing changed in the background check that Aegis maintained for Securus that would have prompted Aegis to question Securus's credibility about following approved use cases; (iii) the number of location requests from Securus was consistent with the number that Aegis would expect from it (i.e., there were no spikes in data to raise a red flag); and (iv) the number of impacted Verizon customers was so small (and apparently only within two relatively limited time spans)." NAL Response at 22 (emphasis in original).

[188] *See* NAL Response at 21-25, 50-54.

[189] NAL Response at 51.

[190] *See NAL*, 35 FCC Rcd at 1721-23, paras. 75-79.

[191] *See* NAL Response at 46, 48-50, 54-56.

[192] *See* NAL Response at 49, 54-55.

contrary to the reasonableness standard reflected in that rule.[193] Rather, we have carefully examined Verizon's procedures, including the fundamental flaw that while Verizon's "system allegedly designed to monitor customer consents [it was] incapable of detecting its opposite."[194] Our assessment under section 64.2010(a) thus is a straightforward evaluation of reasonableness, consistent with the text of the rule.

### 3. Verizon Bore the Burden of Production

59. As an initial matter, the Commission notes that for the reasons discussed above and the analysis contained in the *NAL*, the preponderance of the evidence shows that Verizon did not use reasonable safeguards throughout the period of the violation.[195] As such, while the *NAL* discussed Verizon's burden of production to demonstrate that its protection of customer CPNI was reasonable,[196] that burden-shifting is not necessary given the preponderance of the evidence. Nonetheless, even if unnecessary to prove Verizon's violations in this matter, the *NAL* properly shifted the burden of production to Verizon.

60. *First*, as the *NAL* explained[197] and consistent with the *2007 CPNI Order*, where there is evidence of an unauthorized disclosure, the Commission will infer from that evidence that a carrier's practices were unreasonable unless the carrier offers evidence demonstrating that its practices were reasonable.[198] In the *NAL*, the Commission found that Verizon failed to demonstrate that its safeguards were reasonable following the disclosure of Securus's unauthorized location-finding service in May 2018.[199]

61. Verizon acknowledges that the *NAL* based its approach on the *2007 CPNI Order*,[200] explaining that "where an unauthorized disclosure has occurred . . . the responsible carrier then shoulders the burden of proving the reasonableness of its measures to protect consumer data."[201] However, Verizon is incorrect when it asserts that the *2007 CPNI Order* cannot support the burden-shifting approach in cases outside of the pretexting context.[202] The *2007 CPNI Order* afforded adequate notice of the application of burden-shifting in this case. The order did not expressly limit burden-shifting to the pretexting context, instead applying more broadly to unauthorized disclosures of CPNI. The rationale applies with equal force to the kind of disclosure at issue here, where a fundamental issue is whether Verizon had reasonable measures to ensure that its customers had in fact consented to the disclosure of their CPNI. Indeed, the breach in the instant case is analogous to pretexting in that it involved fraud in order to obtain access to CPNI.[203] Broadly, in relation to Securus's entire unauthorized location-finding

---

[193] *See* NAL Response at 54-55.

[194] *NAL*, 35 FCC Rcd at 1720, para. 70.

[195] *See NAL*, 35 FCC Rcd at 1717-24, paras.58-82.

[196] *See NAL*, 35 FCC Rcd at 1701-02, 1717, 1722, paras.8, 59, 60, 76.

[197] *See NAL*, 35 FCC Rcd at 1701-02, para. 8.

[198] *See 2007 CPNI Order*, 22 FCC Rcd at 6959, para. 63 (noting that where there is evidence of an unauthorized disclosure, the Commission "will infer . . . that the carrier did not sufficiently protect that customer's CPNI" and that "[a] carrier then must demonstrate that the steps it has taken to protect CPNI from unauthorized disclosure, including the carrier's policies and procedures, are reasonable in light of the threat posed by pretexting and the sensitivity of the customer information at issue").

[199] *See NAL*, 35 FCC Rcd at 1717-24, paras. 58-82.

[200] *See* NAL Response at 43 (citing *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 (2007) (*2007 CPNI Order*)).

[201] *NAL*, 35 FCC Rcd at 1717, para. 59.

[202] *See* NAL Response at 43.

[203] The breach at issue here arguably falls within the letter of criminal pretexting. *See* 18 U.S.C. § 1039.

service, Securus used the pretext that it was requesting location information from Verizon for its approved use case and that it had explicit customer opt-in consent for the disclosure. Likewise, Hutcheson used the pretext that he had legal authorization or consumer consent when requesting location information from Securus.[204] Therefore, applying the burden-shifting to this case is appropriate even to the extent that the disclosures here could be said not to have been pretexting of the same form described in the *2007 CPNI Order*.

62. *Second*, Verizon admits that an evidentiary presumption is valid if the circumstances (here, a breach of CPNI) giving rise to that presumption make it "more likely than not" that the presumed fact (here, that CPNI safeguards were unreasonable) exists.[205] The Commission finds that the unauthorized disclosure in this case gave rise to a rebuttable presumption that Verizon did not reasonably protect customer location information from unlawful access.[206] As already discussed, the entire Securus location-finding program was based upon unauthorized disclosures. Though the disclosures to Hutcheson were particularly egregious (given they were essentially doubly unauthorized), *all* of the Securus requests made under the false guise of the approved use case and Verizon's resultant disclosures of consumer location information were unauthorized. Verizon's existing safeguards and oversight failed to notice and (absent the *New York Times* article) may have never realized that the unauthorized Securus location-finding program existed. Nonetheless, Verizon argues that the Commission cannot use the Securus and Hutcheson breaches to support shifting the burden of production to Verizon to provide evidence of the reasonableness of their post-May 2018 security practices.[207] Specifically, Verizon asserts that because no provider can achieve perfection, "a single unauthorized disclosure of CPNI is a manifestly poor predictor of the reasonableness of a carrier's measures to safeguard CPNI," thus undercutting the reasonableness of any burden shifting here.[208] We disagree.

63. In the *NAL*, we found that Verizon apparently violated section 222(c) of the Act and section 64.2007(b) of our rules in connection with its unauthorized disclosures of CPNI to Hutcheson.[209] This is further bolstered by the Department of Justice's case against Hutcheson.[210] And though the Commission opted to admonish Verizon only for the unauthorized disclosures made to Hutcheson, it would have been appropriate to admonish Verizon for all the disclosures it made to Securus in relation to the unauthorized location-finding service. In the *NAL*, we clearly explained that, pursuant to section 217 of the Act,[211] carriers cannot disclaim their obligations to protect customer CPNI by delegating those

[204] As explained in the *NAL*, "Hutcheson submitted thousands of unauthorized location requests via the Securus service between 2014 and 2017, in some cases 'upload[ing] entirely irrelevant documents including his health insurance policy, his auto insurance policy, and pages selected from Sheriff training manuals" in lieu of genuine legal process.'" *NAL*, 35 FCC Rcd at 1709, para. 26; *see also supra* para. 14 (citing Hutcheson Sentencing Memo).

[205] See NAL Response at 42.

[206] *See 2007 CPNI Order*, 22 FCC Rcd at 6929, 6959, paras. 3, 63. A presumption is only permissible if there is "a sound and rational connection between the proved and inferred facts," and when "proof of one fact renders the existence of another fact so probable that it is sensible and timesaving to assume the truth of [the inferred] fact . . . until the adversary disproves it." *Chemical Mfrs. Ass'n v. Department of Transp.,* 105 F.3d 702, 705 (D.C. Cir. 1997) (quoting *NLRB v. Curtin Matheson Scientific, Inc.,* 494 U.S. 775, 788-89 (1990)) (internal citation and quotation marks removed).

[207] *See* NAL Response at 42-44.

[208] NAL Response at 43.

[209] *See NAL*, 35 FCC Rcd at 1714, para. 49. "The evidence reflects that Hutcheson used the Securus service to obtain the location information of Verizon customers. Verizon shared the information with LocationSmart, which the shared it with 3Cinteractive, which then shared it with Securus . . . ." *Id*. at 1714, para. 50.

[210] *See, e.g.*, Hutcheson Sentencing Memo.

[211] 47 U.S.C. § 217.

obligations to third parties.[212] In its NAL Response, Verizon does not dispute that a "third-party LBS provider in the location aggregator program breached its contractual obligations and—without Verizon's knowledge or approval—apparently shared Verizon customer location data with an unauthorized party for an unauthorized purpose" in providing location data to Hutcheson.[213] We reiterate here that "Verizon is not absolved from liability simply because it was not directly responsible for operating the programs under which unauthorized disclosures occurred."[214] Further, section 222(c)(1) of the Act[215] makes the responsibility for avoiding unauthorized disclosures a carrier obligation and prohibits use and disclosure except in certain narrow circumstances, without any reasonableness criterion. Verizon should, therefore, be able to justify any unauthorized disclosure. Given that multiple breaches occurred here and that the "reasonable measures" obligation is a *continuing* obligation, the Commission's application of an evidentiary presumption based upon the disclosures involving Hutcheson and the imposition of a burden to produce evidence of reasonable protections during the relevant violations period was reasonable—particularly because, as discussed, those safeguards did not materially change in the interim timeframe.

