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

In the Matter of	)	
	)	
T-Mobile USA, Inc.	)	File No.: EB-TCD-18-00027702
	)	NAL/Acct. No.: 202032170003
	)	FRN: 0006945950

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 T-Mobile USA, Inc. (T-Mobile or Company).[1] In the *NAL*, the Commission admonished T-Mobile 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 T-Mobile $91,630,000 for failing to take reasonable steps to protect its customers' location information. After

[1] *T-Mobile USA, Inc.*, Notice of Apparent Liability for Forfeiture and Admonishment, 35 FCC Rcd 1785 (2020) (*NAL*).

reviewing the Company's response to the *NAL*,[2] we find no reason to cancel or withdraw the proposed penalty. However, pursuant to additional factual evidence provided in T-Mobile's NAL Response relevant to the forfeiture calculation, we reduce the proposed penalty by $11,550,000, and therefore impose a penalty of $80,080,000 against T-Mobile.

II. BACKGROUND

A. Legal Background

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

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

[2] *T-Mobile USA, Inc*., Response to Notice of Apparent Liability for Forfeiture and Admonishment (filed May 7, 2020) (on file in EB-TCD-18-00027702) (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 T-Mobile are "telecommunications services." *See* 47 U.S.C. § 332(c)(1); H.R. Conf. Rep. No. 104-458 at 125 (1996) ("This definition [of 'telecommunications service'] is intended to include commercial mobile service.").

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

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

[10] 47 CFR § 64.2007(b).

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

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

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

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

---

[11] 47 CFR § 64.2003(k).

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

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

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

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

[16] *See* 47 CFR § 64.2007(b).

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

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

[19] *See* 47 CFR § 64.2010(b)-(d).

[20] *See* 47 CFR § 64.2010(e)-(f).

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

[22] 47 CFR § 64.2010(a).

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

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

B. Factual Background

8. *Customer Location Information and T-Mobile's Location-Based Services Business Model.* T-Mobile provides mobile voice and data services to consumers throughout the United States by enabling consumer mobile phones to make and receive calls or transmit data on T-Mobile's wireless network.[26] As part of its business, T-Mobile ran a Location-Based Services (LBS) program until February 8, 2019. Through the LBS program, T-Mobile 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] T-Mobile 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, T-Mobile sold access to its customers' location information (directly or indirectly) to 75 third-party entities (including the two Aggregators).[29]

---

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

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

[25] 47 U.S.C. § 217.

[26] *See* T-Mobile US, Inc., 2021 Annual Report, https://s29.q4cdn.com/310188824/files/doc_financials/2021/ar/TMUS-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 1790-99, paras. 12-38.

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

[29] *See* NAL Response at 57. The NAL Response identified factual errors in the *NAL* related to the number of entities involved in T-Mobile's LBS program; the *NAL* listed 83 total entities (including the two Aggregators), but the NAL Response provided clarification that eight entities were counted twice. See *NAL*, 35 FCC Rcd at 1792, para. 14; NAL Response at 57.

9. The T-Mobile LBS program was largely governed via contractual provisions that vested T-Mobile with oversight authority over the Aggregators. The Aggregators then entered into their own contracts with various LBS providers. This arrangement meant that it was LBS providers who were obligated "to notify [customers] and collect affirmative customer consent for any use of location information"[30] – not the Aggregators or T-Mobile. T-Mobile 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 provisions with the Aggregators.[31] 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.[32] As a result, T-Mobile did not independently verify the customers' consent before providing access to the location data. T-Mobile explained that there were various acceptable mechanisms for the LBS providers and Aggregators to obtain consent, including via text message (with consumer responding with their consent), website interaction, and implicit consent "where the consumer is requesting a service that quite clearly relies on location data, such as roadside assistance services."[33]

10. According to T-Mobile, in order to participate in the LBS program and access consumers' location information, "the Aggregator was required to submit to T-Mobile a completed questionnaire that provided information about the location-based service provider and the proposed use case or 'campaign.'"[34] T-Mobile explains that using the questionnaires, the Company would receive a "detailed description" of the LBS provider's "notice and consent process, data security mechanisms and data retention policies,"[35] which was reviewed and then (if it met certain standards) approved by T-Mobile.[36] Once approved, T-Mobile asserts that it would assign a "campaign-specific ID."[37] That ID was to be used by the LBS provider for every location information request it submitted to the Aggregator, and then likewise transmitted from the Aggregator to T-Mobile, which T-Mobile asserts allowed the Company "to track each campaign."[38]

11. T-Mobile had broad authority under its contracts with the Aggregators to quickly terminate access to customer location information and to "suspend the transmission of location information" to any LBS provider the Company "believed was not complying with its obligations."[39] In addition, T-Mobile "had the right to terminate its relationship with each Aggregator, for any reason, upon

[30] *See NAL*, 35 FCC Rcd at 1793, para. 16 (citing Response to Letter of Inquiry from T-Mobile USA, Inc., to Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau at 10, Introduction (Nov. 30, 2018) (on file in EB-TCD-18-00037702 (LOI Response)).

[31] *See NAL*, 35 FCC Rcd at 1792-94, paras. 16-19.

[32] *See NAL*, 35 FCC Rcd at 1793, para. 16 (citing LOI Response at 10, Introduction).

[33] *NAL*, 35 FCC Rcd at 1793, para. 17 (citing E-mail from David Solomon, Wilkinson Barker Knauer, LLC, Counsel for T-Mobile USA, Inc., to Michael Epshteyn, Assistant Division Chief, Telecommunications Consumers Division, FCC Enforcement Bureau (Jan. 28, 2019, 18:27 ET) (on file in EB-TCD-18-00027702) (T-Mobile E-mail)).

[34] *NAL*, 35 FCC Rcd at 1793, para. 17 (citing LOI Response at 7-8, 11, Response to Question 1).

[35] *NAL*, 35 FCC Rcd at 1793, para. 17 (citing LOI Response at 7-8, 11, Response to Question 1).

[36] *NAL*, 35 FCC Rcd at 1793, para. 17 (citing LOI Response at 7-8, Introduction).

[37] *NAL*, 35 FCC Rcd at 1793, para. 18 (citing LOI Response at 11, Response to Question 1).

[38] *NAL*, 35 FCC Rcd at 1793, para. 18 (citing LOI Response at 11, Response to Question 1).

[39] *NAL*, 35 FCC Rcd at 1793-94, para. 19 (citing LOI Response at T-MOBILE00013594, Response to Request for Documents No. 3, 2014 Location Aggregator License Agreement between T-Mobile and TechnoCom Corporation d/b/a LocationSmart (executed on May 20, 2014, by Stephen Leptich, Sr., Corporate Counsel, for T-Mobile USA, Inc., and by Mario Proietti, CEO for LocationSmart), Sections 7.2-3 (T-Mobile-LocationSmart Agreement); LOI Response at TMOBILE0001230, Response to Request for Documents No. 3, 2014 Location Aggregator License Agreement between T-Mobile and Zumigo, Inc. (executed on Feb. 11, 2014, by Stephen Leptich, Sr., Corporate Counsel, for T-Mobile USA, Inc., and by Chirag Bakshi, CEO for Zumigo), Sections 7.2-3 (T-Mobile-Zumigo Agreement)).

30 days' prior written notice, or immediately upon the Aggregator's breach of the contract's confidentiality and data security terms."[40]

12. T-Mobile also had the authority to conduct audits and other internal reviews of the LBS program. According to T-Mobile, it conducted two risk assessments of its Aggregators (in 2016 and 2018) to confirm, among other things, whether they "were following the policies and procedures set forth in their contracts with T-Mobile."[41] T-Mobile asserts that both assessments found that "the Aggregators were properly obtaining consent before accessing T-Mobile customer location information."[42] However, T-Mobile also admits that both assessments identified "recommendations to enhance program governance" – with the questionnaire used to assess LBS providers the result of a recommendation from the 2016 assessment.[43] T-Mobile did not describe any of the recommendations from the 2018 assessment.[44] Finally, T-Mobile claims that both the Company and the Aggregators "reviewed consent records" as part of "periodic assessments," but T-Mobile did not provide any further information about the results of such periodic assessments.[45]

13. *T-Mobile's Discovery of Potential Misuse of Customers' Location Information in 2017*. On or around July 2017, T-Mobile "learned through a third party that an unidentified location-based service provider was using an obfuscated website domain to provide wireless device-tracking services to bail bond and similar companies without the wireless customer's authorization."[46] T-Mobile investigated the allegation and eventually identified LocateUrCell as the LBS provider misusing customer location information.[47] LocateUrCell was only approved to receive T-Mobile customer location information for its approved campaign (providing customers the ability to locate their missing phones); LocateUrCell worked with the Aggregator LocationSmart.[48] T-Mobile contacted LocationSmart in September 2017, informing the Aggregator that its access to customer location information would be suspended unless it provided a satisfactory response to T-Mobile's inquiry about LocateUrCell within 24 hours.[49] It was only then that T-Mobile learned LocationSmart had "'terminated its contract with LocateUrCell and permanently disabled LocateUrCell's access to T-Mobile customer location data on September 12, 2017, after LocateUrCell failed to respond to LocationSmart's request for records demonstrating customer consent.'"[50] T-Mobile concedes that LocateUrCell's unauthorized disclosures were made possible and remained hidden because the unauthorized requests were "hosted on the same system" and "used the same campaign ID" as the authorized requests.[51] Thus, "T-Mobile could not differentiate between location information requests for the authorized LocateUrCell phone-finding service from location information requests for the unauthorized . . . tracking service."[52] Following this incident, "T-Mobile 'sought assurances' from LocationSmart regarding

[40] *NAL*, 35 FCC Rcd at 1794, para. 19 (T-Mobile-LocationSmart Agreement, Sections 7.2-3; T-Mobile-Zumigo Agreement, Sections 7.2-3).

[41] *NAL*, 35 FCC Rcd at 1794, para. 20 (citing LOI Response at 18, Response to Question 11).

[42] *NAL*, 35 FCC Rcd at 1794, paras. 21-22 (citing LOI Response at 18, Response to Question 11).

[43] *NAL*, 35 FCC Rcd at 1794, paras. 21-22 (citing LOI Response at 18, Response to Question 11).

[44] *See NAL*, 35 FCC Rcd at 1794, para. 22.

[45] *NAL*, 35 FCC Rcd at 1794, para. 23 (citing LOI Response at 14, Response to Question 5.e.).

[46] NAL Response at 52; *see also NAL*, 35 FCC Rcd at 1794-95, para. 24.

[47] NAL Response at 52.

[48] *See NAL*, 35 FCC Rcd at 1794-95, para. 24.

[49] *See NAL*, 35 FCC Rcd at 1795, para. 25 (citing LOI Response at 17, Response to Question 10).

[50] *NAL*, 35 FCC Rcd at 1795, para. 25 (quoting LOI Response at 17-18, Response to Question 10).

[51] *NAL*, 35 FCC Rcd at 1795, para. 26 (quoting LOI Response at 18, Response to Question 10).

[52] *NAL*, 35 FCC Rcd at 1795, para. 26 (citing LOI Response at 18, Response to Question 10).

its monitoring of location-based service providers and 'reminded' LocationSmart about its contractual obligations to notify T-Mobile of any non-compliance it detected."[53]

14. *Unauthorized Access and Use of Customer Location Information*. On May 10, 2018, the *New York Times* published an article that detailed security breaches involving T-Mobile's (and other carriers') practice of selling access to customer location information.[54] 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.[55] Not only was Securus's location-finding service outside the scope of its approved "campaign" or any agreement with either Aggregator (and thus had not been reviewed by T-Mobile), 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.[56] Securus obtained location services from a company called 3Cinteractive, and 3Cinterative obtained T-Mobile's consumers' location information pursuant to a contract with the Aggregator LocationSmart.[57] Similar to the 2017 LocateUrCell incident, T-Mobile again conceded that it had "no way" to distinguish requests that were unrelated to the authorized campaign (which involved an inmate collect-calling service) from valid, campaign-related requests because "Securus offered this [unauthorized] service using the [same] campaign ID that T-Mobile had assigned" to the approved campaign.[58]

15. 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.[59] 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.[60] In order to do so, users (including Hutcheson) were required to input the telephone number of the device they wanted to

---

[53] *NAL*, 35 FCC Rcd at 1795, para 25 (quoting LOI Response at 17, Response to Question 10).

[54] *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.

[55] *See NAL*, 35 FCC Rcd at 1795-1796, paras. 27-28 (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).

[56] *See NAL*, 35 FCC Rcd at 1795-96, paras. 27-28 (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).

[57] *See NAL*, 35 FCC Rcd at 1796, para. 29.

[58] *See NAL*, 35 FCC Rcd at 1796-97, para. 30 (citing LOI Response at 10, 19, Introduction, Response to Question 12).

[59] *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.

[60] *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 1795-96, paras. 27-28.

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.'"[61] As soon as Hutcheson (or any other authorized user) submitted his request and uploaded a document, the Securus LBS platform would *immediately* provide the requested location information (regardless of the adequacy of the uploaded document).[62] 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."[63] Those "false and fraudulent documents" included "his health insurance policy, his auto insurance policy, and pages selected from Sheriff training materials."[64] Hutcheson "submitted thousands of Securus LBS requests and obtained the location data of hundreds of individual phone subscribers without valid legal authorization."[65]

16. *T-Mobile's Response to the Securus Disclosures*. T-Mobile terminated Securus's and 3Cinteractive's access to T-Mobile customer location information on May 11, 2018, following the *New York Times* article.[66] Later, on October 26, 2018, T-Mobile notified the Aggregators that their existing contracts would not be renewed once they expired on March 9, 2019, which would effectively end T-Mobile's LBS program.[67]

17. More than seven months after the *New York Times* article revealing the Securus disclosures, T-Mobile was made aware of a similar incident involving one of the Company's LBS providers, MicroBilt. In a January 8, 2019, *Motherboard* article, it was reported that access to customer location information was sold and resold, with little or no oversight, within the bail bonds industry, and that this led to consumers being tracked without their knowledge or consent—including by MicroBilt.[68] T-Mobile first learned of this from a *Motherboard* reporter on January 3, 2019.[69] According to T-Mobile, "the MicroBilt application that T-Mobile had received [in 2016] did not indicate that 'Microbilt would disclose the location information to any third party.'"[70] Thus, on January 4, 2019, MicroBilt's Aggregator in the LBS program (Zumigo) informed T-Mobile that it had "suspended transmission of any T-Mobile customer location information to MicroBilt"[71] and T-Mobile itself (as a "duplicative technical measure") "permanently disabled access to its customers' location information by Zumigo for the purpose of transmitting it to MicroBilt."[72] In a repeat of the aftermath following both the LocateUrCell incident and the Securus disclosure, "T-Mobile was again unable to differentiate requests for customer location

[61] Hutcheson Sentencing Memo at 3; *see also NAL*, 35 FCC Rcd at 1795-96, para. 27.

