Before the
Federal Communications Commission
Washington, DC 20554

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

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; and Commissioner Starks approving in part, dissenting in part and issuing a statement.

TABLE OF CONTENTS

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. 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

[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/.

[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/.

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 $48,318,750 against Verizon Communications (Verizon 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 Verizon apparently disclosed its customers' location information, without their consent, to a third party who was not authorized to receive it. In addition, even after a highly publicized incident put the Company on notice that its safeguards for protecting customer location information were inadequate, Verizon apparently did not reform them for many months—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 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

[3] *Id.*

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

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

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

[7] 47 U.S.C. § 222(a).

[8] 47 U.S.C. § 222(c), (h)(1)(A) (emphasis added). "Telecommunications service" is defined as "the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used." 47 U.S.C. § 153(53). The mobile voice services provided by Verizon are "telecommunications services." *See* 47 U.S.C. § 332(c)(1); H.R. Conf. Rep. No. 104-458 at 125 (1996) ("This definition [of 'telecommunications service'] is intended to include commercial mobile service.").

[9] 47 CFR § 64.2001 *et seq.*

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. 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, disclosure, or access to CPNI after being given notice of the use, disclosure, or access and not objecting thereto.[13] However, in response to the problem of data brokers on the web selling call detail and other telephone records procured without customer consent,[14] the Commission amended its rules in the *2007 CPNI Order* to require carriers to obtain opt-in approval from a customer before disclosing that customer's CPNI to a carrier's joint venture partner or independent contractor.[15] 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."[16] Given that observation, the Commission concluded that sharing of data with partners and contractors "warrants a requirement of express prior customer authorization,"[17] 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.[18] 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."[19] 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

[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] *See* 47 CFR § 64.2007(b).

[12] 47 CFR § 64.2003(k).

[13] *See* 47 CFR § 64.2003(l).

[14] *2007 CPNI Order*, 22 FCC Rcd at 6928, para. 2.

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

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

[17] *Id.*; *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.").

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

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

provided by a carrier to a joint venture partner or independent contractor.[20] Thus, with limited exceptions, a carrier may only use, disclose, or permit access to CPNI with the customer's opt-in approval.[21]

7. *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."[22] 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."[23] 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.[24] It also adopted password and account notification requirements.[25]

8. 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."[26] 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 reasonable.[27] 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,"[28] while also heeding industry warnings that adopting prescriptive rules detailing specific security practices could be counterproductive.[29] 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.[30] The Commission expected that carriers would employ

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

[21] *See* 47 CFR § 64.2007(b).

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

[23] 47 CFR § 64.2010(a) (emphasis added).

[24] *See* 47 CFR § 64.2010(b)-(d).

[25] *Id.* § 64.2010(e)-(f).

[26] *2007 CPNI Order*, 22 FCC Rcd at 6959–60, para. 65.

[27] *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.

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

[29] *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")).

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

effective protections that are best suited to their particular systems.[31] 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."[32] 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.[33] 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.[34]

9. *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."[35]

10. *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[36] and providers of interconnected Voice over Internet Protocol services.[37] 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.[38]

---

[31] *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.*

[32] 47 CFR § 64.2010(a).

[33] *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.").

[34] 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 a cybersecurity framework which features instructive practices and guidelines for organizations to reference. The publication can be useful in determining whether particular cybersecurity actions are reasonable by comparison. The model cybersecurity 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 Security, Reliability and Interoperability Council, CSRIC Best Practices, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data.

[35] 47 U.S.C. § 217.

[36] 47 U.S.C. § 222.

[37] *2007 CPNI Order*, 22 FCC Rcd at 6954-57, paras 54-59.

[38] 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.").

