Before the
Federal Communications Commission
Washington, DC 20554

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

NOTICE OF APPARENT LIABILITY FOR FORFEITURE AND ADMONISHMENT

Adopted: February 28, 2020 **Released: February 28, 2020**

By the Commission: Chairman Pai and Commissioner O'Rielly issuing separate statements; Commissioner Rosenworcel dissenting and issuing a statement; Commissioner Starks approving in part, dissenting in part and issuing a statement.

TABLE OF CONTENTS

Heading Paragraph #

I. INTRODUCTION 1
II. BACKGROUND 4
A. Legal Framework 4
B. Factual Background 12
1. T-Mobile's Wireless Network Services and Customer Location Information 12
2. T-Mobile's Location-Based Services Business Model 13
3. T-Mobile's Discovery of LocateUrCell's Unauthorized Use of T-Mobile Customers' Location Information 24
4. T-Mobile's Actions After the Publication of Reports of Unauthorized Access to and Use of Customer Location Information 27
III. DISCUSSION 39
A. Customer Location Information Constitutes CPNI 41
B. T-Mobile Apparently Violated Section 222 and the CPNI Rules by Disclosing CPNI to a Missouri Sheriff Without Authorization 49
C. T-Mobile Apparently Failed to Take Reasonable Measures to Protect CPNI 58
D. Proposed Forfeiture 79
IV. REQUESTS FOR CONFIDENTIALITY 92
V. ORDERING CLAUSES 95

I. INTRODUCTION

1. The wireless phone is a universal fixture of modern American life. Ninety-six percent of all adults in the United States own a mobile phone.[1] Of those mobile phones, the majority are smartphones that provide Internet access and apps, which Americans use to read, work, shop, and play.

[1] Pew Research Center, Demographics of Mobile Device Ownership and Adoption in the United States – Mobile Fact Sheet (June 12, 2019), https://www.pewresearch.org/internet/fact-sheet/mobile/.

More than almost any other product, consumers "often treat [their phones] like body appendages."[2] The wireless phone goes wherever its owner goes, at all times of the day or night. For most consumers, the phone is always on and always within reach.[3] And every phone must constantly share its (and its owner's) location with its wireless carrier because wherever it goes, the networks must be able to find it to know where to route calls.

2. The American public and federal law consider such information highly personal and sensitive—and justifiably so. As the Supreme Court has observed, location data associated with wireless service "provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations."[4] Section 222 of the Communications Act requires carriers to protect the confidentiality of certain customer data related to the provision of telecommunications service, including location information. The Commission has advised carriers that this duty requires them to take "every reasonable precaution" to safeguard their customers' information.[5] The Commission has also warned carriers that the FCC would "[take] resolute enforcement action to ensure that the goals of section 222 are achieved."[6]

3. Today, we do exactly that. In this Notice of Apparent Liability, we propose a penalty of $91,630,000 against T-Mobile USA, Inc. (T-Mobile or Company) for apparently violating section 222 of the Communications Act and the Commission's regulations governing the privacy of customer information. We find that T-Mobile apparently disclosed its customers' location information, without their consent, to third parties who were not authorized to receive it. In addition, 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.

II. BACKGROUND

A. Legal Framework

4. The Act and the Commission's rules govern and limit telecommunications carriers' use and disclosure of certain customer information. Section 222(a) of the Act imposes a general duty on telecommunications carriers to "protect the confidentiality of proprietary information" of "customers."[7] 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."[8] The Commission has issued regulations implementing the privacy

---

[2] Pew Research Center, Americans' Views on Mobile Etiquette, Chapter 1: Always on Connectivity (Aug. 26, 2015), https://www.pewresearch.org/internet/2015/08/26/chapter-1-always-on-connectivity/.

[3] *Id.*

[4] *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (internal quotation marks and citations omitted).

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

[6] *2007 CPNI Order*, 22 FCC Rcd at 6959-60, para. 65.

[7] 47 U.S.C. § 222(a).

[8] *Id.* § 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-

requirements of section 222 (CPNI Rules),[9] and has amended those rules over time. Most relevant to this proceeding are the rules that the Commission adopted governing customer consent to the use, sharing, or disclosure of CPNI and those relating to carriers' duty to discover and protect against unauthorized access to CPNI.

5. *Customer Consent to Disclose CPNI.* With limited exceptions, a carrier may only use, disclose, or permit access to CPNI with customer approval.[10] Generally, carriers must obtain the "opt-in approval" of their customers before disclosing CPNI.[11] This means that a carrier must obtain the customer's "affirmative, express consent allowing the requested CPNI usage, disclosure, or access after the customer is provided appropriate notification of the carrier's request . . . ."[12]

6. In the Wireless Communications and Public Safety Act of 1999,[13] 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.[14] In July 2002, the Commission declined, in response to a petition for rulemaking submitted by CTIA, to adopt rules to implement these amendments to section 222 "[b]ecause the statute imposes clear legal obligations and protections for consumers and because we do not wish to artificially constrain the still-developing market for location-based services."[15] The Commission 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."[16]

7. Prior to 2007, the Commission's rules permitted telecommunications carriers to share customers' CPNI with joint venture partners and independent contractors for certain purposes based on a customer's "opt-out approval." This means that a customer is deemed to have consented to a particular use of, disclosure of, or access to CPNI after being given notice of the use, disclosure, or access and not objecting thereto.[17] However, in response to the problem of data brokers on the web selling call detail and other telephone records procured without customer consent,[18] the Commission amended its rules in the *2007 CPNI Order* to require carriers to obtain opt-in approval from a customer before disclosing that

---

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.").

[9] *See* 47 CFR § 64.2001 *et seq*.

[10] 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).

[11] 47 CFR § 64.2007(b).

[12] *Id.* § 64.2003(k).

[13] Pub. L. No. 106-81, 113 Stat. 1286.

[14] *See* H.R. Rep. No. 106-25, 106th Cong., 1st Sess. 7 (1999); *see also* S. Rep. No. 106-138, 106th Cong., 1st Sess. (1999).

[15] *Request by Cellular Telecommunications and Internet Association to Commence Rulemaking to Establish Fair Location Information Practices*, WT Docket No. 01-72, Order, 17 FCC Rcd 14832, 14832, para. 1 (2002) (*2002 Order Denying Petition for Rulemaking*).

[16] *Id.* at 14834, para. 5 (citing H.R. Rep. No. 106-25 at 15).

[17] *See* 47 CFR § 64.2003(l).

[18] *See 2007 CPNI Order*, 22 FCC Rcd at 6928, para. 2.

customer's CPNI to a carrier's joint venture partner or independent contractor.[19] The Commission recognized that "once the CPNI is shared with a joint venture partner or independent contractor, the carrier no longer has control over it and thus the potential for loss of this data is heightened."[20] Given that observation, the Commission concluded that sharing of data with partners and contractors "warrants a requirement of express prior customer authorization,"[21] which would allow individual consumers to determine if they want to bear the increased risk associated with sharing CPNI with independent contractors and joint venture partners.[22] The Commission emphasized the importance of obtaining express consent particularly because a carrier cannot simply rectify the harms resulting from a breach by terminating its agreement, "nor can the Commission completely alleviate a customer's concerns about the privacy invasion through an enforcement proceeding."[23] The Commission further concluded that contractual safeguards cannot obviate the need for explicit customer consent, as such safeguards would not change the fact that the risk of unauthorized CPNI disclosures increases when such information is provided by a carrier to a joint venture partner or independent contractor.[24] Thus, with limited exceptions, a carrier may only use, disclose, or permit access to CPNI with the customer's opt-in approval.[25]

8. *Reasonable Measures to Safeguard CPNI.* The Commission also recognized in the *2007 CPNI Order* that reliance on the opt-in approval requirement alone is insufficient to protect customers' interest in the privacy of their CPNI, finding that at least some data brokers had obtained access to call detail information because of the ease with which a person could pretend to be a particular customer or other authorized person in order to obtain access to that customer's call detail or other private communications records, a practice known as "pretexting."[26] In light of the harms arising from pretexting, the Commission adopted rules requiring carriers to "take reasonable measures to *discover* and *protect* against attempts to gain unauthorized access to CPNI."[27] To provide some direction on how carriers should protect against pretexting schemes, 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.[28] It also adopted password and account notification requirements.[29]

9. 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."[30] Where there is evidence of an unauthorized disclosure, the Commission specified that it will infer from that evidence that a carrier's practices were unreasonable unless the carrier offers evidence demonstrating that its practices were

[19] *Id.* at 6947-53, paras. 37-49.

[20] *Id.* at 6948, para. 39.

[21] *Id.* at 6948, para. 39; *see also id.* at 6949, para. 41 ("Further, we find that an opt-in regime will clarify carriers' information sharing practices because it will force carriers to provide clear and comprehensible notices to their customers in order to gain their express authorization to engage in such activity.").

[22] *Id.* at 6950, para. 45.

[23] *Id.* at 6949, para. 42.

[24] *Id.* at 6952, para. 49.

[25] *See* 47 CFR § 64.2007(b).

[26] *2007 CPNI Order*, 22 FCC Rcd at 6928, para. 1 & n.1.

[27] 47 CFR § 64.2010(a) (emphasis added).

[28] *See id.* § 64.2010(b)-(d).

[29] *See id.* § 64.2010(e)-(f).

[30] *2007 CPNI Order*, 22 FCC Rcd at 6959–60, para. 65.

reasonable.[31] This burden-shifting approach reflects the Commission's expectation that carriers "take every reasonable precaution to protect the confidentiality of proprietary or personal customer information,"[32] while also heeding industry warnings that adopting prescriptive rules detailing specific security practices could be counterproductive.[33] The Commission chose to "allow carriers to determine what specific measures will best enable them to ensure compliance with" the requirement that they remain vigilant in their protection of CPNI.[34] The Commission expected that carriers would employ effective protections that are best suited to their particular systems.[35] Carriers are not expected to eliminate every vulnerability to the security of CPNI, but they must employ "reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI."[36] They must also take reasonable measures to protect the confidentiality of CPNI—a permanent and ongoing obligation to police disclosures and ensure proper functioning of security measures.[37] A variety of government entities provide guidance and publish best practices that are intended to help companies evaluate the strength of their information security measures.[38]

---

[31] *See id*. 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"). This approach, which the Commission articulated in the context of pretexting, is particularly applicable here, where a fundamental issue is whether the Company had reasonable measures to ensure that its customers had in fact consented to the disclosure of their CPNI with third parties. Since at least 2007, it has been foreseeable that entities seeking to gain unauthorized access to CPNI would use false pretenses—of one sort or another—to do so.

[32] *Id.* at 6959, para. 64 (citing 47 CFR § 64.2010(a)).

[33] *See id.* at 6945-46, paras. 33-36 (citing, *inter alia*, CTIA Comments (May 1, 2006) at 6 (arguing that "prescriptive rules detailing specific security practices that must be followed by all carriers do nothing more than provide a road map to criminals and erect a barrier that prevents carriers from adopting new security measures in response to constantly evolving threats")).

[34] *Id.* at 6945-46, para. 34.

[35] *Id.* at 6959, para. 64. The Commission explained, for example, that although it declined to impose "audit trail" obligations on carriers at that time, it "expect[ed] carriers through audits or other measures to take reasonable measures to discover and protect against" activity indicative of unauthorized access. *Id.* Similarly, the Commission expected that a carrier would "encrypt its CPNI databases if doing so would provide significant additional protection . . . at a cost that is reasonable given the technology a carrier already has implemented," but the Commission did not specifically impose encryption requirements. *Id*.

[36] 47 CFR § 64.2010(a).

[37] *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.").

[38] 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) and the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC) 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://www nist.gov/privacy-framework/privacy-framework; 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

10. *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."[39]

11. *The Scope of the Commission's Authority*. Our authority to bring action for violations of section 222 of the Communications Act and the CPNI Rules is limited to actions against providers of telecommunications services[40] and providers of interconnected Voice over Internet Protocol services.[41] To the extent that other entities act unfairly or deceptively by mishandling or failing to protect wireless customer location information, federal civil enforcement authority rests with the Federal Trade Commission, an agency of general jurisdiction.[42]

B. Factual Background

1. T-Mobile's Wireless Network Services and Customer Location Information

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.[43] The mobile phones of T-Mobile subscribers, like those of customers of other carriers, periodically register with nearby network signal towers.[44] T-Mobile uses the information generated from this registration activity to ensure the proper functioning of its network and to provide the services to which its customers subscribe.[45] Because T-Mobile knows the location of its network signal towers, T-Mobile is able to calculate the approximate geographic location of the mobile phones communicating with its towers.[46] This type of location information—which is created even when the customer does not have an active established connection, such as a voice call or data usage—may at times be helpful to consumers. For example, in emergencies, the location of a customer's mobile phone can enable first responders and law enforcement to assist. Location information is also used for non-emergency location-based services, such as roadside assistance, delivery tracking, and fraud prevention.[47] Other widely used

---

Security, Reliability, and Interoperability Council, CSRIC Best Practices, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data.

[39] 47 U.S.C. § 217.

[40] *Id.* § 222.

[41] *2007 CPNI Order*, 22 FCC Rcd at 6954-57, paras 54-59.

[42] 15 U.S.C. § 45(a)(2) ("The [Federal Trade] Commission is hereby empowered and directed to prevent persons . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.").

[43] *See* T-Mobile, Inc., 2018 Annual Report, https://s22.q4cdn.com/194431217/files/doc_financials/2018/TMUS-2018-Annual-Report.pdf.

[44] *See* FCC, Wireless Telecommunications Bureau, Location-Based Services: An Overview of Opportunities and Other Considerations at 11-12 (May 2012), https://docs.fcc.gov/public/attachments/DOC-314283A1.pdf (discussing how location information is derived from communications between mobile phones and cellular base stations) (*2012 LBS Report*).

[45] *See* Response to Supplemental Letter of Inquiry, from T-Mobile USA, Inc., to Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, at 2, Introduction (June 7, 2019) (on file in EB-TCD-18-00027702) (Supplemental LOI Response).