[62] *See* Hutcheson Sentencing Memo at 3-4; *see also NAL*, 35 FCC Rcd at 1795-96, para. 27.

[63] Hutcheson Sentencing Memo at 4; *see also NAL*, 35 FCC Rcd at 1796, para. 28.

[64] Hutcheson Sentencing Memo at 4; *see also NAL*, 35 FCC Rcd at 1796, para. 28.

[65] Hutcheson Sentencing Memo at 4; *see also NAL*, 35 FCC Rcd at 1796, para. 28.

[66] *See NAL*, 35 FCC Rcd at 1797, para. 31 (citing LOI Response at 9-10, Introduction).

[67] *See NAL*, 35 FCC Rcd at 1797, para. 32 (citing LOI Response at 15, Response to Question 6, Supplemental LOI Response at 6, Response to Question 1).

[68] *See NAL*, 35 FCC Rcd at 1798, para. 35 (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).

[69] *See NAL*, 35 FCC Rcd at 1797, para. 33 (citing T-Mobile E-mail).

[70] *NAL*, 35 FCC Rcd at 1797, para. 33 (quoting T-Mobile E-mail).

[71] *See NAL*, 35 FCC Rcd at 1797, paras. 34 (citing T-Mobile E-mail; Response to Supplemental Letter of Inquiry, from T-Mobile USA, Inc., to Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, at 12, Response to Question 5.c. (June 7, 2019) (on file in EB-TCD-18-00027702 (Supplemental LOI Response)).

[72] *NAL*, 35 FCC Rcd at 1797-98, para. 34 (quoting Supplemental LOI Response at 12, Response to Question 5.c.)

information that were made for purposes authorized by T-Mobile from those that were not"[73] because MicroBilt's malfeasance "'was masked as a permissible use.'"[74]

18. It was not until February 8, 2019, that T-Mobile's LBS program (and the sharing of the Company's customers' location information) finally ceased—in other words, 275 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.[75]

19. *Notice of Apparent Liability*. On February 28, 2020, the Commission issued the *T-Mobile NAL* proposing a $91,630,000 fine against T-Mobile for its apparent willful and repeated violation of section 222 of the Act and section 64.2010 of the Commission's CPNI Rules for failing to have reasonable protections in place to prevent unauthorized access to customer location information. In the *NAL*, the Commission also admonished T-Mobile for apparently disclosing its customers' location information, without their consent, to a third party who was not authorized to receive it.

20. On May 7, 2020, T-Mobile filed a response to the *NAL*.[76] T-Mobile makes a number of arguments as to why the *NAL* should be withdrawn and cancelled. T-Mobile argues that location information is not CPNI and thus is not subject to the Act and the Commission's rules, and that even if it was, the Company did not have fair notice that location information would be classified as CPNI.[77] T-Mobile 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.[78] T-Mobile argues that the forfeiture amount is arbitrary and capricious.[79] Finally, T-Mobile contends that the forfeiture amount is incorrect insofar as the *NAL* either miscounts the number of LBS providers and/or their termination dates from the LBS program in the forfeiture calculation.[80]

III. DISCUSSION

21. The Commission proposed a forfeiture in this case in accordance with section 503(b) of the Communications Act of 1934, as amended (Act),[81] section 1.80 of the Commission's rules,[82] and the Commission's *Forfeiture Policy Statement*.[83] 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

[73] *NAL*, 35 FCC Rcd at 1798, para 34.

[74] *NAL*, 35 FCC Rcd at 1798, para 34 (quoting Supplemental LOI Response at 12, Response to Question 5.c.).

[75] *See NAL*, 35 FCC Rcd at 1798, para. 37 (citing Supplemental LOI Response at 7, Response to Question 1.d); NAL Response at 34. T-Mobile did not accelerate the expiration of its agreements with the Aggregators, which terminated on March 9, 2019. *See* Supplemental LOI Response at 7, Response to Question 1.d.

[76] *See* NAL Response.

[77] NAL Response at 10-16.

[78] NAL Response at 22-38.

[79] NAL Response at 35-40.

[80] NAL Response at 57-60.

[81] 47 U.S.C. § 503(b).

[82] 47 CFR § 1.80.

[83] *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).

such other matters as justice may require."[84] We have fully considered T-Mobile's NAL Response, which includes a variety of legal and factual arguments. With one exception, we find none of T-Mobile's arguments persuasive. Upon review of T-Mobile's NAL Response[85] and a further review of the evidence in the record, we will adjust the forfeiture calculation to account for updated evidence related to (1) the termination dates for various entities in the LBS Program and (2) eight entities that were each counted twice in the original forfeiture calculation. We therefore reduce the $91,630,000 forfeiture proposed in the *NAL* by $11,550,000, and impose a penalty of $80,080,000.

A. Location Information is CPNI

22. As the *NAL* explained in more detail, the customer location information disclosed in T-Mobile's LBS program is CPNI under the Act and our rules.[86] 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."[87] The customer location information used in T-Mobile's LBS program falls squarely within this definition. T-Mobile's arguments to the contrary[88] are largely reiterations of arguments the Commission considered and found unpersuasive in the *NAL*. Consistent with the analysis of location data found in the *NAL*, we remain persuaded that the location data at issue here constitute CPNI.

23. *First*, the customer location information at issue here relates to the location of a telecommunications service—i.e., T-Mobile's commercial mobile service.[89] 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. T-Mobile 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.[90]

24. We conclude that the location information at issue here meets the first prong of the CPNI definition under either of two alternative interpretations. For one, we believe that the relevant statutory language is best read as referring to "information that relates to the . . . location, . . . of a telecommunications service . . . ."[91] 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

[84] 47 U.S.C. § 503(b)(2)(E).

[85] *See* NAL Response at 57 (noting that T-Mobile had inadvertently submitted duplicate entries for various LBS providers in its response to a letter of inquiry).

[86] *See NAL*, 35 FCC Rcd at 1799-1801, paras. 41-48.

[87] 47 U.S.C. § 222(h)(1)(A) (emphasis added).

[88] *See* NAL Response at 2-3, 10-16.

[89] *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").

[90] *See NAL*, 35 FCC Rcd at 1800, para. 43.

[91] 47 U.S.C. § 222(h)(1)(A).

preceding terms such as "location."[92] 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.[93] And our interpretation squares more readily with section 222(d)(1), which preserves carriers' ability to use CPNI to "initiate" service[94]—an event that, aspects of which, ordinarily occur before the service is in "use."

25. The location information at issue here readily fits within that interpretation of the first prong of the CPNI definition. T-Mobile'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 T-Mobile's ability to use its network to determinate that location—is reasonably understood as associated with or a reference to the location of the T-Mobile telecommunications service.[95] Consequently, consistent with our assessment in the *NAL*,[96] we find this to be information that "relates to" the location of T-Mobile's telecommunications service within the meaning of the first prong of the CPNI definition.[97]

26. In the alternative, even if the term "of use" modified "location," we still conclude the information at issue fits within the first prong of the definition of CPNI. T-Mobile does not dispute the *NAL*'s explanation that customers' devices and T-Mobile's network regularly exchange information as necessary for customers to send and receive calls.[98] To the extent that T-Mobile contends that this does not represent use of the telecommunications service because it merely enables the provision of that service, T-Mobile 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*,[99] we believe that T-

---

[92] *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'").

[93] We are unpersuaded by T-Mobile's claim that interpreting "of use" to modify only "amount" would lead to anomalies because "information relating to the 'quantity, technical configuration, [or] type . . . of a telecommunications service' . . . would relate to the network itself, not the information of individual customers." NAL Response at 12 (emphasis omitted). Even if the information relates in part to the network, it also relates to an individual customer by identifying characteristics of the telecommunications service subscribed to by that customer. *See, e.g.*, *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, 8064-65, para. 2 (1998) ("CPNI includes information that is extremely personal to customers as well as commercially valuable to carriers," including "the types of service offerings to which the customer subscribes").

[94] 47 U.S.C. § 222(d)(1).

[95] *See, e.g.*, *NAL*, 35 FCC Rcd at 1790, para. 12 ("T-Mobile provides mobile voice and data services to consumers throughout the United States by enabling consumer mobile phones to make and receive calls or transmit data on T-Mobile's wireless network.").

[96] *See, e.g.*, *NAL*, 35 FCC Rcd at 1799-1801, paras. 43, 46.

[97] *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").

[98] *NAL*, 35 FCC Rcd at 1799-1800, para. 43.

[99] *See, e.g.*, *NAL*, 35 FCC Rcd at 1799-1801, paras. 43, 46.

Mobile's customers subscribe to its commercial mobile service to enable them to receive and transmit calls, and when customers' devices are exchanging communications with T-Mobile'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.[100]

27. We also are unpersuaded by T-Mobile'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 T-Mobile gleans from other language in section 222.[101] In addition to the *NAL*'s responses in this regard,[102] 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:[103] 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*.[104] 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.[105]

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

---

[100] 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").

[101] *See, e.g.*, NAL Response at 13-15.

[102] *NAL*, 35 FCC Rcd at 1800, para. 45.

[103] This interpretive approach is consistent with how the Commission has approached the interpretation of section 222 in other contexts in the past. *See, e.g.*, *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, 8084-85, para 32 (1998) (distinguishing the interpretation of different language in section 222(a), (c)(1), and (d)(1), given that, "[u]nder well-established principles of statutory construction, 'where Congress has chosen different language in proximate subsections of the same statute,' we are 'obligated to give that choice effect'"). Particularly given that T-Mobile neglects this textual distinction in its attempts to rely on legislative history or the rule of lenity, we reject its claims in that regard. *See* NAL Response at 14 n.30.

[104] Given this predominant—but not exclusive—focus of the 1999 amendments to section 222, the references to call location information in the legislative history cited by T-Mobile is not surprising. *See* NAL Response at 14 n.30. But nothing in the legislative history persuades us that Congress meant to exclude non-call location data from the definition of CPNI.

[105] *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*).

> T-Mobile provides wireless telephony services to the affected customers because they have chosen T-Mobile to be their provider of telecommunications service—in other words, they have a carrier-customer relationship. . . . T-Mobile's customers provided their wireless location data to T-Mobile because of their customer-carrier relationship with T-Mobile, ...[106]

29. 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."[107] A relationship presumes associations involving at least two parties, and we conclude that it must be understood with that context in mind, rather than focused single-mindedly on one side of the relationship. Our accounting for the customer's viewpoint is also supported by the statutory text's focus on whether the information "is made available to the carrier by the customer"—rather than "obtained by the carrier"—"solely by virtue of the carrier-customer relationship."[108] Thus, we reject any suggestion by T-Mobile that the location information at issue here is not CPNI and does not depend exclusively on the carrier-customer relationship[109]—we find that suggestion belied by the technical and marketplace realities here, as experienced by T-Mobile customers.

30. Finally, we also note that when a customer subscribes to T-Mobile's commercial mobile service, T-Mobile "must be aware of and use the device's location in order for [the Company] to enable customers to send and receive calls,"[110] and the customer has no choice but to reveal that location to T-Mobile. T-Mobile does not dispute that the carrier-customer relationship fully enables T-Mobile to obtain the location data at issue here. Likewise, T-Mobile does not claim that a customer, having subscribed to its commercial mobile service, entered a separate agreement with T-Mobile for the provision of that location information—or that T-Mobile's voice customers had any way to avoid providing that information if they wanted to subscribe to T-Mobile's commercial mobile service. Under circumstances such as these, we conclude that the location information at issue from T-Mobile's commercial mobile service customers was "made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[111]

31. Although we find that reasoning sufficient to resolve the application of the second prong of the CPNI definition, we independently conclude that the same decision is warranted even if we parse the matter more finely. For example, T-Mobile has sought to rely on the theory that location information can be associated with a data session for a non-telecommunications service, taking such location information outside the purview of "CPNI."[112] But we are not persuaded that the fact that location information can be associated with a non-telecommunications service the carrier also provides 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

---

[106] *See NAL*, 35 FCC Rcd at 1800, para. 44.

[107] 47 U.S.C. § 222(h)(1)(A).

[108] 47 U.S.C. § 222(h)(1)(A).

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

[110] *NAL*, 35 FCC Rcd at 1800, para. 43.

[111] 47 U.S.C. § 222(h)(1)(A).

[112] *See, e.g.*, NAL Response at 10 ("An idle device or a device used for a data session . . . is not being used for a 'telecommunications service,' and location information regarding such a device does not fall within the definition of CPNI.").

sufficient to obligate T-Mobile's customers to make their location data available to T-Mobile,[113] 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."[114] We recognize that section 153(51) of the Act provides that "[a] telecommunications carrier shall be treated as a common carrier under [the Act] only to the extent that it is engaged in providing telecommunications services."[115] But we are far from that scenario here, given the many necessary links to T-Mobile's telecommunications services for the CPNI definition to apply. For one, the protections of section 222(c) only apply with respect to "information that relates to" certain characteristics of "a telecommunications service subscribed to by any customer of" T-Mobile.[116] And the information must have been provided by consumers in a manner that reflects the statutorily required nexus to T-Mobile's telecommunications service.[117] 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 T-Mobile would prefer.

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

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

33. We reject T-Mobile's claim that it lacked fair notice that its practices involving customer location information were subject to the Communications Act and potential penalties thereunder.[118] The language of section 222 demonstrates that customer location information is CPNI; T-Mobile's practices involving CPNI, including customer location information, therefore unquestionably are regulated under the Act and the CPNI Rules; T-Mobile's failure to comply with the requirements of the Act and the CPNI 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.

34. T-Mobile argues that the "the duties and requirements set forth in the NAL have never been articulated before and cannot, consistent with the fundamental principles of fair notice and due process, serve as a basis for holding T-Mobile liable for conduct that occurred in the past."[119] T-Mobile is mistaken. To the extent these arguments relate to T-Mobile's actions addressing the shortcomings in its LBS program, they will be discussed in section III.C, below.[120] With regard to T-Mobile's argument that

---

[113] 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 T-Mobile 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.

[114] *2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9616, para 23.

[115] 47 U.S.C. § 153(51).

[116] 47 U.S.C. § 222(h)(1)(A).

[117] 47 U.S.C. § 222(h)(1)(A).

[118] *See* NAL Response at 16, 38-43.

[119] NAL Response at 38.

