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

In the Matter of	)	
	)	
AT&T, Inc.	)	File No.: EB-TCD-18-00027704
	)	NAL/Acct. No.: 202032170004
	)	FRN: 00057193701

FORFEITURE ORDER

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

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

TABLE OF CONTENTS

Heading Paragraph #

I. INTRODUCTION

1. On February 28, 2020, the Commission issued a Notice of Apparent Liability for Forfeiture and Admonishment (*NAL*) against AT&T, Inc. (AT&T or Company).[1] In the *NAL*, the Commission admonished AT&T 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 AT&T $57,265,625 for failing to take reasonable steps to protect its customers' location information. After

[1] *AT&T, Inc.*, Notice of Apparent Liability for Forfeiture and Admonishment, 35 FCC Rcd 1743 (2020) (*NAL*).

reviewing the Company's response to the *NAL*,[2] we find no reason to cancel, withdraw, or reduce the proposed penalty, and impose a penalty of $57,265,625 against AT&T.

II. BACKGROUND

A. Legal Background

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

3. *Customer Consent to Disclose CPNI.* With limited exceptions, a carrier may only use, disclose, or permit access to CPNI with customer approval.[9] Generally, carriers must obtain a customer's "opt-in approval" before disclosing that customer's CPNI.[10] This means that a carrier must obtain the customer's "affirmative, express consent allowing the requested CPNI usage, disclosure, or access after the customer is provided appropriate notification of the carrier's request . . . ."[11]

4. This opt-in requirement has been in place since 2007, when the Commission amended its rules in the *2007 CPNI Order* after finding that once carriers disclosed CPNI to third parties, including

---

[2] *AT&T, Inc*., Response to Notice of Apparent Liability for Forfeiture and Admonishment (filed May 7, 2020) (on file in EB-TCD-18-00027704) (NAL Response or Response).

[3] *See generally NAL*.

[4] 47 U.S.C. § 222.

[5] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6959, para. 64 (2007) (*2007 CPNI Order*).

[6] 47 U.S.C. § 222(a).

[7] 47 U.S.C. § 222(c), (h)(1)(A) (emphasis added). "Telecommunications service" is defined as "the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used." 47 U.S.C. § 153(53). The mobile voice services provided by AT&T are "telecommunications services." *See* 47 U.S.C. § 332(c)(1); H.R. Conf. Rep. No. 104-458 at 125 (1996) ("This definition [of 'telecommunications service'] is intended to include commercial mobile service.").

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

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

[10] 47 CFR § 64.2007(b).

[11] 47 CFR § 64.2003(k).

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

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

6. The Commission made clear that the specific customer authentication requirements it adopted were "minimum standards" and emphasized the Commission's commitment "to taking resolute enforcement action to ensure that the goals of section 222 [were] achieved."[21] Although carriers are not expected to eliminate every vulnerability to the security of CPNI, they must employ "reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI."[22] They must also take reasonable measures to protect the confidentiality of CPNI—a permanent and ongoing obligation to police disclosures and ensure proper functioning of security measures.[23] As the Commission stated in the

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

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

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

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

[16] *See* 47 CFR § 64.2007(b).

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

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

[19] *See* 47 CFR § 64.2010(b)-(d).

[20] *See* 47 CFR § 64.2010(e)-(f).

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

[22] 47 CFR § 64.2010(a).

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

NAL, several government entities provide guidance and publish best practices that are intended to help companies evaluate the strength of their information security measures.[24]

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

B. Factual Background

8. *Customer Location Information and AT&T Location-Based Services Business Model.* AT&T 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 AT&T's wireless network.[26] As part of its business, AT&T ran a Location-Based Services (LBS) program until March 2019. Through the LBS program, AT&T sold access to its customers' location information to companies known as "location information aggregators," who then resold access to such information to third-party location-based service providers or in some cases to intermediary companies who then resold access to such information to location-based service providers.[27] AT&T had arrangements with two location information aggregators: LocationSmart and Zumigo (the Aggregators).[28] Each Aggregator, in turn, had arrangements with location-based service providers. In total, AT&T sold access to its customers' location information (directly or indirectly) to 88 third-party entities (including the two Aggregators).[29]

9. The AT&T LBS program was largely governed via contractual provisions that vested AT&T with oversight authority over the Aggregators. The Aggregators then entered into their own contracts with various LBS providers. This arrangement meant that it was the LBS providers who were obligated "to provide notice and obtain consent" from consumers—not the Aggregators or AT&T. AT&T asserts that its LBS program was subject to a number of safeguards and that the LBS providers and Aggregators had to satisfy various requirements, which were memorialized in and governed by contract

---

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

[25] 47 U.S.C. § 217.

[26] *See* AT&T, Inc., 2021 Annual Report, https://investors.att.com/~/media/Files/A/ATT-IR-V2/financial-reports/annual-reports/2021/complete-2021-annual-report.pdf.

[27] The *NAL* includes a more complete discussion of the facts and history of this case and is incorporated herein by reference. *See NAL*, 35 FCC Rcd at 1748-56, paras. 11-30.

[28] AT&T does not contend that its customers consented to these arrangements with the Aggregators.

[29] *See NAL*, 35 FCC Rcd at 1748-50, paras. 12-13 (citations omitted).

provisions with the Aggregators and any parties that AT&T directly sold location information to.[30] The contracts obligated the Aggregators to monitor the practices of the location-based service providers—including by making sure the LBS providers notified customers and collected affirmative customer consent for any use of location information.[31] However, AT&T did not verify the customers' consent before providing access to the location information; instead it claimed to verify on a daily basis that each request for information was tied to a consent record.[32] In addition, each LBS provider was contractually required to access and use AT&T customer location information only for a specific purpose (known as a "Use Case") that was reviewed and approved by AT&T in advance.[33] AT&T had broad authority under its contracts with the Aggregators to quickly terminate access to customer location information if an Aggregator engaged in conduct that exposed AT&T to "sanctions, liability, prosecution or other adverse consequences under applicable law."[34]

10. AT&T also had the authority to conduct audits and other internal reviews of the LBS program. According to AT&T, between January 2016 and May 2019, it conducted five reviews or audits of its disclosure of customer location information to third parties.[35] The Company claims that three of the five analyses are subject to attorney-client privilege, however, and submitted the results only of the two reviews that AT&T treated as non-privileged.[36] The results of those two audits identified various issues of concern. One audit, which reviewed the Aggregators' compliance with AT&T information security requirements for third-party vendors, identified numerous instances of non-compliance with security requirements by both Aggregators.[37] The other audit, focused on a review of AT&T's controls over certain disclosures of customer location information for the provision of location-based services, identified issues related to the "completeness of subscriber consents" and "record retention practices regarding subscriber consents."[38] AT&T averred that the issues identified in both audits were

[30] *See NAL*, 35 FCC Rcd at 1750-51, paras. 15-17 (citations omitted).

[31] *See NAL*, 35 FCC Rcd at 1750, para. 16 (citing Response to Initial Letter of Inquiry from AT&T, to Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, at 6, Response to Question 1 (Nov. 14, 2018) (on file in EB-TCD-18-00027704) (LOI Response)).

[32] *See NAL*, 35 FCC Rcd at 1750-51, para. 16 (citing Response to Supplemental Letter of Inquiry from AT&T, to Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, at 11, Response to Question 9 (May 24, 2019) (on file in EB-TCD-18-00027704) (Supplemental LOI Response)).

[33] *See NAL*, 35 FCC Rcd at 1750, para. 15.

[34] *See NAL*, 35 FCC Rcd at 1751, para. 17 (citing LOI Response at ATT-LOI-00013380, Response to Request for Documents No. 3, 2016 Master Agreement between AT&T Corp. and TechnoCom Corporation d/b/a LocationSmart, at Section 8.2 - Termination or Suspension (executed on Feb. 17, 2016 by Mario Proietti, CEO for LocationSmart and Glenn C. Girard, Assoc Dir. Customer Contracts-AT&T Services, Inc.); LOI Response at ATT-LOI-00025859, Response to Request for Documents No. 3, 2014 Master Agreement between AT&T Corp. and Zumigo, Inc., Section 8.2 – Termination or Suspension (executed on Apr. 25, 2014 by Chira Bakshi, CEO for Zumigo and Ana Castaneda, Contract Specialist for AT&T)). The contracts required the Aggregators to indemnify AT&T for various types of claims, including those arising from privacy violations, but did not provide for any other remedy—such as direct restitution to affected customers—in the event of breach.

[35] *See NAL*, 35 FCC Rcd at 1751, para. 18 (citing LOI Response at 19-21, Response to Question 11; Supplemental LOI Response at 16, Response to Question 15).

[36] *See NAL*, 35 FCC Rcd at 1751, para. 18 (citing LOI Response at 20-21, Response to Question 11; Supplemental LOI Response at 16, Response to Question 15).

[37] *See NAL*, 35 FCC Rcd at 1751-52, para. 18 (citing LOI Response at 19-20, Response to Question 11).

[38] *See NAL*, 35 FCC Rcd at 1751, para. 18 (citing LOI Response at 20, Response to Question 11).

remediated.[39] AT&T provided the general topics of the remaining three audits, but declined to produce any other information concerning those privileged reviews.

11. *Unauthorized Access and Use of Customer Location Information*. On May 10, 2018, the *New York Times* published an article that detailed security breaches involving AT&T's (and other carriers') practice of selling access to customer location information.[40] 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.[41] Not only was Securus's location-finding service outside the scope of its approved "Use Case" or any agreement with either Aggregator (and thus had not been reviewed by AT&T), 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.[42] AT&T conceded that it was unable to distinguish location requests unrelated to the authorized Use Case (which involved an inmate collect-calling service) because each request included a customer consent record that was identical to the records received for the approved service.[43]

12. 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.[44] 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.[45] In order to do so, users (including Hutcheson) were required to input the telephone number of the device they wanted to locate, and then "upload a document manually checking a box, the text of which stated, '[b]y checking this box, I hereby certify the attached document is an official document giving permission to look up the location on this phone number requested.'"[46] As soon as Hutcheson (or any other authorized user) submitted his request and uploaded a document, the Securus LBS platform would *immediately* provide

[39] *See NAL*, 35 FCC Rcd at 1751-52, para. 18 (citing LOI Response at 19-20, Response to Question 11; Supplemental LOI Response at 9, Response to Question 7).