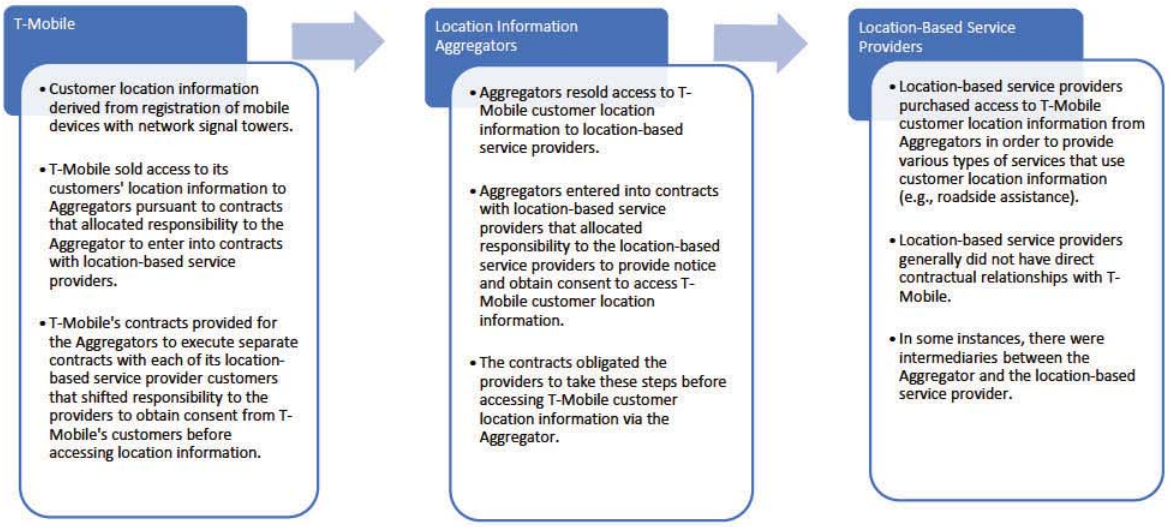
[46] *2012 LBS Report* at 11-12.

[47] *See* Response to Letter of Inquiry, from T-Mobile USA, Inc., to Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, at 2, Introduction (Nov. 30, 2018) (on file in EB-TCD-18-00027702) (LOI Response).

forms of location-based services include real-time mapping, navigation, and local weather forecasting services, although these generally rely on GPS-based location finding rather than customer location information derived from the provision of wireless service.[48]

2. T-Mobile's Location-Based Services Business Model

13. Until February 8, 2019, T-Mobile provided location-based service providers access to its customers' location information through a chain of contract-based business arrangements.[49] T-Mobile sold access to customer 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. T-Mobile had arrangements with two aggregators: LocationSmart and Zumigo (the Aggregators).[50] Each Aggregator, in turn, had arrangements with numerous location-based service providers. The most basic form of these relationships is illustrated in Fig. 1:



[48] Location information derived from the interaction between a subscriber's mobile phone and a carrier's network is distinct from the location information generated by capabilities on a subscriber's phone, which calculates a phone's location by measuring its distance to Global Positioning System (GPS) satellites and through other capabilities. Many popular apps use device-based location functionality to provide consumers with location-based service (including mapping and navigation services) and do not rely on the location information collected by carriers. There are a variety of location positioning methods and protocols in wireless networks that are based on mobile radio signals, and some of these radio signals are configurable and/or controlled by the network operator and not the consumer. *See* Rohde & Schwarz, LTE Location Based Services Technology Introduction – White Paper, at 11, Fig. 7 – Supported positioning methods in LTE (Sept. 2013), https://cdn rohde-schwarz.com/pws/dl_downloads/dl_common_library/dl_brochures_and_datasheets/pdf_1/LTE_LBS_White_Paper.pdf.

[49] Supplemental LOI Response at 17, Response to Question 9.

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

14. T-Mobile apparently sold access to its customers' location information, directly or indirectly, to the following 83 third parties, including the two Aggregators: [redacted] 3Cinteractive, [redacted] LocationSmart, [redacted] MicroBilt, [redacted] ecurus, [redacted] and Zumigo, Inc.[51]

15. T-Mobile asserts that it structured its location-based services program "such that only two entities," the Aggregators, had "direct access to the [T-Mobile Service Delivery Gateway] and thus to T-Mobile customer location data," subject to certain "contractual, procedural, and technical safeguards."[52] According to T-Mobile, the Service Delivery Gateway is a platform that provides access to internal T-Mobile application programming interfaces, including "Location APIs" which the Aggregators used to request T-Mobile customer location information.[53] T-Mobile explains that the Aggregators, in turn, contracted with location-based service providers.[54] T-Mobile did not have contracts with the location-based service providers to which it permitted the Aggregators to disclose its customers' location information.

16. *T-Mobile's Contracts with the Aggregators.* According to T-Mobile, it enforced its policies and practices relating to the disclosure of customer location information through its contractual agreement with the Aggregators.[55] As described by T-Mobile, its contracts with the Aggregators required the Aggregators to:

> (a) secure express prior consent from T-Mobile customers before the disclosure of, use of, or access to, customers' location data, authorizing use of T-Mobile customer location data only upon affirmative consent of the end user; (b) maintain, and provide for T-Mobile review, records demonstrating such consent; (c) comply with the CTIA [Best Practices and Guidelines for Location Based Services];[56] and (d) secure T-Mobile's prior approval before permitting [location-based service providers] to disclose, use, or access customer location information in connection with providing [a location-based service]. The agreements also mandate[d] that [the Aggregators]

[51] LOI Response at 12, Response to Question 3, Exh. 1.

[52] *Id.* at 7-8, Introduction.

[53] *Id.* at 7, 14, Response to Question 5.d.

[54] *Id.* at 7, Introduction.

[55] *Id.* at 10, Introduction.

[56] CTIA, Best Practices and Guidelines for Location Based Services, https://www.ctia.org/the-wireless-industry/industry-commitments/best-practices-and-guidelines-for-location-based-services (CTIA Guidelines) (last visited Feb. 5, 2020).

> contractually bind each [location-based service provider] they do business with to agree and comply with these same obligations.[57]

According to T-Mobile, its contracts with the Aggregators also specified that the Aggregators would monitor the practices of the location-based service providers, including compliance with the requirement that location-based service providers notify and collect affirmative customer consent for any use of location information.[58]

17. As T-Mobile describes the process, before an Aggregator gave a location-based service provider access to T-Mobile customer 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"; a detailed description of the location-based service provider's notice and consent process; and information about the location-based service provider's data security mechanisms and data retention policies.[59] According to T-Mobile, it reviewed the information provided in the questionnaires and only approved the use of customer location information for specific purposes and only when the location-based service provider committed to obtaining the affirmative, opt-in consent of the individual whose device was to be located.[60] Although T-Mobile did not dictate the manner of obtaining consent, the consent mechanisms that it approved generally fell into one of five categories: (1) text messages requesting the customer respond and confirm consent; (2) interactive voice response systems prompting the customer to confirm consent by saying yes or pressing a specific number; (3) website interaction; (4) "implicit" consent "where the consumer is requesting a service that quite clearly relies on location data, such as roadside assistance services";[61] or (5) in-person opt-in consent.[62]

18. According to T-Mobile, upon approving a new use of customer location information by a location-based services provider, T-Mobile would assign a "campaign-specific ID" to be used by the provider when making location requests of the Aggregator and that the Aggregator would then use to make location information requests of T-Mobile.[63] T-Mobile asserts that use of the "campaign-specific ID allow[ed] T-Mobile to track each campaign."[64]

19. T-Mobile had broad authority under its contracts with the Aggregators to quickly terminate access to its customer location information.[65] The contracts permitted the Company to suspend the transmission of location information to any location-based service provider that it believed was not

---

[57] LOI Response at 10, Introduction.

[58] *Id.* at 14, Response to Question 5.e.

[59] *Id.* at 7-8, 11, Response to Question 1.

[60] *Id.* at 7-8, Introduction.

[61] *Id.* at 7,13, Introduction, Response to Question 5.b.

[62] *See* 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).

[63] LOI Response at 11, Response to Question 1.

[64] *Id.*

[65] 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).

complying with its obligations.[66] T-Mobile also had the right to terminate its relationship with each Aggregator, for any reason, upon 30 days' prior written notice, or immediately upon the Aggregator's breach of the contract's confidentiality and data security terms.[67]

20. *T-Mobile's Internal Reviews and Auditing*. According to T-Mobile, it conducted two risk assessments of its Aggregator program to confirm, among other things, whether LocationSmart and Zumigo were following the policies and procedures set forth in their contracts with T-Mobile.[68] T-Mobile provides brief summaries of those risk assessments but, claiming attorney-client privilege, the Company has not shared the assessments with the Enforcement Bureau.[69]

21. With respect to its 2016 assessment, T-Mobile explains that the assessment was conducted with the assistance of [redacted] a third-party consultant, and the assessment determined that the Aggregators were properly obtaining consent before accessing T-Mobile customer location information.[70] At the same time, T-Mobile acknowledges that the report "made several recommendations to enhance program governance" and T-Mobile claims that as a result of its 2016 assessment, it "made some changes to the processes and controls used to manage the Location Aggregators and [location-based service] providers."[71] T-Mobile does not detail what those changes were, except that they included adoption of the location-based service provider questionnaire discussed above.[72]

22. According to T-Mobile, it conducted a second risk assessment in 2018 that was planned for and initiated in the first half of the year.[73] As described by T-Mobile, the 2018 assessment, which was also conducted with the assistance of [redacted] determined that the Aggregators were properly obtaining consent before accessing T-Mobile customer location information.[74] Nonetheless, T-Mobile acknowledges that the assessment resulted in "several recommendations to enhance program governance," but it does not describe what those recommendations were.[75]

23. In addition to the two risk assessments, T-Mobile claims that both T-Mobile and the Aggregators reviewed consent records collected from location-based service providers as part of "periodic assessments."[76] T-Mobile does not provide any information about the results of those periodic assessments.

3. T-Mobile's Discovery of LocateUrCell's Unauthorized Use of T-Mobile Customers' Location Information

24. On or around July 2017, T-Mobile learned that a location-based service provider named LocateUrCell was potentially misusing T-Mobile customer location information.[77] T-Mobile had

---

[66] T-Mobile-LocationSmart Agreement, Sections 7.2-3; T-Mobile-Zumigo Agreement, Sections 7.2-3.

[67] *Id.*

[68] LOI Response at 18, Response to Question 11.

[69] *See* Log of Documents Withheld as Privileged by Thread, submitted as part of LOI Response (Nov. 30, 2018) (on file in EB-TCD-18-00027702) (T-Mobile Privilege Log).

[70] LOI Response at 19, Response to Question 11.

[71] *Id.*

[72] *Id.*

[73] *Id.*

[74] *Id.*

[75] *Id.*

[76] *Id.* at 14, Response to Question 5.e.

[77] *Id.* at 17, Response to Question 10.

authorized LocateUrCell, a location-based service provider and customer of LocationSmart, to receive customer location information to provide consumers with the ability to locate their missing phones. Upon investigation, T-Mobile discovered that LocateUrCell was also operating an unapproved campaign.[78] Without the knowledge or authorization of T-Mobile, LocateUrCell was reselling access to T-Mobile customer location information to "bail bonding and similar companies to track the location of T-Mobile customer devices without customer consent."[79]

25. In September 2017, T-Mobile contacted LocationSmart to let it know that T-Mobile would suspend access to T-Mobile's customer information unless it received a satisfactory response to its inquiry about LocateUrCell within 24 hours, and to remind LocationSmart of its obligation to ensure that only approved service providers and services were accessing T-Mobile customers' location information.[80] At that point, T-Mobile learned that LocationSmart "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."[81] In response to its discovery of LocateUrCell's disclosure of T-Mobile customers' location information without their consent, T-Mobile "sought assurances" from LocationSmart regarding its monitoring of location-based service providers and "reminded" LocationSmart about its contractual obligations to notify T-Mobile of any non-compliance it detected.[82]

26. According to T-Mobile, LocateUrCell was able to disclose T-Mobile customer location information without customer consent and without T-Mobile's knowledge because T-Mobile could not differentiate between location information requests for the authorized LocateUrCell phone-finding service from location information requests for the unauthorized LocateUrCell location tracking service.[83] According to T-Mobile, this was because both services were "hosted on the same system" and "both the authorized and unauthorized services used the same campaign ID."[84]

4. T-Mobile's Actions After the Publication of Reports of Unauthorized Access to and Use of Customer Location Information

27. On May 10, 2018, the *New York Times* reported on security breaches involving T-Mobile's (and other carriers') practice of selling access to customer location information.[85] Specifically, Securus Technologies, Inc. (Securus), a provider of telecommunications services to correctional facilities throughout the United States, also operated a "location-finding service" that enabled law enforcement and corrections officials to access the location of a mobile device belonging to customers of major wireless carriers, including T-Mobile, *without* the device owner's knowledge or consent.[86] According to the article, Securus required users to certify that they had the authority to perform location searches and to upload an appropriate document, such as a court order or warrant, that provided legal authorization for the

[78] *Id.*

[79] *Id.* at 17-18, Response to Question 10.

[80] *Id.* at 17, Response to Question 10.

[81] *Id.* at 17-18, Response to Question 10.

[82] *Id.* at 17, Response to Question 10.

[83] *Id.* at 18, Response to Question 10.

[84] *Id.*

[85] *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.

[86] *Id.*

location request.[87] Securus did not, however, assess the adequacy of the purported legal authorizations submitted by users of its location-finding service.[88]

28. The *New York Times* article described how then-Missouri Sheriff Cory Hutcheson used the Securus service, without legal authorization, to access location information about anyone he pleased.[89] Another newspaper later reported that 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.[90] Among those apparently tracked by Hutcheson in this manner were his predecessor as Sheriff, a Missouri Circuit Judge, and at least five highway patrol officers.[91]

29. T-Mobile does not deny the existence of what it describes as the Securus "Real Time Location Service."[92] Nor does it deny the abuse of that service by Hutcheson. Instead, T-Mobile asserts that it did not authorize the Securus Real Time Location Service.[93] According to T-Mobile, until May 2018, Securus had authorization from T-Mobile to access customer location information only as part of a "Geofencing campaign" that allowed officials in detention facilities to confirm that a wireless user receiving a collect call from an inmate was not within a certain distance of the detention center.[94] As described by T-Mobile, the Geofencing campaign it approved allowed Securus to purchase access to T-Mobile customer information only if, in connection with a collect call from a correctional facility, a call recipient was informed, via a prerecorded message, that their location information would be collected, and they had pressed a button to consent to the collection of their location information to proceed with the call.[95] Based on Securus's representation that it had received proper consent from the T-Mobile customer to share the customer's information (which was transmitted from Securus to an intermediary called 3Cinteractive, then from 3Cinteractive to LocationSmart, and finally from LocationSmart to T-Mobile), T-Mobile transmitted a customer's location information to Securus (via LocationSmart and 3Cinteractive).[96]

30. T-Mobile asserts that Securus was able to conceal its Real Time Location Service from T-Mobile "by offering its unauthorized service under the guise of Securus's previously approved Geofencing campaign."[97] T-Mobile reiterates that "[n]either Securus, the intermediate location aggregator 3Cinteractive, nor LocationSmart submitted the Real Time Location Service that Securus was

---

[87] *Id*.

[88] *Id*.

[89] *Id.*

[90] *See* 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.

[91] *See* Complaint, *William T. Cooper et al. vs. Sheriff Cory Hutcheson*, Case: 1:17-cv-00073 (E.D. Mo. May 8, 2017) (on file in EB-TCD-18-00027702).

[92] LOI Response at 9, Introduction.

[93] *Id.* at 9-10, Introduction.

[94] *Id*.