64. *Third*, Verizon misinterprets the *NAL* when it argues that the Commission improperly shifted the burden of persuasion to the Company.[216] To the contrary, the Commission properly (and consistent with APA precedent) shifted only the burden of *production*, and not the burden of *persuasion*, to Verizon. The unauthorized disclosure at issue gave rise to a rebuttable presumption that Verizon did not adequately protect customer information from unlawful access. The burden of production then shifted to Verizon to offer evidence that it had reasonable safeguards in place.

65. Rather than taking reasonable steps to safeguard its customers' location information after the Securus/Hutcheson disclosures were reported,[217] Verizon placed its customers' location information at continuing risk of unauthorized access through its failure to terminate its program or impose reasonable safeguards to protect its customers' location information. For these reasons, we conclude that Verizon failed in its obligation under section 222 and our rules to have reasonable measures in place to discover and protect against attempts to gain unauthorized access to its customers' CPNI.

### D. The Forfeiture Amount is Lawful and Consistent with FCC Precedent

66. After considering the evidence in the record, the relevant statutory factors, the Commission's *Forfeiture Policy Statement*, and the arguments advanced by Verizon in the NAL Response, we find that Verizon is liable for a total forfeiture of $46,901,250 for its violations of section

---

[212] *See NAL*, 35 FCC Rcd at 1702, para. 9. Under section 217, "the act, omission, or failure of any officer, agent, or other person acting for or employed by any common carrier or user, acting within the scope of his employment, shall in every case be also deemed to be the act, omission, or failure of such carrier or user as well as that of the person." 47 U.S.C § 217.

[213] *See* NAL Response at 18. Verizon argues that Hutcheson's unauthorized location lookups, which they concede apparently violated Securus's legal obligations including safeguarding its customers' CPNI, did not violate the Act or the Commission's rules insofar as the information was shared as required by law under section 222(c)(1). *Id.* at 20 n.17. We find Verizon's argument unavailing. Although Verizon speculates that some of the lookups may have had a law enforcement basis, those lookups were certainly not submitted through the appropriate channels for law enforcement requests, and Verizon cannot now claim that they were "required by law" when it did not treat them as such in the first place. Further, as explained in the *NAL*, "Securus did not . . . assess the adequacy of the purported legal authorizations submitted by users of its location-finding service." *NAL*, 35 FCC Rcd at 1708, para.25.

[214] *See NAL*, 35 FCC Rcd at 1715, para.52; *see also id*. at 1716, para. 54 n.145 (explaining that where a carrier makes disclosures to a third party where the third party is not acting on behalf of the carrier to fulfill the relevant responsibilities of the carrier under section 222, the carrier's disclosure of CPNI to the third party would be unauthorized in violation of section 222(c)(1)).

[215] 47 U.S.C. § 222(c)(1).

[216] *See* NAL Response at 40-42.

[217] Many of the possible reasonable steps were enumerated in the *NAL*. *See NAL*, 35 FCC Rcd at 1721-23, paras. 75-79.

222 of the Act and section 64.2010 of the Commission's rules—a reduction of $1,417,500 from the $48,318,750 forfeiture proposed in the *NAL*.[218] As explained in the *NAL*, this figure resulted from applying a base forfeiture of $40,000 for the first day of each such violation and a $2,500 forfeiture for the second and each successive day the violations continued (excluding the 30-day grace period granted by the Commission).[219] The Commission found in the *NAL* that Verizon apparently engaged in 65 continuing violations—one for each ongoing relationship with a third-party LBS provider or aggregator that had access to Verizon customer location information more than 30 days after publication of the *New York Times* report—and that each violation continued until Verizon terminated the corresponding entity's access to customer location information.[220] Using this methodology, the Commission found Verizon apparently liable for a total base forfeiture of $32,215,500. Upon considering the nature of the violations and the risk of harm they posed to consumers, the Commission then applied a 50% upward adjustment to the base forfeiture amount, resulting in a total proposed forfeiture of $48,318,750.[221]

67. Verizon challenges these forfeiture calculations with five principal arguments. *First*, Verizon asserts that it did not engage in any "willful" violations and suggests that any forfeiture penalty should take such non-willfulness into account.[222] *Second*, Verizon claims that it would be arbitrary and capricious to impose a forfeiture under section 222 when there had been no unauthorized disclosures during the limitation period.[223] *Third*, Verizon argues that the *NAL* describes at most a single continuing violation, not a separate violation for each of the 65 entities participating in Verizon's LBS program. As such, according to Verizon, the forfeiture exceeds the applicable statutory maximum.[224] *Fourth*, Verizon argues that even if the Commission could calculate the forfeiture based upon the number of LBS providers and how long they had access to customer location information, the proposed forfeiture relies upon incorrect facts and therefore is calculated incorrectly. Specifically, Verizon states that a number of LBS program participants ceased accessing Verizon customer location information before the dates identified in the *NAL*, and two of them never actually participated in the program in the first place.[225] *Fifth* and finally, Verizon challenges the Commission's application of a 50% upward adjustment to the base forfeiture, claiming both that it rests upon a misunderstanding of an internal Verizon document and that it impermissibly cites to the same factors used for determining the base forfeiture amount.[226]

68. As we discuss below, to account for the non-participation in Verizon's LBS program of two entities that were included in the original forfeiture calculation, we reduce the forfeiture proposed in the *NAL* by $1,417,500. However, we are not persuaded by any of Verizon's other arguments and decline to cancel or further reduce the forfeiture proposed in the *NAL*.

### 1. Verizon Willfully Violated the Act and the Commission's Rules

69. According to Verizon, the *NAL* does not establish that it engaged in "willful" violations of section 222 and the Commission's rules. Verizon asserts that because it took steps to safeguards its customers' information and "did not consciously or deliberately fail to act to protect CPNI," it cannot be

[218] Any entity that is a "Small Business Concern" as defined in the Small Business Act (Pub. L. 85-536, as amended) may avail itself of rights set forth in that Act, including rights set forth in 15 U.S.C. § 657, "Oversight of Regulatory Enforcement," in addition to other rights set forth herein.

[219] *NAL*, 35 FCC Rcd at 1726, para. 86.

[220] *NAL*, 35 FCC Rcd at 1726, para. 87.

[221] *NAL*, 35 FCC Rcd at 1727-28, paras. 90-93.

[222] NAL Response at 56.

[223] NAL Response at 56-57.

[224] NAL Response at 57-58.

[225] NAL Response at 57-58.

[226] NAL Response at 57-58.

said to have "willfully" violated any requirement.[227] Thus, Verizon maintains, the *NAL* in actuality bases the penalty on section 503(b)'s "repeated" prong, and any forfeiture should reflect that.

70. These arguments lack merit. The term "willful," as used in section 503(b) of the Act, does not have the restrictive meaning that Verizon would assign to it. As the Commission has previously stated:

> . . . the word "willfully", as employed in Section 503(b), does not require a showing that the [party] knew he was acting wrongfully; it requires only that the Commission establish that the licensee knew that he was doing the acts in question – in short, that the acts were not accidental (such as brushing against a power knob or switch).[228]

71. Verizon's invocation of *Telrite*, which provides that a violation is "willful" if it involves "'the conscious and deliberate commission or omission of [any] act, irrespective of any intent to violate' the law,"[229] does not persuade us otherwise. As *Telrite* provides, the issue is not whether Verizon *intended* to violate the law, but whether it deliberately engaged in the acts or omissions that the Commission found to have constituted an apparent violation of the law. Verizon does not dispute that it designed, implemented, and operated its LBS program or that it is responsible for that program's structure and performance. Therefore, because the Commission found that the safeguards that Verizon had in place for customer location information—as consciously and deliberately implemented by Verizon—did not meet the requirements of section 222 of the Act and section 64.2010 of the Commission's rules, then Verizon "willfully" violated those provisions.

72. Furthermore, as Verizon acknowledges, section 503(b) applies when a carrier "willfully *or* repeatedly" fails to comply with an applicable requirement,[230] and does not require that both prongs of the clause be met. Thus, even if Verizon had not engaged in "willful" violations, a forfeiture penalty under section 503(b) still would be appropriate. But, as discussed, Verizon's failure to have reasonable protections in place for customer location information was "willful" for purposes of section 503. And, by continuing to operate its LBS program in the absence of reasonable safeguards, Verizon both willfully and repeatedly[231] violated section 222 of the Act and section 64.2010 of the Commission's rules.

#### 2. The Commission Did Not Need to Find Unauthorized Access to CPNI During the Limitations Period

73. Verizon challenges as arbitrary and capricious the imposition of a forfeiture penalty for when there has been no "actionable unauthorized disclosure" and claims that, at a minimum, the Commission should have taken this into account when setting the base forfeiture.[232] Verizon also contends that the base forfeiture amounts of $40,000 for the first day of a violation and $2,500 for the second and each successive day that the violation continued are so excessive as to be arbitrary and

---

[227] NAL Response at 56.

[228] *Midwest Radio-Television Inc., Memorandum Opinion and Order*, 40 F.C.C. 163, 167, para. 11 (1963). *See also Playa Del Sol Broadcasters*, Order on Review, 28 FCC Rcd 2666, 2667-68, paras. 4, 6 (2013); *USA Teleport, Inc*., Memorandum Opinion and Order, 26 FCC Rcd 6431, 6434, para. 9 (EB 2011).

[229] NAL Response at 28 (citing *Telrite Corp.*, Notice of Apparent Liability for Forfeiture & Order, 23 FCC Rcd 7231, para. 12 (2008) (quoting 47 U.S.C. § 312(f)(1)) (alteration in original)).