[40] *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.

[41] *See NAL*, 35 FCC Rcd at 1752-53, 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).

[42] *See NAL*, 35 FCC Rcd at 1752-53, 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).

[43] *See NAL*, 35 FCC Rcd at 1753, para. 23.

[44] *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.

[45] *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 1752-53, paras. 20-21.

[46] Hutcheson Sentencing Memo at 3; *see also NAL*, 35 FCC Rcd at 1752, para. 20.

the requested location information (regardless of the adequacy of the uploaded document).[47] 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."[48] Those "false and fraudulent documents" included "his health insurance policy, his auto insurance policy, and pages selected from Sheriff training materials."[49] Hutcheson "submitted thousands of Securus LBS requests and obtained the location data of hundreds of individual phone subscribers without valid legal authorization."[50]

13. *AT&T's Response to the Securus Disclosures*. AT&T terminated Securus's access to AT&T customer location information in May 2018, following the *New York Times* article.[51] In June 2018, AT&T announced that it would phase out access to location information for the Aggregators and certain location-based service providers, except for those that the Company identified as offering public benefits, such as emergency services or fraud prevention.[52] Although AT&T did not specify how long the process would take, according to AT&T it terminated the access of 36 location-based service providers to its customer location information by the end of 2018.[53] In November 2018, AT&T told Enforcement Bureau staff that it planned to implement "enhanced" notice and consent measures for location information-sharing in 2019 for the remaining location-based service providers, though in its NAL Response the Company states that those efforts were rendered moot by its January 10, 2019, decision to completely shut down the LBS program.[54] According to AT&T, it terminated the access to its customer location information of an additional 28 location-based service providers by the end of January 2019 and an additional 10 such providers by the end of February 2019.[55]

14. AT&T's decision to end its LBS program followed a January 8, 2019, Motherboard article alleging 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.[56] That article focused in part on the activities of a company called MicroBilt, whose access to customer location information was suspended by AT&T on January 4, 2019.[57] On January 10, 2019, AT&T announced that "[i]n light of recent reports about misuse of location services, we decided to eliminate all location aggregator services—even those with clear consumer benefits" and stated that its location-based service program would end in March 2019.[58] While AT&T states that it sent

[47] *See* Hutcheson Sentencing Memo at 3-4; *see also NAL*, 35 FCC Rcd at 1752, para. 20.

[48] Hutcheson Sentencing Memo at 4; *see also NAL*, 35 FCC Rcd at 1753, para. 21.

[49] Hutcheson Sentencing Memo at 4; *see also NAL*, 35 FCC Rcd at 1753, para. 21.

[50] Hutcheson Sentencing Memo at 4; *see also NAL*, 35 FCC Rcd at 1753, para. 21.

[51] *See NAL*, 35 FCC Rcd at 1753, para. 23.

[52] *See NAL*, 35 FCC Rcd at 1754, para. 25 (citing Supplemental LOI Response at 1, Introduction); *see also* NAL Response at 29.

[53] *See NAL*, 35 FCC Rcd at 1754, para. 25; *see also* NAL Response at 29.

[54] *See NAL*, 35 FCC Rcd at 1754, para. 25; NAL Response at 31-32.

[55] *See NAL*, 35 FCC Rcd at 1755-56, para. 29; NAL Response at 34.

[56] *See NAL*, 35 FCC Rcd at 1755, para. 27 (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).

[57] *See NAL*, 35 FCC Rcd at 1755, para. 26.

[58] *See* Alfred Ng, *AT&T is Cutting Off All Location-Data Sharing Ties in March*, CNET (Jan. 11, 2019), https://www.cnet.com/news/at-t-is-cutting-off-all-location-data-sharing-ties-by-march/.

notices of termination to the two Aggregators in January 2019,[59] it was not until March 29, 2019, that its LBS program (and the sharing of AT&T's customers' location information) finally ceased.[60] In other words, the Company did not finally terminate its location-based service program until March 29, 2019,[61] or 323 days from when the *New York Times* first reported on the Securus location-finding service, as well as the abuse of that service by Hutcheson.

15. *Notice of Apparent Liability*. On February 28, 2020, the Commission issued the *AT&T NAL* proposing a $57,265,625 fine against AT&T 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 *AT&T NAL*, the Commission also admonished AT&T for apparently disclosing its customers' location information, without their consent, to a third party who was not authorized to receive it.

16. On May 7, 2020, AT&T filed a response to the *NAL*.[62] AT&T makes a number of arguments as to why the *NAL* should be withdrawn and cancelled. AT&T argues that location information is not CPNI and thus is not subject to the Act and the Commission's CPNI Rules, and that even if it was, the Company did not have fair notice that it would be classified as CPNI.[63] AT&T 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.[64] Finally, AT&T argues that the forfeiture amount is arbitrary and capricious.[65]

III. DISCUSSION

17. The Commission proposed a forfeiture in this case in accordance with section 503(b) of the Communications Act of 1934, as amended (Act),[66] section 1.80 of the Commission's rules,[67] and the Commission's *Forfeiture Policy Statement*.[68] 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."[69] We have fully considered AT&T's NAL Response, which includes a variety of legal and factual arguments, but we find none of them persuasive. We therefore affirm the $57,265,625 forfeiture proposed in the *NAL*.

---

[59] *See NAL*, 35 FCC Rcd at 1755-56, para. 29 & n.111 (citing Supplemental LOI Response at 2, Response to Question 1).

[60] *See NAL*, 35 FCC Rcd at 1755-56, para. 29 (citing Supplemental LOI Response at 2, Response to Question 1; Further Response, LBS Chart Attachment); NAL Response at 34.

[61] *See NAL*, 35 FCC Rcd at 1756, para. 29 (citing Supplemental LOI Response at 1-2, Introduction); NAL Response at 34.

[62] *See* NAL Response.

[63] NAL Response at 4-17.

[64] NAL Response at 17-35.

[65] NAL Response at 35-40.

[66] 47 U.S.C. § 503(b).

[67] 47 CFR § 1.80.

[68] *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).

[69] 47 U.S.C. § 503(b)(2)(E).

A. Location Information is CPNI

18. As the *NAL* explained in more detail, the customer location information disclosed in AT&T's LBS program is CPNI under the Act and our rules.[70] 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."[71] The customer location information used in AT&T's LBS program falls squarely within this definition. AT&T's arguments to the contrary[72] 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.

19. *First*, the customer location information at issue here relates to the location of a telecommunications service—i.e., AT&T's commercial mobile service.[73] 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. AT&T 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.[74]

20. 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 . . . ."[75] 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."[76] Our interpretation also better squares with the broader operation of section 222. If the language "of use" modified every term in the preceding list, it would lead to apparently anomalous results. For instance, although the phrase "amount of use of a telecommunications service" plainly refers at least to the number and length of telephone calls, it is not clear what "technical configuration of use" would mean. And our interpretation squares more readily with section 222(d)(1), which preserves carriers' ability to use CPNI to "initiate" service[77]—an event that, aspects of which, ordinarily occur before the service is in "use."

21. The location information at issue here readily fits within that interpretation of the first prong of the CPNI definition. AT&T'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 AT&T's ability to use its network to determinate that location—is reasonably understood as associated

---

[70] *See NAL*, 35 FCC Rcd at 1757-59, paras. 33-41.

[71] 47 U.S.C. § 222(h)(1)(A) (emphasis added).

[72] *See* NAL Response at 5-11.

[73] *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").

[74] *See NAL*, 35 FCC Rcd at 1757, para. 35.

[75] 47 U.S.C. § 222(h)(1)(A).

[76] *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'").

[77] 47 U.S.C. § 222(d)(1).

with or a reference to the location of the AT&T telecommunications service.[78] Consequently, consistent with our assessment in the *NAL*,[79] we find this to be information that "relates to" the location of AT&T's telecommunications service within the meaning of the first prong of the CPNI definition.[80]

22. 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. AT&T does not dispute the *NAL*'s explanation that customers' devices and AT&T's network regularly exchange information as necessary for customers to send and receive calls.[81] To the extent that AT&T contends that this does not represent use of the telecommunications service because it merely enables the provision of that service, AT&T 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*,[82] we believe that AT&T's customers subscribe to its commercial mobile service to enable them to receive and transmit calls. When customers' devices are exchanging communications with AT&T'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.[83]

23. Nor do AT&T's arguments about the source and intended purpose of the location data at issue here persuade us to reach a contrary result. AT&T contends that the location data at issue here were generated via a different mechanism than is used to ensure connectivity to the network for purposes of commercial mobile service and certain other services, and that AT&T obtained them with the intent of using them for purposes of its LBS initiative, rather than its provision of commercial mobile service.[84] But nothing in the text of the first prong of the CPNI definition turns on the classification of the service or technology used to obtain the information, nor on the carriers' stated intent in collecting it. So long as the information "relates to" one or more of the specified criteria, the other factors raised by AT&T do not matter. And as noted above, the information at issue here "relates to" the location of the

[78] *See, e.g.*, *NAL*, 35 FCC Rcd at 1748, para. 11 ("AT&T 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 AT&T's wireless network.").

[79] *See, e.g.*, *NAL*, 35 FCC Rcd at 1757, 1758, paras. 35, 38.

[80] *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").

[81] *NAL*, 35 FCC Rcd at 1757, para. 35.

[82] *See, e.g.*, *NAL*, 35 FCC Rcd at 1757, 1758, paras. 35, 38.

[83] 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").

[84] NAL Response at 7. To the extent that AT&T assumes that the functionality used to obtain the location information for its LBS initiative was not itself a telecommunications service, we need not, and thus do not, address that here because our conclusions do not turn on that point.

telecommunications service (or to the location of use of that service), regardless of how AT&T obtained the information and how it planned to use the information.