[120] Among such arguments, T-Mobile argues that "nowhere had the Commission stated that implied consent . . . would not be deemed 'express authorization' under Section 222(f)." *See* NAL Response at 39. For the reasons discussed below in paragraphs 60-66, we reject T-Mobile's argument. Pursuant to the CPNI Rules and the Commission's interpretation of section 222(f) itself, it is clear that *explicit* consent is required for the use, disclosure, (continued….)

it did not have fair notice of what it describes as a "30-day clock" to respond to the Securus incident, T-Mobile is mistaken.[121] The 30-day period cited in *NAL* was not a deadline for which T-Mobile required fair notice, but rather a grace period during which the Commission used its discretion and did not assess a fine.[122]

35. T-Mobile also argues that before the Commission imposes what the Company mischaracterizes as a "new interpretation" of CPNI, the Commission must first "ensure that it has statutory authority to do so and amend its regulations . . . ."[123] But the Commission is not limited to this option. When, as in this case, a carrier's conduct falls within an area subject to regulation by the Commission, it is well established that enforcement action is a proper vehicle to adjudicate the specific bounds of what is lawful and what is not, subject to principles of fair notice.[124]

36. Contrary to T-Mobile'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.[125] As the D.C. Circuit has said, "[t]he fair notice doctrine, which is couched in terms of due process, provides redress only if an agency's interpretation is 'so far from a reasonable person's understanding of the regulations that they could not have fairly informed the regulated party of the agency's perspective.'"[126] 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.[127]

---

and provision of access to call location information under section 222(f). Accordingly, T-Mobile was on notice that implied consent would not be deemed "express authorization" under section 222(f).

[121] *See* NAL Response at 39 (asserting that fair notice was not provided because the "Commission had *never* stated that a carrier would have just 30 days to fully investigate and implement its response to information about a misappropriation of location data—much less specified that this 30-day clock would begin to run upon the publication of allegations *in a media report*.").

[122] However, T-Mobile'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 T-Mobile with a grace period to either end the program or reform its practices.

[123] *See* NAL Response at 16.

[124] *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").

[125] *See* NAL Response at 16 (claiming that this is a new interpretation of CPNI). However, this is not a "new interpretation" and, in any event, 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").

[126] *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").

[127] *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

(continued….)

37. 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."[128] Thus, T-Mobile 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."[129] 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."[130] In addition, notwithstanding its instant fair notice claims, T-Mobile previously asserted to the Commission that it treated *all* customer location information in the same way—whether T-Mobile classified it as CPNI or not.[131]

38. Further, our conclusion that the location data at issue here fall within the definition of CPNI flows from the text of section 222 is consistent with the Commission's approach to interpreting that provision in prior precedent. As noted, CPNI is defined by statute, in relevant part, to include "information that relates to . . . the location . . . of a telecommunications service."[132] 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."[133] Our interpretation of those provisions above relies on the statutory text, interpreted consistent with ordinary tools of statutory interpretation, and is consistent with prior Commission precedent.

39. Finally, T-Mobile had fair notice of its obligations with respect to CPNI under section 64.2010 of the Commission's rules. In pertinent part, that rule provides that "[t]elecommunications carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI."[134] 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]

---

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).

[128] *2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9617, para. 24 n.54.

[129] *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").

[130] *2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9617, para. 24 n.54.

[131] *See NAL*, 35 FCC Rcd at 1800, para. 45 n.126 (quoting Supplemental LOI Response at 9 n.33, Response to Question 2) ("T-Mobile emphasized that it 'follows the same policies and practices—and provides the same level of protection—for Customer Location Information' that it claims is not CPNI 'as it does for Customer Location Information that is CPNI.'"). *See also* LOI Response at 2-6, Introduction. T-Mobile stated that its Location Aggregator program "is based upon customer consent and complies with the standards and requirements of Section 222(f) of the Act and the voluntary CTIA Guidelines." *Id.* at 2. As T-Mobile pointed out in its LOI Response, section 222(f) governs the use, disclosure, and access to Call Location CPNI. *Id.*; *see also* 47 U.S.C. 222(f).

[132] 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'").

[133] 47 U.S.C. § 222(h)(1)(A).

[134] 47 CFR § 64.2010(a).

carriers to take additional steps to protect the privacy of CPNI to the extent such additional measures are feasible for a particular carrier."[135] Rather than listing "specific measures must implement to avoid fraudulent misappropriation of [location] data" as T-Mobile suggests,[136] the Commission granted carriers flexibility to incorporate the specific measures and practices that are consistent with their otherwise-existing "technological choices."[137] 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.[138] 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.[139] 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."[140] Contrary to T-Mobile's argument otherwise,[141] this guidance provides sufficient direction for T-Mobile to understand its obligations under the rule as relevant here.[142]

40. Thus, T-Mobile 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) T-Mobile would be subject to forfeiture penalties for failing to protect that customer location information as required under section 222 and the CPNI Rules.

C. T-Mobile Failed to Take Reasonable Steps to Protect CPNI

41. T-Mobile violated section 222 of the Act and section 64.2010 of the Commission's rules by failing to take reasonable measures to discover and protect against attempts to gain unauthorized access to its customers' location information.[143] While the Commission's rules recognize that companies cannot prevent all data breaches, they 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

---

[135] *2007 CPNI Order*, 22 FCC Rcd at 6959, para. 64.

[136] *See* NAL Response at 39.

[137] *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").

[138] *2007 CPNI Order*, 22 FCC Rcd at 6946, para. 35.

[139] *2007 CPNI Order*, 22 FCC Rcd at 6952-53, para. 49.

[140] *2007 CPNI Order*, 22 FCC Rcd at 6959-60, para. 65.

[141] *See* NAL Response at 41-43.

[142] Accordingly, we reject T-Mobile's argument that "[s]ection 64.2010(a) is too general a standard to support the NAL's conclusion that T-Mobile's actions in this case were unreasonable." *Id.* at 43. T-Mobile 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, T-Mobile'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).

[143] 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.").

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

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

42. As an initial matter, we conclude that it was not just disclosures to Hutcheson that were unauthorized. Rather, Securus's entire location-finding service[147] (as detailed in paragraphs 14-15, above) was predicated on unauthorized disclosures. Consistent with T-Mobile'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 T-Mobile).[148] T-Mobile conceded that it was unable to distinguish location requests unrelated to the authorized use case (which involved an inmate collect-calling service).[149] And, to be clear, none of the records submitted in connection with the location-finding service evinced a consumer's actual opt-in consent. Therefore, every time Securus submitted a request for location information under the guise of its approved use case (a use case that required consumer consent) and T-Mobile provided the requested location information, a separate, unauthorized disclosure occurred. Separately and independently, there is no indication that the law enforcement requests were properly reviewed by Securus, as evidenced by the ready success of Hutcheson's thinly veiled ruse.[150] 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 T-Mobile's unauthorized disclosure of location information to

[144] *See* NAL Response at 31.

[145] *See* NAL Response at 23-38.

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

[147] *See NAL*, 35 FCC Rcd at 1795-96, paras. 27-28 (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).

[148] *See* LOI Response at 9-10, Introduction; *NAL*, 35 FCC Rcd at 1796-97, paras. 29-30; *see also, e.g.*, NAL Response at 17, 31..

[149] *See NAL*, 35 FCC Rcd at 1797-98, para. 34.

[150] *See* Hutcheson Sentencing Memo at 3-4 (explaining that after uploading documents that were blatantly not legal authorizations, location information was immediately transmitted with no intervening time for any documents to be reviewed for validity); *NAL*, 35 FCC Rcd at 1796, para. 28 (describing Hutcheson's uploading of documents that were blatantly not legal authorizations in order to obtain location information). As the *NAL* explained, "T-Mobile does not deny the existence of what it describes as the Securus 'Real Time Location Service,'" nor does T-Mobile "deny the abuse of that service by Hutcheson." *NAL*, 35 FCC Rcd at 1796, para. 29. T-Mobile likewise does not dispute here that Hutcheson was able to access location data by providing documents that were blatantly not legal authorizations as described in the *NAL* and confirmed in the Hutcheson Sentencing Memo, and also does not provide any reason to believe that Securus (let alone T-Mobile) could have or would have made that assessment before providing the location data. While T-Mobile states in its NAL Response that entries in a spreadsheet relied upon in the *NAL* "contain no information demonstrating . . . that any CPNI was disclosed without lawful authorization," NAL Response at 9, it does not elaborate on any theory of how T-Mobile possibly could have obtained the authorization it was required to obtain under section 222(c)(1) and section 64.2007(b) of the rules under the circumstances here. We thus are unpersuaded by that cursory assertion.

Securus. Second, Hutcheson likewise submitted blatantly fake requests to Securus under the guise of law enforcement, resulting in Securus's unauthorized disclosure of location information to Hutcheson.[151]

43. T-Mobile attempts to avoid this conclusion by contending that it cannot be held responsible for the unauthorized disclosures because "Securus and other third-party location-based service providers can neither be deemed 'agent[s]' of T-Mobile nor 'person[s] acting for' T-Mobile within the meaning of Section 217, at least when they misappropriate information provided by T-Mobile."[152] But as the *NAL* explained, "[t]o the extent that the third parties were *not* acting on behalf of the carrier, the carrier itself would have provided those third parties with access to its customers' CPNI without obtaining for themselves the approval required by section 222(c)(1)—thus violating federal law."[153] Although the *NAL* noted that "T-Mobile does not appear to argue that situation is present here,"[154] the totality of the record persuades us that this is, in fact, the import of the facts and T-Mobile's arguments here.

44. In making these arguments, T-Mobile appears to conflate distinct obligations it is subject to under section 222 of the Act and the Commission's rules. In particular, T-Mobile contends that "the NAL suggests that Section 217 of the Act would allow it to hold T-Mobile strictly liable for the acts of the third-party location-based service providers, even if T-Mobile's program reasonably protected customer location information."[155] Even setting aside T-Mobile's erroneous assumption about the reasonableness of its safeguards, carriers' legal duty to "take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI" under section 64.2010(a) of the rules is separate from the additional restriction on unauthorized use or disclosure in section 222(c)(1) of the Act and section 64.2007(b) of the Commission's rules.[156] Rather than incorporating some kind of *de minimis* exception or reasonableness standard, section 222(c)(1)'s statutory restriction on use and disclosure is unequivocal, as likewise reflected in section 64.2007(b) of the Commission's rules.[157] And as the *NAL* further explained, "the obligation to protect CPNI falls on *telecommunications carriers*; the carrier must obtain customer approval to use, disclose, or permit someone else to access the CPNI for any purpose not strictly related to the purpose for which it was provided to the carrier."[158] "If T-Mobile was relying on third parties to satisfy its obligations to obtain consent, then it is [as] liable for those third parties' failures as it would be if they had been the failures of T-Mobile itself. If not, then T-Mobile effectively granted those third parties the capability to access the CPNI of its customers without customer approval."[159] T-Mobile does not contend that it directly obtained the required approval from the customers whose location information it was sharing—nor could it, given that its entire location-based services program was premised on the LBS providers obtaining customer authorization.[160] And T-Mobile now contends that under the circumstances at issue here, "Securus and other third-party location-based service providers can neither be deemed 'agent[s]' of T-Mobile nor 'person[s] acting for' T-Mobile within the meaning of

---

[151] *See* Hutcheson Sentencing Memo at 3-4 (Hutcheson "uploaded legally defective search warrants that either did not authorize the acquisition of location data, were unsigned, or had no connection to the targeted phone user" and in "most of these instances . . . even notarized his own signature."); *see also NAL*, 35 FCC Rcd at 1796, para. 28.

[152] NAL Response at 31.

[153] *NAL*, 35 FCC Rcd at 1803, para. 54 n.145.

[154] *NAL*, 35 FCC Rcd at 1803, para. 54 n.145.

[155] NAL Response at 31.

[156] 47 U.S.C. § 222(c)(1); 47 CFR § 64.2007(b).

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

[158] *NAL*, 35 FCC Rcd at 1802, para. 52.

[159] *NAL*, 35 FCC Rcd at 1803, para. 56.

[160] *See, e.g.*, *NAL*, 35 FCC Rcd at 1792-93, paras. 16-17; NAL Response at 24-26.

Section 217."[161] Therefore, consistent with the *NAL*, we find that the Securus disclosures, including those made to Hutcheson, were unauthorized and T-Mobile was appropriately admonished in relation to such disclosures.

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

45. The Commission affirms the *NAL* and finds that T-Mobile 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 T-Mobile did not have reasonable protections in place prior to the 2018 *New York Times* article detailing the Securus/Hutcheson breaches,[162] but also that T-Mobile failed to promptly address its demonstrably inadequate CPNI safeguards after the Securus/Hutcheson disclosures.[163]

46. T-Mobile attempts to excuse its unreasonable practices by cataloging the steps it did take before and after the *New York Times* article. T-Mobile argues that, prior to the Securus disclosure, its efforts conformed to the CTIA Guidelines for ensuring customer consent to the use of location data.[164] Specifically, T-Mobile states that its safeguards included: "numerous contractual, procedural, and technical safeguards designed to protect the privacy of customer location data; to ensure that customer consent was obtained; and to limit uses of the data to comply with the Act and industry best practices established in the CTIA LBS Guidelines."[165]

47. The safeguards that T-Mobile 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.[166]

As for the other safeguards that T-Mobile 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.[167] To the extent that T-Mobile's safeguards relied on trusting Aggregators and location-based service providers to honor their contractual commitments, consistent with the *NAL* we find that "such trust alone was" not "a reasonable safeguard here," particularly in light of the regulatory history regarding attempts to obtain unauthorized access to CPNI in general and in the case of T-Mobile location-based data in particular.[168]

---

[161] NAL Response at 31.

[162] *See NAL*, 35 FCC Rcd at 1804-07, paras. 58-68.

[163] *See NAL*, 35 FCC Rcd at 1807-10, paras. 69-78.

[164] *See* NAL Response at 7, 23, 24, 25, 27, 28-29, 42, 54, 55.

[165] NAL Response at 23.

[166] *NAL*, 35 FCC Rcd at 1806, para. 65 n.170.

[167] *See NAL*, 35 FCC Rcd at 1804-06, paras. 61-65.

[168] *NAL*, 35 FCC Rcd at 1807, para. 68. T-Mobile contends that "it is the *Commission's* burden to show that T-Mobile did *not* take steps to ensure that its contracts were being followed." NAL Response at 24-25. But our analysis does not turn on the theory that T-Mobile did not take any steps to ensure that its contracts were being followed. Setting aside broader questions regarding burden shifting that we address in the following section, *see infra* section III.C, the regulatory history, bolstered by the facts and our analysis of the contractual protections (continued….)