[230] 47 U.S.C. § 503(b)(1)(B) (emphasis added).

[231] For the purposes of section 503, "repeated" only requires that a party acted (or failed to act) more than once or, if the act or failure to act is continuous, for more than one day. *See, e.g., Playa Del Sol Broadcasters*, Order on Review, 28 FCC Rcd 2666, 2668, para. 4 (2013).

[232] NAL Response at 56-57.

capricious given that, among other considerations, no unauthorized disclosure occurred during the limitations period.[233]

74. We reject this argument. The forfeiture here is based not upon any unauthorized disclosures (which, in the case of Hutcheson, occurred outside the limitations period) but rests upon Verizon's subsequent conduct—namely, how "[a]fter learning of Hutcheson's practices, Verizon placed its customers' location information at continuing risk of unauthorized access through its failure to expeditiously terminate its program or impose reasonable safeguards to protect its customers' location information."[234]

75. Moreover, with respect to the specific amounts chosen for the base forfeiture, these figures were neither excessive nor arbitrary and capricious, but reflected the Commission's careful consideration of the relevant statutory factors. Section 503 of the Act requires the Commission to ". . . take into account the nature, circumstances, extent, and gravity of the violation and, with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other matters as justice may require."[235] The plain language of the statute provides the Commission with broad discretion to assess proposed penalties based on the statutory factors, up to the statutory maximum.

76. In selecting the base forfeitures that it did, the Commission explained that the chosen amounts "(1) . . . provide a meaningful distinction between the violations in this case and those of other cases involving less egregious facts; and (2) . . . provide consistency with other consumer protection cases involving serious harm to consumers."[236] The Commission also found that "this base forfeiture appropriately deters wrongful conduct and reflects the increased risk consumers face when their information is not secured in a timely manner."[237] Given the broad discretion afforded to the Commission under section 503, as well as the *NAL*'s examination of how the relevant statutory factors intersected with the facts of this case, we reject Verizon's claim that the Commission acted arbitrarily or capriciously in setting the base forfeiture amount.

### 3. The Commission Reasonably Found that Verizon Engaged in 65 Continuing Violations

77. Section 503(b) of the Act authorizes the Commission to impose a forfeiture against Verizon of up to $204,892 for each day of a continuing violation, up to a statutory maximum of $2,048,915 "for any single act or failure to act."[238] The Commission found that, because Verizon permitted 65 separate entities to access its customers' location information in the apparent absence of reasonable safeguards, the Company engaged in 65 continuing violations of section 222 of the Act and section 64.2010 of the Commission's rules. Verizon challenges this methodology, arguing that "[e]ither Verizon took reasonable measures with respect to the location aggregator program, or it did not," and contends that "the number of entities is irrelevant to that analysis."[239] Verizon therefore asserts that there could have been at most one continuing violation (subject to the $2,048,915 penalty cap) and the *NAL*'s

[233] NAL Response at 56-57.

[234] *NAL*, 35 FCC Rcd at 1724, para. 82.

[235] 47 U.S.C. § 503(b).

[236] *NAL*, 35 FCC Rcd at 1726, para. 86.

[237] *NAL*, 35 FCC Rcd at 1726, para. 86.

[238] *See* 47 U.S.C. § 503(b)(2)(B); 47 CFR § 1.80(b)(2). These amounts reflect inflation adjustments to the forfeitures specified in section 503(b)(2)(B) ($100,000 per violation or per day of a continuing violation and $1,000,000 per any single act or failure to act). *See Amendment of Section 1.80(b) of the Commission's Rules, Adjustment of Civil Monetary Penalties to Reflect Inflation*, Order, DA 19-1325 (EB 2019).

[239] NAL Response at 57.

finding of 65 separate continuing violations (one for each LBS provider or Aggregator) constitutes an impermissible attempt to circumvent the statutory maximum.[240]

78. We reject this argument. Neither section 503(b) nor the forfeiture guidelines in section 1.80 of the Commission's rules speak to the application of the phrase "single act or failure to act," or otherwise to the calculation of the number of violations, in the CPNI or data security context.[241] Moreover, in calculating a proposed penalty under section 222, the Commission previously applied a methodology under which a systemic failure to protect customer information constituted significantly more than a single violation. In *TerraCom*, the Commission stated that "[e]ach document containing [proprietary information] that the Companies failed to protect constitutes a separate violation for which a forfeiture may be assessed."[242] The Commission further observed that "[e]ach unprotected document constitutes a continuing violation that occurred on each of the 81 days [until] the date that the Companies remedied the failure . . . ."[243]

79. The Commission in *TerraCom* elected to ground its forfeiture calculation in the number of unprotected documents (which it "conservatively estimate[ed]" as more than 300,000),[244] but that approach was not mandated under section 503, section 222, or the Commission's rules. Similarly, in this case, the Commission reasonably exercised its authority to find that each unique relationship between Verizon and an LBS provider or aggregator represented a distinct failure to reasonably protect customer CPNI and therefore a separate violation of section 222 of the Act and section 64.2010 of the Commission's rules. Each such relationship relied upon a distinct and unique contractual chain (from Verizon to the Aggregator, then from the Aggregator to the LBS provider) and was premised to involve a specific, individually-approved "Use Case" that had been reviewed and authorized by Verizon. Treating these separate channels for the disclosure of location information—each of which, although unique, suffered from the same fundamental vulnerabilities discussed in the *NAL* and above—as separate violations was thus rational and properly within the Commission's discretion.

80. The approach taken in the *NAL* was not only reasonable, it was—contrary to Verizon's claim that it exceeded the statutory maximum—eminently *conservative*. As described in the *NAL*, Verizon's practices placed the sensitive location information of *all* of its customers at unreasonable risk of unauthorized disclosure. As such, the Commission could well have chosen to look to the total number of Verizon subscribers when determining the number of violations (and under that analysis, the violations presumably would have continued until the very last LBS provider's access to customer location information was cut off).[245] Using that methodology—and taking into account the tens of millions of consumers whose highly sensitive location information was made vulnerable by Verizon—would have resulted in a significantly higher forfeiture than what was proposed in the *NAL*.

81. Furthermore, even under the framework applied in the *NAL*, the Commission could have calculated the proposed forfeiture based upon every single entity with access to Verizon customer location information up to the statutory maximum ($204,892 per day up to $2,048,915 for each and every

[240] NAL Response at 58.

[241] 47 U.S.C. § 503(b); 47 CFR § 1.80(b).

[242] *TerraCom*, 29 FCC Rcd at 13343, para. 50.

[243] *TerraCom*, 29 FCC Rcd at 13343, para. 50.

[244] *TerraCom*, 29 FCC Rcd at 13343, para. 52. The Commission's investigation into apparent violations of consumer privacy requirements in *TerraCom* was resolved by a consent decree in which the companies admitted to violating sections 201(b) and 222(a) of the Act. *See TerraCom, Inc. and YourTel America, Inc.*, Order and Consent Decree, 30 FCC Rcd 7075, 7084, at para. 20 (EB 2015).

[245] Although it involved a data breach—and not, as in this case, an ongoing failure to maintain reasonable safeguards such that customer data was placed at unreasonable risk of unauthorized disclosure—*TerraCom* supports applying a customer-centric forfeiture calculation that takes into account the number of customers whose data was inadequately protected. *See TerraCom*, 29 FCC Rcd at 13343, para. 50.

LBS provider). That would have resulted in a far higher fine than the approach that was taken (applying a $40,000 forfeiture for the first day of the violation and a $2,500 forfeiture for each successive day the violation continued). Instead, the Commission took a conservative approach, giving Verizon a 30-day grace period with no fines assessed, limiting the number of continuing violations to every day that each related LBS provider operated in the apparent absence of reasonable measures to protect CPNI and therefore left Verizon customers' CPNI vulnerable to unlawful disclosure, and assessing a far lower fine per day for the continuing violations than it could have. This approach recognized the Commission's need to show that such violations are serious and ensured the proposed forfeiture amounts act as a powerful deterrent for future failures to reasonably protect CPNI.

82. We also reject any claim that Verizon's due process rights were violated because it lacked fair notice that its LBS practices would potentially make it liable for a penalty in excess of the $2,048,915 statutory maximum for a single continuing violation. Consistent with our earlier discussion of Verizon's fair notice claims,[246] we find that this argument lacks merit. Customer location information is CPNI that is subject to protection under section 222 of the Act and section 64.2010 of the Commission's rules. Verizon knew, or should have known, that failing to reasonably protect CPNI carries with it significant potential penalties that may be associated with more than one violation. Indeed, the Commission has in the past proposed penalties for what could be viewed as a system-wide violation on a more granular basis that would yield higher penalties that would result from treating the violation as a single continuing violation.[247] Independently, we observe that the penalties at issue here are governed by section 503 of the Act, with which we fully comply in our decision.[248] As the D.C. Circuit has recognized, where a statute specifies maximum penalties, the statute itself provides fair notice of all penalties within that limit.[249]

#### 4. The Commission Will Reduce the Forfeiture Amount by $1,417,500

83. Verizon asserts that even if the Commission's forfeiture methodology is permissible, the calculations in the *NAL* are based on incorrect facts. Specifically, for the 65 entities whose ongoing access to customer location information factored into the forfeiture amount, the *NAL* cites two separate termination dates (one for 60 of the entities and the other for the remaining 5).[250] According to Verizon, "a number of those third parties actually ceased accessing any location information before those dates."[251] Verizon's claim is supported by a Declaration and Exhibit that purport to show the "Date of Last Location Access/Request" for each LBS entity, a number of which fall upon dates prior to those listed in the *NAL*.[252]

84. We are not persuaded that this merits a reduction in the forfeiture amount. The calculations in the *NAL* were not based on when Verizon actually transmitted customer location information to particular LBS providers. Rather, it was those entities' *ability* to access location information at the time of their choosing, and in the apparent absence of reasonable safeguards, that the forfeiture calculation was based upon. The fact that certain providers may not have exercised that ability (which they retained until the termination dates set forth in the *NAL*) does not affect our analysis.