24. We also are unpersuaded by AT&T'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 what AT&T gleans from other language in section 222.[85] In addition to the *NAL*'s responses in this regard,[86] 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:[87] All *location* information is protected as CPNI under (h)(1)(A). But carriers can disclose *call location* information for 911 purposes under (d)(4), which makes sense because 911 calls are *calls*. Nor would it have been irrational for Congress to expressly require opt-in consent for call location information in section 222(f)(1) if the definition of CPNI encompasses other forms of location information, as well. At the time the provision was enacted in 1999, Congress might reasonably have viewed call location information as obviously sufficiently sensitive to necessitate opt-in approval requirements while leaving it to the Commission's discretion whether to require opt-in approval for other location information, just as for other information falling within the definition of CPNI more generally. In addition, the Commission's references to "calls" in a prior order that was focused in significant part on data regarding customers' calls—and which did not purport to exhaustively address the application of section 222 to mobile wireless service—cannot reasonably be read as setting forth the outer bounds of the Commission's understanding of section 222.[88]

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

> AT&T provides wireless telephony services to the affected customers because they have chosen AT&T to be their provider of telecommunications service—in other words, they have a carrier-customer relationship. . . . AT&T's customers provided their wireless location data to AT&T because of their customer-carrier relationship with AT&T, ...[89]

In sum, the *NAL* reasoned that "[a]lthough AT&T might also provide non-common-carrier services to the same customer," the customer provided the relevant data "by virtue of the carrier-customer relationship."[90]

26. The *NAL* did not specify with precision the standard for applying the second prong of the CPNI definition, and although we elaborate further on some of its contours here, we likewise need not resolve that question with specificity because we find that prong met here under a range of possible approaches. We begin by observing that the second prong of the CPNI definition is focused on a "relationship"—namely, the "carrier-customer relationship."[91] A relationship presumes associations

---

[85] *See, e.g.*, NAL Response at 5-6.

[86] *NAL*, 35 FCC Rcd at 1758, para. 39.

[87] 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'").

[88] *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*).

[89] *See NAL*, 35 FCC Rcd at 1757-58, para. 36.

[90] *NAL*, 35 FCC Rcd at 1758, para. 37.

[91] 47 U.S.C. § 222(h)(1)(A).

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."[92] Thus, although AT&T suggests that its acquisition of the location information at issue here is in some technical sense distinct from, or does not depend exclusively on, the carrier-customer relationship,[93] we find that belied by the technical and marketplace realities here, as experienced by AT&T customers.

27. As the *NAL* explains, when a customer subscribes to AT&T's commercial mobile service, AT&T "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."[94] AT&T does not dispute that the carrier-customer relationship fully enables AT&T to obtain the location data at issue here. Although AT&T does contend that it "used distinct technological platforms to obtain location data for purposes of LBS lookups and voice services,"[95] it does not claim that a customer, having subscribed to its commercial mobile service, entered a separate agreement with AT&T for the provision of that location information—or that AT&T's voice customers had any way to avoid providing that information if they wanted to subscribe to AT&T's commercial mobile service. Under circumstances such as these, we conclude that the location information at issue from AT&T's commercial mobile service customers was "made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[96]

28. 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. As discussed in the *NAL*, for example, AT&T has sought to rely on the theory that its offering of bundled telecommunications service and information services take location data outside the purview of "CPNI."[97] But we are not persuaded that AT&T's inclusion of multiple services in a bundle—which includes one or more telecommunications services—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

[92] 47 U.S.C. § 222(h)(1)(A). Insofar as AT&T refers at times to a question of whether it "received the relevant location information '*solely* by virtue of' its voice telecommunications service," *see, e.g.*, NAL Response at 9, the focus on AT&T's "voice 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, AT&T disputes whether the location information at issue meets the statutory definition of CPNI in section 222(h)(1)(A), *see* NAL Response at 5-11, but does not contend that, if it does meet that definition, section 222(c)(1) nonetheless should not be interpreted to apply here.

[93] *See, e.g.*, NAL Response at 8-11.

[94] *NAL*, 35 FCC Rcd at 1758, para. 40.

[95] NAL Response at 9.

[96] 47 U.S.C. § 222(h)(1)(A).

[97] *See, e.g.*, *NAL*, 35 FCC Rcd at 1758, para. 37; *see also, e.g.*, NAL Response at 9-11 (raising similar arguments). AT&T does not catalog all the various services included in its bundles, and given that at least some of the services identified by AT&T have been classified as information services under existing Commission precedent, we need not otherwise evaluate the possible classifications of all of AT&T possible service offerings for purposes of our analysis here.

AT&T's customers to make their location information available to AT&T,[98] and in evaluating the second 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."[99] AT&T points out 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."[100] But we are far from that scenario here, given the many necessary links to AT&T's telecommunications services for the CPNI definition to apply.[101] 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" AT&T.[102] And the information must have been provided by consumers in a manner that reflects the statutorily required nexus to AT&T's telecommunications service.[103] 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 AT&T would prefer.[104]

29. Finally, we reject AT&T's argument that because it also gathered location information from consumers who only subscribed to information services (e.g., tablets) and did not partake of telecommunications services, *none* of the location information has been gathered solely by virtue of the customer-carrier relationship.[105] Against the backdrop of the analysis above, that only bears on the status of the information from those specific, non-voice, customers. The *NAL*'s proposed forfeitures turn not on specific effects on specific customers individually but on AT&T's corporate practices as a whole with respect to the entities that received LBS data.[106] AT&T does not contend that the LBS data that it

---

[98] 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 AT&T to obtain the location information at issue here. *Bostock v. Clayton Cty.*, 140 S. Ct. 1731, 1739 (2019) (In contrast to the statute at issue there, Congress "could have added '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.

[99] *2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9616, para 23.

[100] 47 U.S.C. § 153(51).

[101] For similar reasons, we reject the suggestion that our approach regulates AT&T under section 222 based on the mere fact that it has the status of a telecommunications carrier, rather than being linked to its specific offering of telecommunications services. *See* NAL Response at 8, 10.

[102] 47 U.S.C. § 222(h)(1)(A).

[103] 47 U.S.C. § 222(h)(1)(A).

[104] AT&T also argues that jurisdiction over this matter lies with the Federal Trade Commission. *See* NAL Response at 12-13. But as we have found here, the data in question is CPNI and therefore properly within the Commission's jurisdiction under section 222 of the Act. As explained in the *NAL*, the Commission has authority to bring action for violations of section 222 of the Communications Act and the CPNI Rules against providers of telecommunications services and providers of interconnected Voice over Internet Protocol services. *See NAL*, 35 FCC Rcd at 1747, para. 10 (citing 47 U.S.C. § 222; *2007 CPNI Order*, 22 FCC Rcd at 6954-57, paras 54-59).

[105] *See* NAL Response at 9-10.

[106] In particular, the *NAL* did not propose forfeitures based on unauthorized disclosure of CPNI associated with particular customers—it proposed forfeitures based on allegations that AT&T failed to take reasonable steps to protect its customers' location information, with forfeitures proposed not on a per-customer basis but on the basis of the days in which AT&T allegedly did not have a reasonable policy in place for particular entities that received LBS data. *See, e.g.*, *NAL*, 35 FCC Rcd at 1768-69, para. 76. And while *FTC v. AT&T Mobility LLC*, 883 F.3d 848 (9th Cir. 2018) (en banc), concluded that the common-carrier limitation on the FTC's authority is activities-based, rather than status-based, it also recognized that "there may be some overlap between the agencies' jurisdiction when the (continued….)

provided, directly or indirectly, to any of the entities associated with the proposed forfeitures in the *NAL* was limited exclusively to data from non-voice customers. Thus, the AT&T practices that formed the basis of the proposed forfeitures in the *NAL* included information from voice customers, which falls within the definition of CPNI for the reasons explained above.

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

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

31. We reject AT&T's claim that it lacked fair notice that its practices involving customer location information were subject to the Communications Act and potential penalties thereunder.[107] The language of section 222 demonstrates that customer location information is CPNI; AT&T's practices involving CPNI, including customer location information, therefore unquestionably are regulated under the Act and the Commission's CPNI Rules; and AT&T'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.

32. AT&T argues that the "proper vehicle" for the Commission to address carriers' LBS practices "would have been a rulemaking or other order with prospective-only application."[108] 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 also a "proper vehicle" to adjudicate the specific bounds of what is lawful and what is not, subject to principles of fair notice.[109]

33. Contrary to AT&T'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 CPNI Rules before enforcing that statute and those rules with respect to those data.[110] As the D.C. Circuit has explained, "[t]he fair notice doctrine, which is couched in terms of due process, provides redress only if an agency's interpretation is 'so far from a reasonable person's understanding of the

FCC's regulations of common carriers affect the non-common-carrier activities of those entities," observing that "[i]n the administrative context, two cops on the beat is nothing unusual." *Id*. at 862. Thus, our interpretation of section 222 is not at odds with the court's decision in *FTC v. AT&T Mobility*.

[107] *See* NAL Response at 14-17.

[108] NAL Response at 14.

[109] *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").

[110] *See* NAL Response at 14 (referring to "the proper vehicle for announcing that [section 222 encompasses LBS location data]" and the punishment of AT&T "for conduct that preceded the announcement"). In any event, however, absolute specificity is not a prerequisite for enforcing a statute or regulation. *See, e.g.*, *Lachman*, 387 F.3d at 56-57 (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").

regulations that they could not have fairly informed the regulated party of the agency's perspective.'"[111] 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.[112]

34. Here, the Commission previously explained in the *2013 Declaratory Ruling* that it would not "set out a comprehensive list of data elements that pertain to a telecommunications service and satisfy the definition of CPNI and those data elements that do not."[113] Thus, AT&T 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 section 222([h])(1) is in fact CPNI."[114] 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."[115] In addition, notwithstanding the fair notice claims it makes now, AT&T previously asserted to the Commission that it treated customer location information in an essentially equivalent manner to CPNI.[116]

35. 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."[117] 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."[118] 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.

36. Finally, AT&T 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

---

[111] *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").

[112] *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).

[113] *2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9617, para. 24 n.54.

[114] *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").

[115] *2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9617, para. 24 n.54.

[116] *See NAL*, 35 FCC Rcd at 1758, para. 37 n.122.

[117] 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'").

