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

In the Matter of	)	
	)	
Sprint Corporation	)	File No.: EB-TCD-18-00027700
	)	NAL/Acct. No.: 202032170005
	)	FRN: 0003774593

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
II. BACKGROUND 2
A. Legal Background 2
B. Factual Background 8
III. DISCUSSION 22
A. Location Information is CPNI 23
B. Sprint Had Fair Notice That Its LBS Practices Were Subject to Enforcement Under the Communications Act 34
C. Sprint Failed to Take Reasonable Steps to Protect CPNI 41
1. Sprint's Customer Location Disclosures to Securus Were Unauthorized and Violated Section 222 42
2. Sprint's Protection of Customer Location Information Was Unreasonable Both Before and After the Securus/Hutcheson Disclosures 46
3. Sprint Bore the Burden of Production 55
D. The Forfeiture Amount is Lawful and Consistent with FCC Precedent 62
1. The Commission Reasonably Found that Sprint Engaged in 11 Continuing Violations 64
2. The Upward Adjustment is Permissible and Warranted 70
E. Section 503(b) Is Employed Here Consistent With the Constitution 73
IV. CONCLUSION 85
V. ORDERING CLAUSES 86

I. INTRODUCTION

1. On February 28, 2020, the Commission issued a Notice of Apparent Liability for Forfeiture and Admonishment (*NAL*)[1] against Sprint Corporation (Sprint or Company).[2] In the *NAL*, the

[1] *Sprint Corporation*, Notice of Apparent Liability for Forfeiture and Admonishment, 35 FCC Rcd 1655 (2020) (*NAL*).

[2] On April 1, 2020, a merger between Sprint Corporation and T-Mobile US, Inc. (T-Mobile), closed. As a result, Sprint became a wholly owned subsidiary of T-Mobile, with the combined companies operating under the name of T-Mobile. Prior to the merger, the Commission issued notices of apparent liability against the then-separate companies of Sprint and T-Mobile in relation to each company's respective location-based service programs. In order to avoid confusion, and as this Forfeiture Order resolves the *NAL* for the actions of Sprint pre-merger, we will continue to refer to Sprint in this Order to avoid confusion.

Commission admonished Sprint 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 Sprint $12,240,000 for failing to take reasonable steps to protect its customers' location information. After reviewing the Company's response to the *NAL*,[3] we find no reason to cancel, withdraw, or reduce the proposed penalty, and impose a penalty of $12,240,000 against Sprint.[4]

II. BACKGROUND

A. Legal Background

2. As set forth fully in the *NAL*,[5] 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).[6] The Commission has advised carriers that this duty requires them to take "every reasonable precaution" to safeguard their customers' information.[7] Section 222(a) of the Act imposes a general duty on telecommunications carriers to "protect the confidentiality of proprietary information" of "customers."[8] 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."[9] 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."[10]

---

[3] *Sprint Corporation*, Response to Notice of Apparent Liability for Forfeiture and Admonishment (filed May 7, 2020) (on file in EB-TCD-18-00027700) (NAL Response or Response).

[4] Prior to the T-Mobile/Sprint merger, the two companies filed applications seeking, among other things, "Commission consent to the transfer of control of the licenses, authorizations, and spectrum leases" from Sprint to T-Mobile. *Applications of T-Mobile US, Inc., and Sprint Corporation, et al., Consent to Transfer Control of Licenses and Authorizations*, WT Docket No. 18-197, Memorandum Opinion and Order, Declaratory Ruling, and Order of Proposed Modification, 34 FCC Rcd 10578, 10580, para. 1 (2019) (*T-Mobile Sprint Order*). We note that the *T-Mobile Sprint Order* stated that Commission's "grant of the Applications is without prejudice to any enforcement actions the Commission . . . may deem appropriate in light of any facts uncovered in any investigations of possible violations of law." *T-Mobile Sprint Order*, 34 FCC Rcd at 10598, para. 46. The Commission explicitly conditioned the grant of the Applications "on New T-Mobile (however structured, whether through merger, consolidation, or otherwise), and its successors, assigns, and transferees, assuming liability for any forfeitures or restitutions that may be imposed by the Commission on Sprint Corporation and its subsidiaries . . . ." *Id*. Therefore T-Mobile is liable for the penalty imposed in this Order.

[5] *See generally NAL*.

[6] 47 U.S.C. § 222.

[7] *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*).

[8] 47 U.S.C. § 222(a).

[9] 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 Sprint 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.").

[10] *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.

3. *Customer Consent to Disclose CPNI.* With limited exceptions, a carrier may only use, disclose, or permit access to CPNI with customer approval.[11] Generally, carriers must obtain a customer's "opt-in approval" before disclosing that customer's CPNI.[12] This means that a carrier must obtain the 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 . . . ."[13]

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.[14] 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.[15] 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."[16] 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.[17] 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.[18]

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).[19] Therefore, the Commission adopted rules requiring carriers to "take reasonable measures to *discover* and *protect* against attempts to gain unauthorized access to CPNI."[20] 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.[21] It also adopted password and account notification requirements.[22]

---

[11] 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).

[12] 47 CFR § 64.2007(b).

[13] 47 CFR § 64.2003(k).

[14] *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.

[15] *2007 CPNI Order*, 22 FCC Rcd at 6950, para. 45.

[16] *2007 CPNI Order*, 22 FCC Rcd at 6949, para. 42.

[17] *2007 CPNI Order*, 22 FCC Rcd at 6952, para. 49.

[18] *See* 47 CFR § 64.2007(b).

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

[20] 47 CFR § 64.2010(a) (emphasis added).

[21] *See* 47 CFR § 64.2010(b)-(d).

[22] *See* 47 CFR § 64.2010(e)-(f).

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."[23] 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."[24] They must also take reasonable measures to protect the confidentiality of CPNI—a permanent and ongoing obligation to police disclosures and ensure proper functioning of security measures.[25] 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.[26]

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."[27]

B. Factual Background

8. *Customer Location Information and Sprint's Location-Based Services Business Model.* Sprint (now T-Mobile)[28] 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 T-Mobile's wireless network.[29] As part of its pre-merger business, Sprint ran a Location-Based Services (LBS) program until May 31, 2019. Through the LBS program, Sprint 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 "sub-aggregators" or intermediary

[23] *2007 CPNI Order*, 22 FCC Rcd at 6959–60, para. 65.

[24] 47 CFR § 64.2010(a).

[25] *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.").

[26] 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.

[27] 47 U.S.C. § 217.

[28] As explained in notes 2 and 4, *supra*, the merger of Sprint and T-Mobile closed on April 1, 2020. That merger was approved by the Commission 2019. *See T-Mobile Sprint Order*, 34 FCC Rcd 10578. As a result, Sprint is a wholly owned subsidiary of T-Mobile, and operates under the name of T-Mobile.

[29] *See* T-Mobile US, Inc., 2021 Annual Report, https://s29.q4cdn.com/310188824/files/doc_financials/2021/ar/TMUS-2021-Annual-Report.pdf (Sprint merged with T-Mobile USA, Inc., on April 1, 2020, after the *NAL* in this matter was issued).

companies who then resold access to such information to location-based service providers.[30] Sprint 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, Sprint sold access to its customers' location information (directly or indirectly) to 86 third-party entities (including the two Aggregators).[31]

9. The Sprint LBS program was largely governed via contractual provisions that vested Sprint with oversight authority over the Aggregators. The Aggregators then entered into their own contracts with various LBS providers, sub-aggregators, and third-party developers.[32] As explained in the *NAL*, "Sprint did not contract directly with the third-party developers but instead delegated all responsibility to the Aggregators to ensure that the sub-aggregators and application developers complied with 'the Aggregator and Third Party Developer obligations' contained in Sprint's contracts with the Aggregators."[33] According to Sprint, the Company "required customer consent to access or share its customer location information" and "application developers and the Aggregators were 'contractually obligated to incorporate conspicuous and stand-alone notice . . . that explains how location information will be accessed, used, stored, disclosed or collected' and that the end user had to 'expressly and affirmatively accept the notice before continuing.'"[34] This arrangement meant Sprint itself did not notify customers and collect affirmative customer consent for the disclosure of customer location information. Sprint asserts that its LBS program was subject to a number of safeguards. This included the contractual obligation "to provide the notice record to Sprint before Sprint provided location information to the Aggregator," as well as a requirement that "the Aggregators and developers . . . document the presentation of notice and receipt of consent in each instance and . . . make those records available to Sprint upon request."[35]

10. Sprint's contracts obligated the Aggregators to ensure that the LBS service providers "complied with Sprint's privacy policy and consumer protection, marketing, data security laws and regulations in addition to the CTIA Guidelines."[36] The contracts also established a "Certification" process that "required the Aggregators to test the sub-aggregators and location-based service providers' applications to ensure they met Sprint's notice, privacy, and data security requirements."[37] The contracts between Sprint and the Aggregators also required that the Aggregators "'obtain prior written consent from Sprint 60 days before the use of any [s]ub-[a]ggregator' and gave Sprint sole discretion 'to approve or

[30] 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 1660-68, paras. 11-31.

[31] *See NAL*, 35 FCC Rcd at 1661-62, paras. 12-13 (citations omitted).

[32] *See NAL*, 35 FCC Rcd at 1662, para. 15 (citing Response to Letter of Inquiry from Sprint Corp. to Kristi Thompson, Chief, Telecommunications Consumer Division, FCC Enforcement Bureau, at RD03-000096, Response to Request for Documents No. 3 at Section 2, Sprint LocationSmart Agreement; LOI at RD03-000134, Response Request for Documents No. 3 at Section 2, Sprint Zumigo Agreement (Oct. 16, 2018) (on file in EB-TCD-18-00027700) (LOI Response)).

[33] *NAL*, 35 FCC Rcd at 1663, para. 16 (citing LOI Response at RD03-000096, Response to Request for Documents No. 3 at Section 2.2-2.3, Sprint-LocationSmart Agreement; LOI at RD03-000134, Response to Request for Documents No. 3 at Section 2.2-2.3, Sprint-Zumigo Agreement).