B. Factual Background

1. Verizon's Wireless Network Services and Customer Location Information

11. Verizon provides mobile voice and data services to consumers throughout the United States by enabling consumer mobile phones to make and receive calls or transmit data on Verizon's wireless network.[39] The mobile phones of Verizon subscribers, like those of customers of other carriers, periodically register with nearby network signal towers.[40] Verizon 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.[41] Because Verizon knows the location of its network signal towers, Verizon is able to calculate the approximate geographic location of the mobile phones communicating with its towers.[42] This type of location information—which is created even when the customer does not have an active established connection, such as a voice call—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.[43] Other widely used 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.[44]

2. Verizon's Location-Based Services Business Model

12. Until March 30, 2019, Verizon provided location-based service providers access to its customers' location information through a chain of contract-based business arrangements.[45] Verizon 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

[39] *See* Verizon Communications, 2018 Annual Report, https://www.verizon.com/about/sites/default/files/2018-Verizon-Annual-Report.pdf.

[40] *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*).

[41] *See* Response to Letter of Inquiry from Verizon to Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, at 4, Response to Question 1 (Oct. 15, 2018) (on file in EB-TCD-18-00027698) (LOI Response).

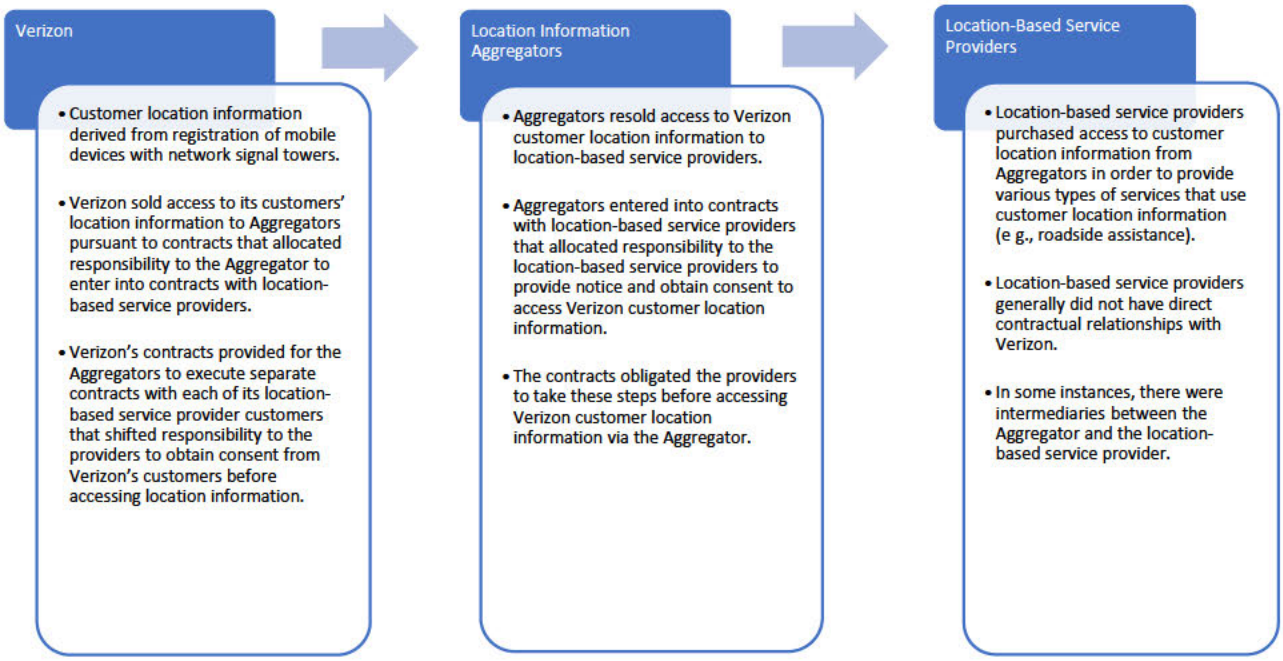
[42] *See 2012 LBS Report* at 11-12.

[43] *See* LOI Response at 2, Response to Question 1.

[44] 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.

[45] Response to Supplemental Letter of Inquiry from Verizon to Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, at 2, Response to Question 1 (June 5, 2019) (on file in EB-TCD-18-00027698) (Supplemental LOI Response).