[118] 47 U.S.C. § 222(h)(1)(A).

access to CPNI."[119] 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."[120] The Commission granted carriers flexibility to incorporate the specific measures and practices that are consistent with their otherwise-existing "technological choices."[121] 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.[122] And in the same order, the Commission likewise identified the limitations of relying on "contractual safeguards" to address risks once CPNI has been disclosed outside the covered carrier.[123] 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."[124] This provides sufficient direction for AT&T to understand its obligations under the rule as relevant here.[125]

37. Thus, AT&T 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) AT&T would be subject to forfeiture penalties for failing to protect that customer location information as required under section 222 and the Commission's rules.[126]

C. AT&T Failed to Take Reasonable Steps to Protect CPNI

38. AT&T 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.[127] While our rules recognize that companies cannot prevent all data breaches, the

[119] 47 CFR § 64.2010(a).

[120] *2007 CPNI Order*, 22 FCC Rcd at 6959, para. 64.

[121] *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").

[122] *2007 CPNI Order*, 22 FCC Rcd at 6946, para. 35.

[123] *2007 CPNI Order*, 22 FCC Rcd at 6952-53, para. 49.

[124] *2007 CPNI Order*, 22 FCC Rcd at 6959-60, para. 65.

[125] AT&T cites *LabMD, Inc. v. FTC*, 894 F.3d 1221, 1235-36 (11th Cir. 2018), but we are not persuaded that case calls for more here. For one, that case deals specifically with requirements for cease-and-desist orders and injunctions. *See, e.g.*, *LabMD*, 894 F.3d at 1234-35. Further, the requirements at issue in that case lacked the supplementing guidance providing greater clarity that we find present in the case of section 64.2010 of the Commission's rules. *See, e.g.*, *LabMD*, 894 F.3d at 1236 (explaining that the proposed court order "is devoid of any meaningful standard informing the court of what constitutes a 'reasonably designed' data-security program"). Separately, AT&T's reliance on contractual safeguards and its failure to investigate key details that would ensure LBS providers only were engaging in authorized uses and disclosures of CPNI appears directly at odds with guidance the Commission has provided. Even where a regulation is amenable to different interpretations, courts have rejected 'fair notice' claims where the regulated entity did not comply with at least some viable interpretation of the requirement. *See, e.g.*, *21st Century Telesis Joint Venture v. FCC*, 318 F.3d 192, 202 (D.C. Cir. 2003).

[126] We reject as inapposite AT&T's argument that the Commission cannot rely on principles of deference to satisfy fair notice requirements. NAL Response at 16-17 (citing *Kisor v. Wilkie*, 139 S. Ct. 2400 (2019); *Christopher v. SmithKline Beecham Corp*., 567 U.S. 142, 158 (2012); *General Electric Co. v. EPA*, 53 F.3d 1324, 1334 (D.C. Cir. 1995); *Gates & Fox Co. v. Occupational Safety & Health Review Commission*, 790 F.2d 154, 156 (D.C. Cir. 1986)). As the analysis above indicates, we are not relying on deference as grounds for finding fair notice of an interpretation of the definition of CPNI for which fair notice would not otherwise exist.

[127] 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.").

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). AT&T contends that the Securus disclosures to Hutcheson did not constitute legal violations of section 222.[128] AT&T then claims that it acted reasonably to protect its customers' location information both before and after the Securus disclosure came to light.[129] AT&T also argues that the Commission improperly shifted the burden of proving that such protections were reasonable to AT&T.[130] We find AT&T's arguments unpersuasive.

1. AT&T's Customer Location Disclosures to Securus Were Unauthorized and Violated Section 222

39. As an initial matter, we conclude that it was not just disclosures to Hutcheson that were unauthorized. Rather, Securus's entire location-finding service[131] (as detailed in paragraphs 11-12, above) was predicated on unauthorized disclosures. Consistent with AT&T's own description of events, the program was outside the scope of not only its approved "Use Case," but also beyond any agreement with either Aggregator (and thus had not been reviewed by AT&T).[132] AT&T conceded that it was unable to distinguish location requests unrelated to the authorized Use Case (which involved an inmate collect-calling service) because each Securus request included a customer consent record that was identical to the records received for the approved service.[133] And, to be clear, none of the "consent records" submitted in connection with the location-finding service evinced a consumer's actual opt-in consent. Therefore, every time Securus submitted a request for location information under the guise of its approved Use Case (a Use Case that required consumer consent) and AT&T provided the requested location information, a separate, unauthorized disclosure occurred.

40. AT&T attempts to avoid this conclusion by: (1) concentrating only on the disclosures made to Hutcheson, not on the overall Securus location-finding program ;[134] and (2) trying to use section 222(c)(1)'s exception for disclosures that are required by law to shield itself.[135] This misses the larger point. Whether or not there was a legitimate law enforcement request for the information is irrelevant if AT&T did not satisfy its own obligations under section 222. AT&T provided the location information to Securus under Securus's false pretenses, and AT&T only did so because it took Securus at its word that

[128] *See* NAL Response at 18-21.

[129] *See* NAL Response at 25-35.

[130] *See* NAL Response at 18-25.

[131] *See NAL*, 35 FCC Rcd at 1752-53, 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).

[132] *See* LOI Response at 17, Response to Inquiry No. 8 ("AT&T never approved this [Securus] program and did not receive the government requests."); *see also, e.g.*, NAL Response at 21 (contending that certain information relied upon in the *NAL* "at most," supported "the proposition that Securus sent Hutcheson location data for certain AT&T customers outside the scope of AT&T's approved use case").

[133] *See NAL*, 35 FCC Rcd at 1753, para. 23.

[134] *See* NAL Response at 24 (saying there is "no patter of data breaches" and that it is "only isolated and dated incidents involving a single errant LBS provider (Securus) with a single bad customer (Hutcheson)").

[135] *See* NAL Response at 20 (relying on 47 CFR § 222(c)(1), which allows disclosure of CPNI "as required by law").

Securus had obtained opt-in consumer consent.[136] This means that AT&T did not review any law enforcement requests and likewise did not provide the information pursuant to a law enforcement request because AT&T did not know there *were* any law enforcement requests in the first place – legitimate or otherwise.[137] 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.[138] Thus, the disclosures made to Hutcheson were doubly unauthorized under section 222(c)(1). First, Securus used the façade of their approved Use Case to hide the true purpose and destination of the request, resulting in AT&T'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.[139] Despite AT&T's arguments, the Company is clearly not "required by law" to disclose location information based on any and every pretense or unsupported request. Therefore, consistent with the *NAL*, we find that the Securus disclosures, including those made to Hutcheson, were unauthorized and AT&T was appropriately admonished in relation to such disclosures.

2. AT&T's Protection of Customer Location Information Was Unreasonable Both Before and After the Securus/Hutcheson Disclosures

41. The Commission affirms the *NAL* and finds that AT&T 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 AT&T did not have reasonable

[136] AT&T's attempt to distinguish whether "location lookups violated Securus's contractual obligations to AT&T" from the question of whether there was a violation of section 222 thus is futile under the circumstances here. *See, e.g.*, NAL Response at 20. As the *NAL* explained, "[t]o the extent that the third parties were *not* acting on behalf of the carrier, the carrier itself would have provided those third parties with access to its customers' CPNI without obtaining for themselves the approval required by section 222(c)(1)—thus violating federal law." *NAL*, 35 FCC Rcd at 1760, para. 37 n.141. Although the *NAL* noted that "AT&T does not appear to argue that situation is present here," *id*., the totality of the record persuades us that this is, in fact, the import of the facts and AT&T's arguments here.

[137] *See* LOI Response at 17, Response to Inquiry No. 8 ("AT&T never approved this [Securus] program and did not receive the government requests."); NAL Response at 20 (stating that "Securus enabled law enforcement officials—without AT&T's knowledge—to access customer location data" in a manner that "violated Securus's contractual obligations to AT&T"). *See also NAL*, 35 FCC Rcd at 1752-53, 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). It is not reasonable to interpret AT&T as having been relying on a third party to disclose information as required by law where AT&T neither knew or approved of the third party doing so.

[138] *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 1753, para. 21 (describing Hutcheson's uploading of documents that were blatantly not legal authorizations in order to obtain location information). As the *NAL* explained, "AT&T does not deny the existence of the Securus location-finding service nor the abuse of that system by Hutcheson." *NAL*, 35 FCC Rcd at 1753, para. 22. AT&T likewise does not dispute here that Hutcheson was, as a general matter, able to access location data by providing documents that were blatantly not legal authorizations as described in the *NAL* and confirmed in the Hutcheson Sentencing Memo. It at most asserts that there conceivably might have been legal authorizations associated with the specifically-identified AT&T customers, *see* NAL Response at 20-21, but does provide any reason to believe that Securus (let alone AT&T) could have or would have made that assessment before providing the location data.

[139] *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 1753, para. 21.

protections in place prior to 2018 *New York Times* article detailing the Securus/Hutcheson breaches,[140] but also that AT&T failed to promptly address its demonstrably inadequate CPNI safeguards after Securus/Hutcheson disclosure.[141]

42. AT&T attempts to excuse its unreasonable practices by cataloging the steps it did take before and after the *New York Times* article. AT&T argues that, prior to the Securus disclosure, its efforts exceeded the CTIA Guidelines for ensuring customer consent to the use of location data.[142] Specifically, AT&T states that its safeguards included: (1) vetting each LBS provider and aggregator; (2) predicating access to location data on individualized preapproval of each LBS provider and each LBS Use Case; (3) limiting a number of LBS providers' access to specific location data even for consenting customers; (4) imposing exceptionally detailed information-security requirements on all LBS providers and aggregators; (5) reviewing customer-consent records daily; and (6) conducting audits and assessments to monitor and strengthen its controls.[143]

43. The safeguards that AT&T had in place before the Securus disclosure were not reasonable. As fully explained in the *NAL*:

> [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.[144]

As for the other safeguards that AT&T 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.[145] To enforce these safeguards, AT&T would have needed to take steps to determine whether they were actually being followed. Further, AT&T 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 (i.e., the Securus/Hutcheson requests absent valid customer consent). Although the Commission requested that AT&T describe its efforts to verify that LBS providers obtained valid customer consent for related location requests,[146] nothing that AT&T 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 AT&T that its contractual safeguards were effective are undermined by the inexorable fact that after the Securus disclosure, AT&T was unable to "compel Securus to cooperate with [its] investigation."[147] As the Commission said in the *NAL*, if AT&T could not compel Securus to cooperate, "it cannot say that the same contract-based system actually protects customer location information from unauthorized access by other entities. [Securus's] . . . refusal [to cooperate] is further

[140] *See NAL*, 35 FCC Rcd at 1761-63, paras. 51-59.