[95] *Id.* at 9, Introduction. *See also* Securus Technologies Location-based Services (LBS) White Paper (Feb. 21, 2018) (on file in EB-TCD-18-00027702).

[96] LOI Response at 9-10, Introduction.

[97] *Id.* at 10, Introduction.

offering for T-Mobile's review and approval."[98] Instead, "Securus offered this service using the [same] campaign ID that T-Mobile had assigned its Geofencing campaign, which T-Mobile had approved."[99] T-Mobile concedes that, as a consequence, it had "no way" of differentiating between location information requests for the authorized Securus Geofencing service from location information requests for the unauthorized Securus Real Time Location Service.[100] T-Mobile claims that Securus has denied its request to identify the individuals whose customer location information may have been obtained without consent "on the basis that releasing such information could compromise ongoing law enforcement investigations."[101]

31. According to T-Mobile, on May 11, 2018, in response to the *New York Times* report and a letter about the Securus program from Senator Ron Wyden,[102] it terminated Securus and 3Cinteractive's access to T-Mobile customer location information.[103]

32. On October 26, 2018, T-Mobile notified the Aggregators that it would not renew their existing agreements, and thus those contracts would terminate on March 9, 2019, the date they were set to expire.[104]

33. On 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.[105] According to T-Mobile, in 2016, it authorized MicroBilt to request customer location information to verify customers' identity in connection with loan applications and to protect against potentially fraudulent loan applications by allowing MicroBilt to verify that the customer's mobile device was near the transaction location.[106] As T-Mobile explains, the MicroBilt application that T-Mobile had received did not indicate that "MicroBilt would disclose the location information to any third party."[107] MicroBilt, in turn, was a customer of Zumigo, an Aggregator that received customer location information from T-Mobile and the other major wireless carriers.[108]

34. On January 4, 2019, Zumigo confirmed for T-Mobile that it had suspended transmission of any T-Mobile customer location information to MicroBilt.[109] That same day, as a "duplicative technical measure," T-Mobile permanently disabled access to its customers' location information by

---

[98] *Id*.

[99] *Id*.

[100] *See id*. at 10, 19, Introduction, Response to Question 12.

[101] *Id.* at 19-20, Response to Question 12.

[102] *See* Letter from Senator Ron Wyden to John Legere, President and Chief Executive Officer, T-Mobile US, Inc. (May 8, 2018), *available at* https://www.wyden.senate.gov/imo/media/doc/wyden-securus-location-tracking-letter-to-tmobile.pdf.

[103] *See* LOI Response at 9-10, Introduction.

[104] *Id*. at 15, Response to Question 6; Supplemental LOI Response at 6, Response to Question 1.

[105] T-Mobile E-mail.

[106] *Id*.

[107] *Id*.

[108] 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.

[109] Supplemental LOI Response at 12, Response to Question 5.c.

Zumigo for the purpose of transmitting it to MicroBilt.[110] According to T-Mobile, it was "unable to identify individual customers that may have been affected by Microbilt's misuse of the Location Aggregator Program because its unauthorized access . . . was masked as a permissible use and T-Mobile was unable to distinguish the unauthorized use from authorized use."[111] In other words, T-Mobile was again unable to differentiate requests for customer location information that were made for purposes authorized by T-Mobile from those that were not.

35. On January 8, 2019, *Motherboard* published an article titled "I Gave a Bounty Hunter $300. Then He Located Our Phone."[112] The article alleged that T-Mobile and other telecommunications carriers' 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.[113] To illustrate the practice, the article described how a "bounty hunter" paid by *Motherboard* used his contacts in the bail bonds industry to access the location of a T-Mobile user's mobile phone.[114] The bounty hunter reportedly received the information from an employee of a bail bonds company that was a customer of MicroBilt.[115]

36. T-Mobile does not dispute the facts as reported in *Motherboard* article that MicroBilt had disclosed T-Mobile customer location information to MicroBilt's third-party customers, including the bail bonds company identified in the *Motherboard* report. Nor does T-Mobile dispute the fact that, while the T-Mobile customer described in the article had given their consent to *Motherboard* to be tracked via their phone, an employee of that bail bonds company apparently accessed a T-Mobile customer's location information for a purpose or campaign that T-Mobile had not approved and in contravention of the customer consent requirements that T-Mobile imposed on Zumigo and that Zumigo was required to impose on MicroBilt.[116]

37. On February 8, 2019—or 274 days after the *New York Times* reported on the Securus location-finding service, as well as the abuse of that service by Hutcheson—T-Mobile ended all location-based service providers' access to customer location information.[117]

38. *Commission Investigation*. The Enforcement Bureau launched an investigation in May 2018 immediately following the *New York Times* report of unauthorized location tracking involving Securus. The Bureau issued a Letter of Inquiry (LOI) to T-Mobile seeking information and documents regarding, among other things, its practices and procedures involving customer location information, its relationships with location information aggregators and location-based service providers, the specific allegations of unauthorized access to location information involving Securus that were detailed by the *New York Times*, and any other identified instances of unauthorized access to location information dating

[110] *Id*.

[111] *Id*. at 12-13, Response to Question 5.c (citing LOI Response at 6-9).

[112] 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.

[113] *Id*.

[114] *Id*.

[115] *Id*.

[116] T-Mobile E-mail.

[117] Supplemental LOI Response at 7, Response to Question 1.d. T-Mobile did not accelerate the expiration of its agreements with the Aggregators, which terminated on March 9, 2019. *Id*.

back to 2016.[118] The Bureau requested additional information and documents from T-Mobile in 2019.[119] T-Mobile submitted responses to the Bureau's initial and supplemental LOIs, as well as approximately 16,000 pages of responsive documents concerning its sale of access to its customer location information to third parties.[120]

III. DISCUSSION

39. We find that T-Mobile apparently willfully and repeatedly violated section 222 of the Act and the accompanying CPNI Rules by improperly disclosing customer location information to Hutcheson without customer approval. The customer location information at issue constitutes CPNI, and it may be used only as permitted by section 222 and our CPNI Rules.

40. We also find that the Company apparently violated section 222 of the Act and section 64.2010(a) of the CPNI Rules by failing to protect the confidentiality of its customers' CPNI and by failing to employ "reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI."[121] In particular, we find that for the better part of a year after T-Mobile became aware of Securus's unapproved location-finding service—and thereby had notice that the "consent records" it received through indirect arrangements with location-based service providers were not reliable indicia of customer consent—the Company's continued reliance on such attenuated consent mechanisms and ineffective monitoring tools apparently did not meet the reasonableness requirement of section 64.2010(a).

A. Customer Location Information Constitutes CPNI

41. We start with a preliminary point: Federal law protects the privacy of the customer location information at issue here. In other words, customer location information is CPNI under the Act and our rules.

42. The customer location information at issue falls squarely within section 222's definition of CPNI. Section 222 defines CPNI as 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."[122] To qualify as location-related CPNI, then, section 222 requires that information meet only two criteria: It must (1) "relate[]" to the "location . . . of a telecommunications service," and (2) it must be "made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[123]

43. The customer location information at issue here meets these two criteria. *First*, it relates to the location of a telecommunications service, i.e., T-Mobile's commercial mobile service.[124] The

---

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

[119] Supplemental Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to Luisa Lancetti, Director, Federal Regulatory, T-Mobile USA, Inc. (Apr. 8, 2019) (on file in EB-TCD-18-00027702) (Supplemental LOI).

[120] *See* LOI Response; Supplemental LOI Response.

[121] 47 CFR § 64.2010(a).

[122] 47 U.S.C. § 222(h)(1)(A) (emphasis added).

[123] *Id*. (defining "customer proprietary network information").

[124] *See id.* § 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").

location data was derived from the wireless mobile devices of T-Mobile's customers communicating with nearby network signal towers to signal the location of those devices. 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. This view finds ample support in Commission precedent, including the *2013 CPNI Declaratory Ruling*, which indicates that the policy considerations remain the same throughout a consumer's use of a mobile device, including the entire process through which the device stands ready to make or receive a call.[125]

44. *Second*, T-Mobile's wireless customers made this information available to T-Mobile because of the carrier-customer relationship embodied in their service agreements. 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. The customer location information to which T-Mobile sold access was generated by the service that T-Mobile provided to those customers. In short, T-Mobile's customers provided their wireless location data to T-Mobile because of their customer-carrier relationship with T-Mobile, so that T-Mobile could use that location information to provide them with a telecommunications service. That makes the location information CPNI.

45. Resisting this straightforward conclusion, T-Mobile points to the inclusion of the term "call location information" in section 222 and asserts that in order to constitute CPNI, customer location information must be the "call location" and "not just a 'location' of the device tangentially related to the provision of the telecommunications service."[126] But the use of the term "call location information" elsewhere in section 222 does not imply that every use of the term "location" in section 222 refers only to the location of the device when actively in use during a call. Arguably, the provision allowing sharing of "call location information" with public safety, family members, and others in emergency situations appears to contemplate allowing the sharing of a device's location outside the context of individual calls, suggesting that even that more specific term includes all location information.[127] But even if the term "call location information" elsewhere in section 222 is limited to information about the location of voice telephone calls, there is no reason to conclude the same about the broader term "location." Given the plain meaning of "location" and the obvious sensitivity of information that a carrier has about the location of its customers, we see no reason to interpret the statute as excluding the location of customer devices when they are not engaged in calls.

46. We remain likewise unpersuaded that location information generated and collected by carriers while a phone is in standby mode (i.e., while a phone is on, but not actively in use during a call) is materially different than any other customer location information generated or collected by the Company. T-Mobile argues that only customer location information that "identifies the origin or terminating point of

[125] *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, 9616, para. 22 (2013) (*2013 CPNI Declaratory Ruling*) (discussing "telephone numbers of calls dialed and received and the location of the device at the time of the calls" and "the location of a customer's use of a telecommunications service"); *id.* at 9617, para. 25 (concluding that even locations of failed calls fall within the definition of CPNI).

[126] Supplemental LOI Response at 8, Response to Question 2. That said, 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." *Id.* at 9 n.33.

[127] *See* 47 U.S.C. § 222(d)(4)(A)-(C).

a voice call" falls within the definition of CPNI.[128] The definition of CPNI, however, does not distinguish between the location information collected by carriers from a mobile device during a telephone call and the location information generated when the device is turned on and available for calls but not engaged in transmitting a voice conversation. In both cases, the location "relates" to the carrier's provision of telecommunications service to the customer, and the customer's location is available to the carrier solely by virtue of its carrier-customer relationship.

47. Having concluded that the customer location information at issue is CPNI under section 222 of the Act, we likewise conclude that the rules governing consent to the use, disclosure, and sharing of CPNI and protection of CPNI, which incorporate the statutory definition by reference,[129] also apply to that customer location information.

48. T-Mobile appears to argue that neither the statutory obligations for approval of the customer and protection of CPNI nor the Commission's CPNI Rules apply to its handling of customer location information. Citing a 2002 statement by the Commission that "no rules [were] necessary" to implement section 222(f)—a section that applies not to CPNI generally but only to "call location information" and "automatic crash notification information"—T-Mobile suggests that the rules the Commission *subsequently* adopted in 2007 for all CPNI have no application here.[130] To be frank, we do not follow T-Mobile's chain of logic. Although the Commission declined to adopt rules in 2002, it did not conclude that the basic statutory protections, the Commission's preexisting CPNI rules, or future rule changes should not apply: "Without some showing that Section 222(f), as read in conjunction with the broader provisions of Section 222, is inadequate to protect consumers, we conclude that any action by the Commission is unnecessary."[131] Five 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 statement that T-Mobile cites.

B. T-Mobile Apparently Violated Section 222 and the CPNI Rules by Disclosing CPNI to a Missouri Sheriff Without Authorization

49. T-Mobile apparently violated section 222(c)(1) of the Act and section 64.2007 of the Commission's rules when it disclosed customer location information to Hutcheson. Section 222(c)(1) states that carriers shall only use, disclose, or permit access to individually identifiable CPNI with the approval of the customer.[132] Section 64.2007 of the Commission's rules states that a telecommunications carrier may only use, disclose, or permit access to its customer's individually identifiable CPNI subject to opt-in approval.[133]

50. 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 then shared it with 3Cinteractive, which then shared it with Securus, which then disclosed it to Hutcheson—despite the absence of T-Mobile customer consent for the disclosures. The evidence shows that between 2014 and 2017, at least three T-Mobile customers' location information was disclosed to Hutcheson, via

[128] Supplemental LOI Response at 8, Response to Question 2.

[129] 47 CFR § 64.2003(g).

[130] *See, e.g.*, LOI Response at 3, Introduction; Supplemental LOI Response at 10, Response to Question 4.d.

[131] *2002 Order Denying Petition for Rulemaking*, 17 FCC Rcd at 14834, para. 5.

[132] 47 U.S.C. § 222(c)(1). There are exceptions in circumstances not relevant here.

[133] 47 CFR § 64.2007(b). There are exceptions in circumstances not relevant here.

Securus, without the customers' consent.[134] Notwithstanding the misconduct of Hutcheson, each such disclosure constitutes a violation of section 222(c)(1) of the Act and section 64.2007 of the Commission's rules for which T-Mobile is responsible.

51. T-Mobile does not dispute that it disclosed its customers' location information to Hutcheson without the customers' consent and in the absence of an exception that would make the consent requirement inapplicable. Instead, T-Mobile argues that Securus exploited its approved "Geofencing" campaign to access customer location information, without customer consent, for its unapproved "Real Time Location Service."[135] T-Mobile explains that notwithstanding the customer notice and authorization requirements it imposed on LocationSmart, and that LocationSmart then imposed on 3Cinteractive and Securus, Securus operated an unapproved location-finding service through which correctional facilities and other law enforcement personnel could access T-Mobile customer location information "potentially without customer consent."[136]

52. We find these arguments unavailing. T-Mobile is not absolved from liability simply because it was not directly responsible for operating the programs under which unauthorized disclosures occurred. Rather, sections 222 and 217 of the Act make clear that ultimate responsibility for these unauthorized disclosures rests with the carrier—in this case, T-Mobile. The restrictions on the use and disclosure of CPNI in section 222 of the Act expressly apply to "telecommunications carriers."[137] Section 222 broadly prohibits telecommunications carriers from using CPNI collected in connection with providing telecommunications service for any purpose other than providing such service or other services "necessary to, or used in" providing such service (for example, publishing directories).[138] Apart from a few exceptions not relevant here,[139] section 222 allows a telecommunications carrier to use CPNI for other purposes only where "required by law or with the approval of the customer."[140] In short, 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.

53. To allow a telecommunications carrier to share CPNI with an entity that is not subject to section 222 without imposing sufficient controls could deprive its customers of the statutory protections of section 222.[141] The Commission recognized this problem in 2007, responding to the reality at that time that individuals' calling records were available for sale on numerous websites.[142] As a result, the Commission determined that it was necessary to further limit the sharing of CPNI with others outside a customer's carrier by requiring carriers to obtain opt-in approval from a customer even before disclosing that customer's CPNI to a carrier's joint-venture partner or independent contractor. "Opt-in approval" is

---

[134] *See* Department of Justice Evidence Records (on file in EB-TCD-18-00027702).