(the Verizon "aggregator program"). Verizon had arrangements with two aggregators: LocationSmart and Zumigo (the Aggregators).[46] Each Aggregator, in turn, had arrangements with numerous location-based service providers. The most basic form of these relationships is illustrated in Fig. 1:



13. Verizon apparently sold access to its customers' location information, directly or indirectly, to third parties, including the two Aggregators. More specifically, Verizon sold access to its customer location information to the two Aggregators, who then approved the resale of such access to the following location-based service providers:[47] 3Cinteractive,

Securus,

14. *Verizon's Contracts with the Aggregators.* Verizon's contracts with the Aggregators called for the Aggregators or their location-based service provider customers to provide notice to customers and obtain consent to use location-based information before they could access Verizon customer location information.[48] Verizon acknowledges that, typically, the location-based service

[46] *Id.*

[47] *See* LOI Response at 5, Response to Question 3.

[48] Supplemental LOI Response at 8, Response to Question 4.

providers, rather than the Aggregators, provided notice to and sought consent from Verizon's customers to access and use their location information.[49] As a result, Verizon's contracts with the Aggregators provided for the Aggregators to enter into their own contracts with their location-based service provider customers that included provisions obligating the location-based service providers to, among other things, provide Verizon's customers with clear disclosure of the way their location information would be "accessed, used, copied, stored, or disclosed" by the location-based service provider and obtain "affirmative, opt-in consent" from Verizon customers or users "prior to accessing, using, storing or disclosing location information."[50] Verizon's contracts also obligated the Aggregators .[51]

15. In addition, Verizon's contracts with the Aggregators included various information security requirements. For example, they obligated the Aggregators to prevent unauthorized disclosure of Verizon's data,

[52] These contracts also called for the Aggregators to comply with consumer protection and data privacy laws and industry best practices.[53] For example, the Aggregators agreed to "

"[54]

16. Verizon had broad authority under its contracts with the Aggregators to terminate their access to customer location information. These contracts permitted the Company [55] Verizon also had the right to terminate its relationship with each Aggregator for any material breach of contract terms,[56] and it could "terminate any arrangement that fail[ed] to meet [Verizon's] standards."[57]

17. *Verizon's Application Review and Ongoing Monitoring*. Verizon did not have contracts with the location-based service providers that accessed its customers' location information. Instead, it

---

[49] *Id.*

[50] *Id.*

[51] LOI Response at VZ-03-0000048, Response to Request for Documents No. 3 (Verizon-LocationSmart Agreement,); LOI Response at VZ-03-0000004-0000005, Response to Request for Documents No. 3 (Verizon-Zumigo Agreement,).

[52] *See* LOI Response at 7, Response to Question 4; LOI Response at 10, Response to Question 8; LOI Response at VZ-03-0000054-0000057, Response to Request for Documents No. 3 (Verizon-LocationSmart Agreement,); LOI Response at VZ-03-0000011-0000013, Response to Request for Documents No. 3 (Verizon-Zumigo Agreement,).

[53] *See* LOI Response at 7, Response to Question 4.

[54] LOI Response at VZ-03-0000007, Response to Request for Documents No. 3 (Verizon-Zumigo Agreement,); LOI Response at VZ-03-0000050, Response to Request for Documents No. 3 (Verizon-LocationSmart Agreement,). *See also* 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 (last visited Feb. 4, 2020).

[55] LOI Response at VZ-03-0000044, Response to Request for Documents No. 3 (Verizon-LocationSmart Agreement,); LOI Response at VZ-03-0000001, Response to Request for Documents No. 3 (Verizon-Zumigo Agreement,).

[56] Pursuant to the contracts, as well, but the contracts did not of Verizon customer data. *See* LOI Response at VZ-03-0000053, Response to Request for Documents No. 3; LOI Response at VZ-03-0000014, Response to Request for Documents No. 3 (section).