[141] *See NAL*, 35 FCC Rcd at 1763-77, paras. 60-70.

[142] *See* NAL Response at 26.

[143] *See* NAL Response at 26.

[144] *NAL*, 35 FCC Rcd at 1762, para. 55.

[145] *See NAL*, 35 FCC Rcd at 1762-1763, paras. 53-59.

[146] *See* Letter from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau to Jeanine Poltronieri, Assistant Vice President, External Affairs, AT&T Services, Inc., Letter of Inquiry at 3, Question 5(e), (Sep. 13, 2018) (on file in EB-TCD-18-00027704).

[147] *NAL*, 35 FCC Rcd at 1764, para. 63.

evidence of the fact that AT&T disclosed CPNI to a third party over which it had little or no control or authority."[148]

44. Likewise, AT&T's safeguards after the Securus disclosure were also unreasonable. AT&T became keenly aware of the inadequacy of its safeguards after the May 2018 *New York Times* article, and again after Securus's resistance to AT&T's subsequent investigation. Nonetheless, AT&T 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, AT&T 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.[149] Although AT&T worked towards implementing an enhanced notice and consent mechanism, this mechanism was never deployed.[150] According to AT&T, the mechanism was never deployed because AT&T decided to shut down its LBS program altogether—in the wake of a report of yet another LBS provider's systems being misused.[151] But the mere fact that AT&T was working on new processes is not sufficient to satisfy its obligation to "take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI."[152] Until the new measures actually are in place, they cannot enable a carrier to "discover and protect against" the harms that are the target of that rule—and thus, they cannot be relied upon to satisfy that rule. Nor does the time and effort involved in AT&T's work on new processes render the procedures that remained in place in the meantime "reasonable" under that rule, given their glaring weaknesses. The Commission has considered all of the data security measures that AT&T implemented in response to the Securus disclosure[153] and concludes that these measures were inadequate.

45. AT&T argues that the Commission "faults AT&T's response [to the Securus disclosure] only because [the Commission] arbitrarily (1) ignores the consumer benefits of LBS services and the social costs of shutting them down and (2) all but ignores the substantial data security measures AT&T took in response to the Securus disclosure."[154] We disagree. The issue here is not whether there are any beneficial services offered by LBS providers, but whether AT&T reasonably protected its customers' location information. And even under AT&T's reasoning, the Company would have no excuse for its failure to promptly terminate every other non-critical LBS provider. 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 AT&T did not have a reliable way of confirming customer consent. The Commission considered AT&T's arguments, but finds they are outweighed by these risks.

46. 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.[155] Rather than taking definitive steps

[148] *NAL*, 35 FCC Rcd at 1764, para. 63.

[149] *See NAL*, 35 FCC Rcd at 1764, para. 60.

[150] *See* NAL Response at 30-32. In connection to implementing its enhanced notice and consent mechanism and ending its LBS program, AT&T argues that the *NAL* "pluck[ed] [a 30-day] deadline from thin air [and] it is arbitrary and capricious." *Id*. at 32. The 30-day period cited in *NAL* was not a deadline but a grace period during which the Commission used its discretion and did not assess a fine. However, AT&T's existing data security practices were unreasonable both before and after the May 2018 article—the article merely exposed those unreasonable practices. As such, the Commission could have assessed a fine *for every single day* such unreasonable practices were in place (both before and after the Securus/Hutcheson disclosures)—the 30 days provided AT&T with a grace period to either end the program or reform its practices.

[151] *See* NAL Response at 33-34.

[152] 47 CFR § 64.2010(a).

[153] *See* NAL Response at 25-35.

[154] *See* NAL Response at 26.

[155] *See NAL*, 35 FCC Rcd at 1765-66, paras. 67-69.

to remedy the obvious LBS program issues, AT&T instead took piecemeal steps. The Commission has fully considered all of the safeguards AT&T implemented after the Securus disclosure and has determined these safeguards to be inadequate because they did not rectify the systemic vulnerabilities at the heart of its LBS program—including relying on third parties to obtain customer consent for the disclosure of location information and failing to verify the validity of that consent.[156]

3. AT&T Bore the Burden of Production

47. 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 AT&T did not use reasonable safeguards throughout the period of the violation.[157] As such, while the *NAL* discussed AT&T's burden of production to demonstrate that its protection of customer CPNI was reasonable,[158] that burden-shifting is not necessary given the preponderance of the evidence. Nonetheless, even if unnecessary to prove AT&T's violations in this matter, the *NAL* properly shifted the burden of production to AT&T.

48. *First*, as the *NAL* explained[159] 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.[160] In the *NAL*, the Commission found that AT&T failed to demonstrate that its safeguards were reasonable following the disclosure of Securus's unauthorized location-finding service in May 2018.[161]

49. AT&T acknowledges that the *2007 CPNI Order*[162] states 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."[163] However, AT&T is incorrect when it asserts that the *2007 CPNI Order* cannot support the burden-shifting approach in cases outside of the pretexting context. The *2007 CPNI Order* afforded adequate notice of the application of burden-shifting in this case. The order did not expressly limit burden-shifting to the pretexting context, instead applying more broadly to unauthorized disclosures of CPNI. The rationale applies with equal force to the kind of disclosure at issue here, where a fundamental issue is whether AT&T 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.[164] Broadly, in relation to Securus's entire unauthorized location-finding service, Securus used the pretext that it was requesting

---

[156] Although AT&T asserts that it worked towards implementing enhanced notice and consent mechanisms, those enhanced mechanisms were never deployed given AT&T's decision to shut down its LBS program altogether. *See* NAL Response at 30-32.

[157] *See NAL*, 35 FCC Rcd at 1761-66, paras. 51-69.

[158] *See NAL*, 35 FCC Rcd at 1746-47, 1761-62, and 1764, paras. 8, 52-53, and 62.

[159] *See NAL*, 35 FCC Rcd at 1746-47, para. 8.

[160] *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").

[161] *See NAL*, 35 FCC Rcd at 1761-66, paras. 51-69.

[162] *See 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*).

[163] *See* NAL Response at 22 (citing *NAL*, 35 FCC Rcd 1746-47, 61-62, at paras. 8, 52).

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

location information from AT&T for its approved Use Case and that it had explicit customer opt-in consent for the disclosure. Likewise, Hutcheson used the pretext that he had legal authorization or consumer consent when requesting location information from Securus.[165] 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.

50. *Second*, AT&T admits that an evidentiary presumption is valid if the circumstances (here, a breach of CPNI) giving rise to that presumption make it "more likely than not" that the presumed fact (here, that CPNI safeguards were unreasonable) exists.[166] The Commission finds that the unauthorized disclosure in this case gave rise to a rebuttable presumption that AT&T did not reasonably protect customer location information from unlawful access.[167] As already discussed, the entire Securus location-finding program was based upon unauthorized disclosures. Though the disclosures to Hutcheson were particularly egregious (given they were essentially doubly unauthorized), *all* of the Securus requests made under the false guise of the approved Use Case and AT&T's resultant disclosures of consumer location information were unauthorized. AT&T'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, AT&T argues that the Commission cannot use the Securus and Hutcheson breaches (particularly as they occurred in 2014-2017) to support shifting the burden of production to the AT&T to provide evidence of the reasonableness of their post-May 2018 security practices.[168] Specifically, AT&T asserts that (1) there is no basis for concluding that LocationSmart or Securus actually committed a legal violation for which AT&T could be vicariously liable and (2) even if such violation was found, it could form no basis for presuming that AT&T responded unreasonably after the violation was found long after it occurred. We disagree.

51. In the *NAL*, we found that AT&T 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.[169] This is further bolstered by the Department of Justice's case against Hutcheson.[170] And though the Commission opted to admonish AT&T only for the unauthorized disclosures made to Hutcheson, it would have been appropriate to admonish AT&T 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,[171] carriers cannot disclaim their obligations to protect customer CPNI by delegating those

[165] As explained in the *NAL*, "Hutcheson submitted thousands of unauthorized location requests via the Securus service between 2014 and 2017, in some cases 'upload[ing] entirely irrelevant documents including his health insurance policy, his auto insurance policy, and pages selected from Sheriff training manuals" in lieu of genuine legal process.'" *NAL*, 35 FCC Rcd at 1753, para. 21; *see also supra* para. 12.

[166] See NAL Response at 23.

[167] *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).

[168] *See* NAL Response at 18-22.

[169] *See NAL*, 35 FCC Rcd at 1759-61, paras. 42-50. "The evidence reflects that Hutcheson used the Securus service to obtain the location information of AT&T customers. AT&T shared the information with LocationSmart, which the shared it with 3Cinteractive, which then shared it with Securus. *Id*. at 1759 at para. 43. "The evidence shows that between 2014 and 2017, at least 147 AT&T customers' location information was disclosed to Hutcheson, via Securus, without the customers' consent." *Id.* at 1759 at para. 43.

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

[171] 47 U.S.C. § 217.

obligations to third parties.[172] In its NAL Response, AT&T does not dispute that Hutcheson's "location lookups violated Securus contractual obligations to AT&T."[173] We reiterate here that "AT&T is not absolved from liability simply because it was not directly responsible for operating the programs under which unauthorized disclosures occurred."[174] Further, section 222(c)(1) of the Act[175] makes the responsibility for avoiding unauthorized disclosures a carrier obligation and prohibits use and disclosure except in certain narrow circumstances, without any reasonableness criterion. AT&T 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.[176]

52. *Third*, AT&T misinterprets the *NAL* when it argues that the Commission improperly shifted the burden of persuasion to the Company.[177] To the contrary, the Commission properly (and consistent with APA precedent) shifted only the burden of *production*, and not the burden of *persuasion*, to AT&T. The unauthorized disclosure at issue gave rise to a rebuttable presumption that AT&T did not adequately protect customer information from unlawful access. The burden of production then shifted to AT&T to offer evidence that it had reasonable safeguards in place.[178]

---

[172] *See NAL*, 35 FCC Rcd at 1747, 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.