[34] *NAL*, 35 FCC Rcd at 1662, para. 15 (quoting LOI Response at 1, Response to Question 1).

[35] *NAL*, 35 FCC Rcd at 1662-63, para. 15 (citing LOI Response at 6, Response to Question 5).

[36] *NAL*, 35 FCC Rcd at 1663, para. 16 (citing LOI Response at RD03-000096, Response to Request for Documents No. 3 at Section 22.11, Sprint LocationSmart Agreement; LOI at RD03-000134, Response to Request for Documents No. 3 at Section 22.11, Sprint Zumigo Agreement).

[37] *NAL*, 35 FCC Rcd at 1663, para. 17 (citing LOI Response at RD03-000096, Response to Request for Documents No. 3 at Section 12, Sprint-LocationSmart Agreement; LOI at RD03-000134, Response to Request for Documents No. 3 at Section 12, Sprint-Zumigo Agreement).

reject each [s]ub-aggregator.'"[38] The contracts contain no such provision with respect to Aggregators' use of third-party developers.

11. Sprint had broad authority under its contracts with the Aggregators to quickly terminate access to customer location information. Sprint could immediately terminate its contract with either Aggregator under a variety of circumstances, including if the Aggregator:

> (1) [F]ailed to impose required obligations on its location-based service provider clients; (2) failed to comply with the contract terms specifying non-disclosure of sensitive information (such as the location information at issue here); (3) failed to "employ administrative, physical, and technical safeguards . . . that prevent the unauthorized collection, access, disclosure, and use" of information provided by Sprint; (4) failed to ensure that the Aggregator's location-based service provider clients complied with Sprint's customer notice requirements; or (5) negligently or knowingly misrepresented the location-based service provider's service or application.[39]

Sprint also had the right to immediately suspend or terminate an Aggregator's access to customer location information for reasons that included a breach of the Aggregator's contractual obligations.[40] Likewise, Sprint could "immediately suspend the transmission of location information by the Aggregator to any sub-aggregator or location-based service provider that Sprint believed was not complying with the obligations that the Aggregators were directed to impose upon them."[41] In addition, Sprint had the right to terminate its contracts with the Aggregators for any reason "upon 90 days written notice."[42]

12. Sprint also had the authority to conduct audits and other internal reviews of the LBS program. Sprint "maintained the right to assess compliance with the terms of agreements with Aggregators, and could seek 'reports, full and complete access to relevant facilities, books, records, procedures, and information.'"[43] Sprint also had the right to audit the performance of the Aggregators once every 12 months,[44] and "had the right to perform audits at any time as necessary if it had a good faith reason to believe a breach of privacy and security obligations had occurred."[45] However, there is no evidence that Sprint exercised any of these contractual provisions before 2018.[46] While Sprint claims that

[38] *NAL*, 35 FCC Rcd at 1663, para. 17 (citing LOI Response at RD03-000096, Response to Request for Documents No. 3 at Section 2.2, Sprint-LocationSmart Agreement; LOI at RD03-000134, Response to Request for Documents No. 3 at Section 2.2, Sprint Zumigo Agreement).

[39] *NAL*, 35 FCC Rcd at 1663, para. 18 (citing LOI Response at RD03-000096, Response to Request for Documents No. 3 at Section 21, Sprint-LocationSmart Agreement; LOI at RD03-000134, Response Request for Documents No. 3 at Section 21, Sprint-Zumigo Agreement).

[40] *NAL*, 35 FCC Rcd at 1663-64, para. 18 (citing LOI Response at 7, Response to Question 5).

[41] *NAL*, 35 FCC Rcd at 1664, para. 18 (citing LOI Response at RD03-000096, Response to Request for Documents No. 3 at Section 14, Sprint-LocationSmart Agreement; LOI at RD03-000134, Response to Request for Documents No. 3 at Section 14, Sprint-Zumigo Agreement).

[42] *NAL*, 35 FCC Rcd at 1663, para. 18 (citing LOI Response at RD03-000096, Response to Request for Documents No. 3 at Section 2.2, Sprint-LocationSmart Agreement; LOI at RD03-000134, Response to Request for Documents No. 3 at Section 2.2, Sprint Zumigo Agreement).

[43] *NAL*, 35 FCC Rcd at 1664, para. 19 (quoting LOI Response at 7, Response to Question 5; LOI Response at RD03-000096, Response to Request for Documents No. 3 at Section 22.7, Sprint-LocationSmart Agreement; LOI at RD03-000134, Response to Request for Documents No. 3 at Section 22.7, Sprint-Zumigo Agreement).

[44] *See NAL*, 35 FCC Rcd at 1664, para. 19 (citing Supplemental LOI Response at 6, Response to Question 5; LOI at RD03-000096, Response to Request for Documents No. 3 at Section 29.7, Sprint-LocationSmart Agreement; LOI at RD03-000134, Response to Request for Documents No. 3 at Section 29.7, Sprint-Zumigo Agreement).

[45] *NAL*, 35 FCC Rcd at 1664, para. 19 (citing Supplemental LOI Response at 6-7, Response to Question 5).

[46] *See NAL*, 35 FCC Rcd at 1664, para. 19.

it "conducted a legal review of both LocationSmart and Zumigo in 2018," it declined to specify the time period of such review, or to provide any information at all about the reviews, citing privilege.[47]

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 Sprint's (and other carriers') practice of selling access to customer location information.[48] 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.[49] Not only was Securus's location-finding service outside the scope of both Securus's stated purpose for accessing Sprint's customers' location information and any agreement with either Aggregator (and thus had not been reviewed by either Aggregator or Sprint), 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.[50] Sprint conceded that it was unable to detect Securus's activities (i.e., location requests unrelated to its stated purpose for accessing location information—which involved an inmate collect-calling service) because of Securus's misrepresentations to the Aggregator.[51] Further, Sprint does not claim that it had any way of distinguishing valid, customer-authorized requests for location information from invalid, unauthorized requests, such as those from Securus's unauthorized-location finding service.

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

[47] *See NAL*, 35 FCC Rcd at 1664, para. 19 (citing LOI Response at 9, Response to Question 11; Supplemental LOI Response at 11, Response to Question 10).

[48] *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.

[49] *See NAL*, 35 FCC Rcd at 1644-65, paras. 20-21 (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).

[50] *See NAL*, 35 FCC Rcd at 1664-65, paras. 20-21 (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).

[51] *See NAL*, 35 FCC Rcd at 1665, para. 22.

[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 1664-65, paras. 20-21.

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. *Sprint's Response to the Securus Disclosures*. Sprint terminated Securus's access to Sprint customer location information on May 17, 2018, following the *New York Times* article.[59] On May 25, 2018, Sprint suspended LocationSmart from its LBS program and stopped sharing customer location information with the Aggregator, having confirmed that "data sharing through LocationSmart and 3Cinteractive 'had occurred for an unknown and unapproved purpose.'"[60] By suspending LocationSmart, Sprint "effectively terminated access to Sprint wireless customer location information for LocationSmart and the 77 entities that purchased access through LocationSmart."[61] According to Sprint, it terminated LocationSmart's contract on June 20, 2018.[62] Also on June 20, 2018, it provided the 90-day notice of termination to Zumigo, which would result in a termination on September 18, 2018.[63]

16. At the same time, Sprint was planning on re-launching its LBS program.[64] As part of this effort in June 2018, Sprint began formalizing certain "Methods & Procedures" to "'complement' the contractual protections for future Aggregators and location-based services;" the Methods & Procedures were finalized in August 2018.[65] According to Sprint, and unlike the Aggregator Contracts, the Methods & Procedures "required Aggregators to submit reports to Sprint that provided detailed information about all companies (including aggregators and sub-aggregators) that used Sprint customer location information," and that such reports had to include "detailed information about how the Sprint customer location information was or would be used."[66] Sprint claims that the Methods & Procedures also "provided expanded internal guidance on what information it could seek in auditing its location-based services partners," including, among other things "reviewing compliance with notice and consent

[54] Hutcheson Sentencing Memo at 3; *see also NAL*, 35 FCC Rcd at 1664, para. 20.

[55] *See* Hutcheson Sentencing Memo at 3-4; *see also NAL*, 35 FCC Rcd at 1664, para. 20.

[56] Hutcheson Sentencing Memo at 4; *see also NAL*, 35 FCC Rcd at 1664-65, para. 21.

[57] Hutcheson Sentencing Memo at 4; *see also NAL*, 35 FCC Rcd at 1664-65, para. 21.

[58] Hutcheson Sentencing Memo at 4; *see also NAL*, 35 FCC Rcd at 1664-65, para. 21.

[59] *See NAL*, 35 FCC Rcd at 1665, para. 23.

[60] *NAL*, 35 FCC Rcd at 1665, para. 24 (quoting LOI Response at 7, Response to Question 6).

[61] *NAL*, 35 FCC Rcd at 1665-66, para. 24.

[62] *See NAL*, 35 FCC Rcd at 1666, para. 25 (citing Letter from Sean Olsen, Manager, Contract Administration, Sprint Corp., to Mario Proietti, CEO, Masoud Motamedi, President, TechnoCom Corporation/Locaid d/b/a LocationSmart (June 20, 2018) (on file in EB-TCD-18-00027700)).

[63] *See NAL*, 35 FCC Rcd at 1666, para. 25 (citing LOI Response at RD03-000180, Response to Request for Documents No. 3).

[64] The *NAL* offers a more complete discussion of Sprint's plans, and is incorporated by reference. *See NAL*, 35 FCC Rcd at 1666, paras. 26-28.

[65] *NAL*, 35 FCC Rcd at 1666, para. 26 (LOI Response at 7, Response to Question 6).