[57] *See* LOI Response at 7, Response to Question 4.

operated an application and approval process for location-based service providers that sought access to Verizon customer location information.[58] According to Verizon, each applicant was required to describe, among other things, the "use case" or purposes for which it would use the location information and the process it would use for providing notice and obtaining opt-in consent from a Verizon customer for use and sharing of the customer's location information.[59] Verizon claims that it only allowed the Aggregators to share Verizon customer location information with location-based service providers for one of six specific types of use cases: "call routing, roadside assistance, proximity marketing, transportation and logistics, fraud mitigation/identity management, and mobile gaming/lottery."[60]

18. According to Verizon, the Company retained a third-party auditor, Aegis Mobile, LLC (Aegis), to perform background checks on companies seeking access to location information before those companies were allowed to obtain it.[61] Aegis would perform an initial verification to determine if each participant in Verizon's location-based services program was "a legitimate company with no consumer protection issues," that its application was within Verizon's approved use cases, and that its notice and consent process met Verizon's requirements.[62] After Aegis completed its review, Verizon would perform its own second vetting review.[63] According to Verizon, the Aggregators were only allowed to provide Verizon customer location information to location-based service providers that Verizon had approved through its application process and only for the use case approved for each such provider.[64]

19. Verizon claims that, in order to ensure that it was providing customer location information after its customers had given their consent, the Company also had Aegis "validate and reconcile" the records of consent events and the records of each access to a subscriber's location "on a daily basis."[65] As described by Verizon, those records of consent events consisted of "the subscriber's mobile device number, the consent action, identifying information of the consent associated with the consent action, and time stamp for the consent action."[66] The separate records of access to subscribers' location information consisted of the subscriber's mobile device number, the consent associated with the location request, and the date and time stamp for each request for access to customer location information.[67] In one of its responses to the Enforcement Bureau, Verizon represents that Aegis "compared aggregator consent and transaction records with Verizon location platform transaction records."[68] But, in a declaration of John Bruner, the President and Chief Executive Officer of Aegis, belatedly submitted to the Enforcement Bureau by Verizon last week, Bruner is clear that the consent records and the transaction records that Aegis reconciled were both submitted by the Aggregators.[69]

[58] *See* Supplemental LOI Response at 14, Response to Question 6.

[59] *See* LOI Response at 2, Response to Question 1; *see also* Supplemental LOI Response at 22, Response to Question 13.

[60] LOI Response at 2, Response to Question 1.

[61] *See* LOI Response at 3, Response to Question 1.

[62] *See* Supplemental LOI Response at 22, Response to Question 13.

[63] LOI Response at 3, Response to Question 1.

[64] LOI Response at 2, Response to Question 1.

[65] LOI Response at 3-5, Response to Question 1; *see also* Supplemental LOI Response at 20-21, Response to Question 13; Declaration of John A. Bruner, Jr., Aegis Mobile, LLC, para. 3 (Feb. 21, 2020) (Bruner Decl.).

[66] Bruner Decl. at para. 3; *see also* LOI Response at 2, 5, 7, 8, Response to Questions 1, 3, 4, 5; Supplemental LOI Response at 20, Response to Question 13.

[67] Bruner Decl. at para. 3; *see also* Supplemental LOI Response at 20, Response to Question 13.

[68] LOI Response at 8, Response to Question 6.

[69] Bruner Decl. at para. 3.

20. Verizon produced to the Enforcement Bureau at least some of the statistical reports prepared by Aegis for Verizon that "reflect the results of Aegis's efforts to match up each transaction"—i.e., a request for access to customer location information—"with a corresponding consent record in the data it received from the Location Aggregators."[70] Those reports indicate that in a substantial number of instances, Aegis was unable to match a request for location information to a consent record in its initial processing of the data.[71] For example, the Aegis report for shows tha

.[72] In other words, the report appears to show that, using the Aggregators' own records,

he report also breaks down Aegis's consent record review by location-based service provider and appears to show that the percentage of transactions that Aegis could not initially match to customer consents varied widely by location-based services provider. For instance, while

"[73]

21. Verizon asserts that the Aegis transaction reports reflect only the initial step of the consent validation process and that, when Aegis was unable to match a transaction record with evidence of consent, it would follow up with the Aggregator.[74] According to Verizon, "[g]iven the sheer volume of transactions and [consent] records being submitted, the fact that the Location Aggregators had to obtain records from their downstream customers," and the fact that records were submitted on a daily basis from location-based service providers, "some number of recordkeeping issues were inevitable."[75] Verizon's recently-filed Bruner declaration explains that Aegis reviewed the records that each Aggregator provided to Verizon and attempted to match the records of location access to the records of consent.[76] In that declaration, Bruner claims that given "the volume of cumulative transactions, changes in content ownership and name during the course of the ['Location Data Integration'] program, and technical matters surrounding file transmission and receipt, it is not surprising that Aegis did not initially find a matching consent record for every request for access submitted."[77] According to Bruner, by following up with the Aggregators or their location-based service provider customers and by correcting misalignments in the data or performing other data operations, Aegis was able to match 99.95% of all records of location requests to the corresponding consent record.[78] According to Bruner, for the remaining 0.05% of records, Aegis spot-checked the records "down to the individual location request consent level" and found no instances in which it was unable to find a corresponding consent record.[79]