[135] LOI Response at 9-10, Introduction.

[136] *Id*. at 9, Introduction.

[137] The Commission extended the applicability of its CPNI Rules to interconnected Voice over Internet Protocol providers in 2007. *See 2007 CPNI Order*, 22 FCC Rcd at 6954-57, paras. 54-59. Congress acknowledged this extension in its 2008 amendments to section 222. *See* Pub. L. No. 110-283, § 301, 122 Stat. 2620, 2625-26, *codified at* 47 U.S.C. § 222(d)(4), (f)(1), (g).

[138] *See* 47 U.S.C. § 222(c)(1).

[139] *See id.* § 222(d) (specifying four exceptions).

[140] *Id*. § 222(c)(1).

[141] *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14860, 14881, paras. 46-47 (2002).

[142] *2007 CPNI Order*, 22 FCC Rcd at 6928-29, para. 2.

defined as a method that "requires that *the carrier* obtain from the customer affirmative, express consent allowing the requested CPNI usage, disclosure, or access after the customer is provided appropriate notification of *the carrier's* request."[143] This was necessary in part "because a carrier is no longer in a position to personally protect the CPNI once it is shared."[144]

54. We recognize that carriers have long relied on third parties—aggregators and/or location-based service providers—to act on their behalf to obtain their customers' consent to the sharing of their CPNI.[145] But such reliance has never meant absolution for carriers. Instead, 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."[146] In other words, a carrier cannot avoid its statutory obligations by assigning them to a third party.

55. So it is unsurprising that the Commission has consistently held that carriers are responsible for the conduct of third parties acting on the carrier's behalf.[147] Just as the Commission recently held that a carrier was "not relieved of liability [for slamming] simply because it provided its telemarketers with a policy manual and sales script and directed its telemarketers to market its service 'through lawful means,'"[148] a carrier is not relieved of its section 222 obligations simply because it contracts with third parties and relies on them to obtain the statutorily required approval—even if it imposed similar obligations by contract. Similarly, in 2012, the Commission found it unnecessary to impose on Lifeline providers an explicit obligation that they, rather than their agents or representatives, review all documentation of eligibility.[149] That was because the carriers themselves would be legally responsible for the acts and omissions of those agents: "[Carriers] may permit agents or representatives to review documentation of consumer program eligibility for Lifeline. However, the [carrier] remains liable for ensuring the agent or representative's compliance with the Lifeline program rules."[150]

56. At bottom, T-Mobile may not have it both ways. If T-Mobile was relying on third parties to satisfy its obligations to obtain consent, then it is 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.

---

[143] 47 CFR § 64.2003(k) (defining "opt-in approval") (emphases added).

[144] *2007 CPNI Order*, 22 FCC Rcd at 6948, para. 39.

[145] To 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. T-Mobile does not appear to argue that situation is present here.

[146] 47 U.S.C. § 217.

[147] *See, e.g.*, *Long Distance Consol. Billing Co.*, Forfeiture Order, 34 FCC Rcd 1871, 1874-75, para. 10 (2019); *Eure Family Ltd. Partnership*, Memorandum Opinion and Order, 17 FCC Rcd 21861, 21863-64, para. 7 (2002); *Long Distance Direct, Inc.*, Memorandum Opinion and Order, 15 FCC Rcd 3297, 3300, para. 9 (2000); *Vista Services Corp.*, Order of Forfeiture, 15 FCC Rcd 20646, 20650, para. 9 (2000); *American Paging, Inc. (of Virginia)*, Memorandum Opinion and Order, 12 FCC Rcd 10417, 10420, para. 11 (1997); *Triad Broadcasting Co., Inc.*, Memorandum Opinion and Order, 96 FCC 2d 1235, 1244, para. 21 (1984); *see also Silv Communication, Inc.*, Notice of Apparent Liability for Forfeiture, 25 FCC Rcd 5178, 5180, para. 5 n.18 (2010).

[148] *Long Distance Consol. Billing Co.*, 34 FCC Rcd at 1875, para. 10.

[149] *Lifeline and Link Up Reform and Modernization*, Report and Order and Further Notice of Proposed Rulemaking, 27 FCC Rcd 6656, 6708-09, para. 110 (2012).

[150] *Id.* at 6709, para. 110.

57. In sum, we find that T-Mobile apparently violated section 222(c)(1) of the Act and section 64.2007(b) of our rules in connection with its unauthorized disclosures of CPNI to Hutcheson.[151]

C. T-Mobile Apparently Failed to Take Reasonable Measures to Protect CPNI

58. T-Mobile apparently violated section 222 of the Act and section 64.2010 of our rules by failing to take reasonable measures to discover and protect against attempts to gain unauthorized access to its customers' location information.[152] The May 10, 2018 *New York Times* report on the Securus and Hutcheson breaches exposed serious inadequacies with the safeguards on which T-Mobile relied to protect its customers' location information. Our investigation shows that T-Mobile failed to promptly address those inadequacies. We therefore conclude that T-Mobile apparently failed to take reasonable measures in a timely fashion to protect its customers' CPNI following that report.

59. In plain terms, our rules recognize that companies cannot prevent all data breaches, but require carriers to take reasonable steps to safeguard their customers' CPNI and to discover attempts to gain access to their customers' CPNI. In the absence of an unauthorized disclosure, the Commission bears the burden of demonstrating that the methods employed by a carrier to safeguard CPNI were unreasonable. But where an unauthorized disclosure *has* occurred—as here—this burden shifts to the carrier. In that case, the Commission treats the unauthorized access to a subscriber's CPNI as *prima facie* evidence that a carrier failed to sufficiently protect the information.[153] The responsible carrier then shoulders the burden of proving the reasonableness of its measures to (1) detect unauthorized attempts to access CPNI and (2) protect CPNI from such attempts.[154]

60. T-Mobile thus bears the burden of demonstrating that the measures it took to safeguard CPNI were reasonable both before and after the Securus and Hutcheson breaches. T-Mobile argues, incorrectly, that its only statutory or regulatory obligation with respect to wireless location CPNI is section 222(f)'s requirement that it obtain "the express prior authorization of the customer" for the use of, disclosure of, or access to such information.[155] But its description of its Aggregator program nevertheless discusses the "contractual, procedural, and technical safeguards"[156] that it employed to safeguard its customers' CPNI. We begin by discussing those safeguards.

61. *First*, T-Mobile asserts that it safeguarded customer location information by allowing only two entities—the Aggregators LocationSmart and Zumigo—direct access to its Service Delivery Gateway.[157] T-Mobile required these entities, in turn, to impose a number of contractual safeguards on the location-based service providers to whom they provided customer location information.[158] T-Mobile presents this arrangement as a safety feature: only two entities had access to its customer location data through its Location APIs.[159] But while that arrangement may have limited the number of parties with *direct* access to its location data, the effect of this arrangement was that the myriad location-based service providers that actually requested and used the location information of T-Mobile customers had no direct contractual relationship with T-Mobile. As a result, T-Mobile could only govern the behavior of the

---

[151] 47 U.S.C. § 222(c)(1); 47 CFR § 64.2007(b).

[152] 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.").

[153] *2007 CPNI Order*, 22 FCC Rcd at 6959–60, para. 65.

[154] *Id*. at 6959–60, para. 65.

[155] LOI Response at 12, Response to Question 4; *see also id*. at 2-6.

[156] LOI Response at 7, Introduction; *see also id.* at 11, 12.

[157] LOI Response at 8, Introduction.

[158] *Id.*

[159] *Id*.

entities that actually received and used the location data of its customers—the location-based service providers—through provisions passed down through an attenuated chain of downstream contracts.

62. *Second*, T-Mobile asserts that it reviewed and approved each new use of customer location information proposed by a location-based service provider.[160] According to T-Mobile, it required location-based service providers to secure what T-Mobile calls "express prior consent of the end user" in connection with each use of location information.[161] T-Mobile also claims that each location-based service provider was required to "produce to T-Mobile, a clear, visual depiction of the consent capture process."[162]

63. However, notwithstanding T-Mobile's claim that it required location-based service providers to secure "express prior consent" from its customers before accessing the customers' location information, T-Mobile admits that it relied only on *implicit* consent in circumstances where a user requested a service "that self-evidently relies on the location of the user's device."[163] We reject T-Mobile's contention that 'express prior consent' can be obtained implicitly. It begs the question of how a location-based service provider could comply with T-Mobile's alleged requirement that each provider "produce a clear visual depiction" of an implicit "consent capture process." And, it is fundamentally inconsistent with the safeguards for CPNI built into the requirement in our rules that carriers solicit and receive "opt-in" approval from their customers before disclosing CPNI to third parties for most purposes, including those at issue here.[164] Pursuant 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.[165] By requiring carriers to obtain affirmative consent from a customer before using, sharing, or disclosing CPNI, the opt-in approval requirements act as a key safeguard against attempts to gain access to CPNI that has not been authorized by a carrier's customers. By approving use cases that provided for "implicit" rather than "affirmative express consent," T-Mobile put its customers' CPNI at needless risk.

64. What's more, there is little evidence that T-Mobile took steps to ensure that location-based service providers fulfilled their commitment to collect either implicit or actual "express affirmative consent" from their customers. T-Mobile admits, for example, that it did not dictate the form, placement, wording, or manner of obtaining consent other than requiring that it be informed and based upon meaningful notice.[166] Furthermore, T-Mobile's contractual arrangements required that the Aggregators—not T-Mobile—ensure that location-based service providers have obtained consent prior to the Aggregators accessing customer location information.[167] T-Mobile likewise relied on Aggregators to maintain the records of consent, which T-Mobile asserts that it reviewed "periodic[ally]."[168] 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.

---

[160] *Id*. at 7, Introduction.

[161] *Id*.

[162] *Id*. at 8, Introduction.

[163] *Id*. at 7, Introduction.

[164] *See* 47 CFR § 64.2007(b).

[165] *See id.* § 64.2003(k). *See also* 47 CFR § 64.2008 (describing the type of notice carriers must provide prior to soliciting customer approval to use, share, or disclose CPNI).

[166] LOI Response at 7, Introduction.

[167] *Id*. at 14, Response to Question 5.e.

[168] *Id*.

65. *Third*, T-Mobile asserts that it maintained control over the Aggregators and their location-based service provider customers through a number of contractual provisions providing for the safeguarding of location data.[169] Specifically, T-Mobile's contractual arrangement with the Aggregators delegated to the Aggregators the obligations to authorize use of T-Mobile customer information only upon the "express prior consent" of the end user; maintain and provide, for T-Mobile's review, records demonstrating such consent; comply with the CTIA Guidelines applicable to location-based service providers;[170] secure T-Mobile's prior approval for each location-based service provider and the use being proposed; and "appropriately secur[e] the location data."[171] T-Mobile largely relied on the Aggregators and any intermediaries to pass down these contractual provisions to their location-based service provider customers. To monitor and enforce these contractual requirements, T-Mobile would have needed to take steps to determine whether they were actually followed. T-Mobile has not shown that it did so. And notwithstanding T-Mobile's contract with LocationSmart, LocationSmart's contract with 3Cinteractive, and 3Cinteractive's contract with Securus, Securus was able to set up a separate program to access and disclose customer location information and operate it *for at least four years* in a manner inconsistent with those contracts and without T-Mobile's knowledge.

66. *Fourth*, T-Mobile asserts that it used technical safeguards to limit access to its Location APIs. T-Mobile asserts that when it approved a new use case, it would assign a "campaign-specific ID," which a provider would use to make location requests of an Aggregator, and which the Aggregator would in turn use to make requests from T-Mobile.[172] Where T-Mobile could not use this information to validate a call location information request on its Location API, it would reject the request.[173] At bottom, this technological safeguard appears to be 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."[174]

67. *Fifth and finally*, T-Mobile asserts that it retained a third-party firm to conduct two risk assessments of its Aggregator program in 2016 and 2018, but it withheld the results of those assessments as privileged.[175] T-Mobile notes that both reports made recommendations to "enhance program governance," but does not provide the findings underlying these recommendations, what those recommendations were, or what actions T-Mobile took in response to the recommendations. Instead, T-Mobile leaves us only with the conclusion that a third-party consultant twice found that the governance of its Aggregator program required "enhanc[ing]," and that it made "some changes" to its "processes and controls" following these findings.[176] From these vague assertions, it is impossible for us to conclude that T-Mobile took meaningful steps to protect customer location information among the 83 entities to which it sold such access.

---

[169] *Id*. at 8, Introduction.

[170] Those 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.

[171] LOI Response at 8, Introduction. T-Mobile does not detail what safeguards would constitute "appropriately securing" the location data.

[172] *Id*. at 11, Response to Question 1.

[173] *Id*.

[174] *Id*. at 18, Response to Question 10.

[175] *Id*.

[176] *Id*. at 18-19, Response to Question 10.

68. In sum, the safeguards implemented by T-Mobile to protect customer location information against unauthorized use relied almost entirely on contractual agreements, passed on to location-based service providers through an attenuated chain of downstream contracts. To the extent that T-Mobile may have had the ability to verify the information submitted in connection with a request for location data, or otherwise demand compliance with its contractual safeguards, it did not seem to meaningfully do so. And it had almost no other visibility or apparent awareness into how the location data it sold access to was used or protected. While business relationships often rely on trusting a counterparty to honor its contractual obligations, it is hard to conclude that such trust alone was a reasonable safeguard here—particularly after T-Mobile learned of LocateUrCell's deception and misuse of its customer location data in July 2017. Long before that incident, however, the industry's experience with pretexting should have apprised T-Mobile of the high risk that bad actors would attempt to gain unauthorized access to T-Mobile's customers' CPNI, particularly by trying to find ways around any systems T-Mobile put in place to authenticate that its customers were actually providing consent to third parties' access to their location information.

69. Setting aside the apparent inadequacy of T-Mobile's safeguards before disclosure of the Securus and Hutcheson breaches, T-Mobile was on clear notice that its safeguards were inadequate after the disclosure, and so we focus on the actions that T-Mobile took, or failed to take, after discovery of those breaches. We find that T-Mobile has apparently failed to demonstrate that its safeguards were reasonable following the disclosure of Securus's unauthorized location-finding service in May 2018. The Securus incident laid bare the fundamental weaknesses of T-Mobile's safeguards with respect to the third parties to which it entrusted its customers' location information. Nevertheless, for 274 days after that incident came to light, T-Mobile continued to sell access to its customers' location information to 80 different entities under the same system that had allowed (1) Securus to provide location information in a manner inconsistent with its approved "campaign," and (2) Hutcheson to easily and improperly access T-Mobile customers' location information. Relying on demonstrably faulty safeguards in the wake of this incident does not appear to have been reasonable.