---

[246] *See supra* 22.

[247] *See, e.g.*, *TerraCom*, 29 FCC Rcd at 13343, paras. 51-52.

[248] 47 U.S.C. § 503.

[249] *Pharon v. Bd. of Gov. of the Fed. Reserve*, 135 F.3d 148, 157 (D.C. Cir. 1998) (applying *BMW of North Am. v. Gore*, 517 U.S. 559 (1996), to a penalty assessed by the Board and concluding that the relevant statutory maximum penalty provisions provided adequate notice).

[250] *NAL*, 35 FCC Rcd at 1726, para. 86.

[251] NAL Response at 58.

[252] NAL Response, Exhibits A and D.

85. Verizon also contends that two of the entities whose participation in the LBS program factored into the forfeiture calculation "never actually participated in the program in the first place."[253] Verizon explains that "[t]wo of the entities identified in VZ's LOI Responses . . . applied to and were approved for participation in the Verizon location aggregator program and, therefore, were included on customer / participant lists, but did not fully integrate to the location platform and never received any subscriber location data in connection with the program."[254]

86. In developing the *NAL*, the Commission relied upon the information furnished to it by Verizon, including a listing of LBS program participants, and reasonably expected that information to be accurate and complete. Nonetheless, in light of the additional details provided by Verizon in the NAL Response, we now exercise our discretion to reduce the forfeiture amount to reflect the fact that two of the 65 entities cited in the *NAL* did not actually participate in the program (and therefore did not have access to customer location information). The *NAL* assigned a base forfeiture of $472,500 for each of those two entities ($40,000 for the first day of the continuing violation and $2,500 for each of the subsequent 173 days, or $40,000 plus $432,500, totaling $472,500). The combined base forfeiture for the two providers is therefore $945,000. The *NAL* applied a 50% upward adjustment to that amount, or an additional $472,500, for a total associated forfeiture of $1,417,500. Accordingly, we now reduce the total forfeiture proposed in the NAL by $1,417,500.

### 5. The Upward Adjustment is Permissible and Warranted

87. Verizon argues that the Commission impermissibly based the 50% upward adjustment to the forfeiture amount proposed in the *NAL* on the same factors that were considered in setting the base forfeiture.[255] Verizon also contends that, in determining the amount of the upward adjustment, the Commission misconstrued the significance of an internal Verizon document and the record-matching reports provided by Aegis and erred in describing the severity of the risk that Verizon's LBS program posed to the Company's customers.[256]

88. We reject these arguments and maintain the 50% upward adjustment proposed in the *NAL*. With regard to the upward adjustment, section 503 of the Act requires the Commission to ". . . take into account the nature, circumstances, extent, and gravity of the violation and, with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other matters as justice may require."[257] The plain language of the statute provides the Commission with broad discretion to assess proposed penalties based on the statutory factors, up to the statutory maximum. Moreover, section 1.80 of the Commission's rules provides a list of possible factors the Commission may use when making a determination to adjust upward or adjust downward the base forfeiture.[258] These factors include, importantly, "egregious misconduct," "substantial harm," "repeated or continuous violation," and "ability to pay/relative disincentive," among others.[259]

89. The Commission weighed these factors when making the determination that the base forfeiture in this case merited a substantial upward adjustment. Verizon's conduct was egregious; the *NAL* detailed how Verizon failed to respond to indications that its consent record audit process, as well as

[253] NAL Response at 58.

[254] NAL Response, Exhibit D, n. 5.

[255] NAL Response at 59.

[256] NAL Response at 58-59.

[257] 47 U.S.C. § 503(b).

[258] 47 CFR § 1.80(b)(10), Table 3.

[259] *Id.*

its overall system for obtaining customer consent for the disclosure of location information, was faulty.[260] Further, revelations in the press about Securus' hidden location information program led to a public outcry and prompted inquiries from members of Congress concerned about carriers' apparent lack of control over highly sensitive location information.[261] Its failure to adequately protect CPNI for a protracted amount of time caused substantial harm by making it possible for "malicious persons to identify the exact locations of Verizon subscribers who belong to law enforcement, military, government, or other highly sensitive positions—thereby threatening national security and public safety"—a threat illustrated by reports that Hutcheson used location information to obtain the precise location of multiple Missouri State Highway Patrol officers on numerous occasions.[262] The violations were continuous over an extended period of time and repeated with two Aggregators and multiple LBS providers. Finally, the Commission took into account Verizon's status as a major telecommunications provider to determine what penalty, when applied, would adequately provide Verizon with the necessary disincentive to engage in similar conduct again in the future. These considerations, taken into account as the Commission lawfully exercised its statutory authority to weigh the relevant factors, justify the resulting upward adjustment. Verizon's arguments to the contrary do not defeat Congress's decision to grant the FCC the power to weigh the factors and make such adjustments "as justice may require."[263] Nor do Verizon's arguments persuade us that the 50% upward adjustment, which is in line with upward adjustments in other cases involving consumer harms,[264] was unwarranted.

### E. Section 503(b) Is Employed Here Consistent With the Constitution

90. We reject Verizon's supplemental constitutional objections that: (1) the FCC combines investigatory, prosecutorial, and adjudicative roles in violation of constitutional due process

---

[260] For the reasons discussed earlier, we reject Verizon's claim that the Commission drew the wrong conclusions from the Aegis audit and consent-matching materials discussed in the NAL. *See supra* III.C.1-2.

[261] *See e.g.*, Letter from Sen. Ronald L. Wyden, Senator, U.S Senate, et al., to Joseph J. Simons, Chairman, Federal Trade Commission, and Ajit Pai, Chairman, Federal Communications Commission (Jan. 24, 2019) (on file in EB-TCD-18-00027704) (this Congressional was signed by 15 United States senators); Letter from Rep. Frank J. Pallone, Jr., Chairman, U.S. House of Representatives Committee on Energy and Commerce, to Ajit Pai, Chairman, Federal Communications Commission (Jan. 11. 2019) (on file in EB-TCD-18-00027704); Maria Dinzeo, *Class Claims AT&T Sold Their Real-Time Locations to Bounty Hunters*, Courthouse News Service (July 16, 2019), https://www.courthousenews.com/class-claims-att-sold-their-real-time-locations-to-bounty-hunters/; Brian Barrett, *A Location-Sharing Disaster Shows How Exposed You Really Are*, Wired (May 19, 2018), https://www.wired.com/story/locationsmart-securus-location-data-privacy/; Press Release, New America's Open Technology Institute, *Privacy Advocates Call on FCC to Hold Wireless Carriers Accountable for Selling Customer Location Information to Third Parties Without Consent* (June 14, 2019), https://www.newamerica.org/oti/press-releases/privacy-advocates-call-fcc-hold-wireless-carriers-accountable-selling-customer-location-information-third-parties-without-consent/ (announcing that New America's Open Technology Institute, the Center on Privacy & Technology at Georgetown Law, and Free Press had filed a complaint with the FCC regarding the sale and disclosure of customer location information by Verizon, AT&T, T-Mobile, and Sprint).

[262] *NAL*, 35 FCC Rcd at 1728, para. 91. Verizon argues that it was not possible under its LBS program for a third party to identify customers' "exact locations." NAL Response at 59. We do not intend to quibble over the precision of the location-finding that Verizon's program had enabled. There is no question that it allowed for determining the location of law enforcement personnel, including whether they were in a certain area or vicinity. It is not difficult to imagine how this capability is susceptible to abuse.

[263] 47 U.S.C. § 503(b).

[264] *See, e.g., Scott Rhodes,* Forfeiture Order, 36 FCC Rcd 705, 728, at para. 54 (2021) (upward adjustment equaling 100% of base forfeiture amount on robocaller/spoofer who made targeted robocalls designed to harass victims); *John C. Spiller, et al.,* Forfeiture Order, 36 FCC Rcd 6225, 6257, at para. 59 (2021) (upward adjustment equaling 50% of base forfeiture amount imposed on robocaller who engaged in illegal spoofing for robocall telemarketing activities); *Adrian Abramovich*, Forfeiture Order, 33 FCC Rcd 4663, 4671, at para. 25, 4674, at para. 33 (2018) (upward adjustment equaling 50% of base forfeiture amount imposed on robocaller who engaged in illegal spoofing for robocall telemarketing activities).

requirements;[265] (2) the issuance of a forfeiture order by the Commission would violate Article III and the Seventh Amendment;[266] and (3) the Commission's ability to choose a procedural approach to enforcement under section 503(b) of the Act is an unconstitutional delegation of legislative power.[267] Verizon's arguments are premised on misunderstandings regarding the relevant statutory framework, the nature of the Commission's actions, and relevant precedent.