48. To enforce these safeguards, T-Mobile would have needed to take steps to determine whether they were actually being followed. Further, T-Mobile would have had to have a way of distinguishing between a legitimate request for customer location information (i.e., made pursuant to valid consumer consent) and an illegitimate one (e.g., the Securus/Hutcheson requests absent valid customer consent). Although the Commission requested that T-Mobile describe its efforts to verify that LBS providers obtained valid customer consent for related location requests,[169] nothing that T-Mobile has provided shows that it made any meaningful efforts or that it could effectively distinguish between valid and unauthorized requests for location information. To the extent that T-Mobile seeks to rely on certain risk assessments conducted in 2016 and 2018, as the *NAL* explained, T-Mobile "withheld the results of those assessments as privileged," and even while conceding "that both reports made recommendations to 'enhance program governance,'" it only provided "vague assertions" about the underlying concerns and any changes it made, rendering it "impossible for us to conclude that T-Mobile took meaningful steps to protect customer location information among the [75] entities to which it sold such access."[170] Further, the LocateUrCell, Securus, and MicroBilt breaches persuade us that the assessments either were not designed to detect vulnerabilities in the consent mechanism or failed meaningfully to do so. And while T-Mobile cites those risk assessments again in response to the *NAL*, it did not provide new information that would enable a different assessment on the record before us.[171]

49. T-Mobile also argues that it "took decisive action" after the *New York Times* article, and that the Company's actions were preferable to taking the steps suggested in the *NAL*, as those steps would have resulted in "[d]isrupting and even jeopardizing people's lives by immediately interfering with . . . valuable [LBS] services."[172] We disagree. The issue here is not whether there are any beneficial services offered by LBS providers, but whether T-Mobile reasonably protected its customers' location information. And even under T-Mobile'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 T-Mobile did not have a reliable way of confirming customer consent. The Commission considered T-Mobile's arguments, but finds they are outweighed by these risks.

50. And any further claim by T-Mobile that its contractual safeguards were effective are undermined by the inexorable fact that after the Securus disclosure, T-Mobile was unable to determine the universe of affected customers because it "claims that Securus has denied its request to identify the individuals whose customer location information may have been obtained without consent"[173] As the Commission said in the *NAL*, "[i]f T-Mobile cannot compel Securus's cooperation with its investigation

---

employed here, leads us to conclude that T-Mobile's attempt to rely on such measures fall short of what is required under section 64.2010(a), at least absent a strong showing regarding T-Mobile enforcement of those provisions that would overcome the contrary evidence. As explained below, the record does not include such a showing here.

[169] *See* Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to Luisa Lancetti, Director, Federal Regulatory, T-Mobile USA, Inc. at 3, Question 5.e (Sept. 13, 2018) (on file in EB-TCD-18-00027702).

[170] *NAL*, 35 FCC Rcd at 1806, para. 67; *see also id*. at 1808, para. 73 (discussing other grounds for discounting the risk assessments).

[171] *See* NAL Response at 26, 32. Without meaningful details about the risk assessments, the Commission cannot rationally conclude that they either helped render T-Mobile's safeguards reasonable or otherwise demonstrated that those safeguards were reasonable either before or after the May 2018 *New York Times* article, particularly in light of the multiple breaches discussed in the *NAL*. *See, e.g.*, *NAL*, 35 FCC Rcd at 1794-98, paras. 24-36. We thus reject T-Mobile's claim that our failure to give more weight to the risk assessments effectively imposes a higher standard than the reasonableness standard imposed under section 64.2010(a) of the Commission's rules. NAL Response at 26.

[172] NAL Response at 32-35.

[173] *NAL*, 35 FCC Rcd at 1808, para. 72.

into unauthorized access to its customers' location information, it cannot say that the same contract-based system actually protects such information from unauthorized access by other entities. Whatever Securus's justification for denying T-Mobile's request, its refusal to cooperate is further evidence of the fact that T-Mobile disclosed CPNI to a third party over which it had little or no control or authority."[174]

51. We also are unpersuaded by T-Mobile's efforts to tout perceived benefits of aspects of its location-based services safeguards. For example, T-Mobile notes that it restricted the number of entities with direct access to its customers' location information and criticizes what it sees as "[t]he NAL's casual dismissal of this important security measure."[175] T-Mobile also asserts benefits from "[g]iving location-based service providers the freedom to tailor notice to be most suited for their respective services."[176] But T-Mobile fails to appreciate that these approaches do not yield unqualified benefits, but carry with them various risks—risks that T-Mobile ineffectually sought to address largely "through provisions passed down through an attenuated chain of downstream contracts."[177] And as the *NAL* explained, T-Mobile's assignment of a campaign-specific ID for access to its Location APIs (a type of software) was "simply a technology-based variant of the honor system on which T-Mobile's other safeguards depended. As T-Mobile learned with the LocateUrCell incident in July 2017, where authorized and unauthorized services used the same campaign-specific ID, 'T-Mobile was not able to readily distinguish the unauthorized data requests from the authorized ones.'"[178]

52. Nor are we persuaded that information about location sharing on T-Mobile's website renders its safeguards reasonable.[179] None of the cited information would have made T-Mobile customers aware of the risk that their location information would be shared without their knowledge—let alone without their consent—as occurred in the Securus and Hutcheson breaches. Nor does it empower consumers to do anything to guard against such risk themselves (even assuming *arguendo* that could be a component of meeting the *carrier's* obligation to take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI under section 64.2010(a)).

53. Likewise, T-Mobile's safeguards after the Securus disclosure were also unreasonable. T-Mobile became keenly aware of the inadequacy of its safeguards after the May 2018 *New York Times* article, and again after Securus's resistance to T-Mobile's subsequent investigation. Nonetheless, T-Mobile 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, T-Mobile 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.[180]

54. We reject T-Mobile's attempt to dispute that the reports of the Securus and Hutcheson breaches should have made T-Mobile aware of the need for greater safeguards.[181] T-Mobile observes that media reports are not always completely accurate and are treated as inadmissible hearsay under the Federal Rules of Evidence and likewise have at times been rejected as reliable evidence by the

[174] *NAL*, 35 FCC Rcd at 1808, para. 72.

[175] NAL Response at 24.

[176] NAL Response at 25.

[177] *NAL*, 35 FCC Rcd at 1804-05, para. 61; *see also, e.g.*, *id*. at 1085-86, para. 64 ("This arrangement, in other words, depended on T-Mobile trusting that the Aggregators obtained the appropriate consent and the Aggregators, in turn, relying on the seemingly unverified assertions of the location-based service providers to whom they sold access to customer location data.").

[178] *NAL*, 35 FCC Rcd at 1806, para. 66. This flaw was again exploited after the Securus/Hutcheson breach by MicroBilt. *See, e.g.*, *NAL*, 35 FCC Rcd at 1807, para. 71.

[179] *See* NAL Response at 27.

[180] *See NAL*, 35 FCC Rcd at 1806, para.69.

[181] *See* NAL Response at 21-22, 35-36, 39-40.

Commission.[182] But whatever one might say about media reports in other contexts, T-Mobile did, in fact, view the May 2018 *New York Times* article as sufficiently reliable to call for some response, explaining that "T-Mobile took decisive action within 24 hours of the *New York Times* article to eliminate the ability of Securus to obtain location information for any purpose."[183] Nor are we persuaded that evidentiary standards governing admissibility in federal court or the statutory standard required for showings in Commission licensing proceedings should govern whether material provides a sufficient basis for a carrier to be on notice of vulnerabilities in its measures to discover and protect against unauthorized disclosures of CPNI.[184] Nothing in the *2007 CPNI Order* that adopted section 64.2010(a) of the Commission's rules suggests that the reasonableness standard was intended to be interpreted based on those other legal frameworks. Indeed, newspaper articles were among the sources of evidence relied upon by the Commission in that proceeding.[185] The case for T-Mobile's ability to ignore the May 2018 *New York Times* article despite its obligations under section 64.2010(a) to discover and protect against breaches is especially weak here, where the *New York Times* article was based in part on charges filed against Hutcheson in state and federal court.[186]

55. Although T-Mobile worked towards implementing an enhanced notice and consent mechanism, this mechanism was never deployed.[187] According to T-Mobile, the mechanism was never deployed because the Aggregators were unable to create the platform T-Mobile's approach would have relied upon, and T-Mobile "could not readily develop a process to obtain customer authorization directly from its customers."[188] But the mere fact that T-Mobile was working on new processes is not sufficient to satisfy its obligation to "take reasonable measures to discover and protect against attempts to gain

[182] *See* NAL Response at 21-22.

[183] NAL Response at 32. Likewise, T-Mobile found the media reliable enough to provide sufficient grounds to act in other situations, as well. *See, e.g.*, *NAL*, 35 FCC Rcd at 1797-98, paras. 33-34 (explaining that "[o]n January 3, 2019, T-Mobile learned from a *Motherboard* reporter that MicroBilt, a credit reporting and consumer finance company, may have been accessing and disclosing customer location information in a manner inconsistent with the approval that T-Mobile had given to access T-Mobile's customers' location information," and that the next day T-Mobile confirmed that Zumigo "had suspended transmission of any T-Mobile customer location information to MicroBilt," while T-Mobile also "permanently disabled access to its customers' location information by Zumigo for the purpose of transmitting it to MicroBilt").

[184] *See* NAL Response at 21-22 (citing cases applying the Federal Rules of Evidence and Commission licensing decisions).

[185] *See, e.g.*, *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6933-35, para. 12 & n.31 (2007) (*2007 CPNI Order*) (stating that "[t]he carriers' record on protecting CPNI demonstrates that the Commission must take additional steps to protect customers from carriers that have failed to adequately protect CPNI," and citing, among other things, Frank Main, *Anyone Can Buy Cell Phone Records: Online Services Raise Security Concerns for Law Enforcement*, Chi. Sun Times, Jan. 5, 2006, at A3; Frank Main, *Cell Call Lists Reveal Your Location: Anybody Can Pay to Track Where You Used Phone*, Chi. Sun Times, Jan. 19, 2006, at A3; and Frank Main, *Blogger Buys Presidential Candidate's Call List: "Nobody's Records Are Untouchable," as $90 Purchase Online Shows*, Chi. Sun-Times, January 13, 2006, at A10.); *id*. at 6933-35, para. 12 & n.37 (stating that "companies have sued dozens of people whom they accuse of fraudulently obtaining phone records," and citing, among other things, Matt Richtel and Miguel Helft, *An Industry Is Based on a Simple Masquerade*, N.Y. Times, Sept. 11, 2006, at C1).

[186] *See, e.g.*, Jennifer Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, N.Y. Times (May 10, 2018), https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html ("Thousands of jails and prisons across the United States use a company called Securus Technologies to provide and monitor calls to inmates. But the former sheriff of Mississippi County, Mo., used a lesser-known Securus service to track people's cellphones, including those of other officers, without court orders, according to charges filed against him in state and federal court. . . . ").

[187] *See* NAL Response at 32-33.

[188] *See* NAL Response at 33.

unauthorized access to CPNI."[189] 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 T-Mobile's work on new processes render the procedures that remained in place in the meantime "reasonable" under that rule, given their glaring weaknesses. Thus after considering all of the data security measures that T-Mobile implemented in response to the Securus disclosure[190] we conclude that these measures were inadequate.

56. T-Mobile further argues that the Commission fails to appropriately account for the fact that the LBS providers "were offering valuable services."[191] We disagree. The issue here is not whether there are any beneficial services offered by LBS providers, but whether T-Mobile reasonably protected its customers' location information. The decision to continue operating under its faulty safeguards after the Securus/Hutcheson breach came to light is all the more dubious given that it was preceded by the LocateUrCell incident, that apparently also "involved a location-based service provider customer of LocationSmart that had been authorized to access T-Mobile customer location information misusing that access to obtain the information for a different purpose, contrary to its approved use case, without customer consent, and without T-Mobile's knowledge or approval."[192] And there is no question of the risks that remained in T-Mobile's measures after the May 2018 *New York Times* article, given the subsequent MicroBilt breach, as discussed in the *NAL*.[193] As already noted in paragraph 49 and note 171, above, because of the sensitive personal information involved, the risks were grave, particularly because T-Mobile demonstrably did not have a reliable way of confirming customer consent.

57. The *NAL* listed numerous steps that could have been taken to squarely address the proven vulnerability, up to and including deploying enhanced measures to verify consumer consent (even directly verifying consumer consent) and shutting down the LBS program.[194] T-Mobile contends that the option identified in the *NAL* of learning the full scope of the breach is at odds with the suggestion that providers should have acted within 30 days, but T-Mobile offers no explanation of why that would be the case.[195] It

[189] 47 CFR § 64.2010(a).

[190] *See* NAL Response at 31-37.

[191] NAL Response at 35. T-Mobile further asserts that these other companies both "were offering valuable services and . . . were not implicated in any way by the Securus incident." NAL Response at 35. Notably, however, T-Mobile's measures were not what identified the unauthorized disclosures in the case of Securus and Hutcheson. Thus, in the face of what we see as the failing in a fundamental aspect of T-Mobile's safeguards, we reject the theory that the reasonableness of those measures can be inferred from the fact that even more unauthorized disclosures have not been publicly identified.

[192] *NAL*, 35 FCC Rcd at 1807, para. 70.

[193] *NAL*, 35 FCC Rcd at 1808-09, para. 74. T-Mobile argues that in the MicroBilt breach "the owner of the phone there actually *consented* to the activity at issue." NAL Response at 50. But that conflates the consent the customers provided to the author of the *Motherboard* article to test the protection of their location information with the opt-in consent T-Mobile was obligated to obtain (either directly or through its agents) before using, disclosing, or permitting access to that information—the latter of which was absent. *See NAL*, 35 FCC Rcd at 1797-98, paras. 33-36. The MicroBilt breach further highlights the flaw in T-Mobile's emphasis that it "completely terminated Securus's ability to access customer location information one day after the *New York Times* article was published, and it also terminated 3CInteractive's access in support of Securus." NAL Response at 18. Those actions did not improve the safeguards for consumers whose location information could be disclosed under the location data sharing arrangements that remained in place.

[194] *See NAL*, 35 FCC Rcd at 1807-10, paras. 70-78.