22. Verizon also claims that Aegis "would look more broadly at trends in the data – e.g., spikes in the number of 'No Consent' results or significant variations between the results in different

[70] Supplemental LOI Response at 21, Response to Question 13.

[71] Bruner Decl. at para. 4.

[72] *See* LOI Response at VZ-0000866, Response to Request for Documents No. 6; Supplemental LOI Response at 20-22, Response to Question 13.

[73] LOI Response at VZ-0000873, Response to Request for Documents No. 6.

[74] Supplemental LOI Response at 21-22, Response to Question 13; Bruner Decl. at paras. 4-5.

[75] Supplemental LOI Response at 22, Response to Question 13.

[76] Bruner Decl.

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

[78] *Id*. at paras. 5-6.

[79] *Id*. at para. 6.

periods of time – to help ensure there were no overarching concerns."[80] And the Bruner declaration echoes those claims and goes even further by asserting that Aegis "also applied fraud analytics techniques to refine its ability to broadly identify potential issues going forward."[81] But neither Verizon nor Aegis offer examples of issues they were able to identify and address through that data analysis.

23. Additionally, Verizon asserts that the consent reports "were just one component of Aegis's broader oversight program" and that Aegis used other methods to ensure that the Aggregators (and their location-based service provider customers) "were complying with their contractual obligations."[82] For example, according to Verizon, Aegis reviewed location-based service providers' consent processes to ensure they were seeking affirmative opt-in consent and used secret shoppers to confirm how a subscriber would be presented with information by the location-based service providers and to test their opt-in consent processes.[83] Verizon also asserts that Aegis would review the providers on a "regular basis" to make sure they were in compliance with their use case, notice, and consent requirements.[84]

24. Verizon further asserts that in addition to these regular practices, it would "review and/or address discrete issues as they were raised" by Aegis or otherwise.[85] In particular, Verizon describes an investigation it conducted after receiving a call in or around August 2017 "alleging that a bail bonds company had obtained access to Verizon subscriber location data without proper subscriber consent."[86] According to Verizon, "[t]he investigation concluded that the unidentified company referenced by the caller likely was [a location-based service provider] that had requested to participate in the aggregator program and been rejected; as such it was not receiving Verizon subscriber location information."[87] The investigation further concluded that while it is

"[88] The report made no recommendations for adopting additional methods to mitigate the risk of approved location-based service providers falsifying consent records to obtain Verizon customer location information without their consent.

3. Verizon's Actions After the Publication of Reports of Unauthorized Access to and Use of Customer Location Information

25. On May 10, 2018, the *New York Times* reported on security breaches involving Verizon's (and other carriers') practice of selling access to customer location information. Specifically, the *New York Times* article reported that 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 Verizon, *without* the device owner's knowledge or

[80] Supplemental LOI Response at 22, Response to Question 13.

[81] Bruner Decl. at para. 7.

[82] Supplemental LOI Response at 22, Response to Question 13.

[83] *See* Supplemental LOI Response at 4, 22, Response to Questions 1, 13.

[84] *Id*. at 22, Response to Question 13.

[85] *Id*. at 12, Response to Question 5.

[86] *Id*. at 13, Response to Question 5.

[87] *Id*. at 12, Response to Question 5.

[88] LOI Response at VZ-0000295, Response to Request for Documents No. 6.

consent.[89] 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 location request.[90] Securus did not, however, review or assess the adequacy of the purported legal authorizations submitted by users of its location-finding service.