91. As a threshold matter, Verizon neglects key aspects of the statutorily-mandated enforcement process applicable here. Pursuant to section 504 of the Act, after the Commission issues a forfeiture order, Verizon is entitled to a trial *de novo* in federal district court before it can be required to pay the forfeiture.[268] Verizon's objection to the combination of investigatory, prosecutorial, and adjudicative roles in the FCC ignores that statutory entitlement to a trial *de novo* in federal district court to ultimately adjudicate its obligation to pay a forfeiture.[269] Likewise, Verizon's claim that a forfeiture order issued under section 503(b) of the Act does not provide it a decision by an Article III court, including via a trial by jury, ignores Verizon's statutory right to a trial *de novo* before it can be required to pay the forfeiture.[270] The statutory right to a trial *de novo* provided for by section 504 of the Act is itself sufficient grounds to reject those two constitutional claims.

92. Independently, there are sufficient grounds to reject Verizon's arguments for other reasons, as well. We discuss each of these in turn below.

93. *Combination of Functions.* With respect to Verizon's claimed due process violation,[271] Verizon fails to demonstrate sufficient grounds for concluding that a combination of functions in the Commission's enforcement process here renders it constitutionally suspect, even apart from Verizon's failure to account for the trial *de novo* under section 504 of the Act. It is true that "a 'fair trial in a fair tribunal is a basic requirement of due process,'" but objections in that regard premised on the combination of functions in an agency "must overcome a presumption of honesty and integrity in those serving as

[265] Letter from Scott H. Angstreich, counsel to Verizon, to Michael Epshteyn and Rosemary Cabral,, Enforcement Bureau, FCC, EB-TCD-18-00027698;, at 2 (filed June 22, 2023) (Verizon June 22, 2023 Supplemental NAL Response).

[266] Verizon June 22, 2023 Supplemental NAL Response at 2.

[267] Verizon June 22, 2023 Supplemental NAL Response at 2-3.

[268] 47 U.S.C. § 504(a); *see also, e.g.*, *Ill. Citizens Comm. for Broadcasting v. FCC*, 515 F.2d 397, 405 (D.C. Cir. 1974) (noting that "a jury trial was available" in an action to collect a forfeiture). That Verizon theoretically might elect to pay the forfeiture voluntarily does not diminish its statutory right to a trial *de novo* in federal district court.

[269] *See, e.g.*, *Concrete Pipe & Prods. of Cal. v. Construction Lab. Pension Trust for S. Cal.*, 508 U.S. 602, 618 (1993) ("Where an initial determination is made by a party acting in an enforcement capacity, due process may be satisfied by providing for a neutral adjudicator to 'conduct a *de novo* review of all factual and legal issues.'").

[270] *Cf. Executive Benefits Insurance Agency v. Arkinson*, 573 U.S. 25, 38-40 (2014) (where a claim raised before a bankruptcy court implicates the judicial power under Article III of the constitution, the bankruptcy court can make proposed findings of fact and conclusions of law for *de novo* review by a federal district court, and even if a bankruptcy court adjudicates such a claim itself, *de novo* review of that decision by a federal district court resolved any Article III concern); *Crowell v. Benson*, 285 U.S. 22, 50-65 (1932) (even in the case of private rights, an agency can make factual findings and render an initial decision of law subject to *de novo* review of issues of jurisdictional fact and of law in an Article III court).

[271] Verizon June 22, 2023 Supplemental NAL Response at 2.

adjudicators."[272] To overcome that presumption requires "a showing of conflict of interest or some other specific reason for disqualification."[273]

94. Verizon fails to demonstrate a concern specific to the Commission's forfeiture order here sufficient to overcome the presumption of honesty and integrity. Insofar as Verizon notes the existence of pending due process claims premised on the combination of functions involving another agency, we are not persuaded to treat those still-pending unadjudicated arguments as warranting the conclusion that there is a genuine due process concern here.[274]

95. Verizon also expresses concern that "the Commission performs its own investigations of alleged violations, prosecutes them by taking enforcement action and issuing an NAL, and adjudicates the merits of any challenges to the NAL in imposing a forfeiture."[275] But these broad-brush objections do not identify specific reasons that a reasonable adjudicator in the Commission's position would be biased in this proceeding—certainly not one sufficient to overcome the background presumption of honesty and integrity on the part of agency adjudicators. To the contrary, finding a due process violation based simply on those would, in large part, turn that background presumption on its head by a requiring a presumption of bias whenever the Commission issued an NAL. Such an understanding would be at odds with the range of scenarios where courts have found no due process concerns with adjudication by individuals despite earlier involvement in a matter.[276]

96. Nor are we otherwise persuaded that due process concerns are present here. The potential to adopt forfeitures—even substantial forfeitures—that would be paid into the U.S. Treasury does not create a risk of financial bias on the part of reasonable adjudicators in the Commission's position.[277] We also are not persuaded that the Commission's decision to issue an NAL proposing even a

---

[272] *Withrow v. Larkin*, 421 U.S. 35, 46, 47 (1975); *see also, e.g.*, *id*. at 47-48 (discussing *FTC v. Cement Institute*, 333 U.S. 683 (1948), where the Court found no due process violation based on the adjudicators' prior investigations, including stated opinions about the legality of certain pricing systems, because "[t]he fact that the Commission had entertained such views as the result of its prior ex parte investigations did not necessarily mean that the minds of its members were irrevocably closed on the subject of the respondents' basing point practice" and in the adjudication at issue "members of the cement industry were legally authorized participants in the hearings" and submit evidence and arguments in defense of their positions); *In re Zdravkovich*, 634 F.3d 574, 579 (D.C. Cir. 2011) ("In *Withrow v. Larkin*, the Supreme Court expressly rejected the claim that due process is violated where '[t]he initial charge or determination of probable cause and the ultimate adjudication' are made by the same agency."); *Ethicon Endo-Surgery v. Covidien*, 812 F.3d 1023, 1029-30 (Fed. Cir. 2016) (observing that "[l]ower courts have also rejected due process challenges to systems of adjudication combining functions in an agency," and collecting illustrative cases).

[273] *Schweiker v. McClure*, 456 U.S. 188, 195 (1982); *see also, e.g.*, *Caperton v. A.T. Massey Coal*, 556 U.S. 868, 881 (2009) (the due process inquiry is "whether the average judge in his position is 'likely' to be neutral, or whether there is an unconstitutional 'potential for bias'").

[274] *See* Verizon June 22, 2023 Supplemental NAL Response at 2 (citing the pending constitutional challenge involving the FTC underlying *Axon Enterprise v. FTC*, 143 S. Ct. 890 (2023)).

[275] Verizon June 22, 2023 Supplemental NAL Response at 2.

[276] For example, the Supreme Court in *Withrow v. Larkin* observed that "judges frequently try the same case more than once and decide identical issues each time, although these issues involve questions both of law and fact," and "the Federal Trade Commission cannot possibly be under stronger constitutional compulsions in this respect than a court," noting also that "a hearing examiner who has recommended findings of fact after rejecting certain evidence as not being probative was not disqualified to preside at further hearings that were required when reviewing courts held that the evidence had been erroneously excluded." *Withrow v. Larkin*, 421 U.S. at 48-49 (internal quotation marks omitted). The Court's willingness to accept continued adjudicator participation even where final—not merely preliminary—decisions previously had been made by the adjudicators strongly supports our analysis here.

[277] *See, e.g.*, *Ward v. Village of Monroeville*, 409 U.S. 57, 59-61 (1972) ("[T]he test is whether the [decisionmaker's] situation is one 'which would offer a possible temptation to the average man as a judge to forget the burden of proof required to convict the defendant, or which might lead him not to hold the balance nice, clear, and true between the state and the accused . . . ,'" and due process was violated where a mayor acted as an adjudicator and also obtained a (continued….)

significant forfeiture is likely to create the risk of bias in the Commission's subsequent decision regarding a forfeiture order. Although the Supreme Court has stated in the context of criminal prosecutions that "there is an impermissible risk of actual bias when a judge earlier had significant, personal involvement as a prosecutor in a critical decision regarding the defendant's case," we find even a significant proposed forfeiture materially distinguishable from the imposition of criminal penalties—particularly the death penalty.[278] For example, we are not persuaded that the Commission's decision to propose a forfeiture in an NAL creates the same degree of risk of an adjudicator becoming "psychologically wedded" to that proposal as in the case of a prosecutor's decision to authorize prosecutors to seek the death penalty, nor does Verizon provide evidence that is the case here.[279] We also do not find that the NAL-initiated enforcement process presents the risk of adjudicators acting on the basis of extra-record information or impressions of the respondent that the Court found of concern in the case of a criminal prosecutor then serving as a judge.[280] In particular, section 503(b) requires a Commission NAL to "set forth the nature of the act or omission charged . . . and the facts upon which such charge is based,"[281] and Verizon has not identified concerns about the decision here being premised on extra-record evidence obtained by the Commission or commissioners in the development of the *NAL*.