[66] *NAL*, 35 FCC Rcd at 1666, para. 26 (citing Supplemental LOI Response at 6, Response to Question 4).

requirements" and "reviewing the Aggregator's process for validating companies receiving location data."[67] Sprint asserts that the new obligations on the Aggregators "'included a requirement for an independent third-party audit of the Location Aggregators on their privacy and data security practices,'"[68] but Sprint "does not explain how, or whether, the Methods & Procedures auditing and review process differed from the audits that Sprint had the right to conduct under the original contracts."[69]

17. On or around August 23, 2018, Sprint re-launched its aggregator LBS program. In August 2018, it executed two new agreements with LocationSmart to permit that Aggregator to access Sprint customer location information and provide it to two LBS providers; the agreements "allowed LocationSmart to obtain Sprint customer location information for 90 days, with monthly renewal up to one year."[70] On September 18, 2018, Sprint's contract with Zumigo terminated.[71] However, on October 16, 2018, "Sprint renewed its previously terminated contract with Zumigo in its entirety"—meaning that unlike LocationSmart, "all of Zumigo's prior location-based service provider clients again had access to Sprint's customer location information."[72]

18. More than seven months after the *New York Times* article revealing the Securus disclosures, Sprint became aware of a similar incident involving the Company's customers' location information. In a January 8, 2019, *Motherboard* article, it was reported that access to customer location information was sold and resold, with little or no oversight, within the bail bonds industry, and that this led to consumers being tracked without their knowledge or consent.[73] That article focused in part on the activities of a company called MicroBilt; MicroBilt was a customer of the Aggregator Zumigo, and Zumigo received customer location information from Sprint and the other major wireless carriers.[74] According to Sprint, before the article's publication, Sprint was entirely unaware that Zumigo was providing LBS services to MicroBilt, as Sprint "was unable to 'identify any record of Zumigo obtaining Sprint's prior written consent before using MicroBilt as a sub-aggregator.'"[75] Sprint does not deny that MicroBilt received Sprint customer location information, and "concedes that it was unable to verify whether Sprint's own credentialing process had been followed with respect to MicroBilt, and that Sprint had no information about whether MicroBilt complied with Sprint's notice-and-consent processes."[76] Sprint claims that despite its demands for additional information and details about Zumigo's relationship

[67] *NAL*, 35 FCC Rcd at 1666, para. 26 (citing Supplemental LOI Response at 7, Response to Question 4).

[68] *NAL*, 35 FCC Rcd at 1666, para. 26 (quoting Supplemental LOI Response at 6-7, Response to Question 4).

[69] *NAL*, 35 FCC Rcd at 1666, para. 26.

[70] *NAL*, 35 FCC Rcd at 1666-67, para. 27 (citing LOI Response at 3, 8, Response to Questions 1, 6).

[71] *See NAL*, 35 FCC Rcd at 1667, para. 28 (citing LOI Response at RD03-000180, Response to Request for Documents No. 3).

[72] *NAL*, 35 FCC Rcd at 1667, para. 28 (citing LOI Response at RD03-000183, Response to Request for Documents No. 3).

[73] *See NAL*, 35 FCC Rcd at 1667, para. 29 (citing Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone*, Motherboard (Jan. 8. 2019), https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-MicroBilt-zumigo-tmobile).

[74] *See NAL*, 35 FCC Rcd at 1667, para. 29 (citing Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone*, Motherboard (Jan. 8. 2019), https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-MicroBilt-zumigo-tmobile).

[75] *NAL*, 35 FCC Rcd at 1667, para. 30 (quoting Supplemental LOI Response at 2, Response to Question 1).

[76] *NAL*, 35 FCC Rcd at 1667, para. 30 (citing Supplemental LOI Response at 2, Response to Question 1).

with MicroBilt, Zumigo did not respond to the Sprint's requests.[77] Sprint terminated its contract with Zumigo on January 9, 2019.[78]

19. It was not until May 31, 2019, that Sprint's LBS program (and the sharing of Sprint's customers' location information) finally ceased—in other words, 386 days after the *New York Times* reported on the Securus location-finding service, as well as the abuse of that service by Hutcheson.[79]

20. *Notice of Apparent Liability*. On February 28, 2020, the Commission issued the *NAL* proposing a $12,240,000 fine against Sprint for its apparent willful and repeated violation of 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 *NAL*, the Commission also admonished Sprint for apparently disclosing its customers' location information, without their consent, to a third party who was not authorized to receive it.

21. On May 7, 2020, Sprint filed a response to the *NAL*.[80] Sprint makes a number of arguments as to why the *NAL* should be withdrawn and cancelled. Sprint 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 location information would be classified as CPNI.[81] Sprint 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.[82] Finally, Sprint argues that the forfeiture amount is arbitrary and capricious.[83]

III. DISCUSSION

22. The Commission proposed a forfeiture in this case in accordance with section 503(b) of the Communications Act of 1934, as amended (Act),[84] section 1.80 of the Commission's rules,[85] and the Commission's *Forfeiture Policy Statement*.[86] 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."[87] We have fully considered Sprint's NAL Response, which includes a variety of legal and factual arguments, but we find none of them persuasive. We therefore affirm the $12,240,000 forfeiture proposed in the *NAL*.

[77] *See NAL*, 35 FCC Rcd at 1668, para. 30 (citing Supplemental LOI Response at 9, Response to Question 5).

[78] *See NAL*, 35 FCC Rcd at 1668, para. 30 (citing Supplemental LOI Response at 3, Response to Question 1).

[79] See *NAL*, 35 FCC Rcd at 1668, para. 30 (citing Supplemental LOI Response at 11, Response to Question 7).

[80] *See* NAL Response.

[81] NAL Response at 6-14, 22-24.

[82] NAL Response at 14-21.

[83] NAL Response at 25-29.

[84] 47 U.S.C. § 503(b).

[85] 47 CFR § 1.80.

[86] *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).

[87] 47 U.S.C. § 503(b)(2)(E).

A. Location Information is CPNI

23. As the *NAL* explained in more detail, the customer location information disclosed in Sprint's LBS program is CPNI under the Act and our rules.[88] 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, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[89] The customer location information used in Sprint's LBS program falls squarely within this definition. Sprint's arguments to the contrary[90] 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.

24. *First*, the customer location information at issue here relates to the location of a telecommunications service—i.e., Sprint's commercial mobile service.[91] 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. Sprint 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.[92]

25. 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 . . . ."[93] 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."[94] 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.[95] And our interpretation squares more readily with section 222(d)(1),

---

[88] *See NAL*, 35 FCC Rcd at 1669-71, paras. 35-45.

[89] 47 U.S.C. § 222(h)(1)(A) (emphasis added).

[90] *See* NAL Response at 6-14.

[91] *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").

[92] *NAL*, 35 FCC Rcd at 1669, para. 37.

[93] 47 U.S.C. § 222(h)(1)(A).

[94] *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'").

[95] We are unpersuaded by Sprint's claim that interpreting "of use" to modify only "amount" would lead to anomalies because "information relating to the 'quantity, technical configuration, [or] type . . . of a telecommunications service' . . . would relate to the network itself, not the information of individual customers." NAL Response at 12 (emphasis omitted). Even if the information relates in part to the network, it also relates to an individual customer by identifying characteristics of the telecommunications service subscribed to by that customer. *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 (continued….)

which preserves carriers' ability to use CPNI to "initiate" service[96]—an event that, aspects of which, ordinarily occur before the service is in "use."

26. The location information at issue here readily fits within that interpretation of the first prong of the CPNI definition. Sprint'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 Sprint's ability to use its network to determinate that location—is reasonably understood as associated with or a reference to the location of the Sprint telecommunications service.[97] Consequently, consistent with our assessment in the *NAL*,[98] we find this to be information that "relates to" the location of Sprint's telecommunications service within the meaning of the first prong of the CPNI definition.[99]

27. 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. Sprint does not dispute the *NAL*'s explanation that customers' devices and Sprint's network regularly exchange information as necessary for customers to send and receive calls.[100] To the extent that Sprint contends that this does not represent use of the telecommunications service because it merely enables the provision of that service, Sprint 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*,[101] we believe that Sprint's customers subscribe to its commercial mobile service to enable them to receive and transmit calls. When customers' devices are exchanging communications with Sprint'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.[102]

28. We also are unpersuaded by Sprint'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

---

Proposed Rulemaking, 13 FCC Rcd 8061, 8064-65, para. 2 (1998) ("CPNI includes information that is extremely personal to customers as well as commercially valuable to carriers," including "the types of service offerings to which the customer subscribes").

[96] 47 U.S.C. § 222(d)(1).

[97] *See, e.g.*, *NAL*, 35 FCC Rcd at 1660, para. 11 ("Sprint 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 Sprint's wireless network.").

[98] *See, e.g.*, *NAL*, 35 FCC Rcd at 1669-70, paras. 37, 39.

[99] *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").

[100] *NAL*, 35 FCC Rcd at 1669, para. 37.

[101] *See, e.g.*, *NAL*, 35 FCC Rcd at 1669-70, paras. 37, 39.

[102] 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").

what Sprint gleans from other language in section 222.[103] In addition to the *NAL*'s responses in this regard,[104] 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:[105] 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*.[106] 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.[107]

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

> Sprint provides wireless telephony services to the affected customers because they have chosen Sprint to be their provider of telecommunications service—in other words, they have a carrier-customer relationship. . . . Sprint's customers provided their wireless location data to Sprint because of their customer-carrier relationship with Sprint, ...[108]

In sum, the *NAL* reasoned that "[a]lthough Sprint (or others) might also provide non-common-carrier services to the same customer," the customer provided the relevant data "by virtue of the carrier-customer relationship."[109]

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

[103] *See, e.g.*, NAL Response at 9-11; *NAL*, 35 FCC Rcd at 1671, para. 44 (citing LOI Response at 5, Response to Question 4; Supplemental LOI Response at 3, Response to Question 2).

[104] *NAL*, 35 FCC Rcd at 1670, para. 40.

[105] 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'"). Particularly given that Sprint neglects this textual distinction in its attempts to rely on legislative history or the rule of lenity, we reject its claims in that regard. *See* NAL Response at 10-11.

[106] Given this predominant—but not exclusive—focus of the 1999 amendments to section 222, the references to call location information in the legislative history cited by Sprint is not surprising. *See* NAL Response at 10. But nothing in the legislative history persuades us that Congress meant to exclude non-call location data from the definition of CPNI.