[195] *See* NAL Response at 35-36. T-Mobile argues that "[p]rior to this NAL, the Commission had never stated that a carrier would have just 30 days to fully investigate and implement its response to information about a misappropriation of location data." *Id*. at 39. As explained in note 121, above, the 30-day period cited in *NAL* was not a deadline but a grace period. The Commission could have, but chose not to, assess a fine during that 30-day interim. However, because T-Mobile's existing data security practices were unreasonable both before and after the (continued….)

also contends that the Commission has not adequately explained why the investigatory efforts that T-Mobile did undertake were inadequate.[196] But insofar as those efforts involve T-Mobile's review of a risk assessment that was commissioned and initiated before it became aware of the Securus breach,[197] the details of which it also has not disclosed,[198] we are not persuaded that they were likely to—or did—meaningfully illuminate the steps T-Mobile needed to take in response to the specific vulnerabilities laid bare by the Securus and Hutcheson breaches. Nor are we persuaded of the adequacy of discussions that T-Mobile states that it had with Securus, given evidence that T-Mobile was unable to get Securus to cooperate fully in its investigations.[199] We also are unpersuaded by T-Mobile's argument that it was not a potentially viable option for it to expeditiously implement enhanced measures to verify consent, such as a direct verification system.[200] The grounds for that claim are not demonstrated by the document it cites regarding its efforts to implement a direct consent verification system.[201] This is underscored by T-Mobile's decision to continue its LBS program and only eventually (and belatedly) expedited cutting off services, and even then it reserved "services such as roadside assistance and medical-alert services" until the end.[202] T-Mobile could have decided to cut off the other services from the start, which would appear to have made the task of taking on direct verification much more discrete and manageable. But ultimately, as the *NAL* observes, "the surest safeguard to protect its customers' CPNI would have been for T-Mobile to expeditiously terminate its location-based service program."[203]

58. Rather than taking definitive steps to remedy the obvious LBS program issues, T-Mobile instead took piecemeal steps. Moreover, the steps T-Mobile took did not rectify the systemic vulnerabilities at the heart of its LBS program—including relying on third parties to obtain customer consent for the disclosure of location information and failing to verify the validity of that consent.

59. T-Mobile's attempts to characterize the Commission as relying on a strict liability-type approach fall short, as well.[204] Section 64.2010 of the rules requires only reasonable measures—not perfect ones—but that is not enough to help T-Mobile here. Contrary to T-Mobile's suggestion, this is not a situation where the Commission is relying on 20/20 hindsight after a breach to find a violation of section 64.2010(a) of the rules based on any shortcoming in a carrier's measures, no matter how small, that results in a strict liability approach which is contrary to the reasonableness standard reflected in that rule.[205] Rather, we have carefully examined T-Mobile's procedures, including the fundamental flaws in

---

May 2018 article (the article having merely *exposed* those unreasonable practices), the Commission could have assessed a fine *for every single day* (both before and after the Securus/Hutcheson disclosures) such unreasonable practices were in place. Instead, the Commission used its discretion and gave T-Mobile a grace period to either end the program or reform its practices.

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

[197] *See NAL*, 35 FCC Rcd at 1794, para. 22.

[198] *See supra* para. 48. In connection with the *NAL*'s identified option of taking steps to determine whether the Securus incident was indicative of a broader vulnerability, T-Mobile also states that "it immediately began considering ways to limit the scope of the program and streamline the customer-consent process." NAL Response at 36. But those are measures that might have been better informed by an assessment of whether the Securus incident was indicative of a broader vulnerability—not steps that could have enabled an assessment of the nature of that vulnerability in the first instance.

[199] *NAL*, 35 FCC Rcd at 1808, para. 72.

[200] *See* NAL Response at 36-37.

[201] *See* NAL Response at 33 & n.97.

[202] NAL Response at 34.

[203] *NAL*, 35 FCC Rcd at 1809-10, para. 77.

[204] *See* NAL Response at 22, 32, 34.

[205] *See* NAL Response at 22-23.

those safeguards, such as the fact that across two Aggregators and three different LBS providers (LocateUrCell, Securus, and MicroBilt) T-Mobile was "unable to differentiate requests for customer location information that were made for purposes authorized by T-Mobile from those that were not."[206] Our assessment under section 64.2010(a) thus is a straightforward evaluation of reasonableness, consistent with the text of the rule.

60. We also reject T-Mobile's arguments regarding the validity of its use of an approach that relied in part on implicit consent. Section 222(c)(1) provides in pertinent part that, absent one of the exceptions specified in that provision, a carrier may not "use, disclose, or permit access to individually identifiable" CPNI "[e]xcept . . . with the approval of the customer."[207] Section 64.2007(b) of the Commission's rules specifies what customer approval is required to comply with section 222(c)(1).[208] In particular, where customer approval is required, it generally must take the form of "opt-in approval" unless the carrier is using individually identifiable CPNI "for the purpose of marketing communications-related services to that customer" or is "disclos[ing] its customer's individually identifiable CPNI, for the purpose of marketing communications-related services to that customer, to its agents and its affiliates that provide communications-related services."[209] Because the location information at issue here does not fall within the scenarios where opt-out customer approval is allowed, as explained in the *NAL* opt-in approval is required here under section 64.2007(b) of the Commission's rules.[210] And as the *NAL* also explained, "[p]ursuant to our rules, opt-in consent means that the customer has given 'affirmative, express consent' after being given appropriate notice of the carrier's request."[211] This does not allow for the use of implicit consent.

61. Commission precedent reinforces our understanding that implicit consent is not a valid option for obtaining opt-in consent. Where the Commission has referred to the notion of implicit or implied consent in connection with CPNI, it has done so in contexts that are very distinct from opt-in approval processes. In some cases, the Commission has referred to consent as implicit or implied where it is addressing the scope of provisions in section 222(c)(1) identifying situations where customer approval is *not* required. In that context, the Commission has stated, for example, that "the language of section 222(c)(1)(A) and (B) reflects Congress' judgment that customer approval for carriers to use, disclose, and permit access to CPNI can be *inferred* in the context of an existing customer-carrier relationship" insofar as those provisions are concerned.[212] Where the Commission referred to implicit or implied approval in connection with a customer approval process, it did so in connection with opt-out—

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

[207] 47 U.S.C. § 222(c)(1).

[208] 47 CFR § 64.2007(b).

[209] 47 CFR § 64.2007(b).

[210] *NAL*, 35 FCC Rcd at 1805, para. 63.

[211] *NAL*, 35 FCC Rcd at 1805, para. 63 (citing 47 CFR §§ 64.2003(k), 64.2008).

[212] *Implementation of the Telecommunications Act of 1996, et al.*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, 8080, para. 23 (1998) (*CPNI Second Report and Order*); *see also, e.g.*, *id*. at 8080, para. 24 ("insofar as the customer consent in sections 222(c)(1)(A) and (B) is inferred rather than based on express customer direction, we conclude that Congress intended that implied customer approval be restricted solely to what customers reasonably understand their telecommunications service to include"); *2007 CPNI Order*, 22 FCC Rcd at 6931-32, para. 8 n.16 ("As the Commission discussed in the *CPNI Order*, 'the language of section 222(c)(1)(A) and (B) reflects Congress' judgment that customer approval for carriers to use, disclose, and permit access to CPNI can be inferred in the context of an existing customer-carrier relationship. This is so because the customer is aware that its carrier has access to CPNI, and, through subscription to the carrier's service, has implicitly approved the carrier's use of CPNI within that existing relationship.'").

rather than opt-in—approval.[213] Thus, Commission precedent supports our view that implicit approval is not consistent with the Commission's requirement of opt-in approval under section 64.2007(b) of the rules.

62. Section 222(f) of the Act likewise supports this conclusion. As the Commission explained in the *NAL*, "[i]n the Wireless Communications and Public Safety Act of 1999, Congress amended section 222 to expressly allow carriers to provide call location information to 911 call centers, to expressly include location information in the definition of CPNI, and to require a user's express prior authorization before location information could be used for commercial purposes."[214] Among those amendments was the enactment of section 222(f)(1), which, as relevant here, specifies that "[f]or purposes of subsection (c)(1) [of section 222], without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to" call location information (as subset of CPNI location information).[215] Section 222(f)(1) requires that customer authorization be both "express" and "prior," and thus narrows the scope of customer authorization that can permissibly serve as a prerequisite for a carrier's use, disclosure, or permitting access to call location information under section 222(c)(1). As explained in the *NAL*, although the Commission did not initially adopt rules to implement the newly-enacted section 222(f), it "found that section 222(f)'s requirement of 'express prior authorization' left 'no doubt that a customer must explicitly articulate approval before a carrier can use that customer's location information.'"[216] Further, as the *NAL* observed, "[f]ive years later, the Commission found that the provisions of section 222, without implementing regulations, were inadequate to protect consumers—hence the adoption of new rules in the *2007 CPNI Order*. And nothing in that order suggests that the Commission intended to carve out location-based CPNI (let alone the 'call location information' discussed in section 222(f)) from those protections" based on the 2002 decision that rules had not been needed at that time.[217] In sum, whether under the Commission's rules or the

---

[213] *See, e.g.*, *Implementation of the Telecommunications Act of 1996, et al.*, Clarification Order and Second Further Notice of Proposed Rulemaking, 16 FCC Rcd 16506, 16511, para. 11 (2001) (referring to "'implicit approval' (through opt-out)"); *CPNI Second Report and Order*, 13 FCC Rcd at 8165, para. 142 ("because carriers generally were not subject to an express prior approval requirement for the use of CPNI under *Computer III*, but rather, were permitted to share CPNI based only on notice and opt-out, the approval that was implied under such an approach was based largely on a customer's notification of his or her CPNI rights").

[214] *NAL*, 35 FCC Rcd at 1787, para. 6 (footnote omitted).

[215] 47 U.S.C. § 222(f)(1).

[216] *NAL*, 35 FCC Rcd at 1787, para. 6 (quoting *Request by Cellular Telecommunications and Internet Association to Commence Rulemaking to Establish Fair Location Information Practices*, Order, 17 FCC Rcd 14832, 14834, para. 5 (2002) (*2002 Order Denying Petition for Rulemaking*)). In support of this interpretation, the Commission cited the provision's legislative history. *2002 Order Denying Petition for Rulemaking*, 17 FCC Rcd at 14834, para. 5 n.16. We note that this accords with common dictionary definitions of "express," as well. *See, e.g.*, *The American Heritage Dictionary*, Fourth Ed., at 303 (Bantam Dell Pub. 2001) (defining "express," among other things, to mean "Definitely and clearly stated. See Syns at **explicit.**"); *Collins English Dictionary*, Millennium Ed., at 544 (HarperCollins Pub. 1998) (defining "express," among other things, to mean "clearly indicated or shown; explicitly stated"); *Merriam-Webster's Deluxe Dictionary*, Tenth Collegiate Ed., at 645 (Merriam-Webster Pub. 1998) (defining "express," among other things, to mean "directly, firmly, and explicitly stated"); *The Oxford Paperback Dictionary & Thesaurus*, at 263 (Oxford Univ. Press 1997) (defining "express," among other things, to mean "definitely stated").

[217] *NAL*, 35 FCC Rcd at 1801, para. 48. T-Mobile states that call location information was not covered by the CPNI rules enacted in 2002. *See* NAL Response at 5 n.7, 40 n.118. However, the Notice of Proposed Rulemaking that led to the *2007 CPNI Order* observed when discussing the section 222(c)(1) requirement of customer consent that Congress subsequently enacted section 222(f) adopting a express prior consent requirement for call location information under section 222(c)(1). *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, et al*, Notice of Proposed Rulemaking, 21 FCC Rcd 1782, 1784, para. 4 n.8 (2006). The Commission included a similar statement in the *2007 CPNI Order*. *2007 CPNI Order*, 22 FCC Rcd at 6931, para. 6 n.11. Consequently, we conclude that the (continued….)

Commission's interpretation of section 222(f) itself, explicit consent is required for the use, disclosure, and provision of access to call location information under section 222(f).

63. We are unpersuaded by T-Mobile's efforts to justify its interpretation of its obligations under section 222 of the Act and the Commission's implementing rules by drawing from sources outside that legal framework. For example, T-Mobile cites 2012 recommendations from the FTC regarding privacy.[218] Not only is the FTC's legal regime governing privacy distinct from that applicable to CPNI,[219] but the 2012 recommendations did not even purport to describe the state of existing law. Instead, the 2012 recommendations were "intended to articulate best practices" that "can be useful to companies as they develop and maintain processes and systems to operationalize privacy and data security practices within their businesses," to "assist Congress as it considers privacy legislation," and "[t]o the extent the framework goes beyond existing legal requirements, the framework is not intended to serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC."[220] Whatever the possible pros and cons of those principles as a policy matter (at least in the marketplace as it existed in 2012), we do not find them instructive in interpreting the language of section 222 of the Act and the Commission's implementing rules.

64. We also reject T-Mobile's attempts to defend its reliance on implicit consent based on "the CTIA LBS Guidelines and industry practice."[221] Even beyond the fact that those are not binding on the Commission's interpretation of section 222 of the Act and the implementing rules, T-Mobile cites nothing in support of its claim regarding "industry practice" regarding the CTIA Guidelines themselves.[222] Furthermore, as already explained, those guidelines "focus on best practices for notice and consent by location-based service providers."[223] Where the carrier's CPNI is at issue, the carrier bears the

---

opt-in rules governing customer consent enacted in the *2007 CPNI Order* are best understood as applying to the full range of scenarios where section 222(c)(1) applies, including to call location information covered by section 222(f)(1). Even assuming *arguendo* that customer authorization requirements for call location information are governed by section 222(f)(1) of the Act rather than the specific opt-in requirements specified in section 64.2007(b) of the rules, the functional result is the same for T-Mobile. The 2002 precedent was clear that "section 222(f)'s requirement of 'express prior authorization' left 'no doubt that a customer must explicitly articulate approval before a carrier can use that customer's location information." *2002 Order Denying Petition for Rulemaking*, 17 FCC Rcd at 14834, para. 5. And the Commission's precedent—describing "implicit" consent as allowed only in scenarios like section 222(c)(1)(A) and (B) where consent is not required at all, or in scenarios where the Commission has allowed opt-out consent—demonstrates that "explicitly articulat[ing] approval" only is incompatible with implicit consent. *See supra* para. 61. Finally, we reiterate that section 222(f)(1) only applies to a subset of CPNI location information—namely, call location information.

[218] *See* NAL Response at 29-30 (citing FTC, *Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers*, at 36-48 (Mar. 2012) (*FTC Privacy Recommendations*), available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protectingconsumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf).

[219] The aspirational statement of individual members of multi-member agencies regarding FCC-FTC coordination on privacy does not give rise to any binding legal obligation governing the Commission's interpretation of section 222 and the implementing rules in a manner that accords with policies under the FTC's privacy authority. *See* NAL Response at 30 n.92 (citing Press Release, FTC, *Joint Statement of FCC Chairman Ajit Pai and Acting FTC Chairman Maureen K. Ohlhausen on Protecting American's Online Privacy*, (rel. Mar. 1, 2017), available at https://www.fcc.gov/document/fcc-chairman-ftc-chairman-protecting-americans-online-privacy). In any event, we are not persuaded to assume that the decade-old *FTC Privacy Recommendations* document (or another decade-old privacy document issued by the White House and cited by T-Mobile) continues to reflect the FTC's—or any federal entity's—current views regarding privacy. *See* NAL Response at 30-31 & n.93.