97. *Trial By Jury.* We also reject Verizon's contention that adjudication of the violations at issue here may not constitutionally be assigned to a federal agency.[282] The Seventh Amendment preserves "the right of trial by jury" in "Suits at common law, where the value in controversy shall exceed twenty dollars,"[283] but the Seventh Amendment applies only to suits litigated in Article III courts, not to administrative adjudications conducted by federal agencies.[284] In determining whether an adjudication involves an exercise of judicial power vested in the federal courts under Article III of the constitution, the Supreme Court has distinguished between "public rights" and "private rights."[285] Congress has broad authority to "assign adjudication of public rights to entities other than Article III courts."[286] Examples of "public rights" litigation involving "cases in which the Government sues in its sovereign capacity to enforce public rights created by statutes within the power of Congress to enact" include enforcement of

---

portion of the fees and costs he imposed in that role, whereas due process was not violated where a mayor acted as an adjudicator but "the Mayor's relationship to the finances and financial policy of the city was too remote to warrant a presumption of bias toward conviction in prosecutions before him as judge."); *Brucker v. City of Doraville*, 38 F.4th 876, 884 (11th Cir. 2022) ("The fact that a judge works for a government, which gets a significant portion of its revenues from fines and fees, is not enough to establish an unconstitutional risk of bias on the part of the judge.").

[278] *Williams v. Pennsylvania*, 579 U.S. 1, 8 (2016) (finding a due process violation where the judge previously had been involved as a prosecutor in authorizing the prosecution to seek the death penalty).

[279] *See Williams v. Pennsylvania*, 579 U.S. at 9 (identifying this concern in the case of a prosecutor that authorized the prosecution to seek the death penalty).

[280] *See Williams v. Pennsylvania*, 579 U.S. at 9-10 (identifying this concern in the case of a prosecutor that authorized the prosecution to seek the death penalty and also citing *In re Murchison*, 349 U.S. 133, 138 (1955), which involved an individual acting in the role of both a grand jury and judge where similar concerns arose); *see also, e.g.*, *Withrow v. Larkin*, 421 U.S. at 54 (explaining that "Murchison has not been understood to stand for the broad rule that the members of an administrative agency may not investigate the facts, institute proceedings, and then make the necessary adjudications").

[281] 47 U.S.C. § 503(b)(4).

[282] AT&T June 22, 2023 Supplemental NAL Response at 2-3.

[283] U.S. Const. amend. VII.

[284] *See, e.g.*, *Oil States Energy Services v. Greene's Energy Group*, 138 S. Ct. 1365, 1379 (2018); *Atlas Roofing Co. v. Occupational Safety & Health Review Commission*, 430 U.S. 442, 455 (1977).

[285] *Oil States*, 138 S. Ct. at 1373 (citation omitted).

[286] *Id*.

federal workplace safety requirements,[287] "adjudicating violations of the customs and immigration laws and assessing penalties based thereon,"[288] adjudicating "whether an unfair labor practice had been committed and of ordering backpay where appropriate,"[289] and the grant or reconsideration of a grant of a patent.[290] That precedent confirms the constitutionality validity of FCC adjudication of violations of the Communications Act, even setting aside the reality that Verizon does, in fact, have the right of a trial *de novo* under section 504 of the Act here. Through section 222 of the Communications Act, Congress "created new statutory obligations"[291] designed to protect consumer privacy even as the communications marketplace became more open to competition,[292] analogous to those previously identified as involving public rights. Congress further "provided for civil penalties" for violations of those obligations, and constitutionally could entrust to the Commission "the function of deciding whether a violation has in fact occurred" when deciding whether to issue a forfeiture order, bringing it well within the "public rights" framework of existing Supreme Court precedent.[293]

98. Relying principally on the Supreme Court's decision in *Tull v. United States* and the Fifth Circuit's decision in *Jarkesy*, Verizon contends that the forfeiture at issue here should fall within the "private rights" framework—requiring adjudication in an Article III court, with the right to a trial by jury.[294] In *Tull*, the government was pursuing a claim in federal district court seeking penalties and an injunction under the Clean Water Act and the district court had denied the defendant's request for a jury trial.[295] But as the Supreme Court also has made clear, Congress can assign matters involving public rights to adjudication by an administrative agency "even if the Seventh Amendment would have required a jury where the adjudication of those rights is assigned to a federal court of law instead."[296] Thus, *Tull* does not address the question of whether Congress can assign the adjudication of a given matter to an administrative agency—it speaks only to the Seventh Amendment implications of a matter that is assigned to an Article III court. To the extent that the Fifth Circuit in *Jarkesy* treated *Tull* as standing for the proposition that causes of action analogous to common-law claims would, as a general matter, need to be adjudicated in Article III courts with a right to trial by jury, we are unpersuaded. As the Supreme Court has held in a post-*Tull* decision, "Congress may fashion causes of action that are closely analogous to common-law claims and place them beyond the ambit of the Seventh Amendment by assigning their

[287] *Atlas Roofing*, 430 U.S. at 450, 461

[288] *Id*. at 451.

[289] *Id*. at 453.

[290] *Oil States*, 138 S. Ct. at 1373.

[291] *Atlas Roofing*, 430 U.S. at 450.

[292] *See, e.g., 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, para 1 (1998) ("Congress recognized, . . . that the new competitive market forces and technology ushered in by the 1996 Act had the potential to threaten consumer privacy interests. Congress, therefore, enacted section 222 to prevent consumer privacy protections from being inadvertently swept away along with the prior limits on competition.").

[293] *Atlas Roofing*, 430 U.S. at 450

[294] Verizon June 22, 2023 Supplemental NAL Response at 2-3 (citing *Tull v. United States*, 481 U.S. 412 (1987) and *Jarkesy v. SEC*, 34 F.4th 446 (5th Cir. 2022)). Verizon also cites Justice Thomas' concurrence in *Axon. Id*. (citing *Axon*, 143 S. Ct. at 911 (Thomas, J., concurring)). However, as relevant here, Justice Thomas was critiquing existing Supreme Court precedent insofar as it had allowed agency adjudication subject to only deferential appellate court review. *Axon*, 143 S. Ct. at 906-09 (Thomas, J., concurring). We are not persuaded to alter our analysis based on one Justice's non-controlling opinion, and we therefore continue to apply existing Supreme Court precedent as it bears on our analysis here.

[295] *Tull*, 481 U.S. at 414-15.

[296] *Atlas Roofing*, 430 U.S. at 455.

resolution to a forum in which jury trials are unavailable."[297] We thus are unpersuaded by Verizon's reliance on *Tull* and *Jarkesy*.[298]

99. *Nondelegation*. Finally, contrary to Verizon's contention,[299] the choice of enforcement processes in section 503(b) of the Act does not constitute an unconstitutional delegation of legislative power. Section 503(b)(3) and (4) of the Act gives the Commission a choice of two procedural paths when pursuing forfeitures: either the NAL-based path most commonly employed by the Commission—which we have used here—or a formal adjudication in accordance with section 554 of the Administrative Procedure Act before the Commission or an administrative law judge.[300] Contrary to Verizon's suggestion, this choice involves the exercise not of legislative power but of executive power. The choice of enforcement process reflected in section 503(b) does not require the Commission to establish general rules governing private conduct of the sort that might implicate potential concerns about unauthorized lawmaking, but instead involves the exercise of enforcement discretion that is a classic executive power.[301]

100. We also are unpersuaded by Verizon's reliance on the Fifth Circuit decision in *Jarkesy* to support its nondelegation concerns. In addition to questions about the merits of the Fifth Circuit's approach in that regard,[302] even on its own terms, *Jarkesy* involved a scenario where the court found that "Congress offered *no guidance* whatsoever" regarding the statutory decision at issue.[303] That is not the case here, however. Although section 503(b) alone does not expressly provide guidance regarding the choice of enforcement process, section 4(j) of the Act directs as a general matter that "[t]he Commission may conduct its proceedings in such manner as will best conduce to the proper dispatch of business and to

---

[297] *Granfinanciera v. Nordberg*, 492 U.S. 33, 52 (1989) (emphasis omitted). We also are unpersuaded by the Fifth Circuit's decision in *Jarkesy* insofar as it interpreted *Granfinanciera* as establishing an additional prerequisite for a public right—namely, "when Congress passes a statute under its constitutional authority that creates a right so closely integrated with a comprehensive regulatory scheme that the right is appropriate for agency resolution." *Jarkesy*, 34 F.4th at 453. But *Granfinanciera* involved a dispute between two private parties, rather than an enforcement action commenced by the government. *Granfinanciera*, 492 U.S. at 51. The *Granfinanciera* Court explained that it had previously applied the public-rights doctrine to sustain "administrative factfinding" in cases "where the Government is involved in its sovereign capacity," but the Court distinguished such cases from "[w]holly private" disputes. *Id*. (citation omitted). It was in the context of private disputes—*i.e.*, "in cases not involving the Federal Government"—where the Court considered whether Congress "has created a seemingly 'private' right that is so closely integrated into a public regulatory scheme as to be a matter appropriate for agency resolution." *Granfinanciera*, 492 U.S. at 54. The Fifth Circuit in *Jarkesy* thus took that holding out of context when it applied it to claims where (as here) the government is involved in its sovereign capacity.

[298] The government has petitioned for certiorari in the *Jarkesy* case. Petition for a Writ of Certiorari, SEC v. Jarkesy, No. 22-859 (filed Mar. 8, 2023).

[299] Verizon June 22, 2023 Supplemental NAL Response at 2-3.

[300] 47 U.S.C. § 503(b)(3), (4).