26. 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.[91] 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.[92] 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.[93]

27. Verizon does not deny the existence of the Securus location-finding service nor the abuse of that system by Hutcheson. Instead, Verizon explains that it had approved Securus's access to Verizon subscriber information for a different purpose.[94] More specifically, Verizon explains that one of the Aggregators, LocationSmart, had a contract with 3Cinteractive, which in turn "supplied location and messaging services to Securus."[95] Verizon emphasizes that Securus had authorization from Verizon to receive its customer location information only to confirm that recipients of collect calls from prisons were "not within a certain distance of the prison from which a collect call was placed."[96] Verizon has offered no information about what steps, if any, it took to identify the Verizon customers whose location information was accessed and used by Securus without their consent.[97]

28. According to Verizon, on May 11, 2018, after publication of the *New York Times* article about Securus's and Hutcheson's misuse of wireless carriers' customer location information, Verizon directed LocationSmart to terminate Securus's and 3Cinteractive's access to Verizon customer location information.[98]

29. According to Verizon, it then "undertook a review to better understand how [the Securus and Hutcheson breaches] could occur despite the contractual, auditing, and other protections" in had in place to protect customer location data."[99] Verizon concluded that "the regular audit did not reveal that Securus was using this data in ways that differed from its approved use case with LocationSmart."[100]

---

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

[90] *Id.*

[91] *Id.*

[92] *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.

[93] *See* Complaint, *Cooper et al. v. Hutcheson*, Case File No. 1:17-cv-00073 (E.D. Mo. May 8, 2017).

[94] Supplemental LOI Response at 15, Response to Question 7.

[95] *Id*.

[96] *See* LOI Response at 11, Response to Question 8; Supplemental LOI Response at 15, Response to Question 7.

[97] *See* Supplemental LOI Response at 16, Response to Question 7.

[98] *Id*.

[99] LOI Response at 12, Response to Question 8.

[100] *Id*.

Verizon asserts the "audit likely did not alert our third party auditor to a potential problem because: (i) Securus was using its profile for the approved use case to access location information for unauthorized purposes; (ii) nothing changed in the background check that the auditor maintains for Securus that would have prompted the auditor to question its credibility about following approved use cases; and (iii) the number of requests from Securus was consistent with the number the auditor would normally expect from them."[101]

30. Verizon also claims that, "[u]pon learning of the incident involving Securus," it conducted an investigation that "did not uncover any new incidents in which a Location Aggregator (or its customer) mispresented that it had customer consent."[102] Verizon does not, however, describe the breadth or depth of its review of the activities of other location-based service providers and the Aggregators in light of the shortcomings of its consent system uncovered by the Securus and Hutcheson breaches.

31. Moreover, through that investigation, Verizon learned of a "vulnerability" that allowed a cybersecurity researcher to gain access on May 16, 2018, "to Verizon customer data through LocationSmart's website via a demonstration page for prospective customers" of LocationSmart.[103] While Verizon emphasizes that "the researcher attempted location queries only for individuals who had first given him their consent,"[104] Verizon does not state that it had authorized this use case for its customers' location information. Instead, Verizon suggests that it was not aware of LocationSmart's use of Verizon customer location information for this purpose before the investigation and states that it "directed both LocationSmart and Zumigo to not use Verizon customer data in any demonstration site going forward."[105] According to Verizon, it "has not identified any other incidents in connection with the location aggregator program involving third parties accessing customer location information without authorization."[106]

32. On June 12, 2018, Verizon notified the two Aggregators that Verizon "intended to terminate the contracts giving them their ability to access and use our customer location data as soon as possible."[107] Nevertheless, four months later, Verizon's working relationship with the Aggregators remained intact. At that time, Verizon informed the Enforcement Bureau that it anticipated terminating its arrangements with the Aggregators by November 30, 2018.[108] According to Verizon, during that interim period, it (1) stopped authorizing any new uses of location information by the Aggregators or the sharing of such information with any new customers of the Aggregators, and (2) strengthened its transaction verification process to identify anomalies in consent requests that might be indicative of a problem (e.g., multiple location requests in a 24-hour period or "an increase in location requests that are out of the ordinary").[109]

33. At the same time that Verizon was undertaking a months long process to phase out its aggregator program, it started a "Direct Location Services" program as an alternative.[110] As Verizon explains, under the Direct Location Services program, location-based service providers could access

[101] *Id*.