[220] *FTC Privacy Recommendations* at iii.

[221] NAL Response at 28.

[222] NAL Response at 28.

[223] *NAL*, 35 FCC Rcd at 1806, para. 65 n.170.

responsibility of ensuring compliance with its obligations under section 222 of the Act and the Commission's implementing rules before that CPNI is used or disclosed or access to it is permitted. The CTIA Guidelines do not speak to that question, and thus even by their terms do not address the legal question at issue here.[224]

65. Further, T-Mobile cites three Commission decisions that T-Mobile alleges demonstrate that the Commission has allowed implicit consent as a way to satisfy the obligation of "prior express consent" under the Telephone Consumer Protection Act (TCPA).[225] However, in one of those decisions the Commission was focused on assessing the *scope* of prior express consent—as opposed to determining whether prior express consent had been provided in the first instance (which would be more analogous to the operative question here).[226] The remaining two decisions turn on the Commission's analysis in the *1992 TCPA Order*.[227] That analysis turned entirely on the Commission's assessment of the legislative history of the TCPA, thus further undercutting any grounds to rely on it by analogy in this distinct legal context.[228]

66. As discussed in the *NAL*, moreover, even under T-Mobile's theory that implicit consent can be permissible, there were many practical problems that plagued in any implementation of such an approach in its LBS program. Consistent with the *NAL*, we are unpersuaded that "a location-based

[224] In addition to the fact that the CTIA Guidelines do not expressly address how carriers satisfy their duties under section 222 and the implementing Commission rules, the Guidelines also do not implicitly do so through their statement that "'[c]onsent may be implicit, such as when users request a service that obviously relies on the location of their device.'" NAL Response at 29 (citing CTIA Guidelines at 5). Building on a concept suggested by T-Mobile's arguments here—that aggregators or LBS providers might better be viewed simply as recipients of CPNI, at least in some cases—that would mean that when CPNI flows to an aggregator or LBS provider, the carrier is "us[ing], disclos[ing], or permit[ting] access" to that CPNI within the meaning of section 222(c)(1). 47 U.S.C. § 222(c)(1). That would require the carrier to obtain customer consent—namely, opt-in consent under section 64.2007(b) of the Commission's rules—before providing those consumers' CPNI to aggregators or LBS providers. The carrier thus would have to have obtained opt-in consent from all customers whose CPNI the carrier would use, disclose, or permit access to in its location-based services initiative. In that scenario, and depending on the details, that opt-in consent could satisfy the carrier's obligations under section 222(c)(1) and section 64.2007(b) of the rules, such that the carrier need not ensure that the aggregator and LBS provider itself obtain customer consent on the carrier's behalf to ensure compliance with section 222. In that case, the LBS provider, consistent with the CTIA Guidelines, still might find it prudent, as a "best practice," to obtain customer consent—and might elect to do so through implicit consent under some circumstances (and subject to any other legal constraints that might apply to the LBS provider). We provide this as an illustrative example of how the CTIA Guidelines still could operate as useful guidance regarding best practices for LBS providers even where what it describes would not be sufficient to satisfy section 222(c)(1) of the Act and section 64.2007(b) of our rules. Because the *NAL* was not premised on that explanation of section 222(c)(1) and section 64.2007(b) of our rules, we make clear that our finding of liability is not predicated on that basis, and we instead describe it only for purposes of this illustrative example of the potential operation of the CTIA Guidelines.

[225] *See* NAL Response at 29-30 (citing *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Report and Order, 7 FCC Rcd 8752, 8769, para. 31 (1992) (*1992 TCPA Order*); *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991; Request of ACA International for Clarification and Declaratory Ruling*, Declaratory Ruling, 23 FCC Rcd 559, 564, para. 9 (2008) (*ACA Declaratory Ruling*); *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991; SoundBite Communications, Inc. Petition for Expedited Declaratory Ruling*, 27 FCC Rcd 15391, 15392, 15394, paras. 2, 7 (2012) (*SoundBite Declaratory Ruling*)).

[226] *See SoundBite Declaratory Ruling*, 27 FCC Rcd at 15394, para. 7 ("For confirmation texts of the type SoundBite describes, we conclude that a consumer's prior express consent to receive text messages from an entity can be reasonably construed to include consent to receive a final, one-time text message confirming that such consent is being revoked at the request of that consumer.").

[227] *See ACA Declaratory Ruling*, 23 FCC Rcd at 564, para. 9 (relying on the Commission's prior decision in the *1992 TCPA Order*, including the legislative history that the Commission had relied upon in that decision).

[228] *1992 TCPA Order*, 7 FCC Rcd at 8769, para. 31.

service provider could comply with T-Mobile's alleged requirement that each provider 'produce a clear visual depiction' of an implicit 'consent capture process.'"[229] As also explained in the *NAL*, the legal regime governing CPNI requires that consent occur only after notice is provided to the consumer.[230] Several of these concerns are echoed in the Commission's approach in the TCPA context. Namely, in concluding that "persons who knowingly release their phone numbers have in effect given their invitation or permission to be called at the number which they have given, absent instructions to the contrary," the Commission was careful to distinguish that scenario from one where "a caller's number is 'captured' by a Caller ID or an ANI device without notice to the residential telephone subscriber."[231] Whether or not one could characterize the Commission's approach in the TCPA context as relying on "implicit" or "implied" consent in some manner,[232] the context distinguishes it sharply from the regime governing disclosure of CPNI. In the *1992 TCPA Order*, the Commission approved calls in a scenario where the consumers provided their phone numbers with a chance to provide "instructions to the contrary" and where the consumer, by virtue of some explicit, volitional action, would have notice that they were opening themselves up to calls at the number they provided. We find those characteristics lacking in T-Mobile's approach here, particularly insofar as vulnerabilities like the Securus and Hutcheson breaches are concerned. Thus, even if we were to give some weight to the Commission's TCPA precedent in this context, it simply reinforces our assessment, consistent with the *NAL*, that T-Mobile's reliance on implicit consent in its LBS program was unreasonable even under T-Mobile's own views regarding the permissibility of implicit consent as a theoretical matter.

3. T-Mobile Bore the Burden of Production

67. 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 T-Mobile did not use reasonable safeguards throughout the period of the violation.[233] As such, while the *NAL* discussed T-Mobile's burden of production to demonstrate that its protection of customer CPNI was reasonable,[234] that burden-shifting is not necessary given the preponderance of the evidence. Nonetheless, even if unnecessary to prove T-Mobile's violations in this matter, the *NAL* properly shifted the burden of production to T-Mobile.

68. *First*, as the *NAL* explained[235] 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.[236] In the *NAL*, the Commission found that T-Mobile failed to demonstrate that its safeguards

[229] *NAL*, 35 FCC Rcd at 1805, para. 64.

[230] *NAL*, 35 FCC Rcd at 1805, para. 64.

[231] *1992 TCPA Order*, 7 FCC Rcd at 8769, para. 31.

[232] T-Mobile cites *Baisden v. Credit Adjustments, Inc*, 813 F.3d 338, 342 (6th Cir. 2016) as stating that the "FCC has "interpreted 'prior express consent' to include a form of 'implied consent'"). NAL Response at 29 & n.88. But the colloquial description of the Commission's *1992 TCPA Order* does not persuade us that the Commission has adopted any general approach to "implicit" or "implied" consent in the TCPA context, let alone that it should be applied in the CPNI context.

[233] *See NAL*, 35 FCC Rcd at 1804-10, paras. 58-78.

[234] *See NAL*, 35 FCC Rcd at 1788-89, 1804, paras. 9, 59-60.

[235] *See NAL*, 35 FCC Rcd at 1788-89, para. 9.

[236] *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").

were reasonable following the disclosure of Securus's unauthorized location-finding service in May 2018.[237]

69. T-Mobile acknowledges that the *NAL* based its approach on the *2007 CPNI Order*,[238] explaining that "where an unauthorized disclosure has occurred . . . the responsible carrier then shoulders the burden of proving the reasonableness of its measures to protect consumer data."[239] However, T-Mobile is incorrect when it asserts that the *2007 CPNI Order* cannot support the burden-shifting approach in cases outside of the pretexting context.[240] 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.[241] The rationale applies with equal force to the kind of disclosure at issue here, where a fundamental issue is whether T-Mobile 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.[242] Broadly, in relation to Securus's entire unauthorized location-finding service, Securus used the pretext that it was requesting location information from T-Mobile 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.[243] 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*.

70. *Second*, T-Mobile recognizes that an evidentiary presumption is valid if the circumstances (here, a breach of CPNI) giving rise to that presumption make it more likely than not that the presumed fact (here, that CPNI safeguards were unreasonable) exists.[244] The Commission finds that the unauthorized disclosure in this case gave rise to a rebuttable presumption that T-Mobile did not reasonably protect customer location information from unlawful access.[245] As already discussed, the entire Securus location-finding program was based upon unauthorized disclosures. Though the

---

[237] *See NAL*, 35 FCC Rcd at 1807-10, paras. 69-78.

[238] *See* NAL Response at 19 (citing *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007) (*2007 CPNI Order*)).

[239] *NAL*, 35 FCC Rcd at 1804, para. 59.

[240] NAL Response at 19.

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

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

[243] 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 at1796, para. 28; *see also supra* para. 15.

[244] See NAL Response at 20 n.52.

[245] *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).

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 T-Mobile's resultant disclosures of consumer location information were unauthorized. T-Mobile'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, T-Mobile argues that the Commission cannot use the Securus and Hutcheson breaches to support shifting the burden of production to T-Mobile to provide evidence of the reasonableness of their post-May 2018 security practices.[246] Specifically, T-Mobile asserts that because no provider can achieve perfection and the appropriate measures to employ can vary by carrier and circumstance, that undercuts the reasonableness of any burden shifting here.[247] We disagree.

71. In the *NAL*, we found that T-Mobile 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.[248] This is further bolstered by the Department of Justice's case against Hutcheson.[249] And though the Commission opted to admonish T-Mobile only for the unauthorized disclosures made to Hutcheson, it would have been appropriate to admonish T-Mobile for all the disclosures it made to Securus in relation to the unauthorized location-finding service.[250] In the *NAL*, we clearly explained that, pursuant to section 217 of the Act,[251] carriers cannot disclaim their obligations to protect customer CPNI by delegating those obligations to third parties.[252] We reiterate here that "T-Mobile is not absolved from liability simply because it was not directly responsible for operating the programs under which unauthorized disclosures occurred."[253] And as the *NAL* explained, "[t]o the extent that the third parties were *not* acting on behalf of the carrier, the carrier itself would have provided those third parties with access to its customers' CPNI without obtaining for themselves the approval required by section 222(c)(1)—thus violating federal law."[254] Further, section 222(c)(1) of the Act[255] makes the responsibility for avoiding unauthorized disclosures a carrier obligation and prohibits use and disclosure except in certain narrow circumstances, without any reasonableness criterion. T-Mobile should, therefore, be able to justify any unauthorized disclosure. Given that multiple breaches occurred here and that the "reasonable measures" obligation is a

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

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

[248] *See NAL*, 35 FCC Rcd at 1801-04, paras. 49-57. "The evidence reflects that Hutcheson used the Securus service to obtain the location information of T-Mobile customers. T-Mobile shared the information with LocationSmart, which the shared it with 3Cinteractive, which then shared it with Securus." *Id*. at 1801-02, para. 50.

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

[250] T-Mobile seeks to analogize the circumstances here to a court that "allows an attorney to access confidential information and the attorney subsequently leaks it." NAL Response at 20. But that analogy in inapt. Implicit in T-Mobile's hypothetical is the notion that the court made a legally sound decision in its original action allowing the attorney access to confidential information, and the attorney, having validly obtained access to that information, then misused it. Here, by contrast, we find that the disclosure of the relevant location information in the Securus/Hutcheson breach was not legally permissible in the first instance under section 222(c)(1) and section 64.2007(b) of the rules. And it is that threshold action for which we hold T-Mobile accountable—not some subsequent abuse or misuse of information by a party whose initial access to the information was entirely lawful.

[251] 47 U.S.C. § 217.

[252] *See NAL*, 35 FCC Rcd at 1790, para. 10. 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.

[253] *See NAL*, 35 FCC Rcd at 1802, para. 52.

[254] *NAL*, 35 FCC Rcd at 1803, para. 54 n.145.

[255] 47 U.S.C. § 222(c)(1).

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.

72. The unauthorized disclosure at issue gave rise to a rebuttable presumption that T-Mobile did not adequately protect customer information from unlawful access. The burden of production then shifted to T-Mobile to offer evidence that it had reasonable safeguards in place.[256]

73. Rather than taking reasonable steps to safeguard its customers' location information after the Securus/Hutcheson disclosures were reported,[257] T-Mobile 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 T-Mobile 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

74. After considering the evidence in the record, the relevant statutory factors, the Commission's *Forfeiture Policy Statement*, and the arguments advanced by T-Mobile in the NAL Response, we find that T-Mobile is liable for a total forfeiture of $80,080,000 for its violations of section 222 of the Act and section 64.2010 of the Commission's rules—a reduction of $11,550,000 from the $91,630,000 forfeiture proposed in the *NAL*.[258] As explained in the *NAL*, this figure resulted from applying a base forfeiture of $40,000 for the first day of each such violation and a $2,500 forfeiture for the second and each successive day the violations continued (excluding the 30-day grace period granted by the Commission).[259] The Commission found in the *NAL* that T-Mobile apparently engaged in 81 continuing violations—one for each ongoing relationship with a third-party LBS provider or aggregator that had access to T-Mobile customer location information more than 30 days after publication of the *New York Times* report—and that each violation continued until T-Mobile terminated the corresponding entity's access to customer location information.[260] Using this methodology, the Commission found T-Mobile apparently liable for a total base forfeiture of $52,360,000. Upon considering the nature of the violations and the risk of harm they posed to consumers, the Commission then applied a 75% upward adjustment to the base forfeiture amount, resulting in a total proposed forfeiture of $91,630,000.[261]

75. T-Mobile challenges these forfeiture calculations with five principal arguments. *First*, T-Mobile argues that the *NAL* describes at most a single continuing violation, not a separate violation for each of the 81 entities participating in T-Mobile's LBS program. As such, according to T-Mobile, the forfeiture exceeds the applicable statutory maximum.[262] *Second*, T-Mobile contends that the forfeiture is disproportionate to the alleged violation, inconsistent with other forfeitures imposed by the Commission,

---

[256] We note that in some instances—most notably with regard to various audits that implicated the LBS program and over which T-Mobile asserted privilege—T-Mobile claimed to have taken certain reasonable steps, but did not produce documentary evidence of those steps. *See NAL*, 35 FCC Rcd at 1806, para. 67.