[301] *See, e.g.*, *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2207 (2021) ("[T]he choice of how to prioritize and how aggressively to pursue legal actions against defendants who violate the law falls within the discretion of the Executive Branch."); *cf. Heckler v. Chaney*, 470 U.S. 821, 832 (1985) (noting that a federal prosecutor's decision not to indict a particular defendant "has long been regarded as the special province of the Executive Branch, inasmuch as it is the Executive who is charged by the Constitution to 'take Care that the Laws be faithfully executed'") (citation omitted); *United States v. Batchelder*, 442 U.S. 114, 121, 124, 126 (1979) (no violation of the nondelegation doctrine when Congress enacted two criminal statutes with "different penalties for essentially the same conduct" and gave prosecutors "discretion to choose between" the two statutes given that Congress had "informed the courts, prosecutors, and defendants of the permissible punishment alternatives available under each [statute]," and thereby "fulfilled its duty").

[302] As discussed above, Supreme Court precedent supports our contrary analysis here, and as previously noted, the government has petitioned for certiorari in the *Jarkesy* case. *See supra* note 298.

[303] *Jarkesy*, 34 F.4th at 462.

the ends of justice."[304] Nothing in section 503(b) precludes the applicability of these considerations to guide the Commission's choice of enforcement process there, and the Commission has interpreted section 4(j) as informing its decision regarding the procedural protections required in adjudicatory proceedings in other contexts in the past.[305] The circumstances here therefore are distinct from those in *Jarkesy* where "Congress offered *no guidance* whatsoever."[306]

## IV. CONCLUSION

101. Based on the record before us and in light of the applicable statutory factors, we conclude that Verizon willfully and repeatedly violated section 222 of the Act[307] as well as section 64.2010 of the Commission's rules[308] by disclosing its customers' location information, without their consent, to a third party who was not authorized to receive it and for failing to take reasonable steps to protect its customers' location information. We decline to withdraw the Admonishment and, having already reduced the forfeiture by $1,417,500 to account for two entities that did not participate in Verizon's LBS program, decline to further reduce or to cancel the forfeiture amount of $46,901,250.

## V. ORDERING CLAUSES

102. Accordingly, **IT IS ORDERED** that, pursuant to section 503(b) of the Act, 47 U.S.C. § 503(b), and section 1.80 of the Commission's rules, 47 CFR § 1.80, Verizon Communications **IS LIABLE FOR A MONETARY FORFEITURE** in the amount of forty-six million, nine-hundred and one thousand, two hundred and fifty dollars ($46,901,250) for willfully and repeatedly violating section 222 of the Act and section 64.2010 of the Commission's rules.

103. Payment of the forfeiture shall be made in the manner provided for in section 1.80 of the Commission's rules within thirty (30) calendar days after the release of this Forfeiture Order.[309] Verizon Communications shall send electronic notification of payment to Shana Yates, Michael Epshteyn, and Kimbarly Taylor, Enforcement Bureau, Federal Communications Commission, at shana.yates@fcc.gov, michael.epshteyn@fcc.gov, and kimbarly.taylor@fcc.gov on the date said payment is made. If the forfeiture is not paid within the period specified, the case may be referred to the U.S. Department of Justice for enforcement of the forfeiture pursuant to section 504(a) of the Act.[310]

104. In order for Verizon Communications to pay the proposed forfeiture, Verizon Communications shall notify Shana Yates at Shana.Yates@fcc.gov of its intent to pay, whereupon an invoice will be posted in the Commission's Registration System (CORES) at https://apps.fcc.gov/cores/userLogin.do. Payment of the forfeiture must be made by credit card using CORES at https://apps.fcc.gov/cores/userLogin.do, ACH (Automated Clearing House) debit from a bank account, or by wire transfer from a bank account. The Commission no longer accepts forfeiture payments

[304] 47 U.S.C. § 154(j).

[305] *See, e.g.*, *Procedural Streamlining of Administrative Hearings*, EB Docket No. 19-214, Report and Order, 35 FCC Rcd 10729, 10734, para. 14 (2020) (looking to the standards in section 4(j) to guide the decision regarding the conduct of adjudicatory proceedings on the basis of a written record without live testimony); *id*. at 10735-36, para. 18 (looking to the standards in section 4(j) to guide the decision regarding whether an adjudication should be heard by the Commission, one or more commissioners, or an ALJ).

[306] *Jarkesy*, 34 F.4th at 462.

[307] 47 U.S.C. § 222.

[308] 47 CFR § 64.2010.

[309] *Id.*

[310] 47 U.S.C. § 504(a).

by check or money order. Below are instructions that payors should follow based on the form of payment selected:[311]

- Payment by wire transfer must be made to ABA Number 021030004, receiving bank TREAS/NYC, and Account Number 27000001. In the OBI field, enter the FRN(s) captioned above and the letters "FORF". In addition, a completed Form 159[312] or printed CORES form[313] must be faxed to the Federal Communications Commission at 202-418-2843 or e-mailed to RROGWireFaxes@fcc.gov on the same business day the wire transfer is initiated. Failure to provide all required information in Form 159 or CORES may result in payment not being recognized as having been received. When completing FCC Form 159 or CORES, enter the Account Number in block number 23A (call sign/other ID), enter the letters "FORF" in block number 24A (payment type code), and enter in block number 11 the FRN(s) captioned above (Payor FRN).[314] For additional detail and wire transfer instructions, go to https://www.fcc.gov/licensing-databases/fees/wire-transfer.
- Payment by credit card must be made by using CORES at https://apps.fcc.gov/cores/userLogin.do. To pay by credit card, log-in using the FCC Username associated to the FRN captioned above. If payment must be split across FRNs, complete this process for each FRN. Next, select "Manage Existing FRNs | FRN Financial | Bills & Fees" from the CORES Menu, then select FRN Financial and the view/make payments option next to the FRN. Select the "Open Bills" tab and find the bill number associated with the NAL Acct. No. The bill number is the NAL Acct. No. with the first two digits excluded (e.g., NAL 1912345678 would be associated with FCC Bill Number 12345678). After selecting the bill for payment, choose the "Pay by Credit Card" option. Please note that there is a $24,999.99 limit on credit card transactions.
- Payment by ACH must be made by using CORES at https://apps.fcc.gov/cores/userLogin.do. To pay by ACH, log in using the FCC Username associated to the FRN captioned above. If payment must be split across FRNs, complete this process for each FRN. Next, select "Manage Existing FRNs | FRN Financial | Bills & Fees" on the CORES Menu, then select FRN Financial and the view/make payments option next to the FRN. Select the "Open Bills" tab and find the bill number associated with the NAL Acct. No. The bill number is the NAL Acct. No. with the first two digits excluded (e.g., NAL 1912345678 would be associated with FCC Bill Number 12345678). Finally, choose the "Pay from Bank Account" option. Please contact the appropriate financial institution to confirm the correct Routing Number and the correct account number from which payment will be made and verify with that financial institution that the designated account has authorization to accept ACH transactions.

105. Any request for making full payment over time under an installment plan should be sent to: Chief Financial Officer – Financial Operations, Federal Communications Commission, 45 L Street NE, Washington, D.C. 20554. Questions regarding payment procedures should be directed to the Financial Operations Group Help Desk by telephone, 1-877-480-3201, or by e-mail, ARINQUIRIES@fcc.gov.

[311] For questions regarding payment procedures, please contact the Financial Operations Group Help Desk by phone at 1-877-480-3201 (option #1).

[312] FCC Form 159 is accessible at https://www.fcc.gov/licensing-databases/fees/fcc-remittance-advice-form-159.

[313] Information completed using the Commission's Registration System (CORES) does not require the submission of an FCC Form 159. CORES is accessible at https://apps.fcc.gov/cores/userLogin.do.

[314] Instructions for completing the form may be obtained at http://www.fcc.gov/Forms/Form159/159.pdf.

106. **IT IS FURTHER ORDERED** that a copy of this Forfeiture Order shall be sent by first class mail and certified mail, return receipt requested, to David L. Haga, Associate General Counsel, Verizon Communications, c/o Scott H. Angstreich, Esq., and Christopher M. Young, Kellogg, Hansen, Todd, Figel & Frederick, P.L.L.C., 1615 M Street, N.W., Suite 400, Washington, D.C. 20036.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

**STATEMENT OF**
**CHAIRWOMAN JESSICA ROSENWORCEL**

Re: *In the Matter of Verizon Communications*, Forfeiture Order, File No.: EB-TCD-18-00027698 (April 17, 2024)

Our smartphones are always with us, and as a result these devices know where we are at any given moment. This geolocation data is especially sensitive. It is a reflection of who we are and where we go. In the wrong hands, it can provide those who wish to do us harm the ability to locate us with pinpoint accuracy. That is exactly what happened when news reports revealed that the largest wireless carriers in the country were selling our real-time location information to data aggregators, allowing this highly sensitive data to wind up in the hands of bail-bond companies, bounty hunters, and other shady actors. This ugly practice violates the law—specifically Section 222 of the Communications Act, which protects the privacy of consumer data. The Commission has long recognized the importance of ensuring that information about who we call and where we go is not for sale. In fact, these enforcement actions—leading to $200 million in fines—were first proposed by the last Administration. By following through with this order, we once again make clear that wireless carriers have a duty to keep our geolocation information private and secure.

**DISSENTING STATEMENT OF**
**COMMISSIONER BRENDAN CARR**

Re: *In the Matter of Verizon Communications*, Forfeiture Order, File No.: EB-TCD-18-00027698 (April 17, 2024)

For more than a decade, location-based service (LBS) providers have offered valuable services to consumers, like emergency medical response and roadside assistance. Up until the initiation of the above-captioned enforcement actions, LBS providers did so by obtaining access to certain location information from mobile wireless carriers like AT&T, Verizon, and T-Mobile. Then, in 2018, a news report revealed that a local sheriff had misused access to an LBS provider's services. That sheriff was rightly prosecuted for his unlawful actions and served jail time. Subsequently, all of the participating carriers ended their LBS programs. So our decision today does not address any ongoing practice.