[102] *Id*.

[103] *Id*. at 12-13, Response to Question 10.

[104] *Id*. at 13, Response to Question 10.

[105] *Id*.

[106] *Id*. at 12-13, Response to Question 10; Supplemental LOI Response at 16, Response to Question 7.

[107] LOI Response at 9, Response to Question 6.

[108] *Id*.; Supplemental LOI Response at 2, Response to Question 1.

[109] LOI Response at 10, Response to Question 6.

[110] *Id*. at 9, Response to Question 6.

Verizon customer location information upon consent for specific use cases, but Verizon itself obtained consent from its customers to share such information with a particular location-based provider.[111] Verizon did so by sending its customer a text message seeking affirmative consent to share the customer's location information, and according to Verizon, it would only share that information with the location-based services provider if its customer responded affirmatively to that request.[112] Verizon has explained that "being able to safeguard its subscribers' location information was one of the main drivers behind Verizon's decision [] to terminate its location aggregator program."[113]

34. Verizon terminated all arrangements with Zumigo by November 30, 2018. Verizon also terminated all arrangements with LocationSmart and its location-based service customers except for arrangements with four companies that provided location-based roadside assistance.[114]

35. By March 30, 2019, Verizon stopped providing LocationSmart and its four remaining customers access to Verizon customer location information.[115]

36. On April 5, 2019, Verizon notified the location-based service providers participating in the Direct Location Services program that it was terminating the program by the end of July 2019.[116] Verizon did not state why it ended its Direct Location Services Program. But having terminated that program, Verizon explains that "[g]oing forward, Verizon can be sure that no third party [ ] can circumvent or compromise [Verizon's] process for ensuring that its customers have consented to the disclosure of their Customer Location Information because Verizon has terminated any such third party access to Customer Location Information."[117]

37. In all, it took 324 days from when the *New York Times* reported on the Securus location-finding service (and the abuse of that service by Hutcheson) for Verizon to end the program that made its customers' location information vulnerable to unauthorized access.[118]

38. *Commission Investigation*. The Enforcement Bureau launched an investigation in May 2018 immediately following the *New York Times* article reporting the unauthorized location tracking involving Securus. The Bureau issued a Letter of Inquiry (LOI) to Verizon 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 back to 2016.[119] The Bureau requested additional information and documents from Verizon in 2019.[120] Verizon submitted responses to the Bureau's initial and supplemental LOIs, as well

[111] Supplemental LOI Response at 3, Response to Question 1.

[112] *Id*. at 3, 9, Response to Questions 1, 4.

[113] *Id*. at 16, Response to Question 7.

[114] *Id*. at 2, Response to Question 1.

[115] *Id*. at 2, Response to Question 1.

[116] *Id*. at 5, Response to Question 1.

[117] *Id*. at 16, Response to Question 7.

[118] *Id*. at 2, Response to Question 1.

[119] Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to Chris Miller, Vice President and Associate General Counsel, Verizon (Sept. 13, 2018) (on file in EB-TCD-18-00027698) (LOI).

[120] Supplemental Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to Chris Miller, Vice President and Associate General Counsel, Verizon (Apr. 8, 2019) (on file in EB-TCD-18-00027698) (Supplemental LOI).

as approximately 6,000 pages of responsive documents concerning its sale of access to its customer location information to third parties.

III. DISCUSSION

39. We find that Verizon 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 almost a year after Verizon 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., Verizon's commercial mobile service.[124] The location data was derived from the wireless mobile devices of Verizon'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. Verizon is therefore providing telecommunications service to these customers whenever it is enabling the customer's device to send and receive calls—regardless of whether the device is actively in use for a call. This view finds ample support in Commission precedent, including the *2013 CPNI Declaratory Ruling*, which indicates

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

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*, Verizon's wireless customers made this information available to Verizon because of the carrier-customer relationship embodied in their service agreements. Verizon provides wireless telephony services to the affected customers because they have chosen Verizon to be their provider of telecommunications service—in other words, they have a carrier-customer relationship. The customer location information to which Verizon sold access was generated by the service that Verizon provided to those customers. In short, Verizon's customers provided their wireless location data to Verizon because of their customer-carrier relationship with Verizon, so that Verizon could use that location information to provide them with a telecommunications service. That makes the location information CPNI.