70. There are several commonsense measures that T-Mobile could have taken following the May 2018 *New York Times* article. One obvious measure would have been to identify the companies involved in the Securus breach and terminate their access until it could verify that these companies had properly safeguarded its customers' location data. T-Mobile did so only in part. T-Mobile terminated all transfers of customer location information to 3Cinteractive and Securus and instructed LocationSmart to do so as well on May 11, 2018. But it did not promptly suspend the access of LocationSmart itself, even though LocationSmart had the contractual obligations to monitor Securus and 3Cinteractive's access to T-Mobile's customer location data. Only later on February 8, 2019—or 274 days after the *New York Times* reported on the Securus location-finding service, as well as the abuse of that service by Hutcheson—did T-Mobile end LocationSmart's access (as well as other entities' access) to customer location information.[177] T-Mobile's decision not to promptly suspend access by LocationSmart in the wake of the Securus incident is even more unreasonable when considered in light of its discovery in 2017 of a breach involving LocateUrCell. That incident, like the Securus one, apparently 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.[178]

71. Another measure would have been to promptly ascertain the full scope and extent of the Securus breach. But T-Mobile lacked the technical ability to identify the individuals affected by the Securus breach or otherwise independently assess the scope of the incident. T-Mobile asserts that it could

[177] Supplemental LOI Response at 7, Response to Question 1.d. T-Mobile did not accelerate the expiration of its agreements with the Aggregators, which terminated on March 9, 2019. *Id.*

[178] LOI Response at 17-18, Response to Question 10.

not distinguish the location requests associated with Securus's unapproved Real Time Location Service from those associated with its approved Geofencing campaign.[179] Thus, one of T-Mobile's technical safeguards—the use of specific "campaign IDs"—was vulnerable to the predictable risk that a third party would use an approved campaign ID to mask location requests made for an unapproved purpose. This specific vulnerability apparently had already been exploited by LocateUrCell in 2017, and it was subsequently exploited again in the MicroBilt breach disclosed in 2019.

72. What is more, the full impact of Securus's unauthorized access to CPNI apparently remains unknown to this day. That is because T-Mobile claims that Securus has denied its request to identify the individuals whose customer location information may have been obtained without consent "on the basis that releasing such information could compromise ongoing law enforcement investigations."[180] Rather than shielding T-Mobile from liability, that admission shows the inherent weakness of T-Mobile's arguments that its contract-based model provided reasonable protection of CPNI. If T-Mobile cannot compel Securus's cooperation with its investigation 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 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.

73. Another measure T-Mobile could have taken was to determine whether the Securus incident was an isolated occurrence or whether it was indicative of a broader vulnerability with T-Mobile's program. This would mean examining not only the companies involved in the Securus incident, but also taking broader efforts to audit similarly situated companies' compliance with T-Mobile's contractual safeguards. Yet T-Mobile has offered no evidence to suggest that it took steps after the publication of the *New York Times* article to identify and remedy the broader security deficiencies exposed by revelations about Securus's location-finding service. T-Mobile's LOI Response describes a risk assessment "that was planned for and initiated in the first half of 2018," prior to the revelations about Securus.[181] This assessment determined, according to T-Mobile, that the Aggregators were properly obtaining the consent of T-Mobile's customers before collecting, using, or disclosing their location information.[182] Yet, the LocateUrCell, Securus, and MicroBilt breaches demonstrate that the assessment was apparently not reasonably designed to detect vulnerabilities in the consent mechanism. Furthermore, T-Mobile has provided no evidence that it sought to determine whether there were other unauthorized programs being operated that allowed access to T-Mobile customer location information in ways that contravened T-Mobile's contracts with its Aggregators. Nor has T-Mobile provided evidence that it sought to determine whether there were unauthorized campaigns—or abuses of authorized campaigns—that were giving users unauthorized access to T-Mobile customer location information. Although T-Mobile claims that it decided to terminate its aggregator program at some point before it submitted its LOI Response in November 2018, the program nonetheless remained in place in apparently the same form until February 8, 2019.

74. Unfortunately, the apparent failure of T-Mobile to impose reasonable safeguards on its program to sell access to customer location information after the *New York Times* article is not merely a matter of theory. On January 8, 2019, *Motherboard* reported on its success purchasing T-Mobile customer location information that was disclosed to MicroBilt.[183] This revealed that, although T-Mobile

[179] *Id*. at 10, Introduction.

[180] *Id*. at 19-20, Response to Question 12.

[181] *Id*. at 19, Response to Question 11.

[182] *Id*.

[183] 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.

had authorized MicroBilt to access location information only for the purpose of mitigating fraud in connection with consumer loans that MicroBilt itself originated, MicroBilt apparently disclosed location information to its own corporate customers, which included members of the bail bonds industry. And, as the *Motherboard* article demonstrated, purchasing access to customer location information provided by a carrier to MicroBilt was not a difficult thing to do—nor did it appear to be difficult for *Motherboard* to unearth the vulnerability.

75. Stepping back, this means that the safeguards that T-Mobile had in place for the 243 days after the *New York Times* article apparently failed to discover yet another case of unauthorized access to customer location information by a whole separate set of entities than were involved in the Securus breaches. Or to put it differently, after the Securus incident demonstrated serious systemic flaws in T-Mobile's safeguards to protect CPNI, T-Mobile continued to rely on those same safeguards so that it could continue to sell access to 81 separate entities—so it is no surprise that those safeguards were subject to an almost identical security vulnerability, reflecting T-Mobile's persistent failure to respond appropriately to these data breaches. And T-Mobile apparently recognized as much on February 8, 2019 when it terminated all location-based service providers' access to customer location information.

76. Yet another measure that T-Mobile could have taken was to enhance the measures it uses to verify customer consent—for example, by directly confirming with customers that they have consented to the use of their location information. After the Securus and Hutcheson breaches came to light, T-Mobile had good reason to doubt the accuracy of the consent records it received from any location-based service provider. As T-Mobile itself explains, Securus's access to location information contrary to its authorized use case, and by extension Hutcheson's misuse of T-Mobile's customers' location data, were concealed from T-Mobile because "[n]either Securus, the intermediate location aggregator 3Cinteractive, nor LocationSmart submitted the Real Time Location Service . . . for T-Mobile's review and approval" and T-Mobile "would have processed [requests related to that service] as if it were an API request from the approved Geofencing campaign[.]"[184] Thus, the Securus and Hutcheson breaches made clear that instead of developing a consent mechanism that would allow T-Mobile to confirm that its customers had actually consented to the sharing of their location information, it created and maintained a system that required it to rely on the unverified representations of third-party location-based service providers that had financial incentives to access that information. Again, T-Mobile apparently recognized as much when it told Enforcement Bureau staff in November 2018 that it [redacted][185] But there is no evidence that T-Mobile ever implemented any of these modifications to its consent verification process. Instead, it left in place a consent verification system that it knew to be flawed, thereby increasing the risk of further unauthorized access.

77. Finally, the surest safeguard to protect its customers' CPNI would have been for T-Mobile to expeditiously terminate its location-based service program. If T-Mobile could not reasonably safeguard the customer location information that it sold access to, then it should have ceased to sell access to that information. Yet it was not until February 8, 2019—274 days after the Securus incident was revealed—that T-Mobile terminated location-based service providers' access to T-Mobile customers' location information.[186] T-Mobile's contracts with the Aggregators included a provision allowing T-Mobile to terminate the agreements for any reason upon 30 days' prior written notice or immediately

[184] T-Mobile LOI Response at 10, Introduction.

[185] *Id*. at 15, Response to Question 6.

[186] Supplemental LOI Response at 6, Response to Question 1.

upon a breach of the contract's confidentiality and data security terms.[187] The time for T-Mobile to have exercised this provision was far earlier—shortly after the Company learned that Securus had been operating a location-finding service without T-Mobile's authorization and despite T-Mobile's existing safeguards. That is especially true given that the Securus breaches were not T-Mobile's first time learning that its contract-based system was insufficient—it should have realized that system's failings after the LocateUrCell incident. T-Mobile fails to explain its inaction in the face of an obvious risk to its customers.

78. T-Mobile apparently did not take any of these reasonable steps. Nor has it presented evidence that it took other reasonable measures that might have cured the flaws exposed by the Securus and MicroBilt breaches. The ease with which Hutcheson accessed location information about any individual of his choosing should have alerted T-Mobile to its lack of visibility into how the location-based service providers were making use of the location information that it entrusted to the Aggregators, and that it needed to change its practices or terminate its location-based service program. After learning of Hutcheson's practices, T-Mobile placed its customers' location information at continuing risk of unauthorized access through its failure to expeditiously terminate its program or impose reasonable safeguards to protect its customers' location information. For these reasons, we conclude that T-Mobile apparently 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.[188]

D. Proposed Forfeiture

79. Section 503(b) of the Act authorizes the Commission to impose a forfeiture against any entity that "willfully or repeatedly fail[s] to comply with any of the provisions of [the Act] or of any rule, regulation, or order issued by the Commission . . . ."[189] Here, section 503(b)(2)(B) of the Act authorizes us to assess 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 a single act or failure to act.[190] In exercising our forfeiture authority, we must consider 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."[191] In addition, the Commission has established forfeiture guidelines; they establish base penalties for certain violations and identify criteria that we consider when determining the appropriate penalty in any given case.[192] Under these guidelines, we may adjust a forfeiture upward for violations that are egregious, intentional, or repeated, or that cause substantial harm or generate substantial economic gain for the violator.[193]

---

[187] T-Mobile-LocationSmart Agreement, Sections 7.2-3; T-Mobile-Zumigo Agreement, Sections 7.2-3.

[188] 47 CFR § 64.2010(a); *see also 2007 CPNI Order*, 22 FCC Rcd at 6959, para. 64 (stating that the Commission expects carriers to "take every reasonable precaution to protect the confidentiality of proprietary or personal customer information").

[189] 47 U.S.C. § 503(b).

[190] *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). The Federal Civil Penalties Inflation Adjustment Act of 1990, Pub. L. No. 101-410, 104 Stat. 890, as amended by the Debt Collection Improvement Act of 1996, Pub. L. No. 104-134, Sec. 31001, 110 Stat. 1321, requires the Commission to adjust its forfeiture penalties periodically for inflation. *See* 28 U.S.C. § 2461 note (4). The Enforcement Bureau announced the Commission's inflation-adjusted penalty amounts for 2020 on December 27, 2019. *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).

[191] 47 U.S.C. § 503(b)(2)(E).

[192] 47 CFR § 1.80(b)(8), Note to paragraph (b)(8).

[193] *Id*.

80. The Commission's forfeiture guidelines in section 1.80(b) of the Commission's rules do not establish a base forfeiture for violations of section 222(c) or the accompanying CPNI Rules.[194] Nor has the Commission calculated forfeitures for the unauthorized disclosure of CPNI previously. Thus, we look to the base forfeitures established or issued in analogous cases for guidance. In 2011 and 2012, the Bureau issued Forfeiture Orders for failure to timely file the annual CPNI compliance certifications required by section 64.2009(e) of the Commission's rules (*CPNI Cases*).[195] Similar to this case, the driving purpose behind the Commission's actions in the *CPNI Cases* was enforcing the protections that Congress established in section 222(c) for consumers' proprietary information. In the *CPNI Cases*, the base forfeiture was between $20,000 and $29,000 for failure to file or failure to respond to a Bureau order to file certain information regarding the carriers' CPNI filings. In 2014, the Commission issued a Notice of Apparent Liability against TerraCom, Inc. and YourTel America, Inc., for apparently violating section 222(a) of the Act.[196] In *TerraCom*, the carriers' failure to secure their computer systems revealed detailed personal information belonging to individual Lifeline program applicants; the Commission proposed a penalty of $8,500,000 in that case.[197]

81. Neither the *CPNI Cases* nor *TerraCom* are directly on point with the conduct in this case, but they nevertheless are helpful in context. We find that T-Mobile's failures to protect CPNI were much more egregious and fundamental than the failures of the carriers in the *CPNI Cases*, which involved the failure to file compliance certifications required by Commission rules. The potential harm that flowed from failure to establish reasonable safeguards to protect customer location information from unauthorized access was significantly greater than the harm posed by a carrier's failure to file CPNI certifications in a timely manner. Consumers carry their smartphones or wireless phones on their person or within easy reach at all times of the day or night. The precise physical location of a wireless device is an effective proxy for the precise physical location of the person to whom that phone belongs at that moment in time. Exposure of this kind of deeply personal information puts those individuals at significant risk of harm—physical, economic, or psychological. For consumers who have job responsibilities in our country's military, government, or intelligence services, exposure of this kind of information can have serious national security implications.

82. In contrast to the CPNI Cases, *TerraCom* addressed a situation of similarly serious threats to privacy—albeit in the context of a different part of section 222. *TerraCom* dealt with exposure of personal information—not CPNI—and the Commission proposed penalties based on language in section 222(a) that had never been examined or codified in a Commission rulemaking. Here, in contrast, the Commission has examined section 222(c) in multiple rulemaking and other proceedings and has promulgated rules necessary to interpret and enforce the statute. That said, the proposed penalty in *TerraCom* was significant in light of the scope of the apparent harm.

83. Apparent Violations of Section 222 of the Act and Section 64.2010 of the Commission's Rules. 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. We propose a base forfeiture of $40,000 for the first day of such a violation and a $2,500 forfeiture for the second day and each successive day that the violation continued. In other contexts involving consumer

[194] *Id*. § 1.80(b).

[195] *See, e.g., Jahan Telecommunication, LLC*, Order of Forfeiture, 27 FCC Rcd 6230 (EB-TCD 2012); *Nationwide Telecom, Inc*., Order of Forfeiture, 26 FCC Rcd 2440 (EB-TCD 2011); *Diamond Phone, Inc*., Order of Forfeiture, 26 FCC Rcd 2451 (EB-TCD 2011); *USA Teleport, Inc*., Order of Forfeiture, 26 FCC Rcd 2456 (EB-TCD 2011); *88 Telecom Corporation*, Order of Forfeiture, 26 FCC Rcd 7913 (EB-TCD 2011); *DigitGlobal Communications, Inc.*, Order of Forfeiture, 26 FCC Rcd 8400 (EB-TCD 2011).

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

[197] *TerraCom*, 29 FCC Rcd at 13343, para. 52.

protections under the Act and the Commission's rules, the Commission has applied a base forfeiture of $40,000 for a single act.[198] We find that the base forfeiture we propose is appropriate (1) to provide a meaningful distinction between the violations in this case and those of other cases involving less egregious facts; and (2) to provide consistency with other consumer protection cases involving serious harm to consumers. We find this base forfeiture appropriately deters wrongful conduct and reflects the increased risk consumers face when their information is not secured in a timely manner.