[173] *See* NAL Response at 20. AT&T argues that Hutcheson's unauthorized location lookups, which they concede violated Securus's legal obligations to AT&T including safeguarding its customers' CPNI, did not violate the Act or the Commission's rules because "section 222(c)(1) expressly authorizes information-sharing "required by law"." *Id.* We find AT&T's argument unavailing. Although AT&T speculates that some of the lookups may have had a law enforcement basis, those lookups were certainly not submitted through the appropriate channels for law enforcement requests, and AT&T cannot now claim that they were "required by law" when it did not treat them as such in the first place. Further, as explained in the *NAL*, "Securus did not . . . assess the adequacy of the purported legal authorizations submitted by users of its location-finding service." *NAL*, 35 FCC Rcd at 1752, para. 20.

[174] *See NAL*, 35 FCC Rcd at 1759, para. 45; *see also id*. at 1760, para. 47 n.141 (explaining that where a carrier makes disclosures to a third party where the third party is not acting on behalf of the carrier to fulfill the relevant responsibilities of the carrier under section 222, the carrier's disclosure of CPNI to the third party would be unauthorized in violation of section 222(c)(1)).

[175] 47 U.S.C. § 222(c)(1).

[176] We thus reject AT&T's claim that burden-shifting based on the Securus disclosures makes no sense when the issue is the reasonableness of AT&T's procedures years after those disclosures. *See* NAL Response at 24-25. As we explain above, the procedures AT&T actually employed—rather than the unimplemented processes it worked on developing—are what matters for assessing compliance with section 64.2010 of the rules. Since the procedures AT&T actually employed did not materially change from the time of the Securus disclosure through the time periods at issue here, the reasonableness of the procedures employed at the time of the Hutcheson disclosure remain fully relevant—and thus shifting the burden of production based on unauthorized disclosures under those procedures is logically consistent. In addition, the disclosures made to Hutcheson are not the only unauthorized disclosures. Disclosures made pursuant to Securus's unauthorized program are all unauthorized, and both pre- and post-dated any disclosures made to Hutcheson.

[177] *See* NAL Response at 22-25.

[178] We note that in some instances—most notably with regard to various audits that implicated the LBS program and over which AT&T asserted privilege—AT&T claimed to have taken certain reasonable steps, but did not produce documentary evidence of those steps. *See NAL*, 35 FCC Rcd at 1751-52, paras. 18-19.

53. Rather than taking reasonable steps to safeguard its customers' location information after the Securus/Hutcheson disclosures were reported,[179] AT&T 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 AT&T failed in its obligation under section 222 and our rules to have reasonable measures in place to discover and protect against attempts to gain unauthorized access to its customers' CPNI.

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

54. After considering the evidence in the record, the relevant statutory factors, the Commission's *Forfeiture Policy Statement*, and the arguments advanced by AT&T in the NAL Response, we find that AT&T is liable for a total forfeiture of $57,265,625 for its violations of section 222 of the Act and section 64.2010 of the Commission's rules.[180] As explained in the *NAL*, this total results 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).[181] The Commission found in the *NAL* that AT&T apparently engaged in 84 continuing violations—one for each ongoing relationship with a third-party LBS provider or aggregator that had access to AT&T customer location information more than 30 days after publication of the *New York Times* report—and that each violation continued until AT&T terminated the corresponding entity's access to customer location information.[182] Using this methodology, the Commission found AT&T apparently liable for a total base forfeiture of $45,812,500. Upon considering the nature of the violations and the risk of harm they posed to consumers, the Commission then applied a 25% upward adjustment to the base forfeiture amount, resulting in a total proposed forfeiture of $57,265,625.[183]

55. AT&T challenges these forfeiture calculations with three principal arguments. *First*, AT&T asserts that the *NAL* describes at most a single continuing violation, not 84 separate violations, and that the upward adjustment was based on the same factors used to determine the base forfeiture for these violations. As such, according to AT&T, the forfeiture exceeds the applicable statutory maximum and violates due process, and both the forfeiture and the upward adjustment are arbitrary and capricious.[184] *Second*, AT&T argues that because it did not engage in "willful or repeated" violations, it cannot be subject to a forfeiture penalty under section 503(b).[185] *Third*, AT&T claims that the Commission bore (and failed to meet) the burden of showing that each of the 84 third-party relationships upon which the forfeiture was based posed a significant threat of unauthorized access to AT&T customer location information.[186] 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*.

---

[179] Many of the possible reasonable steps were enumerated in the *NAL*. *See NAL*, 35 FCC Rcd at 1764-66, paras. 61-69.

[180] 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.

[181] *NAL*, 35 FCC Rcd at 1778, para. 75.

[182] *NAL*, 35 FCC Rcd at 1778-79, para. 76.

[183] *NAL*, 35 FCC Rcd at 1780, para. 79.

[184] NAL Response at 35-38, 37 n.29.

[185] NAL Response at 38.

[186] NAL Response at 39-40.

1. The Commission Reasonably Found that AT&T Engaged in 84 Continuing Violations That Warranted an Upward Adjustment

56. Section 503(b) of the Act authorizes the Commission to impose a forfeiture against AT&T 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."[187] According to AT&T, the NAL describes at most one continuing violation for which a penalty may be assessed—namely, the "fail[ure] . . . to have reasonable [data security] measures in place."[188] AT&T asserts that because the *NAL* describes that failure in unitary terms, and because the *NAL* does not suggest that AT&T "should have tailored distinct safeguards to specific LBS providers," the Commission can only find there to have been one continuing violation (subject to the $2,048,915 penalty cap).[189] AT&T also claims that the NAL justifies the base forfeiture and the upward adjustment on the same factors and that doing so is arbitrary and capricious.[190] Thus, AT&T contends, the *NAL's* finding of 84 separate continuing violations (one for each LBS provider or aggregator) constitutes an impermissible attempt to circumvent the statutory maximum set by Congress.

57. We reject these arguments. 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.[191] 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."[192] 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 . . . ."[193]

58. 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),[194] 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 AT&T 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.[195] Each such relationship relied upon a distinct and unique contractual chain (from

---

[187] *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).

[188] NAL Response at 36 (citing *Notice*, 35 FCC Rcd at 1766-67, para. 70).

[189] NAL Response at 36-37.

[190] NAL Response at 37 n.29.

[191] 47 U.S.C. § 503(b); 47 CFR § 1.80(b).

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

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

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

[195] Because our approach adheres to the requirements of section 503 of the Act, we reject AT&T's nondelegation and excessive fines clause arguments that were premised on the theory that the Commission was seeking to evade those requirements. *See* NAL Response at 37.

AT&T 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 AT&T. 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.

59. The approach taken in the *NAL* was not only reasonable, it was—contrary to AT&T's claim that it led to a "stratospheric" penalty that was "astronomically higher" than the statutory maximum—eminently *conservative*, both in terms of the base forfeiture and the upward adjustment. 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."[196] The plain language of the statute provides the Commission with broad discretion to assess proposed penalties based on the statutory factors, up to the statutory maximum. Moreover, section 1.80 of the Commission's rules provides a list of possible factors the Commission may use when making a determination to adjust upward or adjust downward the base forfeiture.[197] These factors include, importantly, "egregious misconduct," "substantial harm," "repeated or continuous violation," and "ability to pay/relative disincentive," among others.[198] The Commission weighed these factors when making the determination that the base forfeiture in this case merited a substantial upward adjustment. AT&T's conduct was egregious; 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.[199] Its failure to adequately protect CPNI for a protracted amount of time caused substantial harm by making it possible for "malicious actors to identify the exact locations of AT&T 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.[200] 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 AT&T's status as a major telecommunications provider to determine what penalty, when applied, would adequately provide AT&T 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. AT&T's arguments to the contrary do not defeat Congress's decision to grant the FCC the power to

[196] 47 U.S.C. § 503(b).

[197] 47 CFR § 1.80(b)(10), Table 3.

[198] *Id.*

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

[200] *NAL*, 35 FCC Rcd at 1780, para. 79.

weigh the factors and make such adjustments "as justice may require."[201] Nor do AT&T's arguments persuade us that the 25% upward adjustment, which is relatively modest compared to upward adjustments in other cases involving consumer harms,[202] was unwarranted.

60. Turning to the per-LBS provider violations, as described in the *NAL*, AT&T'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 AT&T 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).[203] Using that methodology—and taking into account the tens of millions of consumers whose highly sensitive location information was made vulnerable by AT&T—would have resulted in a significantly higher forfeiture than what was proposed in the *NAL*.

61. 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 AT&T 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 AT&T 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 AT&T 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.

62. We also reject AT&T's assertion that its 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 AT&T's fair notice claims,[204] 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. AT&T 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.[205] 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.[206] As the D.C. Circuit has

---

[201] 47 U.S.C. § 503(b).

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

[203] Although it involved a data breach—and not, as in this case, an ongoing failure to maintain reasonable safeguards such that customer data were 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 were inadequately protected. *See TerraCom*, 29 FCC Rcd at 13343, para. 50.

[204] *See supra* B.

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

[206] 47 U.S.C. § 503.

recognized, where a statute specifies maximum penalties, the statute itself provides fair notice of all penalties within that limit.[207]

2. AT&T Willfully and Repeatedly Violated the Act and the Commission's Rules

63. AT&T asserts that it cannot be subject to a forfeiture penalty under section 503(b)(1)(B) of the Act because that provision applies only to "willful[] or repeated[]" violations.[208] According to AT&T, because the *NAL* "describes at most a unitary continuing violation," it does not allege any "repeated" failure to comply with statutory or regulatory requirements. And, AT&T claims, the violation cannot be "willful" because the *NAL* does not allege that AT&T acted in knowing violation of any requirement.