[107] *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*).

[108] *NAL*, 35 FCC Rcd at 1671, para. 43.

[109] *NAL*, 35 FCC Rcd at 1671, para. 43.

"relationship"—namely, the "carrier-customer relationship."[110] 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-customer relationship."[111] Thus, we reject any suggestion by Sprint that the location information at issue here is not CPNI and does not depend exclusively on the carrier-customer relationship[112]—we find that suggestion belied by the technical and marketplace realities here, as experienced by Sprint customers.

31. As the *NAL* explains, when a customer subscribes to Sprint's commercial mobile service, Sprint "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."[113] Sprint does not dispute that the carrier-customer relationship fully enables Sprint to obtain the location data at issue here. Likewise, Sprint does not claim that a customer, having subscribed to its commercial mobile service, entered a separate agreement with Sprint for the provision of that location information—or that Sprint's voice customers had any way to avoid providing that information if they wanted to subscribe to Sprint's commercial mobile service. Under circumstances such as these, we conclude that the location information at issue from Sprint's commercial mobile service customers was "made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[114]

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, Sprint has sought to rely on the theory that the Company "is acting as an information service provider when it is selling access to its customers' location information" and that the entire LBS program was an "information service,"[115] to take any location information outside the purview of CPNI. But we are not persuaded that the fact that location information can be associated with a non-telecommunications service the carrier also provides (or otherwise facilitates) 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 Sprint's customers to make their location data available to Sprint,[116] and in evaluating the second

[110] 47 U.S.C. § 222(h)(1)(A).

[111] 47 U.S.C. § 222(h)(1)(A). Insofar as Sprint has suggested "that it is acting as an information service provider when it is selling access to its customers' location information," and thus its receipt of such location information is not "solely by virtue of" its telecommunications service (*see, e.g.*, NAL, 35 FCC Rcd at 1671, para. 43), the focus on Sprint'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, Sprint disputes whether the location information at issue meets the statutory definition of CPNI in section 222(h)(1)(A), *see* NAL Response at 6-10, but does not contend that, if it does meet that definition, section 222(c)(1) nonetheless should not be interpreted to apply here.

[112] *See, e.g.*, NAL Response at 10-11 (claiming that because it may be acquired from an "idle device or a device used for a data session" the location information is not CPNI).

[113] *NAL*, 35 FCC Rcd at 1671, para. 44.

[114] 47 U.S.C. § 222(h)(1)(A).

[115] *NAL*, 35 FCC Rcd at 1670-71, paras. 42-43 (citing Supplemental LOI Response at 3-4, Response to Question 2).

[116] 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 Sprint to obtain the location information at issue here. *Bostock v. Clayton* (continued….)

prong of the CPNI 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."[117] We recognize 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."[118] But we are far from that scenario here, given the many necessary links to Sprint's telecommunications services for the CPNI definition to apply. 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" Sprint.[119] And the information must have been provided by consumers in a manner that reflects the statutorily required nexus to Sprint's telecommunications service.[120] 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 Sprint would prefer.

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

B. Sprint Had Fair Notice That Its LBS Practices Were Subject to Enforcement Under the Communications Act

34. We reject Sprint's claim that it lacked fair notice that its practices involving customer location information were subject to the Communications Act and potential penalties thereunder.[121] The language of section 222 demonstrates that customer location information is CPNI; Sprint's practices involving CPNI, including customer location information, therefore unquestionably are regulated under the Act and the Commission's CPNI Rules; and Sprint'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.

35. Sprint argues that the *NAL* "violates due process because the Commission has never previously explained its newfound view that all location information derived from a wireless network is CPNI, nor has it announced any rule requiring providers to shut down or fundamentally alter an entire line of business within 30 days of a press report."[122] Sprint's arguments are unavailing. As an initial matter, Sprint mischaracterizes the 30-day period during which the Commission did not assess a fine, arguing that the Company did not have fair notice of what it describes as a "rule requiring providers to shut down or fundamentally alter an entire line of business within 30 days of a press report."[123] Sprint is mistaken, as the 30-day period cited in *NAL* was not a deadline for which Sprint required fair notice, but rather a grace period during which the Commission used its discretion and did not assess a fine.[124]

Cty., 140 S. Ct. 1731, 1739 (2019) (In contrast to the statute at issue there, Congress "could have added '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.

[117] *2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9616, para 23.

[118] 47 U.S.C. § 153(51).

[119] 47 U.S.C. § 222(h)(1)(A).

[120] 47 U.S.C. § 222(h)(1)(A).

[121] *See* NAL Response at 4, 13, 21-24

[122] NAL Response at 21.

[123] *See* NAL Response at 24.

[124] However, Sprint'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 (continued….)

36. Sprint also argues that before the Commission imposes what the Company mischaracterizes as a "newfound view" of CPNI,[125] the Commission must first have "either put this language into [the regulation] itself, or at least referenced this language in [the regulation]."[126] But the Commission is not limited to this option. 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 a proper vehicle to adjudicate the specific bounds of what is lawful and what is not, subject to principles of fair notice.[127] Contrary to Sprint's assertion, the Commission is not required by principles of fair notice to announce that LBS data, in particular, meets the definition of CPNI under section 222 of the Act or the Commission's CPNI Rules before enforcing that statute and those rules with respect to such data.[128] As the D.C. Circuit has said, "[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.'"[129] 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.[130]

37. We reject Sprint's argument that the Commission has improperly applied the *2013 Declaratory Ruling* in this case.[131] In the *2013 Declaratory Ruling*, the Commission previously explained 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."[132] Thus, Sprint 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 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

---

fine *for every single day* such unreasonable practices were in place (both before and after the Securus/Hutcheson disclosures)—the 30 days provided Sprint with a grace period to either end the program or reform its practices.

[125] *See* NAL Response at 4, 21-24.

[126] *Id.* at 23 (quoting *United States v. Chrysler Corp*., 158 F.3d 1350, 1356 (D.C. Cir. 1998).

[127] *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").

[128] *See* NAL Response at 4, 21-24 (claiming that this is a newfound view of CPNI). However, this is not a "newfound view" and, in any event, absolute specificity is not a prerequisite for enforcing a statute or regulation. *See, e.g.*, *United States v. Lachman*, 387 F.3d 42, 56-57 (1st Cir. 2004) (stating the "mere fact that a statute or regulation requires interpretation does not render it unconstitutionally vague," and that case law "do[es] not stand for the proposition that any ambiguity in a regulation bars punishment").

[129] *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").

[130] *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).

[131] *See* NAL Response at 23-24.

[132] *2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9617, para. 24 n.54.

section 222([h])(1) is in fact CPNI."[133] 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."[134] In addition, notwithstanding the fair notice claims it makes now, Sprint previously asserted to the Commission that it treated customer location information in an essentially equivalent manner to CPNI.[135]

38. 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 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."[136] 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."[137] 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.

39. Finally, Sprint 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."[138] 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."[139] The Commission granted carriers flexibility to incorporate the specific measures and practices that are consistent with their otherwise-existing "technological choices."[140] 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.[141] And in the same order, the Commission likewise identified the limitations of relying on "contractual safeguards" to address risks

[133] *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").

[134] *2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9617, para. 24 n.54.

[135] *See* LOI Response at 1, Response to Question 1. Sprint stated that "it implements CTIA's Best Practices and Guidelines for LBS and requires compliance with the same in contracts related to LBS." *Id*. Sprint "requires customer consent to access or share the customer's location information" except for certain instances involving child safety and lawful demands for location information in response to government investigation. *Id*.

[136] 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'").

[137] 47 U.S.C. § 222(h)(1)(A).

[138] 47 CFR § 64.2010(a).

[139] *2007 CPNI Order*, 22 FCC Rcd at 6959, para. 64.

[140] *2007 CPNI Order*, 22 FCC Rcd 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").

[141] *2007 CPNI Order*, 22 FCC Rcd at 6946, para. 35.

once CPNI has been disclosed outside the covered carrier.[142] 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."[143] This guidance provides sufficient direction for Sprint to understand its obligations under the rule as relevant here.

40. Thus, Sprint 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) Sprint would be subject to forfeiture penalties for failing to protect that customer location information as required under section 222 and the Commission's CPNI Rules.

C. Sprint Failed to Take Reasonable Steps to Protect CPNI

41. Sprint 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.[144] 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). Sprint contends that the Securus disclosures to Hutcheson did not constitute legal violations of section 222 for which Sprint can be held responsible.[145] Sprint then claims that it acted reasonably to protect its customers' location information both before and after the Securus disclosure came to light.[146] Sprint also argues that the Commission improperly shifted the burden of proving that such protections were reasonable to Sprint.[147] We find Sprint's arguments unpersuasive.

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

42. As an initial matter, we conclude that it was not just disclosures to Hutcheson that were unauthorized. Rather, Securus's entire location-finding service[148] (as detailed in paragraphs 13-14, above) was predicated on unauthorized disclosures. Consistent with Sprint's own description of events, the program was outside the scope of not only its approved purpose, but also beyond any agreement with either Aggregator (and thus had not been reviewed).[149] Sprint conceded that it was unable to distinguish location requests unrelated to the authorized purpose (which involved an inmate collect-calling service).[150] And, to be clear, none of the records submitted in connection with the location-finding

[142] *2007 CPNI Order*, 22 FCC Rcd at 6952-53, para. 49.

[143] *2007 CPNI Order*, 22 FCC Rcd at 6959-60, para. 65.

[144] 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.").

[145] *See* NAL Response at 20-21.

[146] *See* NAL Response at 17-20.

[147] *See* NAL Response at 15-17.

[148] *See NAL*, 35 FCC Rcd at 1664-65, paras. 20-21 (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).

[149] *See* LOI Response at 8, Response to Question 8; *NAL*, 35 FCC Rcd at 1665, paras. 22-23.

[150] *See NAL*, 35 FCC Rcd at 1665, 1683-84, paras. 22, 84.