84. We recognize that T-Mobile took one reasonable step towards improving its safeguards by terminating Securus and 3Cinteractive's access to T-Mobile customer location information on May 11, 2018, one day after the *New York Times* report.[199] But that step did not protect customer location information at all from the other 81 entities that had access to it. These included location-based service providers and the two Aggregators—and constitute 81 separate continuing violations. We find that T-Mobile apparently did not take reasonable steps to safeguard that CPNI until January 4, 2019—a full 239 days after the *New York Times* report—for MicroBilt, and until February 8, 2019—274 days after the report—for the remaining 80 entities. Even though no carrier can be expected to fully investigate and take remedial actions on the same day it learns that its safeguards are inadequate, T-Mobile's failure to take reasonable steps to safeguard that information in the 30 days after discovering the breach constitutes a continuing violation of our rules. We therefore calculate each continuing violation from June 9, 2018, or 30 days after publication of the May 10, 2018 *New York Times* report, and apply a base forfeiture of $40,000 and a $2,500 forfeiture for the second day and each successive day the violation occurred. These calculations are set forth in Table 1 below:

Table 1: Calculation of Base Forfeiture Penalty

Number of Entities	Time Period	Days of Continuing Violation	Base
1	June 9, 2018 to January 4, 2019	209	$560,000
80	June 9, 2018 to February 8, 2019	244	$51,800,000
		Total:	**$52,360,000**

Accordingly, we find T-Mobile apparently liable for a forfeiture in the amount of $52,360,000 for its apparent violations of section 222 of the Act and section 64.2010 of our rules.

85. Apparent Violations of Section 222(c)(1) of the Act and Section 64.2007(b) of the Commission's Rules. Although we find that T-Mobile apparently violated the Act and our rules for its unauthorized disclosures of CPNI to Hutcheson, the one-year statute of limitations bars any forfeiture for those violations.[200] We thus instead exercise our discretion to admonish T-Mobile for its unauthorized disclosures of CPNI to Hutcheson.[201]

[198] *See, e.g., Advantage Telecommunications Corp.*, Forfeiture Order, 32 FCC Rcd 3723 (2017); *Preferred Long Distance, Inc.*, Forfeiture Order, 30 FCC Rcd 13711 (2015).

[199] LOI Response at 10.

[200] *See* 47 U.S.C. § 503(b)(6)(B).

[201] *See, e.g.*, *WDT World Discount Telecommunications Co., Inc.*, Notice of Apparent Liability for Forfeiture and Admonishment, 31 FCC Rcd 12571 (EB 2016); *Life on the Way Communications, Inc.*, Notice of Apparent Liability for Forfeiture and Admonishment, 28 FCC Rcd 1346 (EB-SED 2013); *Locus Telecommunications, Inc.*, Notice of Apparent Liability for Forfeiture and Admonishment, 26 FCC Rcd 17073 (EB 2011).

86. Unlike other federal agencies,[202] the Commission's authority to propose a monetary forfeiture for violations by a common carrier such as T-Mobile is statutorily limited to the one-year period before issuance of the associated notice of apparent liability.[203] In this case, Hutcheson's unauthorized access to T-Mobile customer location information ceased by April 2017, when he was arrested by the FBI and state law enforcement authorities. Thus, the statute of limitations on these violations ran out in April 2018, one month before the unauthorized disclosures even came to light in the May 2018 *New York Times* report. As the Act states and courts have affirmed, the countdown clock on the Commission's statutory deadline for action begins when a violation *occurs*, rather than when it is discovered.[204] Accordingly, we are prohibited by statute from imposing a forfeiture penalty when the underlying violation occurred years ago, as was the case with T-Mobile's unauthorized disclosures to Hutcheson.

87. Upward Adjustment. Given the totality of the circumstances, and consistent with the Commission's *Forfeiture Policy Statement*,[205] we also conclude that a significant upward adjustment is warranted. The responsibility for safeguarding the location information of its customers rested squarely on the Company, making it highly culpable. T-Mobile knew as early as July 2017, when it learned that LocateUrCell was operating an unapproved campaign, that relying on provisions in its contract with LocationSmart was not at all successful at protecting customer location information against misuse.[206] By that time, it knew that the measures it was relying upon to limit use of CPNI to approved campaigns were inadequate because LocateUrCell was easily able to use the campaign ID of its approved campaign for location requests associated with an unapproved use.[207] Its apparent failure to take account of that incident to swiftly recognize the systematic flaws in its safeguards after the *New York Times* report warrants a substantial upward adjustment.

88. In addition, designing a program that disclosed CPNI to location-based service providers based on the "implicit consent" of its customers shows reckless disregard for the statutory and regulatory requirements applicable to CPNI generally and to customer location information specifically.[208] Although T-Mobile claims in its response to the Bureau's supplemental LOI that it "treats Customer Location Information that is CPNI as it does all CPNI,"[209] that is hard to reconcile with its admission that it has

---

[202] In contrast to the one-year limitation on Commission investigation and action, many other federal agencies—including but not limited to the Federal Trade Commission—enjoy a five-year statute of limitations period within which to investigate and pursue civil penalties. *See* 28 U.S.C. § 2462 (providing, in part, "Except as otherwise provided by Act of Congress, an action, suit or proceeding for the enforcement of any civil fine, penalty, or forfeiture, pecuniary or otherwise, shall not be entertained unless commenced within five years from the date when the claim first accrued. . .").

[203] *See* 47 U.S.C. § 503(b)(6)(B). Notwithstanding the one-year statute of limitations, the Enforcement Bureau can and frequently does enter into agreements with the targets of investigations in order to pause the statute of limitations while an investigation is underway. These agreements are commonly referred to as "tolling agreements." In this investigation, the Enforcement Bureau entered into a tolling agreement with T-Mobile so that we may assess penalties for conduct going as far back as April 30, 2018.

[204] *See* 47 U.S.C. § 503(b)(6)(B); *see also Gabelli v. SEC*, 568 U.S. 442, 450 (2013) (holding that "discovery rule" for delaying commencement of statute of limitations is inapplicable to civil enforcement action by Securities and Exchange Commission, and observing that "[t]here are good reasons why the fraud discovery rule has not been extended to Government enforcement actions for civil penalties").

[205] *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).

[206] *See supra* Part II.B.3.

[207] *See supra* paras. 70-71.

[208] *See supra* paras. 63-64.

[209] Supplemental LOI Response at 9, Response to Question 3.

apparently relied on merely implicit consent to establish a customer's approval given that the Commission's CPNI Rules plainly require "opt-in approval" for such uses.

89. The violations at issue occurred over an extended period of time and placed consumers at significant risk of harm. Moreover, the harm included the potential 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. In this case, the risk was not merely theoretical; Hutcheson did in fact obtain the precise location of multiple Missouri State Highway Patrol officers on numerous occasions.

90. We find that an upward adjustment of 75% above the $52,360,000 base forfeiture, or the amount of $39,270,000, is justified in these circumstances, will protect the interests of consumers, and deter entities from violating the Commission's rules in the future.[210]

91. Therefore, after applying the *Forfeiture Policy Statement*, section 1.80 of the Commission's rules, and the statutory factors, we propose a total forfeiture of $91,630,000, for T-Mobile's apparent willful and repeated violations of section 222 of the Act[211] and section 64.2010 of the Commission's rules.[212]

IV. REQUESTS FOR CONFIDENTIALITY

92. T-Mobile has requested that some of the materials it submitted to the Commission in this matter be withheld from public inspection, pursuant to section 0.459 of our rules.[213] With respect to the particular information set forth in this Notice of Apparent Liability, with the exception of the name of T-Mobile's consultant, we conclude that there is a significant public interest in revealing this information to the public by publicly releasing an almost entirely unredacted version of this *Notice*. We further conclude that this interest outweighs whatever competitive harms to T-Mobile and others might result from the disclosure of this information, and therefore partially deny T-Mobile's request.

93. The Commission may publicly reveal even otherwise confidential business information if, after balancing the public and private interests at stake, it finds that it would be in the public interest to do so.[214] At the outset, we find a strong public interest in the public knowing T-Mobile's practices with

---

[210] *See, e.g.*, *Forfeiture Policy Statement*, 12 FCC Rcd at 17098, para. 20 (recognizing the relevance of creating the appropriate deterrent effect in choosing a forfeiture); *see also* 47 CFR § 1.80(b)(8), Note to paragraph (b)(8) (identifying upward adjustment criteria for section 503 forfeitures).

[211] 47 U.S.C. § 222.

[212] 47 CFR § 64.2010.

[213] T-Mobile requested confidential treatment of only a limited amount of information in its responses to the Letters of Inquiry sent by the Bureau and, in subsequent correspondence, further narrowed its request. It currently seeks confidential treatment only with respect to (a) the names of the entities that contracted with LocationSmart and Zumigo to obtain T-Mobile customer location data, except for those entities whose names are already public; (b) the name of the third-party consultant that assisted T-Mobile with the 2016 and 2018 risk assessments; and (c) the information regarding potential future business plans appearing on page 15 of its LOI Response. E-mail from David Solomon, Wilkinson Barker Knauer LLP, Counsel for T-Mobile USA, Inc., to Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau (Feb. 20, 2020, 19:02 ET) (on file in EB-TCD-18-00027702) (Solomon Feb. 20 E-mail).

[214] *See Establishing the Digital Opportunity Data Collection, Modernizing the FCC Form 477 Data Program,* Report and Order and Second Further Notice of Proposed Rulemaking, 34 FCC Rcd 7505, 7522-23, para. 40 & n.100 (2019) (noting long-established authority to release even otherwise confidential information after a balancing of the public and private interests at stake); *American Broadband & Telecommunications Company and Jeffrey S. Ansted*, Notice of Apparent Liability for Forfeiture and Order, 33 FCC Rcd 10308, 10366, para. 184 (2018); *Chrysler v. Brown*, 441 U.S. 281, 292-94 (1979); *Schreiber v. FCC*, 381 U.S. 279, 291-92 (1965); 47 U.S.C. §

respect to the location-based services and customer location information at issue, including to whom the carrier provided access to such information. This conclusion is further supported by both the sensitivity of the location information involved, the large number of customers potentially affected, and the fact that the extent of any additional improper disclosure remains unknown. The public therefore has a strong interest in understanding the facts supporting this *Notice*, so that they can understand the risks, if any, that T-Mobile's practices posed to their location data. We further find that the benefits of revealing the information contained in this *Notice* greatly outweigh any private interest T-Mobile or others may have in keeping confidential the entities with whom T-Mobile shared customer location data. This is all the more true given that T-Mobile argues that it required these entities to obtain affirmative consent from T-Mobile's customers for the sharing of their location data.[215] Thus, the identity of these entities should already be widely known and was required by T-Mobile to be divulged to its affected customers. And to the extent that T-Mobile's customers did not provide their consent, we find that it would be contrary to the public interest to allow the location-based service providers, the intermediaries, the Aggregators, or T-Mobile to keep these identities hidden from, among others, the very customers whose private location information was shared for the commercial benefit of these entities. With respect to T-Mobile's possible future business plans discussed in this *Notice*, we find that the harm, if any, to T-Mobile from making them public would be minimal given both the general and inchoate nature of the plans, as well as T-Mobile's acknowledgment that its competitors are already aware of the plans to the extent they are revealed in this *Notice*.[216]

94. Because T-Mobile's requests are being ruled on by the Commission, and not the Bureau, in the first instance, we will not release the unredacted version of this *Notice* for 10 business days to allow T-Mobile or a relevant third party to file a petition for reconsideration;[217] if any party avails themselves of this opportunity, we will continue to withhold the information from public inspection until we have ruled on the petition(s).[218] If, after 10 business days, T-Mobile or a relevant third party has not filed a petition for reconsideration or sought a judicial stay with regard to this partial denial of T-Mobile's confidentiality request, the material will be made publicly available.[219]

V. ORDERING CLAUSES

95. Accordingly, **IT IS ORDERED** that, pursuant to section 503(b) of the Act[220] and section 1.80 of the Commission's rules,[221] T-Mobile USA, Inc. is hereby **NOTIFIED** of this **APPARENT LIABILITY FOR A FORFEITURE** in the amount of ninety-one million, six hundred thirty thousand dollars ($91,630,000) for willful and repeated violations of section 222 of the Act[222] and section 64.2010 of the Commission's rules.[223]

154(j) ("The Commission may conduct its proceedings in such manner as will best conduce to the proper dispatch of business and the ends of justice."); 47 CFR § 0.461(f)(4).

[215] LOI Response at 7-8, Introduction.

[216] *See* Solomon Feb. 20 E-mail.

[217] The Aggregators, intermediaries, and location-based service providers, to the extent that they are third-party owners of some of the information for which T-Mobile has requested confidential treatment, may file a petition for reconsideration with respect to their own information.

[218] *Cf.* 47 CFR § 0.459(g).

[219] *See id*. § 0.455(g).

[220] 47 U.S.C. § 503(b).

[221] 47 CFR § 1.80.

[222] 47 U.S.C. § 222.

[223] 47 CFR § 64.2010.

96. **IT IS FURTHER ORDERED** that T-Mobile USA, Inc. is hereby **ADMONISHED** for its apparent violations of section 222(c) of the Act[224] and section 64.2007 of the Commission's rules.[225]

97. **IT IS FURTHER ORDERED** that, pursuant to section 1.80 of the Commission's rules,[226] within thirty (30) calendar days of the release date of this Notice of Apparent Liability for Forfeiture, T-Mobile USA, Inc. **SHALL PAY** the full amount of the proposed forfeiture or **SHALL FILE** a written statement seeking reduction or cancellation of the proposed forfeiture consistent with paragraphs 97-98 below.

98. T-Mobile USA, Inc. shall send electronic notification of payment to Michael Epshteyn and Rosemary Cabral, Enforcement Bureau, Federal Communications Commission, at michael.epshteyn@fcc.gov and rosemary.cabral@fcc.gov on the date said payment is made. Payment of the forfeiture must be made by credit card, ACH (Automated Clearing House) debit from a bank account using the Commission's Fee Filer (the Commission's online payment system),[227] or by wire transfer. 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:[228]

- Payment by wire transfer must be made to ABA Number 021030004, receiving bank TREAS/NYC, and Account Number 27000001. A completed Form 159 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 may result in payment not being recognized as having been received. When completing FCC Form 159, 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).[229] 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 the Commission's Fee Filer website at https://apps.fcc.gov/FeeFiler/login.cfm. To pay by credit card, log-in using the FRN captioned above. If payment must be split across FRNs, complete this process for each FRN. Next, select "Pay bills" on the Fee Filer Menu, and select the bill number associated with the NAL Account – the bill number is the NAL Account number with the first two digits excluded – and then 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 the Commission's Fee Filer website at https://apps.fcc.gov/FeeFiler/login.cfm. To pay by ACH, log in using the FRN captioned above. If payment must be split across FRNs, complete this process for each FRN. Next, select "Pay bills" on the Fee Filer Menu and then select the bill number associated to the NAL Account – the bill number is the NAL Account number with the first two digits excluded – and choose the "Pay from Bank Account" option. Please contact the appropriate financial institution to confirm the correct Routing Number and the correct account number

[224] 47 U.S.C. § 222(c).