64. These arguments lack merit. The terms "willful" and "repeated," as used in section 503(b) of the Act, do not have the restrictive meaning that AT&T would assign to them. As the Commission previously stated in *Midwest Radio-Television*:

> . . . the word "willfully", as employed in Section 503(b), does not require a showing that the [party] knew he was acting wrongfully; it requires only that the Commission establish that the licensee knew that he was doing the acts in question – in short, that the acts were not accidental (such as brushing against a power knob or switch).[209]

AT&T contends that "willful" should not be interpreted by reference to the definition in section 312(f) as the Commission has done previously, but instead should be interpreted to require "at least a knowing violation or reckless disregard of law, citing the Supreme Court's decision in *Safeco Ins. Co. of Am. v. Burr*, 551 U.S. 47 (2007).[210] We find instead that the Commission's historical approach to interpreting "willfully" in section 503(b) is on firmer footing than AT&T suggests. The Commission's interpretation reflected in *Midwest Radio-Television*, which predated the enactment of section 312(f), was premised on interpretations from Commission precedent interpreting "willful" elsewhere in the Act and Commission rules, and a consideration of court cases from other fields, along with the legislative history of the then-recently enacted "willful[] or repeated[]" language of section 503(b).[211] Although *Safeco* states that "where willfulness is a statutory condition of civil liability, we have generally taken it to cover not only knowing violations of a standard, but reckless ones as well," it also recognizes that "'willfully' is a 'word of many meanings whose construction is often dependent on the context in which it appears.'"[212] Particularly given that *Midwest Radio-Television* was decided close in time to the enactment of the relevant language in section 503(b), and included an analysis of precedent interpreting willfulness as it had been used elsewhere in the Act previously,[213] that more highly relevant context persuades us to continue to follow the *Midwest Radio-Television Inc.* approach to interpreting "willfully" in section

---

[207] *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).

[208] 47 U.S.C. § 503(b)(1)(B).

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

[210] *See* NAL Response at 38 n.32.

[211] *Midwest Radio-Television,* 40 F.C.C. at 1665-67, paras. 8-11.

[212] *Safeco*, 551 U.S. at 57.

[213] *Midwest Radio-Television,* 40 F.C.C. at 166, para. 9.

503(b).[214] Separately and independently, however one might use the legislative history of section 312(f) to interpret section 312(f) itself, the relevant Conference Report indicates that the definitions enacted in section 312(f) were "consistent with the Commission's application of those terms ["willfully" and "repeatedly"] in Midwest Radio-Television Inc., 45 F.C.C. 1137 (1963)."[215] That can be seen as Congressional endorsement of the interpretations in *Midwest Radio-Television*, or at least more instructive than such legislative history otherwise commonly might be viewed.

65. Likewise, for the purposes of section 503, "repeated" only requires that a party acted (or failed to act) more than once or, if the act or failure to act is continuous, for more than one day.[216] In the present case, both are true—AT&T not only failed to meet its obligations to have reasonable protections of customer CPNI repeatedly with each LBS provider and Aggregator, but also failed to meet such obligations for more than one day. Thus, by continuing to operate its LBS program in the absence of reasonable safeguards, AT&T willfully and repeatedly violated section 222 of the Act and section 64.2010 of the Commission's rules.

3. The Commission Rightfully Treated LBS Providers Equally for Purposes of Calculating Violations

66. AT&T also challenges the Commission's finding that each and every LBS provider and aggregator relationship that AT&T left in place more than 30 days after the *New York Times* report involved a failure to reasonably protect CPNI. AT&T contends that, because some of these 84 entities were "well known and highly reputable" companies, they did not "pose a realistic data-security threat" and the Commission should not have treated them uniformly for purposes of determining the number of violations and calculating the proposed penalty.[217]

67. We disagree. The exact level of threat posed by each LBS entity is both unquantifiable and beside the point. The Commission determined that the system of safeguards, under which these entities each operated pursuant to individual contracts and differing approved Use Cases, did not meet the reasonableness requirement of section 64.2010. Of particular significance is the fact that, at all times relevant to the violations period, AT&T still had not implemented a consent mechanism that would enable it to verify that a customer's purported consent to the disclosure of location information was legitimate. As noted in the *NAL*, "[a]fter the Securus and Hutcheson breaches came to light, AT&T had good reason to doubt the accuracy of the consent records it received from *any* location-based service provider."[218] The reputation of any particular third party is no substitute for implementing reasonable safeguards to protect customer location information that AT&T made available to that entity (and potentially its individual employees and contractors). Indeed, even "well known and highly reputable" companies such as AT&T

[214] As the Commission has noted, a federal district court decision declined to enforce the *Midwest Radio-Television* decision. *See Application For Review Of Southern California Broadcasting Company Licensee, Radio Station Kiev(Am) Glendale, California*, Memorandum Opinion and Order, 6 FCC Rcd 4387, 4387-88, para. 5 (1991) (referencing *U.S. v. Midwest Radio–Television, Inc*., 249 F. Supp. 936, 937 (D. Minn. 1966)). However, that district court decision does not reflect any statutory analysis, nor does it otherwise grapple with the Commission and court precedent interpreting willfulness under other provisions of the Act and Commission rules, let alone any of the other considerations relied on in *Midwest Radio-Television*.

[215] H.R. Conf. Rep. 97-765, at 51, 1982 U.S.C.C.A.N. 2261, 2295 (Aug. 19, 1982).

[216] *See, e.g., Playa Del Sol Broadcasters*, Order on Review, 28 FCC Rcd 2666, 2668, para. 4 (2013); *Hale Broadcasting Corporation*, 79 FCC2d 169, 171, para. 5 (1980); *Midwest Radio-Television,* 40 F.C.C. at 168, paras. 15-16. Although AT&T contends that the Commission cannot find a repeated violation here, it does not offer any particular interpretation of the term "repeated." *See* NAL Response at 38.

[217] NAL Response at 39-40.

[218] *NAL*, 35 FCC Rcd 1758, para. 39 (emphasis added).

are not immune to security threats posed by insiders.[219] Accordingly, we reject AT&T's argument that the Commission erred in finding 84 separate continuing violations for the 84 entities that AT&T continued to provide with access to customer location information.

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

68. We reject AT&T's supplemental constitutional objections that: (1) the FCC combines prosecutorial and adjudicative roles in violation of constitutional due process requirements;[220] (2) the issuance of a forfeiture order by the Commission would violate Article III and the Seventh Amendment;[221] 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.[222] AT&T's arguments are premised on misunderstandings regarding the relevant statutory framework, the nature of the Commission's actions, and relevant precedent.

69. As a threshold matter, AT&T 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, AT&T is entitled to a trial *de novo* in federal district court before it can be required to pay the forfeiture.[223] AT&T's objection to the combination of 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.[224] Likewise, AT&T'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 AT&T's statutory right to a trial *de novo* before it can be required to pay the forfeiture.[225] 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.

---

[219] *See AT&T Services, Inc*., Order and Consent Decree, 30 FCC Rcd 2808 (EB 2015) (resolving an investigation into unauthorized access to CPNI perpetrated by employees at three different AT&T call centers).

[220] Letter from C. Frederick Beckner III, counsel to AT&T, to Michael Epshteyn and Rosemary Cabral,, Enforcement Bureau, FCC, EB-TCD-18-00027704, at 2 (filed June 22, 2023) (AT&T June 22, 2023 Supplemental NAL Response).

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

[222] AT&T June 22, 2023 Supplemental NAL Response at 3. AT&T also claims in passing that "[t]he Bureau's compulsory investigative process, in which targets are compelled to respond to often excessively broad requests for information—upon threat of additional enforcement action and without an appropriate opportunity to object or appeal—also raises serious due process concerns." *Id*. at 2 n.6. AT&T does not explain how, exactly, the investigatory process used by the Enforcement Bureau either here or more generally violates due process, however, nor how such concerns bear on the ultimate validity of the Commission's action in this forfeiture order. We thus reject that undeveloped claim as a reason not to proceed with a forfeiture order here.

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

[224] *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.'").

[225] *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).

70. Independently, there are sufficient grounds to reject AT&T's arguments for other reasons, as well. We discuss each of these in turn below.

71. *Combination of Functions.* With respect to AT&T's claimed due process violation,[226] AT&T fails to demonstrate sufficient grounds for concluding that a combination of functions in the Commission's enforcement process here renders it constitutionally suspect, even apart from AT&T'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."[227] To overcome that presumption requires "a showing of conflict of interest or some other specific reason for disqualification."[228]

72. AT&T fails to demonstrate a concern specific to the Commission's forfeiture order here sufficient to overcome the presumption of honesty and integrity. Insofar as AT&T 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.[229]

73. AT&T also expresses concerns that the Commission "(1) affords the respondents no hearing before an ostensibly neutral ALJ in any NAL-based proceeding; (2) does not wall itself off from enforcement staff when adjudicating such a proceeding; and (3) can impose massive financial penalties at the conclusion of its administrative case."[230] 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, the first of AT&T's 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.[231]

---

[226] AT&T June 22, 2023 Supplemental NAL Response at 2.

[227] *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).

[228] *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'").

[229] *See* AT&T 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), as well as other pending challenges in the Fifth Circuit and the U.S. District Court for the District of Columbia).

[230] AT&T June 22, 2023 Supplemental NAL Response at 2.

[231] 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 (continued….)

74. As to AT&T's second concern, both the Communications Act[232] and the Administrative Procedure Act[233] require formal separation of personnel in specific circumstances not present here, and the Supreme Court has cautioned against requiring agencies to follow procedures beyond those specified by statute.[234] Particularly against the backdrop presumption of honesty and integrity on the party of agency adjudicators, AT&T identifies nothing specific to this case that would persuade us to depart from Congress' assessment of when formal separation of personnel is required.

75. Nor does the third concern cited by AT&T persuade us that due process concerns are present here. The potential to adopt forfeitures—even substantial forfeitures—that would be paid into the U.S. Treasury does not create a risk of financial bias on the part of reasonable adjudicators in the Commission's position.[235] 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.[236] 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 AT&T provide evidence that is the case here.[237] 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

---

held that the evidence had been erroneously excluded." *Withrow v. Larkin*, 421 U.S. at 48-49 (internal quotation marks omitted). The Court's willingness to accept continued adjudicator participation even where final—not merely preliminary—decisions previously had been made by the adjudicators strongly supports our analysis here.

We are unpersuaded to rely on precedent cited by AT&T that does not grapple with the presumption of honesty and integrity on the part of agency adjudicators. In particular, in *Propert v. Dist. of Columbia*, a vehicle owner challenged a D.C. enforcement regime for "junk" cars, and given the subjectivity of the standard being applied, the court observed that because "[t]he officer to whom appeal may be made is the same officer who decides that the vehicle is 'junk' in the first place; . . . serious questions as to impartiality arise"—but without considering any presumption of honesty and integrity. 948 F.2d 1327, 1333-34 (D.C. Cir. 1991).