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 purpose (a purpose that required consumer consent) and Sprint provided the requested location information, a separate, unauthorized disclosure occurred. 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.[151] Thus, the disclosures made to Hutcheson were doubly unauthorized under section 222(c)(1): first, Securus used the façade of their approved purpose to hide the true purpose and destination of the request, resulting in Sprint'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.[152]

43. Sprint attempts to avoid this conclusion by contending that it cannot be held responsible for the unauthorized disclosures because "Securus and other third-party location-based service providers can neither be deemed 'agent[s]' of Legacy Sprint nor 'person[s] acting for' Legacy Sprint within the meaning of Section 217, at least when they misappropriate information provided by Legacy Sprint."[153] But 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."[154] Although the *NAL* noted that "Sprint does not appear to argue that situation is present here,"[155] the totality of the record persuades us that this is, in fact, the import of the facts and Sprint's arguments here.

44. In making these arguments, Sprint appears to conflate distinct obligations it is subject to under section 222 of the Act and the Commission's rules. In particular, Sprint contends that "the NAL suggests that Section 217 of the Act would allow it to hold Legacy Sprint strictly liable for the acts of the third-party location-based service providers, even if Legacy Sprint's program reasonably protected customer location information."[156] Even setting aside Sprint's erroneous assumption about the reasonableness of its safeguards, carriers' legal duty to "take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI" under section 64.2010(a) of the rules is separate from the additional restriction on unauthorized use or disclosure in section 222(c)(1) of the Act and section 64.2007(b) of the Commission's rules.[157] Rather than incorporating some kind of *de minimis*

[151] *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 1664-65, para. 21 (describing Hutcheson's uploading of documents that were blatantly not legal authorizations in order to obtain location information). As the *NAL* explained, "Sprint does not deny the existence of the Securus location-finding service nor the abuse of that system by Hutcheson." *NAL*, 35 FCC Rcd at 1665, para. 22. Sprint likewise does not dispute here that Hutcheson was able to access location data by providing documents that were blatantly not legal authorizations as described in the *NAL* and confirmed in the Hutcheson Sentencing Memo, and also does not provide any reason to believe that Securus (let alone Sprint) could have or would have made that assessment before providing the location data. While Sprint states in its NAL Response that entries in a spreadsheet relied upon in the *NAL* "contain no information demonstrating . . . that any CPNI was disclosed without lawful authorization," NAL Response at 6, it does not elaborate on any theory of how Sprint possibly could have obtained the authorization it was required to obtain under section 222(c)(1) and section 64.2007(b) of the rules under the circumstances here. We thus are unpersuaded by that cursory assertion.

[152] *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 1664-65, para. 21.

[153] NAL Response at 20.

[154] *NAL*, 35 FCC Rcd at 1673, para. 51 n.147.

[155] *NAL*, 35 FCC Rcd at 1673, para. 51 n.147.

[156] NAL Response at 20.

[157] 47 U.S.C. § 222(c)(1); 47 CFR § 64.2007(b).

exception or reasonableness standard, section 222(c)(1)'s statutory restriction on use and disclosure is unequivocal, which is likewise reflected in section 64.2007(b) of the Commission's rules.[158] And as the *NAL* further explained, "the obligation to protect CPNI falls on *telecommunications carriers*; the carrier must obtain customer approval to use, disclose, or permit someone else to access the CPNI for any purpose not strictly related to the purpose for which it was provided to the carrier."[159] As the *NAL* explained, "[i]f Sprint was relying on third parties to satisfy its obligations to obtain consent, then it is as liable for those third parties' failures as it would be if they had been the failures of Sprint itself. If not, then Sprint effectively granted those third parties the capability to access the CPNI of its customers without customer approval."[160]

45. As already noted, Sprint contends that under the circumstances at issue here, Securus and other third-party LBS providers are neither agents nor persons acting for Sprint within the meaning of section 217.[161] Despite this contention, Sprint does not claim that it directly obtained the required approval from the customers whose location information it was sharing—nor could it, given that its entire location-based services program was premised on the LBS providers obtaining customer authorization.[162] Therefore, consistent with the *NAL*, we find that the Securus disclosures, including those made to Hutcheson, were unauthorized and Sprint was appropriately admonished in relation to such disclosures.

2. Sprint'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 Sprint 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 Sprint did not have reasonable protections in place prior to 2018 *New York Times* article detailing the Securus/Hutcheson breaches,[163] but also that Sprint failed to promptly address its demonstrably inadequate CPNI safeguards after Securus/Hutcheson disclosure.[164]

47. Sprint attempts to excuse its unreasonable practices by cataloging the steps it did take before and after the *New York Times* article. As discussed in the *NAL*, Sprint argues that, prior to the Securus disclosure, its efforts conformed to the CTIA Guidelines for ensuring customer consent to the use of location data.[165] As the *NAL* further explains, Sprint states that its safeguards included various contractual, procedural, and technical safeguards.[166]

48. The safeguards that Sprint had in place before the Securus disclosure were not reasonable. As fully explained in the *NAL*:

---

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

[159] *NAL*, 35 FCC Rcd at 1672-73, para. 49.

[160] *NAL*, 35 FCC Rcd at 1674, para. 53.

[161] NAL Response at 20.

[162] *See, e.g.*, *NAL*, 35 FCC Rcd at 1662-63, para. 15.

[163] *See NAL*, 35 FCC Rcd at 1674-76, paras. 55-63.

[164] *See NAL*, 35 FCC Rcd at 1677-80, paras. 64-75.

[165] *See NAL*, 35 FCC Rcd at 1662, 1674-75, 1676, paras. 14, 58, 62.

[166] *See NAL*, 35 FCC Rcd at 1662-64, 1674-76, paras. 14-19, 58-63. In its NAL response, Sprint does not meaningfully elaborate on those safeguards. *See, e.g.*, NAL Response at 19 (asserting that Sprint's "short-term contracts [with the Aggregators] contained strong measures to protect location information," without further elaboration).

> [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. 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.[167]

As for the other safeguards that Sprint implemented to protect its customers' location information against unauthorized access, these safeguards relied almost entirely upon contractual agreement, passed on to location-based service providers through an attenuated chain of downstream contracts.[168] To enforce these safeguards, Sprint would have needed to take steps to determine whether they were actually being followed. Further, Sprint would have had to have a way of distinguishing between a legitimate request for customer location information (i.e., made pursuant to valid consumer consent) and an illegitimate one (e.g., the Securus/Hutcheson requests absent valid customer consent). Although the Commission requested that Sprint describe its efforts to verify that LBS providers obtained valid customer consent for related location requests,[169] nothing that Sprint has provided shows that it made any meaningful efforts or that it could effectively distinguish between valid and unauthorized requests for location information. And any further claim by Sprint that its contractual safeguards were effective are undermined by the inexorable fact that after the Securus disclosure, Sprint was unable to "compel Securus to cooperate with Sprint's investigation."[170] Likewise, the shortcoming in Sprint's reliance on contractual protections is further reinforced by Sprint's inability to obtain information from Zumigo about its relationship with MicroBilt, as evidenced by the fact that "Zumigo ignored Sprint's questions."[171] "Whatever a company's justification for denying or ignoring Sprint's requests for information, the refusals are further evidence of the fact that Sprint disclosed CPNI to third parties over which it had little or no control or authority."[172]

49. Likewise, Sprint's safeguards after the Securus disclosure were also unreasonable. Sprint became keenly aware of the inadequacy of its safeguards after the May 2018 *New York Times* article, and again after Securus's resistance to Sprint's subsequent investigation. Nonetheless, Sprint 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 implementing reasonable safeguards, Sprint 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.[173]

50. We reject Sprint's attempt to dispute that the reports of the Securus and Hutcheson breaches should have made Sprint aware of the need for greater safeguards.[174] Sprint observes that media reports are not always completely accurate and are treated as inadmissible hearsay under the Federal Rules of Evidence and likewise have at times been rejected as reliable evidence by the Commission.[175]

---

[167] *NAL*, 35 FCC Rcd at 1676, para. 62.

[168] *See NAL*, 35 FCC Rcd at 1674-76, paras. 58-63.

[169] *See* Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to Maureen Cooney, Head of Privacy, Office of Privacy, Government Affairs, Sprint Corp. at 3, Question 5.e (Sept. 13, 2018) (on file in EB-TCD-18-00027700) (LOI).

[170] *NAL*, 35 FCC Rcd at 1677-78, para. 68. As the Commission said in the *NAL*, "[t]he weakness of Sprint's arguments that its contract-based model provided reasonable protection of CPNI is further underscored" by the fact that Sprint could not compel Securus to cooperate. *Id*.

[171] *NAL*, 35 FCC Rcd at 1677-78, para. 68.

[172] *NAL*, 35 FCC Rcd at 1677-78, para. 68.

[173] *See NAL*, 35 FCC Rcd at 1677, para. 64.

[174] *See* NAL Response at 3-4, 14-15, 17-18.

[175] *See* NAL Response at 18.

But whatever one might say about media reports in other contexts, in fact Sprint did view the May 2018 *New York Times* article as sufficiently reliable to call for some response, for example, explaining that "[a]fter reports of the Securus incident, Legacy Sprint suspended location information sharing with LocationSmart on May 25, 2018, once it confirmed that data sharing via LocationSmart with 3CInteractive and with Securus had occurred for an unknown and unapproved purpose."[176] Nor are we persuaded that evidentiary standards governing admissibility in federal court or the statutory standard required for showings in Commission licensing proceedings should govern whether material provides a sufficient basis for a carrier to be on notice of vulnerabilities in its measures to discover and protect against unauthorized disclosures of CPNI.[177] Nothing in the *2007 CPNI Order* that adopted section 64.2010(a) of the Commission's rules suggests that the reasonableness standard was intended to be interpreted based on those other legal frameworks. Indeed, newspaper articles were among the sources of evidence relied upon by the Commission in that proceeding.[178] The case for Sprint's ability to ignore the May 2018 *New York Times* article despite its obligations under section 64.2010(a) of the rules to discover and protect against breaches is especially weak here, where the *New York Times* article was based in part on charges filed against Hutcheson in state and federal court.[179]

51. Although Sprint touts the fact that after the May 2018 *New York Times* article it "suspended location information sharing with LocationSmart on May 25, 2018,"[180] the *NAL* explained that Sprint "undermined this step by reinstating LocationSmart (and two of its customers) into the program" three months later.[181] Further, cutting off some LBS providers' access to Sprint location information did not improve the safeguards for consumers whose location information could be disclosed under the location data sharing arrangements that remained in place. While Sprint contends that its

[176] NAL Response at 18-19. Likewise, Sprint found the media reliable enough to provide sufficient grounds to act in other situations, as well. *See, e.g.*, NAL Response at 19 ("In January 2019, [Sprint] learned through media reports that Zumigo allegedly worked with a company call MicroBilt as a sub-aggregator with respect to LBS. [Sprint] could not identify any record of Zumigo obtaining [Sprint's] prior written consent before using MicroBilt as a sub-aggregator, as it was required to do by contract. Accordingly, [Sprint] demanded that information sharing with MicroBilt immediately cease. . . ." (citations omitted)).