[225] 47 CFR § 64.2007.

[226] *Id*. § 1.80.

[227] Payments made using the Commission's Fee Filer system do not require the submission of an FCC Form 159.

[228] For questions regarding payment procedures, please contact the Financial Operations Group Help Desk by phone at 1-877-480-3201 (option #6), or by e-mail at ARINQUIRIES@fcc.gov.

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

from which payment will be made and verify with that financial institution that the designated account has authorization to accept ACH transactions.

99. Any request for making full payment over time under an installment plan should be sent to: Chief Financial Officer—Financial Operations, Federal Communications Commission, 445 12th Street, SW, Room 1-A625, Washington, DC 20554.[230] Questions regarding payment procedures should be directed to the Financial Operations Group Help Desk by phone, 1-877-480-3201, or by e-mail, ARINQUIRIES@fcc.gov.

100. The written statement seeking reduction or cancellation of the proposed forfeiture, if any, must include a detailed factual statement supported by appropriate documentation and affidavits pursuant to sections 1.16 and 1.80(f)(3) of the Commission's rules.[231] The written statement must be mailed to the Office of the Secretary, Federal Communications Commission, 445 12th Street, SW, Washington, DC 20554, ATTN: Enforcement Bureau – Telecommunications Consumers Division, and must include the NAL/Account Number referenced in the caption. The statement must also be e-mailed to Michael Epshteyn at michael.epshteyn@fcc.gov and Rosemary Cabral at rosemary.cabral@fcc.gov.

101. The Commission will not consider reducing or canceling a forfeiture in response to a claim of inability to pay unless the petitioner submits: (1) federal tax returns for the most recent three-year period; (2) financial statements prepared according to generally accepted accounting practices; or (3) some other reliable and objective documentation that accurately reflects the petitioner's current financial status. Any claim of inability to pay must specifically identify the basis for the claim by reference to the financial documentation.

102. **IT IS FURTHER ORDERED**, pursuant to section 0.459(g) of the Commission's rules,[232] that the Requests for Confidential Treatment filed by T-Mobile USA, Inc. in this proceeding **ARE DENIED IN PART**, to the extent specified herein.

103. **IT IS FURTHER ORDERED** that a copy of this Notice of Apparent Liability for Forfeiture shall be sent by first class mail and certified mail, return receipt requested, to Christopher Koegel, Director, Federal Regulatory Affairs, T-Mobile US, Inc., 601 Pennsylvania Ave., N.W., Suite 800, Washington, DC 20004, and David Solomon, Wilkinson, Barker, Knauer LLP, 1800 M Street N.W., Suite 800 N, Washington, DC 20036.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

[230] *See* 47 CFR § 1.1914.

[231] 47 CFR §§ 1.16, 1.80(f)(3).

[232] 47 CFR § 0.459(g).

STATEMENT OF
CHAIRMAN AJIT PAI

Re: *T-Mobile USA, Inc.*, File No.: EB-TCD-18-00027702.

For most Americans, their wireless phone goes wherever they go. And every phone must constantly share its—and its owner's—location with a wireless carrier in order to enable the carrier to know where to route calls. Information about a customer's location is highly personal and sensitive. As the U.S. Supreme Court has observed, this type of information "provides an intimate window into a person's life."[1] This makes it critical that all telecommunications carriers protect the confidentiality of their customers' location information. Congress has made this requirement clear in the Communications Act. And the Commission has made this requirement clear in its implementing rules.

Today, we also make clear that we will not hesitate to vigorously enforce these statutory provisions and regulations. After a thorough investigation, we find that all of our nation's major wireless carriers apparently failed to comply with these vitally important requirements. In brief, long after these companies were on notice that their customers' location data had been breached, they continued to sell access to that data for many months without taking reasonable measures to protect it from unauthorized disclosure. This FCC will not tolerate any telecommunications carrier putting American consumers' privacy at risk. We therefore propose fines against these four carriers totaling more than $200 million.

For their diligent work on this item, I'd like to thank Rosemary Cabral, Rebecca Carino, Michael Epshteyn, Rosemary Harold, Jermaine Haynes, Erica McMahon, Ann Morgan, Shannon Lipp, Tanishia Proctor, Nakasha Ramsey, Phil Rosario, Mika Savir, Daniel Stepanicich, David Strickland, Raphael Sznajder, Kristi Thompson, David Valdez, and Shana Yates of the Enforcement Bureau; Justin Faulb, Lisa Hone, Melissa Kirkel, Kris Monteith, and Zach Ross of the Wireline Competition Bureau; Martin Doczkat, Aspasia Paroutsas, and Robert Pavlak of the Office of Engineering and Technology; Michael Carlson, Douglas Klein, Marcus Maher, Linda Oliver, Joel Rabinovitz, and Bill Richardson of the Office of General Counsel; and Virginia Metallo of the Office of Economics and Analytics. Our Enforcement Bureau staff reviewed more than 50,000 pages of documents during the course of this complex investigation, and their painstaking efforts to uncover the details of what happened enabled us to take this strong enforcement action. While this nitty-gritty investigative work is not glamorous and can take longer than some in the peanut gallery might like, it is indispensable to building a case that will stand up in a court of law rather than only garnering some headlines.

[1] *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018).

STATEMENT OF
COMMISSIONER MICHAEL O'RIELLY

Re: *T-Mobile USA, Inc.*, File No.: EB-TCD-18-00027702.

The pocket-sized technology that nearly everyone carries today is capable of amazing functionality, including the ability to pinpoint exact locations, which has recognizable benefits. Yet, this technology can be used for nefarious purposes as well. The privacy breaches that were reported in the press related to these notices of apparent liability (NALs) are serious and warrant further investigation to determine exactly what happened, whether the parties violated current law, and if so, how such events can be prevented in the future. There is enough evidence contained within these four documents to warrant NALs, and as such I will vote to approve. However, it should be noted that I do so with serious reservations. I would have expected more well-reasoned items than what is presented here, especially given the yearlong plus investigation. Significant revisions and a more in-depth discussion of what occurred will be necessary before I will consider supporting any forfeiture.

Specifically, I am concerned that we do not have all the relevant facts before us, and that we either haven't heard or sufficiently considered counter arguments from AT&T, Sprint, T-Mobile, and Verizon. Not only was additional information filed just days ago, but when the parties discussed these cases with my office, it was readily apparent that the record was incomplete. It is also unclear as to whether the Commission has a firm grasp of the services that were actually being offered to consumers, when these services were offered and/or terminated, and whether many of the location-based offerings included to justify the substantial proposed fines were involved in any actual violations. It also would have been preferable to engage the parties in conversation prior to issuing the NALs, to establish a more solid foundation from which to consider appropriate penalties. The parties appear to have had barely any chance to discuss the potential violations and the legal basis behind the NALs with the Enforcement Bureau's investigators, which undermined their opportunity to explain their underlying practices and ultimately shed more light on the whole situation.

Equally important, I am not convinced that the location information in question was obtained as the result of a "call" or as part of a "telecommunications service," raising questions about the application of our section 222 authority. The item seems to rely on the argument that these companies obtain location information solely to connect the device to the network for the purpose of sending and receiving voice calls. That seems to be a major stretch, because the same connection is needed in order to send data, which is not a telecommunications service under the Commission's sound decision to declare it a Title I service. Beyond the important jurisdictional concern relating to the breadth of our legal authority, more facts are needed to contemplate all of the various applications at issue and how the location information is obtained.

In the end, I am hopeful that these issues can be sorted out, especially when AT&T, Sprint, T-Mobile, and Verizon reply to these NALs. I look forward to developing a fulsome record and discussing these alleged violations with the parties. I want to be clear that I remain open minded on this entire matter.

STATEMENT OF
COMMISSIONER JESSICA ROSENWORCEL
DISSENTING

Re: *T-Mobile USA, Inc.*, File No.: EB-TCD-18-00027702.

This investigation is a day late and a dollar short. Our real-time location information is some of the most sensitive data there is about us, and it deserves the highest level of privacy protection. It did not get that here—not from our nationwide wireless carriers and not from the Federal Communications Commission. For this reason, I dissent.

Everywhere we go our smartphones follow. They power the connections that we count on for so much of modern life. But because they are always in our palms and pockets, they are collecting gobs of data about everything we are doing—and where we are doing it.

That means our phones know our location at any given moment. This geolocation data is especially sensitive. It's a record of where we've been and by extension, who we are. If it winds up in the wrong hands, it could provide criminals and stalkers with the ability to locate any one of us with pinpoint accuracy. It could be sold to domestic abusers or anyone else who wishes to do us harm. Its collection and distribution or sale without our permission or without reasonable safeguards in place is a violation of our most basic privacy norms. It's also a violation of the law.

But what we've learned is that it happened anyway. In May 2018, *The New York Times* reported that our wireless carriers were selling our real-time location information to data aggregators. Then in January 2019 *Motherboard* revealed that bounty hunters and other shady businesses had access to this highly sensitive data. Further reporting by *Vice* pieced together just how this sensitive data wound up in the hands of hundreds of bounty hunters who were willing to sell it to anyone for just a few hundred dollars. It turns out wireless carriers sold access to individual real-time location information to data aggregators, who then sold it to a skip-tracing firm, who then sold it to a bail-bond company, who then sold it to individual bounty hunters.

If that sounds like a tortured chain of data possession, it is. And if you don't remember giving this kind of permission or signing up for the sale of your geolocation data on a black market, you're not alone. Comb through your wireless contract, it's a good bet there is nothing in there that discloses your carrier could monetize your real-time location in this way.

It should have been simple for the FCC to take action to stop this practice under Section 222 of the Communications Act. But that didn't happen. Instead, for months this agency said nothing except that it was investigating. It did not provide the public with any details, despite the ongoing risk to the security of every one of us with a smartphone. As a result, the sale of our most sensitive location information continued for far too long under the watch of this agency.

All told, taking nearly two years to address these troubling revelations is a stain on this agency's public safety record. It's a testament to how little it makes privacy a priority.

That's why starting last year I took on this issue on my own. I took to television and spoke on cable and broadcast news about how a black market was developing where anyone could buy information about where we are and what we are doing based on location data from our wireless devices. I wrote every nationwide wireless carrier and asked them to state whether they had ended their arrangements to sell location data and what steps they were taking to secure any data that had already been shared. I made these letters public. I also made public the responses. In the course of doing so, I am pleased to report that I was able to secure the first public statements from inside this agency about what carriers were doing with our location information.

I am also pleased that at my request the FCC is taking the necessary steps to remove redactions in the text of this long-awaited enforcement action that would have covered up exactly what happened with our location data. We should care more about protecting the privacy of consumers than the privacy of companies' business practices—especially when they violate the law.

However, in the end I find this enforcement action inadequate. There are more than 270 million smartphones in service in the United States and this practice put everyone using them at a safety risk. The FCC heavily discounts the fines the carriers could owe under the law and disregards the scope of the problem.

Here's why. At the outset, the FCC states that this impermissible practice should be the subject of a fine for every day that it was ongoing. But right at the outset the agency gives each carrier a thirty-day pass from this calculation. This thirty day "get-out-of-jail-free" card is plucked from thin air. You'll find it in no FCC enforcement precedent. And if you compare it to every data security law in the country, this stands as an outlier. In fact, state privacy laws generally require companies to act on discovered breaches on a much faster timetable—in some cases, less than a week. Real-time location data is some of the most sensitive information available about all of us and it deserves the highest level of privacy protection. Permitting companies to turn a blind eye for thirty days after discovering this data is at risk falls short of any reasonable standard.

Next, the FCC engages in some seriously bureaucratic math to discount the violations of our privacy laws. The agency proposes a $40,000 fine for the violation of our rules—but only on the first day. For every day after that, it imposes only a $2,500 fine for the same violation. But it offers no acceptable justification for reducing the fine in this way. Plus, given the facts here—the sheer volume of those who could have had their privacy violated—I don't think this discount is warranted.

In sum, it took too long to get here and we impose fines that are too small relative to the law and the population put at risk. But this effort is far from over. Because when the FCC releases a Notice of Apparent Liability, it is just early days. The fines are not final until after the carriers that are the subject of this action get a chance to respond. That means there is still work to do—and this agency cannot afford to wait another year to do it. If past practice is any guide, we all have reason to be concerned.

STATEMENT OF COMMISSIONER GEOFFREY STARKS
APPROVING IN PART AND DISSENTING IN PART

Re: *T-Mobile USA, Inc.*, File No.: EB-TCD-18-00027702.

Taking control of our personal information is one of the defining civil rights issues of our generation. Practically every day, we learn about new data harms: algorithmic and facial recognition bias; companies failing to protect our most sensitive information from hackers and thieves; and "pay to track" schemes that sell location information to third parties. These practices put all Americans at risk, and they are especially insidious because they replicate and deepen existing inequalities in our society.

In recent months, consumers have become increasingly aware of how much private information trails behind them as they go about their days. In December 2019, the New York Times opinion series *One Nation, Tracked* brought renewed focus to the issue of smartphone tracking.[1] Their stories illustrated, sometimes in frightening detail, how much can be learned about a person from the location of their smartphone. Using supposedly anonymous location data, the Times was able to follow the movements of identifiable Americans, from a singer who performed at President Trump's inauguration to President Trump himself.

The findings by journalists at the New York Times, Motherboard, and many other outlets unsettle us for good reason. Your location at any time goes to the heart of personhood—where you live, who you see, where you go, and where you worship. And tracking over time can build a picture of a life in intimate detail. Disclosure of those coordinates and patterns isn't just creepy; it can leave us vulnerable to safety threats and intrusions never before possible on such a comprehensive scale. And because people of color rely more heavily on smartphones for internet access than other Americans, they bear these harms disproportionately.

For those "freaked out" by their reporting, the Times offered a number of steps consumers can take to limit access to the location data, including blocking location sharing and disabling mobile advertising IDs. Those can be good steps, but they are no defense against your wireless carrier. Your carrier needs to know where you are to complete your calls. Because it is simply impossible to use a mobile phone—an important part of participation in our modern economy—without giving location data to one of the carriers, our rules about how that they can use customer location data must be strict and strictly enforced.

For that reason, I am pleased that the Notices of Apparent Liability we vote on today confirm that misuse of customer location data by AT&T, Verizon, Sprint, and T-Mobile violate the Commission's rules. These serious violations damaged Americans' faith in our telephone system, and I am pleased that we have reached bipartisan agreement that enforcement is appropriate here. I cannot fully approve these Notices, however, because in conducting these investigations and determining the appropriate penalty, we lost track of the most important part of our case—the very consumers we are charged with protecting. Because I strongly believe we should have determined the number of customers impacted by the abuses and based our forfeiture calculations on that data—calculations that would have been possible if we had investigated more aggressively—I must dissent in all remaining parts of the item.