[232] 47 U.S.C. § 409.

[233] 5 U.S.C. § 554.

[234] *See, e.g.*, *Vermont Yankee Nuclear Power Corp. v. Nat. Res. Def. Council*, 435 U. S. 519, 524 (1978).

[235] *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.").

[236] *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).

[237] *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).

case of a criminal prosecutor then serving as a judge.[238] 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,"[239] and AT&T 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*.

76. To the extent that AT&T purports to identify concerns about the neutrality of two specific commissioners, we reject those arguments, as well. In particular, AT&T contends that statements accompanying the *NAL* by then-Commissioner Rosenworcel and Commissioner Starks "criticized the NAL for not being punitive enough."[240] However, what is relevant for purposes of evaluating bias in an adjudicatory proceeding is whether "a disinterested observer may conclude that [the agency] has in some measure adjudged the facts as well as the law of a particular case in advance of hearing it."[241] Properly understood, the portions of the separate statements quoted by AT&T address a legal or policy issue—the methodology used to calculate the proposed forfeiture—along with the related issue of the Commission's failure to gather facts that would have enabled it to calculate a forfeiture using a different methodology.[242] That does not reflect any prejudgment of the facts to be resolved in the adjudication resulting from the *NAL*—to the contrary, the commissioners' statements demonstrate that they viewed the ultimate issues as unresolved at that time.[243] We thus reject AT&T's claims of a due process violation through our implementation of the section 503(b) NAL-based process here.

77. *Trial By Jury.* We also reject AT&T's contention that adjudication of the violations at issue here may not constitutionally be assigned to a federal agency.[244] The Seventh Amendment preserves "the right of trial by jury" in "Suits at common law, where the value in controversy shall exceed twenty dollars,"[245] but the Seventh Amendment applies only to suits litigated in Article III courts, not to administrative adjudications conducted by federal agencies.[246] In determining whether an adjudication involves an exercise of judicial power vested in the federal courts under Article III of the constitution, the

---

[238] *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").

[239] 47 U.S.C. § 503(b)(4).

[240] AT&T June 22, 2023 Supplemental NAL Response at 2 (citing *NAL*, 35 FCC Rcd at 1778 (Statement of Commissioner Jessica Rosenworcel Dissenting) (*Rosenworcel Statement*) and *NAL*, 35 FCC Rcd at 1779 (Statement of Commissioner Geoffrey Starks Approving In Part and Dissenting In Part) (*Starks Statement*)).

[241] *Cinderella Career & Finishing Schs., Inc. v. FTC*, 425 F.2d 583, 591 (D.C. Cir. 1970).

[242] *See, e.g.*, *Rosenworcel Statement*, 35 FCC Rcd at 1778 (criticizing the proposed forfeiture as relying on "bureaucratic math to discount the violations of our privacy laws" leading to proposed forfeitures "that are too small relative to the law and the population put at risk"); *Starks Statement*, 35 FCC Rcd at 1779 (stating that "I strongly believe we should have determined the number of customers impacted by the abuses and based our forfeiture calculations on that data").

[243] *See, e.g.*, *Rosenworcel Statement*, 35 FCC Rcd at 1778 ("[W]hen the FCC releases a Notice of Apparent Liability, it is just early days. The fines are not final until after the carriers that are the subject of this action get a chance to respond. That means there is still work to do . . . ."); *id*. (observing that the *NAL* merely "proposes" certain fines); *Starks Statement*, 35 FCC Rcd at 1781-83 (repeatedly describing the forfeiture amounts as merely "proposed" in the *NAL*).

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

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

[246] *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).

Supreme Court has distinguished between "public rights" and "private rights."[247] Congress has broad authority to "assign adjudication of public rights to entities other than Article III courts."[248] 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,[249] "adjudicating violations of the customs and immigration laws and assessing penalties based thereon,"[250] adjudicating "whether an unfair labor practice had been committed and of ordering backpay where appropriate,"[251] and the grant or reconsideration of a grant of a patent.[252] That precedent confirms the constitutional validity of FCC adjudication of violations of the Communications Act, even setting aside the reality that AT&T 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"[253] designed to protect consumer privacy even as the communications marketplace became more open to competition,[254] 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.[255]

78. Relying on the Fifth Circuit's decision in *Jarkesy*, AT&T 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 common law negligence.[256] Even on its own terms, however, *Jarkesy* did not deal with a claim that was analogized to common-law negligence.[257] By contrast, the Supreme Court itself has held that an agency could conduct adjudications to enforce federal workplace-safety rules, even though workplace-safety disputes historically had been resolved through "common-law actions for negligence and wrongful death."[258] Given that Supreme Court precedent, we are not persuaded by AT&T's attempt to implicate Article III

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

[248] *Id*.

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

[250] *Id*. at 451.

[251] *Id*. at 453.

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

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

[254] *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.").

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

[256] AT&T June 22, 2023 Supplemental NAL Response at 2-3 (citing *Jarkesy v. SEC*, 34 F.4th 446 (5th Cir. 2022)). AT&T also cites Justice Thomas' concurrence in *Axon. Id*. (citing *Axon*, 143 S. Ct. at 907 (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.

[257] *Jarkesy*, 34 F.4th at 455.

[258] *Atlas Roofing*, 430 U.S. at 445.

and the Seventh Amendment based on asserted analogies to common-law negligence, even taking the Fifth Circuit's decision in *Jarkesy* on its own terms.

79. Separately, AT&T also quotes the statement in *Jarkesy* that "actions seeking civil penalties are akin to special types of actions in debt from early in our nation's history which were distinctly legal claims."[259] In support of that statement, the Fifth Circuit cited the Supreme Court's decision in *Tull v. United States*.[260] 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.[261] 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."[262] Thus, *Tull* does not address the question of whether Congress can assign the adjudication of a given matter to an administrative agency—it speaks only to the Seventh Amendment implications of a matter that is assigned to an Article III court. To the extent that the Fifth Circuit in *Jarkesy* treated *Tull* as standing for the proposition that causes of action analogous to common-law claims would, as a general matter, need to be adjudicated in Article III courts with a right to trial by jury, we are unpersuaded. As the Supreme Court has held in a post-*Tull* decision, "Congress may fashion causes of action that are closely analogous to common-law claims and place them beyond the ambit of the Seventh Amendment by assigning their resolution to a forum in which jury trials are unavailable."[263] We thus are unpersuaded by AT&T's reliance on *Jarkesy*.[264]

80. *Nondelegation*. Finally, contrary to AT&T's contention,[265] 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.[266] Contrary to AT&T'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

[259] AT&T June 22, 2023 Supplemental NAL Response at 3 (quoting *Jarkesy*, 34 F.4th at 454-55).

[260] *Jarkesy*, 34 F.4th at 454-55 (citing *Tull v. United States*, 481 U.S. 412, 418-19 (1987)).

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

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

[263] *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.

[264] As AT&T notes, the government has petitioned for certiorari in the *Jarkesy* case. AT&T June 22, 2023 Supplemental NAL Response at 3 n.8; *see also* Petition for a Writ of Certiorari, SEC v. Jarkesy, No. 22-859 (filed Mar. 8, 2023).

[265] AT&T June 22, 2023 Supplemental NAL Response at 3.

[266] 47 U.S.C. § 503(b)(3), (4).

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.[267]

81. We also are unpersuaded by AT&T'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,[268] 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.[269] 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 the ends of justice."[270] 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.[271] The circumstances here therefore are distinct from those in *Jarkesy* where "Congress offered *no guidance* whatsoever."[272]

IV. CONCLUSION

82. Based on the record before us and in light of the applicable statutory factors, we conclude that AT&T willfully and repeatedly violated section 222 of the Act[273] as well as section 64.2010 of the Commission's rules[274] 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 $57,265,625 forfeiture proposed in the *NAL*.

V. ORDERING CLAUSES

83. 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, AT&T, Inc., **IS LIABLE FOR A**

---

[267] *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").

[268] 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 264.

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

[270] 47 U.S.C. § 154(j).

[271] *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).

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

[273] 47 U.S.C. § 222.

[274] 47 CFR § 64.2010.

MONETARY FORFEITURE in the amount of fifty-seven million, two-hundred and sixty-five thousand, six hundred and twenty-five dollars ($57,265,625) for willfully and repeatedly violating section 222 of the Act and section 64.2010 of the Commission's rules.

84. 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.[275] AT&T, Inc., shall send electronic notification of payment to Shana Yates, Michael Epshteyn, and Kimbarly Taylor, Enforcement Bureau, Federal Communications Commission, at shana.yates@fcc.gov, michael.epshteyn@fcc.gov, and kimbarly.taylor@fcc.gov on the date said payment is made. If the forfeiture is not paid within the period specified, the case may be referred to the U.S. Department of Justice for enforcement of the forfeiture pursuant to section 504(a) of the Act.[276]

85. In order for AT&T, Inc. to pay the proposed forfeiture, AT&T, Inc. 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:[277]

- 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[278] or printed CORES form[279] 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).[280] 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.

[275] *Id.*

[276] 47 U.S.C. § 504(a).

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

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

[279] 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.

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

- 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.

86. 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.

87. **IT IS FURTHER ORDERED** that a copy of this Forfeiture Order shall be sent by first class mail and certified mail, return receipt requested, to David R. McAtee II, Senior Executive Vice President and General Counsel, AT&T, Inc., c/o Jonathan E. Nuechterlein, Esq., and C. Frederick Beckner III, Esq., Sidley Austin LLP, 1501 K Street, N.W., Washington, DC, 20005.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

STATEMENT OF
CHAIRWOMAN JESSICA ROSENWORCEL

Re: *In the Matter of AT&T Inc.*, Forfeiture Order, File No.: EB-TCD-18-00027704 (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 AT&T Inc.*, Forfeiture Order, File No.: EB-TCD-18-00027704 (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]

[1] 47 U.S.C. § 222(h)(1)(A).

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.

[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 AT&T Inc.*, Forfeiture Order, File No.: EB-TCD-18-00027704 (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.