[177] *See* NAL Response at 18 (citing cases applying the Federal Rules of Evidence and Commission licensing decisions).

[178] *See, e.g.*, *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, 6933-35, para. 12 & n.31 (2007) (*2007 CPNI Order*) (stating that "[t]he carriers' record on protecting CPNI demonstrates that the Commission must take additional steps to protect customers from carriers that have failed to adequately protect CPNI," and citing, among other things, Frank Main, *Anyone Can Buy Cell Phone Records: Online Services Raise Security Concerns for Law Enforcement*, Chi. Sun Times, Jan. 5, 2006, at A3; Frank Main, *Cell Call Lists Reveal Your Location: Anybody Can Pay to Track Where You Used Phone*, Chi. Sun Times, Jan. 19, 2006, at A3; and Frank Main, *Blogger Buys Presidential Candidate's Call List: "Nobody's Records Are Untouchable," as $90 Purchase Online Shows*, Chi. Sun-Times, January 13, 2006, at A10.); *id*. at 6933-35, para. 12 & n.37 (stating that "companies have sued dozens of people whom they accuse of fraudulently obtaining phone records," and citing, among other things, Matt Richtel and Miguel Helft, *An Industry Is Based on a Simple Masquerade*, N.Y. Times, Sept. 11, 2006, at C1).

[179] *See, e.g.*, 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 ("Thousands of jails and prisons across the United States use a company called Securus Technologies to provide and monitor calls to inmates. But the former sheriff of Mississippi County, Mo., used a lesser-known Securus service to track people's cellphones, including those of other officers, without court orders, according to charges filed against him in state and federal court. . . . ").

[180] *See* NAL Response at 18-19. Sprint also had provided Zumigo 90 days' notice of termination, but ended up renewing its contract with that aggregator in October 2018. NAL Response at 19; *NAL*, 35 FCC Rcd at 1679-80, para. 74.

[181] *NAL*, 35 FCC Rcd at 1677, para. 66.

contracts with the Aggregators after the May 2018 *New York Times* article contained "strong measures to protect location information,"[182] as with Sprint's prior reliance on contracts, such protections only could be meaningful if effectively enforced. As the *NAL* explained, new procedures that Sprint developed for use in conjunction with the contractual protections "failed to address key weaknesses with Sprint's location-based services program, and there is little evidence that Sprint actually followed through with these policies in a way that had any meaningful impact."[183] Furthermore, "the January 8, 2019, *Motherboard* report on its success purchasing customer location information that was disclosed to MicroBilt perfectly illustrates the vulnerability that remained in Sprint's aggregator program" given that Sprint's "so-called 'improved' safeguards . . . failed to (1) detect the presence of an apparently unauthorized location-based service provider able to submit requests via Zumigo or (2) prevent that entity from obtaining Sprint's customer location information without consent."[184] Thus, after considering all of the data security measures that Sprint implemented in response to the Securus disclosure,[185] we conclude that these measures were inadequate.

52. Sprint further argues that the Commission fails to appropriately account for the fact that the LBS providers were providing "valuable services."[186] We disagree. The issue here is not whether there are any beneficial services offered by LBS providers, but whether Sprint reasonably protected its customers' location information. And there is no question of the risks that remained in Sprint's measures after the May 2018 *New York Times* article, given the subsequent unknown and unapproved access by MicroBilt, as discussed in the *NAL*.[187] 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 Sprint did not have a reliable way of confirming customer consent. The Commission considered Sprint's arguments, but finds they are outweighed by these risks.

53. 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.[188] Rather than taking definitive steps to remedy the obvious LBS program issues, Sprint instead took piecemeal steps. Moreover, the steps Sprint took did not rectify the systemic vulnerabilities at the heart of its LBS program—including relying

[182] NAL Response at 19.

[183] *NAL*, 35 FCC Rcd at 1678-79, para. 71; *see also id*. at 1666, para. 26 (discussing the measures Sprint began formalizing in June 2018); *id*. at 1678, para. 69 ("Sprint failed to provide any evidence showing that it sought to uncover other unauthorized programs, abuses in its authorized programs, or other weaknesses in its oversight of access to customer location information.").

[184] *NAL*, 35 FCC Rcd at 1679, paras. 72-73. Sprint asserts that "there is no evidence or allegation that any location information was improperly disclosed in relation to those [post-*New York Times* article] contracts." NAL Response at 19. But pointing to specific unauthorized disclosures for particular, identified customers is not the only possible grounds for finding Sprint's procedures unreasonable. Our analysis of the merits of those procedures, particularly when coupled with the MicroBilt's access that was unknown to Sprint and nonetheless had access to Sprint customers' location information starkly reveal the flaws in Sprint's safeguards.

[185] *See* NAL Response at 18-20.

[186] NAL Response at 20. Sprint further asserts that Zumigo not only was offering valuable services but "was not implicated in the Securus incident." NAL Response at 19. Notably, however, Sprint'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 Sprint's safeguards, we reject the theory that the reasonableness of those measures in the case of Zumigo can be inferred from the fact that even more unauthorized disclosures have not been publicly identified.

[187] *NAL*, 35 FCC Rcd at 1679, paras. 72-73; *see also* NAL Response at 19-20 (discussing MicroBilt's access to Sprint customers' location information and Sprint's resulting decision to terminate its contract with Zumigo).

[188] *See NAL*, 35 FCC Rcd at 1677-80, paras. 65-74.

on third parties to obtain customer consent for the disclosure of location information and failing to verify the validity of that consent.

54. Sprint's attempts to characterize the Commission as relying on an extreme strict liability-type approach fall short, as well.[189] Section 64.2010 of the rules requires only reasonable measures—not perfect ones—but that is not enough to help Sprint here. Contrary to Sprint'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, yielding an approach that results in strict liability contrary to the reasonableness standard reflected in that rule.[190] Rather, we have carefully examined Sprint's procedures, including the fundamental flaws in those safeguards, such as the shortcomings in Sprint's reliance on contractual protections to ensure customer consent.[191] Our assessment under section 64.2010(a) thus is a straightforward evaluation of reasonableness, consistent with the text of the rule.

3. Sprint Bore the Burden of Production

55. 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 Sprint did not use reasonable safeguards throughout the period of the violation.[192] As such, while the *NAL* discussed Sprint's burden of production to demonstrate that its protection of customer CPNI was reasonable,[193] that burden-shifting is not necessary given the preponderance of the evidence. Nonetheless, even if unnecessary to prove Sprint's violations in this matter, the *NAL* properly shifted the burden of production to Sprint.

56. *First*, as the *NAL* explained[194] 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.[195] In the *NAL*, the Commission found that Sprint failed to demonstrate that its safeguards were reasonable following the disclosure of Securus's unauthorized location-finding service in May 2018.[196]

57. Sprint acknowledges that the *NAL* based its approach on the *2007 CPNI Order*,[197] 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."[198] However, Sprint is incorrect when it asserts that the *2007 CPNI Order* cannot support the burden-shifting approach in cases

[189] *See* NAL Response at 15, 18, 20.

[190] *See* NAL Response at 15, 18.

[191] *NAL*, 35 FCC Rcd at 1674-80, paras. 55-75; NAL Response at 18-20.

[192] *See NAL*, 35 FCC Rcd at 1674-80, paras. 55-75.

[193] *See NAL*, 35 FCC Rcd at 1658-59, 1674, 1677, paras. 8, 56-57, 67.

[194] *See NAL*, 35 FCC Rcd at 1658-59, para. 8.

[195] *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").

[196] *See NAL*, 35 FCC Rcd at 1674-80, paras. 55-75.

[197] *See* NAL Response at 15-16 (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*)).

[198] *NAL*, 35 FCC Rcd at 1674, para. 56.

outside of the pretexting context.[199] 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.[200] The rationale applies with equal force to the kind of disclosure at issue here, where a fundamental issue is whether Sprint 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.[201] Broadly, in relation to Securus's entire unauthorized location-finding service, Securus used the pretext that it was requesting location information from Sprint for its approved purpose 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.[202] 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*.

58. *Second*, Sprint recognizes 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.[203] The Commission finds that the unauthorized disclosure in this case gave rise to a rebuttable presumption that Sprint did not reasonably protect customer location information from unlawful access.[204] 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 purpose and Sprint's resultant disclosures of consumer location information were unauthorized. Sprint'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, Sprint argues that the Commission cannot use the Securus and Hutcheson breaches to support shifting the burden of production to Sprint to provide evidence of the reasonableness of their post-May 2018 security practices.[205] Specifically, Sprint asserts that because no provider can achieve perfection and the appropriate measures to employ can vary by carrier and circumstance, that undercuts the reasonableness of any burden shifting here.[206] We disagree.

---

[199] NAL Response at 16.

[200] We thus reject Sprint's claim that "the Commission is attempting to expand the approach" to burden shifting under the *2007 CPNI Order* "without ever having grappled with" petitions seeking reconsideration of that aspect of the *2007 CPNI Order*. NAL Response at 19 n.50. Burden shifting here falls within the scope of what was provide for in the *2007 CPNI Order*, which was not stayed pending action on those petitions for reconsideration. And in any case, Sprint has availed itself of the opportunity to contest the substantive merits of burden shifting in this enforcement proceeding.