[257] Many of the possible reasonable steps were enumerated in the *NAL*. *See NAL*, 35 FCC Rcd at 1807-10, paras. 69-78.

[258] 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.

[259] *NAL*, 35 FCC Rcd at 1811, para. 83.

[260] *NAL*, 35 FCC Rcd at 1812, para. 84.

[261] *NAL*, 35 FCC Rcd at 1813-1814, paras. 87-91.

[262] NAL Response at 44-46.

and so excessive as to be unconstitutional.[263] *Third*, T-Mobile argues that the proposed forfeiture is not in accordance with the Commission's own *Forfeiture Policy Statement*.[264] *Fourth*, T-Mobile challenges the Commission's application of a 75% upward adjustment to the base forfeiture, disputing both the factors cited in calculating the upward adjustment and arguing that the Commission impermissibly cited to the same factors used for determining the base forfeiture amount.[265] *Fifth* and finally, T-Mobile argues that even if the Commission could calculate the forfeiture based upon the number of LBS providers and how long they had access to customer location information, the proposed forfeiture relies upon incorrect facts and therefore is calculated incorrectly. Specifically, T-Mobile asserts that the NAL overcounted the number of LBS program participants by listing several duplicate entities. T-Mobile also states that it terminated certain LBS providers' access to customer location information prior to the two termination dates listed in the *NAL*.[266]

76. As we discuss below, to account for additional information provided by T-Mobile about the number of participants in its LBs program and when it terminated those participants' access to customer location information, we reduce the forfeiture proposed in the *NAL* by $11,550,000. However, we are not persuaded by any of T-Mobile's other arguments and decline to cancel or further reduce the forfeiture proposed in the *NAL*.

1. The Commission Reasonably Found that T-Mobile Engaged in 81 Continuing Violations

77. Section 503(b) of the Act authorizes the Commission to impose a forfeiture against T-Mobile 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."[267] The Commission found that, because T-Mobile permitted 81 separate entities to access its customers' location information in the apparent absence of reasonable safeguards, the Company engaged in 81 continuing violations of section 222 of the Act and section 64.2010 of the Commission's rules. T-Mobile challenges this methodology, arguing that "[n]one of the 81 entities included in this calculation was accused of misappropriating data" and that to the extent T-Mobile violated section 64.2010 by allowing them to continue operating, it "did not have any reason or occasion to make 81 separate decisions."[268] T-Mobile therefore asserts that there could have been at most one continuing violation (subject to the $2,048,915 penalty cap) and the *NAL*'s finding of 81 separate continuing violations (one for each LBS provider or Aggregator) constitutes an impermissible attempt to circumvent the statutory maximum.[269]

78. We reject this argument. Neither section 503(b) nor the forfeiture guidelines in section 1.80 of the Commission's rules speak to the application of the phrase "single act or failure to act," or otherwise to the calculation of the number of violations, in the CPNI or data security context.[270] 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

[263] NAL Response at 46-50.

[264] NAL Response at 50-51.

[265] NAL Response at 52-56.

[266] NAL Response at 57-58.

[267] *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).

[268] NAL Response at 45.

[269] NAL Response at 44-45.

[270] 47 U.S.C. § 503(b); 47 CFR § 1.80(b).

[proprietary information] that the Companies failed to protect constitutes a separate violation for which a forfeiture may be assessed."[271] 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 . . . ."[272]

79. The Commission in *TerraCom* elected to ground its forfeiture calculation in the number of unprotected documents (which it "conservatively estimate[ed]" as more than 300,000),[273] 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 T-Mobile and an LBS provider or aggregator represented a distinct failure to reasonably protect customer CPNI and therefore a separate violation of section 222 of the Act and section 64.2010 of the Commission's rules. Each such relationship relied upon a distinct and unique contractual chain (from T-Mobile 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 T-Mobile. Treating these separate channels for the disclosure of location information—each of which, although unique, suffered from the same fundamental vulnerabilities discussed in the *NAL* and above—as separate violations was thus rational and properly within the Commission's discretion.

80. The approach taken in the *NAL* was not only reasonable, it was—contrary to T-Mobile's claim that it exceeded the statutory maximum—eminently *conservative*. As described in the *NAL*, T-Mobile'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 T-Mobile 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).[274] Using that methodology—and taking into account the tens of millions of consumers whose highly sensitive location information was made vulnerable by T-Mobile—would have resulted in a significantly higher forfeiture than what was proposed in the *NAL*.

81. Furthermore, even under the framework applied in the *NAL*, the Commission could have calculated the proposed forfeiture based upon every single entity with access to T-Mobile 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 T-Mobile 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 T-Mobile customers' CPNI vulnerable to unlawful disclosure, and assessing a far lower fine per day for the continuing violations than it could have. This approach recognized the Commission's need to show that such violations are serious and ensured the proposed forfeiture amounts act as a powerful deterrent for future failures to reasonably protect CPNI.

82. We also reject any claim that T-Mobile's due process rights were violated because it lacked fair notice that its LBS practices would potentially make it liable for a penalty in excess of the

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

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

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

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

$2,048,915 statutory maximum for a single continuing violation. Consistent with our earlier discussion of T-Mobile's fair notice claims,[275] 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. T-Mobile 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.[276] 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.[277] As the D.C. Circuit has recognized, where a statute specifies maximum penalties, the statute itself provides fair notice of all penalties within that limit.[278]

2. The Forfeiture is not Excessive, Disproportionate, or Unconstitutional

83. T-Mobile contends that the proposed forfeiture "is grossly disproportionate to the conduct at issue and reflects a startling departure from prior forfeitures."[279] T-Mobile points to other significant forfeitures proposed or levied by the Commission—such as the $120 million and $82.1 forfeitures imposed in the *Abramovich* and *Roesel* spoofed illegal robocall cases—and notes that they generally involved fraud, efforts to mislead consumers, intent to harm consumers, and the reaping of financial benefits from unlawful conduct.[280] T-Mobile maintains that, by contrast, it did not engage in behavior "even *remotely approaching* the malfeasance present in these matters" and its conduct did not result in any comparable harm.[281]

84. T-Mobile may not have engaged in fraud or otherwise sought to mislead or harm consumers, but that does not mean that its actions in this case were not egregious or worthy of a significant monetary penalty. As stated in the NAL, "even after highly publicized incidents put the Company on notice that its safeguards for protecting customer location information were inadequate, T-Mobile apparently continued to sell access to its customers' location information for the better part of a year without putting in place reasonable safeguards—leaving its customers' data at unreasonable risk of unauthorized disclosure."[282] As further explained in the *NAL*, the potential exposure of their location information put those customers "at significant risk of harm—physical, economic, or psychological."[283]

85. The base forfeiture amounts selected in the NAL properly took these risks to T-Mobile's customers into account. Moreover, they reflected the Commission's careful consideration of the relevant statutory factors. Section 503 of the Act requires the Commission to ". . . take into account the nature, circumstances, extent, and gravity of the violation and, with respect to the violator, the degree of

---

[275] *See supra* B.

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

[277] 47 U.S.C. § 503.

[278] *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).

[279] NAL Response at 46.

[280] NAL Response at 46-47 (*citing Adrian Abramovich, Marketing Strategy Leaders, Inc., and Marketing Leaders, Inc.*, 33 FCC Rcd 4663, 4667-68 para. 14, 4668 para. 15, 4677 para. 38 (2018); *Best Insurance Contracts, Inc., and Philip Roesel, dba Wilmington Insurance Quotes*, 33 FCC Rcd 9204, 9211 para. 17, 9212 para. 22, 9214 para. 28 (2018)).

[281] NAL Response at 48.

[282] *NAL*, 35 FCC Rcd at 1786, para. 3.

[283] *NAL*, 35 FCC Rcd at 1811, para. 81.

culpability, any history of prior offenses, ability to pay, and such other matters as justice may require."[284] 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.

86. In selecting the base forfeitures that it did, the Commission explained that the chosen amounts "(1) . . . provide a meaningful distinction between the violations in this case and those of other cases involving less egregious facts; and (2) . . . provide consistency with other consumer protection cases involving serious harm to consumers."[285] The Commission also found that "this base forfeiture appropriately deters wrongful conduct and reflects the increased risk consumers face when their information is not secured in a timely manner."[286] Given the broad discretion afforded to the Commission under section 503, as well as the *NAL*'s examination of how the relevant statutory factors intersected with the facts of this case, we reject T-Mobile's claim that the forfeiture amount is excessive or disproportionate.

87. We also reject T-Mobile's argument that the proposed forfeiture is "so grossly excessive" as to violate basic principles of due process and the Eight Amendment's prohibition against excessive fines.[287] In evaluating a claim that a forfeiture is excessive under the Eighth Amendment, one especially probative factor is whether the fine is within the prescribed statutory maximum for the underlying offense.[288] Here, as discussed, the forfeiture falls well below the statutory limit.[289] Further, T-Mobile, as a telecommunications carrier, falls squarely within the class of entities section 222 of the Act and the Commission's implemented rules was designed to address.[290] And as discussed in this section,[291] the nature of the harm from T-Mobile's conduct was very serious notwithstanding T-Mobile's attempts to claim otherwise.[292] Thus, we find there is no merit to T-Mobile's challenge to the constitutionality of the forfeiture amount.

3. The Forfeiture Comports with the Commission's *Forfeiture Policy Statement*

88. T-Mobile also claims the proposed base forfeiture amount is "wildly inconsistent" with the Commission's own rules.[293] Specifically, T-Mobile cites to the Commission's *Forfeiture Policy*

[284] 47 U.S.C. § 503(b).

[285] *NAL*, 35 FCC Rcd at 1812, para. 83.

[286] *NAL*, 35 FCC Rcd at 1812, para. 83.

[287] NAL Response at 48.

[288] *See Newell Recycling Co. v. EPA*, 231 F.3d 204, 210 (5th Cir. 2000) (internal quotation marks omitted). Similarly, the D.C. Circuit readily upheld the Commission's imposition of the maximum statutory penalty (adjusted for inflation) against an unlicensed radio operator who challenged that penalty as excessive. *See Grid Radio v. FCC*, 278 F.3d 1314, 1322 (D.C. Cir. 2002) (noting that the statutory amount was "neither indefinite nor unlimited," and that it did not "seem excessive in view of the [petitioner's] continued and willful violation of the licensing requirement"). *See also Scott Malcolm*, Order on Reconsideration, 33 FCC Rcd 2410, 2413-14, para. 11 (2018) ("Because the forfeiture was within the statutory limits, there is a strong indication that it was not excessive.").

[289] *See supra* III.D.1.

[290] *See, e.g.*, *Scott Malcolm*, 33 FCC Rcd at 2413, para. 10 (noting that an additional consideration under Eighth Amendment analysis is "whether the person fined is within the class of persons for whom the authorizing statute was principally designed").

[291] *See generally* III.D.

[292] *See, e.g.*, *Scott Malcolm*, 33 FCC Rcd at 2413, para. 10 (noting that an additional consideration under Eighth Amendment analysis is "the nature of the harm caused by the sanctioned person's conduct").

[293] NAL Response at 50.

Statement[294] and section 1.80 of the Commission's Rules[295] (into which the terms of the *Forfeiture Policy Statement* were codified), which reserve the highest base penalty (the statutory maximum) for violations involving misrepresentation/lack of candor. According to T-Mobile, there is an unjustifiable discrepancy between that base forfeiture amount (approximately $200,000) and the base forfeitures proposed in the *NAL*, which T-Mobile calculates to be more than three times as much, or approximately $650,000.[296] T-Mobile contends that, because its alleged violations were much less egregious than ones involving misrepresentation/lack of candor, it should be subject to lower base forfeiture amounts.

89. We disagree with T-Mobile's reasoning and calculations. In drawing the distinction that it does, T-Mobile fails to compare apples to apples. Rather than the $204,892 statutory maximum for a single violation or each day of a continuing violation that is cited by T-Mobile, the relevant point of comparison is the $2,048,915 overall statutory maximum for any single act or failure to act involving a *continuing* violation. As explained in the *NAL*, the "violations in this case were continuing in nature, extending each day that the Company's location-based services operated in the apparent absence of reasonable measures to protect CPNI."[297] Thus, even total base forfeitures of approximately $650,000 (as T-Mobile calculates the number) are well under the approximately $2 million statutory maximum that is applicable to each continuing violation in this case and that would potentially have been proposed, as the base forfeitures, if the violations had involved misrepresentation/lack of candor.

4. The Upward Adjustment is Permissible and Warranted

90. T-Mobile argues that the Commission failed to properly justify the 75% upward adjustment to the forfeiture amount proposed in the *NAL*. T-Mobile contends that two of the factors cited by the Commission in connection with the upward adjustment—the 2017 LocateUrCell incident and T-Mobile's acceptance of implied consent for certain LBS services—do not involve wrongful or egregious conduct and thus cannot rationally serve as aggravating factors.[298] T-Mobile also claims that the third factor cited in the *NAL*—the duration of the violation and the risk of harm it posed to consumers—was already considered in setting the base forfeiture amount and therefore constitutes arbitrary double counting.[299]

91. We reject these arguments and maintain the 75% upward adjustment proposed in the *NAL*. With regard to the upward adjustment, section 503 of the Act requires the Commission to ". . . take into account the nature, circumstances, extent, and gravity of the violation and, with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other matters as justice may require."[300] 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 FCC'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.[301] These factors include, importantly, "egregious misconduct," "substantial harm," "repeated or continuous violation," and "ability to pay/relative disincentive," among others.[302]

---

[294] *Forfeiture Policy Statement*, 12 FCC Rcd 17087.

[295] 47 CFR § 1.80.

[296] NAL Response at 50-51. T-Mobile derives this figure by dividing the total base forfeiture of $52,360,000 by the number of alleged violations (81), for a per-violation amount of $646,419.75.

[297] *NAL*, 35 FCC Rcd at 1811, para. 83.

[298] NAL Response at 52-55.

[299] NAL Response at 55-56.

[300] 47 U.S.C. § 503(b).

[301] 47 CFR § 1.80(b)(10), Table 3.

[302] *Id.*

92. The Commission weighed these factors when making the determination that the base forfeiture in this case merited a substantial upward adjustment. T-Mobile's conduct was egregious; the *NAL* detailed how T-Mobile failed to respond reasonably to the 2017 LocateUrCell incident and how it showed reckless disregard for CPNI requirements by relying on "implicit consent" for the disclosure of location information.[303] Further, revelations in the press about Securus's 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.[304] Its failure to adequately protect CPNI for a protracted amount of time caused substantial harm by making it possible for "malicious persons to identify the exact locations of T-Mobile 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.[305] 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 T-Mobile's status as a major telecommunications provider to determine what penalty, when applied, would adequately provide T-Mobile 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. T-Mobile's arguments to the contrary do not defeat Congress's decision to grant the FCC the power to weigh the factors and make such adjustments "as justice may require."[306] Nor do T-Mobile's arguments persuade us that the 75% upward adjustment, which is in line with upward adjustments in other cases involving consumer harms,[307] was unwarranted.