Enforcement Authority

Congress has clearly directed carriers to protect our location information, and these Notices confirm that this protection exists even when no call is in progress. Going forward, there should be no dispute about this basic legal conclusion.

[1] Stuart A. Thompson and Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy," New York Times (Dec. 19, 2019).

This is a responsibility that can't be delegated away. Carriers are responsible for the actions of their agents and sub-contractors. This is a well-established principle, and it recognizes the special nature of the customer-carrier relationship. We trust our wireless carrier to provide high-quality service, and we don't expect that our carrier is going to monetize that relationship.

None of these carriers should be surprised that we take the protection of customer data so seriously. In 2007, the Commission addressed the problem of "pretexting," where data brokers would impersonate customers to fool carriers into disclosing confidential customer information. We revamped our rules and, for the first time, required that carriers obtain "opt-in" consent to the disclosure of customer information, rather than presenting it as an "opt-out."

Regrettably, these investigations show that carriers did not heed that warning. Despite the clear message from the FCC, these carriers did not treat the protection of their customers' data as a key responsibility. Instead, they delegated responsibility for protecting this sensitive information to aggregators and third-party location service providers. They subjected these arrangements to varying degrees of oversight, but all were ineffective and failed to prevent the problem. Significant penalties are more than justified.[2]

Delays

Today's action has been too long delayed. As the Notices point out, the Commission has been investigating these matters for nearly two years. And the investigations show that, even after the problems with their location data sharing programs became readily apparent, the carriers took months to shut them down. Indeed, nearly one year ago, I published an op-ed in the NY Times about the slow pace of this investigation, and the need for the FCC to "act swiftly and decisively to stop illegal and dangerous pay-to-track practices."[3] I had no idea it would be another 11 months before we finally acted.

From the beginning, it has been difficult to get the facts straight. The carriers repeatedly told the public that they were stopping their location sharing program while hiding behind evasive language and contractual terms. For example, on June 15, 2018, Verizon told Senator Ron Wyden, "[w]e are initiating a process to terminate our existing agreements for the location aggregator program."[4] But Verizon didn't terminate its aggregator agreements until November 2018, and didn't end all of its location data sharing programs until April 2019. With respect to the other carriers, on June 19, 2018, the Washington Post reported:

> AT&T then said in a statement Tuesday that it also will be ending its relationship with location data aggregators "as soon as practical" while ensuring that location-based services that depend on data sharing, such as emergency roadside assistance, can continue

[2] In fact, just a few years ago, the Enforcement Bureau entered into multi-million-dollar consent decrees with these same carriers involving a similar problem— the unauthorized billing of customers by third-party vendors where the carriers sought to delegate their consumer protection responsibility via contract. As in the cases at issue here, the carriers claimed that they weren't responsible for unlawful billing because their contracts had requirements placing any responsibility on the downstream companies. The carriers we find liable today did a fundamental disservice to their customers when they simply "passed the buck" to these location data aggregators and service providers. Failure to supervise their agents is no defense. *See Cellco Partnership d/b/a Verizon Wireless,* Order and Consent Decree, 30 FCC Rcd 4590 (Enf. Bur. 2015) (requiring $90 million in payments and restitution to consumers to settle allegations that Verizon charged consumers for third-party products and services that the consumers did not authorize; *Sprint Corp.,* Order and Consent Decree, 30 FCC Rcd 4575 (Enf. Bur. 2015) ($68 million); *AT&T Mobility LLC,* Order and Consent Decree, 29 FCC Rcd 11803 (Enf. Bur. 2014) (($105 million); *T-Mobile USA, Inc.*, Order and Consent Decree, 29 FCC Rcd 15111 (Enf. Bur. 2014) ($90 million).

[3] Geoffrey Starks, "Why It's So Easy for a Bounty Hunter to Find You," New York Times (April 19, 2019).

[4] Letter from Karen Zacharia, Chief Privacy Officer, Verizon, to Senator Ron Wyden, dated June 15, 2018.

> to function. Sprint said in a statement that it cut ties with LocationSmart on May 25, and has begun cutting ties with the data brokers who received its customers' location data.
>
> T-Mobile chief executive John Legere tweeted: "I've personally evaluated this issue & have pledged that @tmobile will not sell customer location data to shady middlemen."[5]

Despite these statements, each of these carriers continued to sell their customers' location data for *months* afterwards. Americans deserve better.

For its part, the FCC also failed to act with sufficient urgency. As a former enforcement official, I recognize the challenges of reviewing the tens of thousands of pages of documents produced in these investigations, but we have conducted similarly extensive investigations much faster. Indeed, we took less time to resolve the highly complex merger between T-Mobile and Sprint, which involved mountains of pages of materials. Given the seriousness of the violations here, the Commission should have invested the resources necessary to get a draft to the Commission faster. By allowing this investigation to drag on when we knew that important public safety and public policy issues were at stake, we failed to meet our responsibilities to the American people.

Consumer Harms

I am concerned that the penalties proposed today are not properly proportioned to the consumer harms suffered because we did not conduct an adequate investigation of those harms. The Notices make clear that, after all these months of investigation, the Commission still has no idea how many consumers' data was mishandled by each of the carriers. I recognize that uncovering this data would have required gathering information from the third parties on which the carriers' relied. But we should have done that via subpoenas if necessary. We had the power—and, given the length of this investigation, the time—to compel disclosures that would help us understand the true scope of the harm done to consumers. Instead, the Notices calculate the forfeiture based on the number of contracts between the carriers and location aggregators, as well as the number of contracts between those aggregators and third-party location-based service providers. That is a poor and unnecessary proxy for the privacy harm caused by each carrier, each of which has tens of millions of customers that likely had their personal data abused. Under the approach adopted today, a carrier with millions more customers, but fewer operative contracts, would get an unfairly and disproportionately lessened penalty. That is inconsistent with our approach in other consumer protection matters and cannot stand.[6] More importantly, basing our forfeiture on a carrier's number of aggregator contracts cannot be squared with our core mission today – to vindicate harmed consumers first and foremost.

---

[5] Brian Fung, "Verizon, AT&T, T-Mobile and Sprint Suspended Selling of Customer Location Data After Prison Officials Were Caught Misusing It," Washington Post (June 19, 2018).

[6] *See, e.g., Scott Rhodes A.K.A. Scott David Rhodes, Scott D. Rhodes, Scott Platek, Scott P. Platek,* Notice of Apparent Liability for Forfeiture, FCC 20-9, 2020 WL 553616 (rel. Jan. 31, 2020) (spoofed robocall violations; calculates the proposed forfeiture of $12,910,000 by assessing a base forfeiture of $1,000 per each of 6,455 verified unlawful spoofed robocalls with a 100% upward adjustment); *Kenneth Moser dba Marketing Support Systems*, Notice of Apparent Liability for Forfeiture, FCC 19-135, 2019 WL 6837865 (rel. Dec. 13, 2019) (spoofed robocall violations; calculates the proposed forfeiture of $9,997,750 by assessing a base forfeiture of $1,000 per each of 5,713 analyzed/verified calls with a 75% upward adjustment); *Long Distance Consolidated Billing Company*, Notice of Apparent Liability for Forfeiture, 30 FCC Rcd 8664 (2015) (slamming and cramming violations; calculates $2.3 million forfeiture by assessing a $40,000 forfeiture for each unlawful bill plus an upward adjustment for misrepresentation) (subsequent history omitted); *Neon Phone Service,* Notice of Apparent Liability for Forfeiture, 32 FCC Rcd 7964 (2017) (slamming and cramming violations; proposing a $3.9 million forfeiture by assessing a base forfeiture of $40,000 for each unlawful bill plus an upward adjustment for egregiousness). *See also TerraCom, Inc. and YourTel America, Inc.,* Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325 (2014) (in proposing a forfeiture for Section 222 violations, citing the number of personal data records exposed by a carrier as the key factor, ultimately resulting in a penalty figure of $8.5 million) (subsequent history omitted).

Make no mistake – there are real victims who've had their privacy and security placed in harm's way. Each of them has a story. As discussed in the Notices, in May 2018, the *New York Times* reported that then-Missouri Sheriff Cory Hutcheson had used Securus technologies, a vendor that all of these wireless carriers allowed to access their customer location data, to conduct thousands of unauthorized location requests, accessing the locations of multiple individuals, including his predecessor as Sheriff, a Missouri Circuit Judge, and at least five highway patrol officers.[7] But I've personally spoken at length with one of those officers, retired Missouri State Highway Patrol Master Sergeant William "Bud" Cooper.

MSgt. Cooper told me that, while leading a homicide unit with the State Highway Patrol, he would investigate cases in the Missouri county where Cory Hutcheson was Sheriff. As they worked together on investigations, M.Sgt. Cooper noticed Hutcheson following up on leads and locating witnesses and suspects very quickly. M.Sgt. Cooper initially thought Hutcheson just had a particularly effective network of informants, but then grew suspicious and asked Hutcheson about his methods. Hutcheson eventually told him that he was using a Securus program to "ping" phone numbers from the investigations to uncover people's locations.

M.Sgt. Cooper suspected "something dirty" was going on. M.Sgt. Cooper began to wonder, based on Hutcheson's behavior towards him and his state trooper colleagues, if Hutcheson was targeting their phones too.

When M.Sgt. Cooper's worst fears were confirmed—that he had been targeted, along with his colleagues and a narcotics investigator—he was "shocked and angry." "I felt violated." This was personal information, akin to "going into someone's home." M.Sgt. Cooper found it "appalling" when it turned out that Hutcheson was obtaining this information based solely on woefully insufficient supporting documentation, including parts of an instruction manual, his vehicle maintenance records, and even an insurance policy. Hutcheson had personally "pinged" phones without authorization "over 2,000 times, and nobody checked."

M.Sgt. Cooper related that the revelations of Hutcheson's spying have threatened the safety of officers in the community and their informants. He reported that it has become harder to convince witnesses to trust police and talk to them, particularly in communities where witnesses fear retaliation. He has devoted his career to upholding the honor and integrity of law enforcement, but with the Hutcheson scandal "we all took a black eye."

M.Sgt. Cooper's story is but one single account of the harm done by the carriers; but we know there are many—perhaps millions—of additional victims, each with their own harms. Unfortunately, based on the investigation the FCC conducted, we don't even know how many there were, and the penalties we propose today do not reflect that impact.

This ignorance not only highlights a problem with today's decisions but a gap in our policymaking. The Commission needs to consider policy changes to protect the rights of consumers. Specifically, we should initiate a rulemaking to require carriers to inform consumers when there has been a breach of their confidential data, so that individual can take steps to protect themselves.

Even setting aside my concerns that our forfeitures are not pegged to the number of consumers harmed, I would still object to the amount of the proposed forfeiture to T-Mobile. It should be higher. As discussed in the Notice, T-Mobile had clear notice back in July 2017 that its contractual protections were failing to prevent location-based service providers from misusing customer location information. T-Mobile knew that one of these service providers was taking customer information and selling it to "bail bonding and similar companies"—aka, bounty hunters. Despite T-Mobile's knowledge of the problem, it took *two months* for the carrier to contact the aggregator company about this issue, and even then, T-Mobile only inquired of the aggregator and reminded it of its contractual obligations. It was the *aggregator* that terminated the service provider's access to T-Mobile customer information soon after hearing from T-Mobile. I believe that T-Mobile was on notice about the problems with its location data

[7] *See, e.g., T-Mobile NAL* at para. 28; *AT&T NAL* at para. 21; *Verizon NAL* at para. 26; *Sprint NAL* at para. 21.

protections back in July 2017 and that the proposed forfeiture amount should reflect that fact – the punishment should fit the crime. Unfortunately, although their legal justification for doing so remains a mystery, a majority of my colleagues disagreed.

Transparency

Our slow response has also impacted our ability to discuss the facts of this case and the Commission's credibility for future investigations. Like other federal agencies, the Commission has a process that allows parties to protect the confidentiality of certain materials submitted to the agency. In their responses to the Bureau's investigation, however, the four carriers named in today's decisions bent that process so far that it is broken. Each of them adopted such an overbroad interpretation of our confidentiality protections that the Enforcement Bureau initially circulated heavily redacted draft decisions that would have made it impossible for the public to understand the key facts in each case.

Sadly, this is not a new phenomenon. The Enforcement Bureau has long struggled with parties asserting overbroad designations of confidentiality. Some parties, including some in these cases, have claimed confidential treatment for nearly the entirety of their responses to the Bureau's Letters of Inquiry, including legal arguments, publicly available facts, and even references to Commission's rules. Both as a former Enforcement Bureau official and as a Commissioner, I have seen such tactics hamstring our ability to vindicate the public interest and deter wrongdoing.

We should have rejected these confidentiality requests—some of which are frankly laughable—as soon as the Bureau reviewed the documents. Instead, many of those assertions were taken at face value, and the original drafts had heavy redactions. It is critical that Americans, particularly the hundreds of millions who use the services of these carriers, understand what happened here. If we let unreasonable and self-serving confidentiality assertions stand, those customers will never have the full picture.

Only after Commissioner Rosenworcel and I objected did the Bureau go back to the parties to challenge the confidentiality requests and negotiate the disclosure of more information. While I am glad that some of the parties reduced their requests, much of this information still remains confidential for now. Some even designated as confidential the number of agreements they had entered with aggregators and location-based service providers. That is frivolous.

The Commission does not have not to tolerate this. Section 0.459 of the Commission's rules establishes a process for resolving confidentiality requests. That process takes time, so we must begin resolving such requests immediately upon receipt. Here, despite the extraordinary length of our investigation, we let this problem fester for too long. Now, because we waited until the orders were before the Commission and then rushed to negotiate with the parties, there is insufficient time for the Section 0.459 process to play out. Even with the reduced redactions, Americans who read these Notices and the news coverage of them today will not have all the facts to which they are entitled. So while I am glad that we are ordering the parties to explain why we should not deny their requests completely, I worry that the carriers will have succeeded in hiding key facts until the spotlight has moved on. The FCC must do better.

* * *

Finally, while today's actions underscore and confirm the power of Section 222, they also highlight the need for additional actions. For example, our action today is limited to the major wireless carriers. But we know from this investigation that they are not the only wrongdoers. Securus, for one example, behaved outrageously. Though Securus holds multiple FCC authorizations, I recognize that there may be legal limitations on the Commission's ability to take enforcement against the company for its misuse of customer location data. But that is no excuse for failing to conduct a comprehensive investigation—including issuing subpoenas to Securus—of the events in question here. That information would have enriched our investigation and could have been provided to other agencies for investigation and enforcement.

Going forward, Americans must be able to place trust in their wireless carriers. I understand that operating businesses at the enormous scale of these companies means relying on third parties for certain services. But these carriers know that the services they offer create risks for users: unauthorized location tracking, SIM hijacking, and billing scams to name just few. Carriers must take responsibility for those people they allow into their operations.

I thank the staff of the Enforcement Bureau for their hard work on these important investigations.