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

[202] 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 at1664-65, para. 21; *see also supra* para. 14.

[203] See NAL Response at 17 n.10.

[204] *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).

[205] *See* NAL Response at 15-17.

[206] *See* NAL Response at 16-17.

59. In the *NAL*, we found that Sprint 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.[207] This is further bolstered by the Department of Justice's case against Hutcheson.[208] And though the Commission opted to admonish Sprint only for the unauthorized disclosures made to Hutcheson, it would have been appropriate to admonish Sprint 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,[209] carriers cannot disclaim their obligations to protect customer CPNI by delegating those obligations to third parties.[210] We reiterate here that "Sprint is not absolved from liability simply because it was not directly responsible for operating the programs under which unauthorized disclosures occurred."[211] And 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."[212] Further, section 222(c)(1) of the Act[213] makes the responsibility for avoiding unauthorized disclosures a carrier obligation and prohibits use and disclosure except in certain narrow circumstances, without any reasonableness criterion. Sprint 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 later violations period was reasonable—particularly because, as discussed, those safeguards did not materially change in the interim timeframe.

60. The unauthorized disclosure at issue gave rise to a rebuttable presumption that Sprint did not adequately protect customer information from unlawful access. The burden of production then shifted to Sprint to offer evidence that it had reasonable safeguards in place.[214]

61. Rather than taking reasonable steps to safeguard its customers' location information after the Securus/Hutcheson disclosures were reported,[215] Sprint 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 Sprint 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.

---

[207] *See NAL*, 35 FCC Rcd at 1672-74, paras. 46-54. "The evidence reflects that Hutcheson used the Securus service to obtain the location information of Sprint customers. Sprint shared the information with LocationSmart, which the shared it with 3Cinteractive, which then shared it with Securus. *Id*. at 1672, para.47.

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

[209] 47 U.S.C. § 217.

[210] *See NAL*, 35 FCC Rcd at 1659, 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.

[211] *See NAL*, 35 FCC Rcd at 1672-73, para. 49.

[212] *NAL*, 35 FCC Rcd at 1673, para. 51 n.147.

[213] 47 U.S.C. § 222(c)(1).

[214] We note that in some instances—most notably with regard to various reviews and investigations that implicated the LBS program and over which Sprint asserted privilege—Sprint claimed to have taken certain reasonable steps, but did not produce documentary evidence of those steps. *See NAL*, 35 FCC Rcd at 1664, 1678, paras. 19, 69.

[215] Many of the possible reasonable steps were enumerated in the *NAL*. *See NAL*, 35 FCC Rcd at 1677-80, paras. 65-74.

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

62. After considering the evidence in the record, the relevant statutory factors, the Commission's *Forfeiture Policy Statement*, and the arguments advanced by Sprint in the NAL Response, we find that Sprint is liable for a total forfeiture of $12,240,000 for its violations of section 222 of the Act and section 64.2010 of the Commission's rules.[216] 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).[217] The Commission found in the *NAL* that Sprint apparently engaged in 11 continuing violations—one for each ongoing relationship with a third-party LBS provider or aggregator that had access to Sprint customer location information more than 30 days after publication of the *New York Times* report—and that each violation continued until Sprint terminated the corresponding entity's access to customer location information.[218] Using this methodology, the Commission found Sprint apparently liable for a total base forfeiture of $6,120,000. Upon considering the nature of the violations and the risk of harm they posed to consumers, the Commission then applied a 100% upward adjustment to the base forfeiture amount, resulting in a total proposed forfeiture of $12,240,000.[219]

63. Sprint challenges these forfeiture calculations with two principal arguments. *First*, Sprint argues that the *NAL* describes at most a single continuing violation, not a separate violation for each of the 11 entities participating in Sprint's LBS program. As such, according to Sprint, the forfeiture exceeds the applicable statutory maximum.[220] *Second*, Sprint challenges the Commission's application of a 100% upward adjustment to the base forfeiture. Sprint argues that in determining the amount of the upward adjustment, the Commission impermissibly cited to the same factors used for determining the base forfeiture amount.[221] Sprint also contends that no upward adjustment is warranted because it did not engage in egregious or intentional misconduct or cause substantial harm to consumers.[222] For the reasons discussed below, we are not persuaded by any of these arguments and decline to cancel or reduce the forfeiture proposed in the *NAL*.

1. The Commission Reasonably Found that Sprint Engaged in 11 Continuing Violations

64. Section 503(b) of the Act authorizes the Commission to impose a forfeiture against Sprint 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."[223] The Commission found that, because Sprint permitted 11 separate entities to access its customers' location information in the apparent absence of reasonable safeguards, the Company engaged in 11 continuing violations of section 222 of the Act and section 64.2010 of the Commission's rules. Sprint challenges this methodology, arguing that "[n]one of the 11 entities included in this calculation was accused of misappropriating data" and that to the extent Sprint violated section

[216] 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.

[217] *NAL*, 35 FCC Rcd at 1682, para. 80.

[218] *NAL*, 35 FCC Rcd at 1682, para. 81.

[219] *NAL*, 35 FCC Rcd at 1683-84, paras. 84-87.

[220] NAL Response at 25-26.

[221] NAL Response at 26.

[222] NAL Response at 26-29.

[223] *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).

64.2010 by allowing them to continue operating, it "did not have any reason or occasion to make 11 separate decisions."[224] Sprint therefore asserts that there could have been at most one continuing violation (subject to the $2,048,915 penalty cap) and the *NAL*'s finding of 11 separate continuing violations (one for each LBS provider or Aggregator) constitutes an impermissible attempt to circumvent the statutory maximum.[225]

65. 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.[226] 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."[227] 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 . . . ." [228]

66. 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),[229] 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 Sprint 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 Sprint 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 Sprint. 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.

67. The approach taken in the *NAL* was not only reasonable, it was—contrary to Sprint's claim that it exceeded the statutory maximum—eminently *conservative*. As described in the *NAL*, Sprint'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 Sprint 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).[230] Using that methodology—and taking into account the tens of millions of

[224] NAL Response at 25.

[225] NAL Response at 26.

[226] 47 U.S.C. § 503(b); 47 CFR § 1.80(b).

[227] *TerraCom Inc. and YourTel America, Inc*., Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325, 13343, para. 50 (2014).

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

[229] *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, para. 20 (EB 2015).

[230] 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.

consumers whose highly sensitive location information was made vulnerable by Sprint—would have resulted in a significantly higher forfeiture than what was proposed in the *NAL*.

68. 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 Sprint customer location information up to the statutory maximum ($204,892 per day up to $2,048,915 for each and every 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 Sprint 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 Sprint 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.

69. We also reject any claim that Sprint'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 Sprint's fair notice claims,[231] 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. Sprint 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.[232] 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.[233] 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.[234]

2. The Upward Adjustment is Permissible and Warranted

70. Sprint argues that the Commission failed to properly justify the 100% upward adjustment to the forfeiture amount proposed in the *NAL.* Sprint contends that certain upward adjustment factors cited in the *NAL*—the duration of the violation and the risk of harm it posed to consumers—were already considered in setting the base forfeiture amount and therefore constitute arbitrary double counting.[235] Sprint also asserts that no upward adjustment is warranted because it did not engage in egregious or intentional misconduct or cause substantial harm to consumers.[236]

71. We reject these arguments and maintain the 100% 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."[237] The plain language of the statute provides the Commission with broad discretion

[231] *See supra* III.B.

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

[233] 47 U.S.C. § 503.

[234] *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).

[235] NAL Response at 26.

[236] NAL Response at 26-29.

[237] 47 U.S.C. § 503(b).

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.[238] These factors include, importantly, "egregious misconduct," "substantial harm," "repeated or continuous violation," and "ability to pay/relative disincentive," among others.[239]

72. The Commission weighed these factors when making the determination that the base forfeiture in this case merited a substantial upward adjustment. Sprint's conduct was egregious; the *NAL* detailed how Sprint apparently did not review third-party proposals for using its customer location information, did not review customer consent records, and did not exercise its right to audit the Aggregators.[240] 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.[241] 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 Sprint 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.[242] 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 Sprint's status as a major telecommunications provider to determine what penalty, when applied, would adequately provide Sprint 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. Sprint's arguments to the contrary do not defeat Congress's decision to grant the Commission the power to weigh the factors and make such adjustments "as justice may require."[243] Nor do Sprint's arguments persuade us that the 100% upward adjustment, which is in line with upward adjustments in other cases involving consumer harms,[244] was unwarranted.

---

[238] 47 CFR § 1.80(b)(10), Table 3.

[239] *Id.*

[240] *NAL*, 35 FCC Rcd at 1683-84, para. 84.

[241] *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 letter 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 Sprint, AT&T, T-Mobile, and Verizon).

[242] *NAL*, 35 FCC Rcd at 1684, para. 85.

[243] 47 U.S.C. § 503(b).

[244] *See, e.g., Scott Rhodes,* Forfeiture Order, 36 FCC Rcd 705, 728, 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, para. 59 (2021) (upward adjustment equaling 50% (continued….)

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

73. We reject Sprint's supplemental constitutional objections that: (1) the FCC combines investigatory, prosecutorial, and adjudicative roles in violation of constitutional due process and separation of powers requirements;[245] (2) the issuance of a forfeiture order by the Commission would violate Article III and the Seventh Amendment;[246] 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.[247] Sprint's arguments are premised on misunderstandings regarding the relevant statutory framework, the nature of the Commission's actions, and relevant precedent.

74. As a threshold matter, Sprint 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, Sprint is entitled to a trial *de novo* in federal district court before it can be required to pay the forfeiture.[248] Sprint'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.[249] Likewise, Sprint'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 Sprint's statutory right to a trial *de novo* before it can be required to pay the forfeiture.[250] 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.