This is not to say that LBS providers have ended their operations. They have simply shifted to obtaining this same type of location information from other types of entities. That is why I encouraged my FCC colleagues to examine ways that we could use these proceedings to address that ongoing practice. But my view did not prevail.

That brings us to the final Forfeiture Orders that the FCC approves today. Back in 2020, after the mobile wireless carriers exited the LBS line of business, the FCC unanimously voted to approve Notices of Apparent Liability (NALs) against the carriers. Even then, it was clear that at least one LBS provider had acted improperly. So I voted for the NALs so we could investigate the facts and determine whether or not the carriers had violated any provisions of the Communications Act.

Now that the investigations are complete, I cannot support today's Orders. This is not to say that the carriers' past conduct should escape scrutiny by a federal agency. Rather, given the nature of the services at issue, the Federal Trade Commission, not the FCC, would have been the right entity to take a final enforcement action, to the extent the FTC determined that one was warranted.

Here's why. Unlike the FTC, Congress has provided the FCC with both limited and circumscribed authority over privacy. Congress delineated the narrow contours of our authority in section 222 of the Communications Act. The services at issue in these cases plainly fall outside the scope of the FCC's section 222 authority. Indeed, today's FCC Orders rest on a newfound definition of customer proprietary network information (CPNI) that finds no support in the Communications Act or FCC precedent. And without providing advance notice of the new legal duties expected of carriers (to the extent we could adopt those new duties at all), the FCC retroactively announces eye-popping forfeitures totaling nearly $200,000,000. These actions are inconsistent with the law and basic fairness. The FCC has reached beyond its authority in these cases.

According to the Orders, our CPNI rules now apply whenever a carrier handles a customer's location information—whether or not it relates to the customer's use of a "telecommunications service" under Title II of the Communications Act. Here, the location information was unrelated to a Title II service. The customer did not need to make a call to convey his or her location. In fact, the carrier could have obtained the customer's location even if the customer had a data-only plan for tablets. Yet the Order concludes that the carriers mishandled CPNI.

That cannot be right. Start with the definition of CPNI, which section 222 of the Communications Act defines as:

> information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a

> telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship.[1]

That definition has two key limitations. First, the information must be of a specific type. As relevant here, CPNI must "relate to" the "location … of use of a telecommunications service." Second, the information must have been obtained in a specific way. The customer must have made his or her location "available to carrier" and "solely by virtue of the carrier-customer relationship."

Take the first limitation. By requiring that the location "relate" to the "use of a telecommunications service," the statute covers a particular type of data known as "call location information"—namely, the customer's location *while making or receiving a voice call*. Section 222 confirms this commonsense reading elsewhere when it expressly refers to "call location information."[2] These statutory references to "call location information" would make no sense if Congress intended for CPNI to cover all location information collected by a carrier, irrespective of particular calls.

The FCC confirmed that "straightforward" interpretation in a 2013 Declaratory Ruling.[3] The definition of CPNI, this agency held, encompassed "telephone numbers of calls dialed and received and the location of the device at the time of the calls."[4] The FCC also clarified that CPNI included "the location, date, and time a handset experiences a network event, such as a dialed or received telephone call [or] a dropped call."[5]

Although the Orders claim CPNI was at play, they do not contend that "call location information" was disclosed. Nor could they. As the Orders concede, the carriers obtained their customers' location whenever a customer's device pinged the carrier's cell site, even when the device was otherwise idle. No voice call was necessary for the carrier to obtain the customer's location. In fact, the carrier could gather the customer's location even if the customer did not have a voice plan. So, the "location" did not "relate to" the "use" of a "telecommunications service" in any meaningful sense.

Turning to the second limitation, it seems implausible to conclude that the carrier obtained the customer's location "*solely* by virtue of the carrier-customer relationship," as section 222 requires. True, many of these customers might have had voice plans, thereby creating a "carrier-customer relationship." But any Title II relationship was, at most, coincidental. The carrier could have obtained the customer's location even in the absence of a call, and even in the absence of a voice plan.

The massive forfeitures imposed in these Orders offend basic principles of fair notice. The FCC has never held that location information other than "call location information" constitutes CPNI. Nor has the FCC stated that a carrier might be liable under our CPNI rules for location information unrelated to a Title II service and collected outside the Title II relationship. So, even if we could proscribe the conduct at issue here through a rulemaking (and I am dubious that we could), it would be inappropriate and unlawful to impose the retroactive liability that these Orders do.

---

[1] 47 U.S.C. § 222(h)(1)(A).

[2] 47 U.S.C. § 222(f)(1) (ordinarily requiring "express prior authorization of the customer" for carrier disclosure of "call location information"); 47 U.S.C. § 222(d)(4) (allowing, however, carrier disclosure of "call location information" in certain emergency situations).

[3] *Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Declaratory Ruling, 28 FCC Rcd 9609, para. 22 (2013).

[4] *Id.* at para. 22.

[5] *Id.* at para. 25.

In the end, these matters should have been handled by the FTC. Our CPNI rules are narrow and do not cover every piece of data collected by an FCC-regulated entity. Besides, as the Communications Act makes clear, carriers are regulated under Title II only when they are engaged in offering Title II services.[6] In situations where an FCC-regulated entity offers a Title I service, such as mobile broadband, the FTC is the proper agency to enforce privacy and data security practices under generally applicable rules of the road. I respectfully dissent.

[6] 47 U.S.C. § 153(51) ("A telecommunications carrier shall be treated as a common carrier under this chapter only to the extent that it is engaged in providing telecommunications services …"); *see also FTC v. AT&T Mobility LLC*, 883 F. 3d 848, 863-64 (9th Cir. 2018) (holding that the FTC's "common carrier" exemption to Section 5 of the FTC Act "bars the FTC from regulating 'common carriers' only to the extent that they engage in common-carriage activity").

**DISSENTING STATEMENT OF**
**COMMISSIONER NATHAN SIMINGTON**

Re: *In the Matter of Verizon Communications*, Forfeiture Order, File No.: EB-TCD-18-00027698 (April 17, 2024)

Today, each of the major national mobile network operators faces a forfeiture for its purported failure to secure the confidentiality of its customer proprietary network information ('CPNI') as it relates to location information of network user devices. While the facts of each alleged violation are somewhat different, the enforcement calculation methodology used to arrive at the forfeitures is shared. Because I am concerned principally with that issue, together with what I view as a significant and undesirable policy upshot common across the actions that the Commission takes today, I will draft one dissent.

There is no valid basis for the arbitrary and capricious finding—enunciated in the Commission's erroneous rationale in *TerraCom Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325 (2014) (*'TerraCom'*) and relied upon today—that a single, systemic failure to follow the Commission's rules (in that case, violations of sections 201(b) and 222(a) of the Act; here, a violation of section 64.2010 of the Rules) may constitute however many separate and continuing violations the Commission chooses to find on the basis of the whole-cloth creation of a novel legal ontology. In *TerraCom*—which was resolved by consent decree and never proceeded to a forfeiture order—the Commission found that each customer record exposed by a single insecure data protection method (some 305,065 records) could be treated as having formed a separate and continuing violation. Here, the Commission purports to count individual location-based services providers (‘LBS’) and aggregators relied upon by each mobile network operator to arrive at its separate and distinct continuing violations.

Whether counting individual exposed customer records or LBS providers and aggregators, the clear effect of the Commission's arbitrary selection of a violation class used to increase the number violations emerging from a single act or failure to act of a regulatee alleged to be in violation of our rules is to exceed our section 503 statutory authority. Here it cannot credibly be argued that any of the mobile network operators, in operating an LBS/aggregator program, committed more than one act relevant for the purposes of forfeiture calculation. It is simply not plausible that Congress intended that the Commission may arrive at forfeitures of any size simply by disaggregating an "act" into its individual constituent parts, counting the members of whatever class of objects may be related to the alleged violation to arrive at whatever forfeiture amount suits a preordained outcome. In this case we exceed our statutory maximum forfeiture by a factor of, in some cases, dozens; in *TerraCom*, we asserted the right to exceed it by thousands.

What's more, the Commission ought to act prudentially here: even assuming, purely *arguendo*, that location-based CPNI were illicitly exposed, let us not forget that, at every moment, any of thousands of unregulated apps may pull GPS location information, Wi-Fi and Bluetooth signal strength, and other fragments of data indicating location from customer handsets at every moment the device is on. Indeed, this can be, and routinely is, accomplished even without consumer permission. By sending a strong market signal that any alleged violation of Commission rules regarding CPNI safekeeping (whether or not the rules actually were violated) can and will result in an outsize fine, we have effectively choked off one of the only ways that valid and legal users of consent-based location data services had to access location data for which legal safeguards and oversight actually exist.

It was available for the Commission to work with the carriers to issue consent decrees to promote best practices to develop further safeguards around location-based and aggregation services, and to actively monitor ongoing compliance in an effort to vouchsafe a regulated means of consensually sharing handset location data with legitimate users of the same. We opt, instead, to appear "tough on crime" in a way that actually reduces consumer data privacy by pushing legitimate users of location data toward unregulated data brokerage. Accordingly, I dissent.