5. The Commission Will Reduce the Forfeiture Amount by $11,550,000

93. T-Mobile asserts that even if the Commission's forfeiture methodology is permissible, the calculations in the *NAL* are based on incorrect facts. Specifically, for the 81 entities whose ongoing

---

[303] *NAL*, 35 FCC Rcd at 1813-14, paras. 87-88. For the reasons discussed earlier, we reject T-Mobile's claim that the Commission drew the wrong conclusions from the LocateUrCell incident and T-Mobile's use of "implied consent" for the disclosure of location information. *See supra* III.C.1-2.

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

[305] *NAL*, 35 FCC Rcd at 1814, para. 89.

[306] 47 U.S.C. § 503(b).

[307] *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).

access to customer location information factored into the forfeiture amount, the *NAL* cites two separate termination dates (one for MicroBilt and the other for the remaining 80 entities).[308] According to T-Mobile, many of the LBS program participants' access to customer location information actually was terminated before the listed date.[309] T-Mobile also claims that the number of LBS providers listed in the NAL (81) reflects duplicates of certain entities and the number of unique participants was in fact 73.[310]

94. In developing the *NAL*, the Commission relied upon the information furnished to it by T-Mobile, including a listing of LBS program participants and when their access to customer location information was terminated, and reasonably expected that information to be accurate and complete.[311] Nonetheless, in light of the additional details provided by T-Mobile in the NAL Response, we now exercise our discretion to reduce the forfeiture amount to reflect the correct number of continuing violations and the length of time those violations continued.

95. Based upon the information provided by T-Mobile, we reduce the base forfeiture by $6,600,000, from $52,360,000 to $45,760,000. This reduction reflects both the double-counting of eight entities in the original *NAL*, as well as the termination dates of certain LBS program participants' access to T-Mobile customer location information. We continue to apply a 75% upward adjustment, or $34,320,000, resulting in a new total forfeiture of $80,080,000 (a reduction of $11,550,000 from the $91,630,000 proposed in the *NAL*).

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

96. We reject T-Mobile's supplemental constitutional objections that: (1) the FCC combines investigatory, prosecutorial, and adjudicative roles in violation of constitutional due process and separation of powers requirements;[312] (2) the issuance of a forfeiture order by the Commission would violate Article III and the Seventh Amendment;[313] 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.[314] T-Mobile's arguments are premised on misunderstandings regarding the relevant statutory framework, the nature of the Commission's actions, and relevant precedent.

97. As a threshold matter, T-Mobile 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, T-Mobile is entitled to a trial *de novo* in federal district court before it can be required to pay the forfeiture.[315] T-Mobile's objection to the combination of investigatory, prosecutorial, and adjudicative roles in the FCC ignores that statutory entitlement to a trial *de novo* in federal district court to

[308] *NAL*, 35 FCC Rcd at 1812, para. 84.

[309] NAL Response at 58-59.

[310] NAL Response at 57.

[311] T-Mobile "acknowledges" that the Commission provided it with an opportunity to supplement the record to correct these errors, but discounts this offer as having been made "at the eleventh hour." NAL Response at 57 n.181.

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

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

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

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

ultimately adjudicate its obligation to pay a forfeiture.[316] Likewise, T-Mobile'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 T-Mobile's statutory right to a trial *de novo* before it can be required to pay the forfeiture.[317] 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.

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

99. *Combination of Functions.* With respect to T-Mobile's claimed due process violation,[318] T-Mobile 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 T-Mobile'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."[319] To overcome that presumption requires "a showing of conflict of interest or some other specific reason for disqualification."[320]

100. T-Mobile fails to demonstrate a concern specific to the Commission's forfeiture order here sufficient to overcome the presumption of honesty and integrity. Insofar as T-Mobile notes the

---

[316] *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.'").

[317] *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).

[318] T-Mobile/Sprint June 22, 2023 Supplemental NAL Response at 2-3. T-Mobile contends that the combination of functions in the FCC "violates due process and the separation of powers under the circumstances presented in this case," T-Mobile/Sprint June 22, 2023 Supplemental NAL Response at 2, but does not develop the separation of powers argument or explain why the combination of functions in the Commission violates existing separation of powers precedent. Consequently, we do not find that a basis to alter our approach in this forfeiture order, and instead focus on those arguments that T-Mobile does develop.

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

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

[320] *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'").

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.[321]

101. T-Mobile also expresses concern that "the Commission performed its own investigations of alleged violations of the Communications Act (based on newspaper articles), prosecuted them by issuing NALs, and plans to resolve any challenges to these NALs itself by imposing forfeitures directly."[322] But these broad-brush objections do not identify specific reasons that a reasonable adjudicator in the Commission's position would be biased in this proceeding—certainly not one sufficient to overcome the background presumption of honesty and integrity on the part of agency adjudicators. To the contrary, finding a due process violation based simply on those concerns would, in large part, turn that background presumption on its head by a requiring a presumption of bias whenever the Commission issued an NAL. Such an understanding would be at odds with the range of scenarios where courts have found no due process concerns with adjudication by individuals despite earlier involvement in a matter.[323]

102. Nor do the "[s]pecial facts and circumstances" that T-Mobile alleges are present persuade us that due process concerns are present here.[324] T-Mobile criticizes the magnitude of the proposed forfeiture and the methodology used to calculate them as reflecting a "break from precedent and policy," that "reflects animosity toward the parties and an unwillingness to neutrally consider the legal and factual arguments that [T-Mobile] raised."[325] 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.[326] 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

[321] *See* T-Mobile/Sprint June 22, 2023 Supplemental NAL Response at 2 (citing the pending constitutional challenge involving the FTC underlying *Axon Enterprise v. FTC*, 143 S. Ct. 890 (2023)).

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

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

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

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

[326] *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.").

imposition of criminal penalties—particularly the death penalty.[327] 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 T-Mobile provide evidence that is the case here.[328] We also do not find that the NAL-initiated enforcement process presents the risk of adjudicators acting on the basis of extra-record information or impressions of the respondent that the Court found of concern in the case of a criminal prosecutor then serving as a judge.[329] 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,"[330] and T-Mobile 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*.

103. Instead, the "[s]pecial facts and circumstances" raised by T-Mobile amount to little more than differences of opinion regarding legal interpretations or the gravity of the violations.[331] We are not persuaded that such differences of opinion—which can arise in virtually every Commission enforcement action—inherently provide any reason to question the Commission's neutrality as an adjudicator. The main thrust of T-Mobile's argument seems to be that "the penalties would be among the largest in the Commission's history and impose penalty amounts typically reserved for fraud or deliberate misconduct" in what T-Mobile characterizes as a "break from precedent and policy."[332] But T-Mobile provides no basis to expect that only fraud or deliberate misconduct can justify penalties of the magnitude at issue here, and we already have explained our rationale for both the methodology for calculating the forfeiture and its ultimate magnitude.[333] Both the Communications Act and Commission rules direct the agency, when deciding on a forfeiture amount, to "take into account the nature, circumstances, extent, and gravity of the violation and, with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other matters as justice may require," and that is precisely what the Commission did here.[334] It is not surprising that the private company that potentially will be subject to a forfeiture might assess the nature and gravity of its violations differently than the Commission, but those differing views are not grounds for finding a likelihood of bias on the part of the Commission. We thus reject T-Mobile's claims of a due process violation through our implementation of the section 503(b) NAL-based process here.

104. *Trial By Jury.* We also reject T-Mobile's contention that adjudication of the violations at issue here may not constitutionally be assigned to a federal agency.[335] The Seventh Amendment preserves "the right of trial by jury" in "Suits at common law, where the value in controversy shall exceed twenty

---

[327] *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).

[328] *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).

[329] *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").

[330] 47 U.S.C. § 503(b)(4).

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

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

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

[334] 47 U.S.C. § 503(b)(2)(E); 47 CFR § 1.80(b)(10).

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

dollars,"[336] but the Seventh Amendment applies only to suits litigated in Article III courts, not to administrative adjudications conducted by federal agencies.[337] In determining whether an adjudication involves an exercise of judicial power vested in the federal courts under Article III of the constitution, the Supreme Court has distinguished between "public rights" and "private rights."[338] Congress has broad authority to "assign adjudication of public rights to entities other than Article III courts."[339] 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,[340] "adjudicating violations of the customs and immigration laws and assessing penalties based thereon,"[341] adjudicating "whether an unfair labor practice had been committed and of ordering backpay where appropriate,"[342] and the grant or reconsideration of a grant of a patent.[343] That precedent confirms the constitutionality validity of FCC adjudication of violations of the Communications Act, even setting aside the reality that T-Mobile 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"[344] designed to protect consumer privacy even as the communications marketplace became more open to competition,[345] 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.[346]

105. Relying principally on the Supreme Court's decision in *Tull v. United States* and the Fifth Circuit's decision in *Jarkesy*, T-Mobile contends that the forfeiture at issue here should fall within the "private rights" framework—requiring adjudication in an Article III court, with the right to a trial by jury—because the violations allegedly are analogous to a common law action in debt.[347] In *Tull*, the government was pursuing a claim in federal district court seeking penalties and an injunction under the

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

[337] *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).

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

[339] *Id*.

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

[341] *Id*. at 451.

[342] *Id*. at 453.

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

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

[345] *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.").

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

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

Clean Water Act and the district court had denied the defendant's request for a jury trial.[348] 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."[349] 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.[350] 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."[351] We thus are unpersuaded by T-Mobile's reliance on *Tull* and *Jarkesy*.[352]

106. *Nondelegation*. Finally, contrary to T-Mobile's contention,[353] 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.[354] Contrary to T-Mobile's suggestion, this choice involves the exercise not of legislative power but of executive power. The choice of enforcement process reflected in section 503(b) does not require the Commission to establish general rules governing private conduct of the sort that might implicate potential concerns about unauthorized lawmaking, but instead involves the exercise of enforcement discretion that is a classic executive power.[355]

---

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

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

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

[351] *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.

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

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

[354] 47 U.S.C. § 503(b)(3), (4).

[355] *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 (continued….)

107. We also are unpersuaded by T-Mobile'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,[356] 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.[357] 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."[358] 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.[359] The circumstances here therefore are distinct from those in *Jarkesy* where "Congress offered *no guidance* whatsoever."[360]

IV. CONCLUSION

108. Based on the record before us and in light of the applicable statutory factors, we conclude that T-Mobile willfully and repeatedly violated section 222 of the Act[361] as well as section 64.2010 of the Commission's rules[362] by disclosing its customers' location information, without their consent, to a third party who was not authorized to receive it and for failing to take reasonable steps to protect its customers' location information. We decline to withdraw the Admonishment and, having already reduced the forfeiture by $11,550,000 to account for eight entities that were each counted twice in the original forfeiture calculation, decline to further reduce or to cancel the forfeiture amount of $80,080,000.

V. ORDERING CLAUSES

109. 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, T-Mobile USA, Inc., **IS LIABLE FOR A MONETARY FORFEITURE** in the amount of eighty million and eighty thousand ($80,080,000) for willfully and repeatedly violating section 222 of the Act and section 64.2010 of the Commission's rules.

---

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").

[356] 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 352.

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

[358] 47 U.S.C. § 154(j).

[359] *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).

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

[361] 47 U.S.C. § 222.

[362] 47 CFR § 64.2010.

110. 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.[363] T-Mobile USA, Inc., shall send electronic notification of payment to Shana Yates, Kimbarly Taylor, and Michael Epshteyn, Enforcement Bureau, Federal Communications Commission, at shana.yates@fcc.gov, kimbarly.taylor@fcc.gov, and michael.epshteyn@fcc.gov on the date said payment is made. If the forfeiture is not paid within the period specified, the case may be referred to the U.S. Department of Justice for enforcement of the forfeiture pursuant to section 504(a) of the Act.[364]

111. In order for T-Mobile USA, Inc. to pay the proposed forfeiture, T-Mobile USA, 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:[365]

- 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[366] or printed CORES form[367] 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).[368] For additional detail and wire transfer instructions, go to https://www.fcc.gov/licensing-databases/fees/wire-transfer.
- Payment by credit card must be made by using CORES at https://apps.fcc.gov/cores/userLogin.do. To pay by credit card, log-in using the FCC Username associated to the FRN captioned above. If payment must be split across FRNs, complete this process for each FRN. Next, select "Manage Existing FRNs | FRN Financial | Bills & Fees" from the CORES Menu, then select FRN Financial and the view/make payments option next to the FRN. Select the "Open Bills" tab and find the bill number associated with the NAL Acct. No. The bill number is the NAL Acct. No. with the first two digits excluded (e.g., NAL 1912345678 would be associated with FCC Bill Number 12345678). After selecting the bill for payment, choose the "Pay by Credit Card" option. Please note that there is a $24,999.99 limit on credit card transactions.
- Payment by ACH must be made by using CORES at https://apps.fcc.gov/cores/userLogin.do. To pay by ACH, log in using the FCC Username associated to the FRN captioned above. If payment must be split across FRNs, complete this process for each FRN. Next, select "Manage Existing FRNs | FRN Financial | Bills & Fees" on the CORES Menu, then select FRN Financial and the view/make payments option next to the FRN. Select the "Open Bills" tab and find the bill number

[363] *Id.*

[364] 47 U.S.C. § 504(a).

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

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

[367] 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.

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

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.

112. 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.

113. **IT IS FURTHER ORDERED** that a copy of this Forfeiture Order shall be sent by first class mail and certified mail, return receipt requested, to Edward H. Smith, Senior Vice President of Public Policy and Government Affairs, and Christopher Koegel, Director, Federal Regulatory Affairs, T-Mobile USA, Inc., c/o J. Wade Lindsay, Esq., Wilkinson Barker Knauer, LLP, 1800 M Street, N.W., Suite 800N, Washington, DC 20036, and Helgi C. Walker, Esq., and Russell B. Balikian, Esq., Gibson, Dunn & Crutcher LLP, 1050 Connecticut Ave., N.W., Washington, DC 20036.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

STATEMENT OF
CHAIRWOMAN JESSICA ROSENWORCEL

Re: *In the Matter of T-Mobile USA, Inc.*, Forfeiture Order, File No.: EB-TCD-18-00027702 (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 T-Mobile USA, Inc.*, Forfeiture Order, File No.: EB-TCD-18-00027702 (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 T-Mobile USA, Inc.*, Forfeiture Order, File No.: EB-TCD-18-00027702 (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.