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

76. *Combination of Functions.* With respect to Sprint's claimed due process violation,[251] Sprint fails to demonstrate sufficient grounds for concluding that a combination of functions in the

---

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, para. 25, 4674, para. 33 (2018) (upward adjustment equaling 50% of base forfeiture amount imposed on robocaller who engaged in illegal spoofing for robocall telemarketing activities).

[245] Letter from Helgi C. Walker and Russell B. Balikian, counsel to T-Mobile/Sprint, to Michael Epshteyn and Rosemary Cabral,, Enforcement Bureau, FCC, EB-TCD-18-00027702 and EB-TCD-18-00027700, at 2-3 (filed June 22, 2023) (T-Mobile/Sprint June 22, 2023 Supplemental NAL Response).

[246] T-Mobile/Sprint June 22, 2023 Supplemental NAL Response at 2.

[247] T-Mobile/Sprint June 22, 2023 Supplemental NAL Response at 3-4.

[248] 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 Sprint theoretically might elect to pay the forfeiture voluntarily does not diminish its statutory right to a trial *de novo* in federal district court.

[249] *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.'").

[250] *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).

[251] T-Mobile/Sprint June 22, 2023 Supplemental NAL Response at 2-3. Sprint contends that the combination of functions in the FCC "violates due process and the separation of powers under the circumstances presented in this case," T-Mobile/Sprint June 22, 2023 Supplemental NAL Response at 2, but does not develop the separation of powers argument or explain why the combination of functions in the Commission violates existing separation of

(continued….)

Commission's enforcement process here renders it constitutionally suspect, even apart from Sprint'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 adjudicators."[252] To overcome that presumption requires "a showing of conflict of interest or some other specific reason for disqualification."[253]

77. Sprint fails to demonstrate a concern specific to the Commission's forfeiture order here sufficient to overcome the presumption of honesty and integrity. Insofar as Sprint 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.[254]

78. Sprint also expresses concern that "the Commission performed its own investigations of alleged violations of the Communications Act (based on newspaper articles), prosecuted them by issuing NALs, and plans to resolve any challenges to these NALs itself by imposing forfeitures directly."[255] 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 concerns 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.[256]

---

powers precedent. Consequently, we do not find that a basis to alter our approach in this forfeiture order, and instead focus on those arguments that Sprint does develop.

[252] *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).

To the extent that Sprint argues that the Supreme Court's decision in "*Withrow* is ripe for overruling," T-Mobile/Sprint June 22, 2023 Supplemental NAL Response at 3, doing so would be a matter for the Supreme Court itself, and we are not persuaded to chart a different approach on our own.

[253] *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'").

[254] *See* T-Mobile/Sprint 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)).

[255] T-Mobile/Sprint June 22, 2023 Supplemental NAL Response at 3.

[256] 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

(continued….)

79. Nor do the "[s]pecial facts and circumstances" that Sprint alleges are present persuade us that due process concerns are present here.[257] Sprint criticizes the magnitude of the proposed forfeiture and the methodology used to calculate them as reflecting a "break from precedent and policy," that "reflects animosity toward the parties and an unwillingness to neutrally consider the legal and factual arguments that [Sprint] raised."[258] 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.[259] We also are not persuaded that the Commission's decision to issue an NAL proposing even a 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.[260] 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 Sprint provide evidence that is the case here.[261] 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.[262] 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,"[263] and Sprint 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*.

---

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.

[257] T-Mobile/Sprint June 22, 2023 Supplemental NAL Response at 3.

[258] T-Mobile/Sprint June 22, 2023 Supplemental NAL Response at 3.

[259] *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 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.").

[260] *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).

[261] *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).

[262] *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").

[263] 47 U.S.C. § 503(b)(4).

80. Instead, the "[s]pecial facts and circumstances" raised by Sprint amount to little more than differences of opinion regarding legal interpretations or the gravity of the violations.[264] We are not persuaded that such differences of opinion—which can arise in virtually every Commission enforcement action—inherently provide any reason to question the Commission's neutrality as an adjudicator. The main thrust of Sprint's argument seems to be that "the penalties would be among the largest in the Commission's history and impose penalty amounts typically reserved for fraud or deliberate misconduct" in what Sprint characterizes as a "break from precedent and policy."[265] But Sprint provides no basis to expect that only fraud or deliberate misconduct can justify penalties of the magnitude at issue here, and we already have explained our rationale for both the methodology for calculating the forfeiture and its ultimate magnitude.[266] Both the Communications Act and Commission rules direct the agency, when deciding on a forfeiture amount, 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," and that is precisely what the Commission did here.[267] It is not surprising that the private company that potentially will be subject to a forfeiture might assess the nature and gravity of its violations differently than the Commission, but those differing views are not grounds for finding a likelihood of bias on the part of the Commission. We thus reject Sprint's claims of a due process violation through our implementation of the section 503(b) NAL-based process here.

81. *Trial By Jury.* We also reject Sprint's contention that adjudication of the violations at issue here may not constitutionally be assigned to a federal agency.[268] The Seventh Amendment preserves "the right of trial by jury" in "[s]uits at common law, where the value in controversy shall exceed twenty dollars,"[269] but the Seventh Amendment applies only to suits litigated in Article III courts, not to administrative adjudications conducted by federal agencies.[270] 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."[271] Congress has broad authority to "assign adjudication of public rights to entities other than Article III courts."[272] 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 federal workplace safety requirements,[273] "adjudicating violations of the customs and immigration laws and assessing penalties based thereon,"[274] adjudicating "whether an unfair labor practice had been committed and of ordering backpay where appropriate,"[275] and the grant or reconsideration of a grant of a patent.[276] That precedent confirms the constitutionality validity of FCC

[264] T-Mobile/Sprint June 22, 2023 Supplemental NAL Response at 3.

[265] T-Mobile/Sprint June 22, 2023 Supplemental NAL Response at 3.

[266] *See supra* Section III.D.

[267] 47 U.S.C. § 503(b)(2)(E); 47 CFR § 1.80(b)(10).

[268] T-Mobile/Sprint June 22, 2023 Supplemental NAL Response at 2.

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

[270] *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).

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

[272] *Id*.

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

[274] *Id*. at 451.

[275] *Id*. at 453.

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

adjudication of violations of the Communications Act, even setting aside the reality that Sprint 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"[277] designed to protect consumer privacy even as the communications marketplace became more open to competition,[278] 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.[279]

82. Relying principally on the Supreme Court's decision in *Tull v. United States* and the Fifth Circuit's decision in *Jarkesy*, Sprint 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—because the violations allegedly are analogous to a common law action in debt.[280] 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.[281] 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."[282] 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.[283] 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 resolution to a

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

[278] *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.").

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

[280] T-Mobile/Sprint June 22, 2023 Supplemental NAL Response at 2 (citing *Tull v. United States*, 481 U.S. 412 (1987) and *Jarkesy v. SEC*, 34 F.4th 446 (5th Cir. 2022)). Sprint 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.

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

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

[283] Sprint also cites *Burgess v. FDIC*, but in pertinent part that district court decision simply applied the binding circuit precedent of *Jarkesy*. T-Mobile/Sprint June 22, 2023 Supplemental NAL Response at 2 (citing *Burgess v. FDIC*, 2022 WL 17173893, at *10–11 (N.D. Tex. Nov. 6, 2022)).

forum in which jury trials are unavailable."[284] We thus are unpersuaded by Sprint's reliance on *Tull* and *Jarkesy*.[285]

83. *Nondelegation*. Finally, contrary to Sprint's contention,[286] 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.[287] Contrary to Sprint'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.[288]

84. We also are unpersuaded by Sprint'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,[289] 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.[290] 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

[284] *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.

[285] 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).

[286] T-Mobile/Sprint June 22, 2023 Supplemental NAL Response at 3-4.

[287] 47 U.S.C. § 503(b)(3), (4).

[288] *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").

[289] 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 285.

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

the ends of justice."[291] 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.[292] The circumstances here therefore are distinct from those in *Jarkesy* where "Congress offered *no guidance* whatsoever."[293]

IV. CONCLUSION

85. Based on the record before us and in light of the applicable statutory factors, we conclude that Sprint willfully and repeatedly violated section 222 of the Act[294] as well as section 64.2010 of the Commission's rules[295] 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 or to cancel or reduce the $12,240,000 forfeiture proposed in the *NAL*.

V. ORDERING CLAUSES

86. 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, Sprint Corporation **IS LIABLE FOR A MONETARY FORFEITURE** in the amount of twelve million, two-hundred and forty thousand dollars ($12,240,000) for willfully and repeatedly violating section 222 of the Act and section 64.2010 of the Commission's rules.

87. 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.[296] Sprint Corporation shall send electronic notification of payment to Shana Yates, Kimbarly Taylor, and Michael Epshteyn, Enforcement Bureau, Federal Communications Commission, at shana.yates@fcc.gov, kimbarly.taylor@fcc.gov, and michael.epshteyn@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.[297]

88. In order for Sprint Corporation to pay the proposed forfeiture, Sprint Corporation 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 by check or money order. Below are instructions that payors should follow based on the form of payment selected:[298]

---

[291] 47 U.S.C. § 154(j).

[292] *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).

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

[294] 47 U.S.C. § 222.

[295] 47 CFR § 64.2010.

[296] *Id.*

[297] 47 U.S.C. § 504(a).

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

- 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[299] or printed CORES form[300] 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).[301] 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.

89. 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.

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

[300] 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.

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

90. **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 Edward H. Smith, Senior Vice President of Public Policy and Government Affairs, and Christopher Koegel, Director, Federal Regulatory Affairs, T-Mobile USA, Inc., 601 Pennsylvania Ave., N.W., Suite 800, Washington, DC 20005.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

STATEMENT OF
CHAIRWOMAN JESSICA ROSENWORCEL

Re: *In the Matter of Sprint Corporation*, Forfeiture Order, File No.: EB-TCD-18-00027700 (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 Sprint Corporation*, Forfeiture Order, File No.: EB-TCD-18-00027700 (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 Sprint Corporation*, Forfeiture Order, File No.: EB-TCD-18-00027700 (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.