45. Resisting this straightforward conclusion, Verizon argues that the location information at issue does not constitute CPNI. Verizon argues that section 222 applies only to "'information that relates to the . . . location . . . of *use* of a telecommunications service.'"[126] Verizon further argues that other location information, such as the location of a customer when they are using a non-telecommunications service (like broadband Internet access service), is not CPNI nor call location information under the Act.[127] We disagree with this reading of the statute. Absent any ellipses, the relevant text defines CPNI to mean "information that relates to the quantity, technical configuration, type, destination, location, and *amount of use* of a telecommunications service."[128] The most natural reading of the statute is that "of use" refers only to its antecedent—"amount"—not to each and every item in the list before. And Verizon's more convoluted interpretation would require us to read "of use" as applying to every term in that list, including "technical configuration"—an outcome neither grammatical nor otherwise sensible. And again, Verizon fails to refute the central point that the Company necessarily obtains location information by virtue of its provision of the telecommunications service when it enables the connection of a customer's device to its network for the purpose of sending and receiving calls, and the customer has no choice but to reveal that location to the carrier. We find Verizon's arguments regarding the classification of location information unpersuasive, particularly in light of the more straightforward reading of the statutory text.

46. We remain likewise unpersuaded that location information generated and collected by

[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] *See* Supplemental LOI Response at 6, Response to Question 2 (quoting 47 U.S.C. § 222(h)(1)(A)) (ellipses in original and emphasis added).

[127] *Id*. at 6-7, Response to Question 2. Verizon also notes that in 2000, CTIA asked the Commission to initiate a rulemaking proceeding to implement and interpret section 222 of the Communications Act as it applies to wireless location information. The Commission declined to initiate this rulemaking, concluding that "the statute imposes clear legal obligations and protections for consumers." *See 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). Rather than concluding that the basic statutory protections, the Commission's preexisting CPNI rules, or future rule changes should not apply, the Commission merely found that additional action was unnecessary at that time. *Id.* at 14834, para. 5. Indeed, Verizon appears to concede that that *Order* demonstrates that section 222 applies to location information, while citing nothing the Commission said there that would support Verizon's unduly narrow understanding of the scope of location information so covered. *See* Supplemental LOI Response at 6-7, Response to Question 2.

[128] 47 U.S.C. § 222(h)(1)(A) (emphasis added).

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. The definition of CPNI 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. Nor does the use of the term "call location information" elsewhere in section 222 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.[129] 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.[130] 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.

48. 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,[131] also apply to that customer location information.

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

49. Verizon 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 Verizon customers. Verizon 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 Verizon customer consent for the disclosures. The evidence shows that between 2014 and 2017, at least 20 Verizon customers' location information was disclosed to Hutcheson, via 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

[129] Notwithstanding Verizon's argument that the location information at issue here constituted "non-call location information," Verizon emphasized that it "nevertheless treated both call location information and non-call location information the same way for consent purposes and maintained the same protections for both" in connection with its location-based service programs. *See* Supplemental LOI Response at 7, Response to Question 3.

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

[131] 47 CFR § 64.2003(g).

[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.

[134] *See* Department of Justice Evidence Records (on file in EB-TCD-18-00027698).

rules for which Verizon is responsible.

51. Verizon 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, Verizon argues that Securus "accessed customer location information for unauthorized purposes, in violation of Verizon's requirements" by exploiting its approved inmate-calling use case to access customer location information, without customer approval, for its unapproved location-finding service.[135] Verizon further explains that "despite the protections that Verizon built into its location aggregation arrangements, it appears that Securus and/or its affiliate 3C Interactive (collectively, 'Securus') impermissibly permitted" access to Verizon customer location information through LocationSmart.[136]

52. We find these arguments unavailing. Verizon 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, Verizon. 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 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

[135] LOI Response at 11-12, Response to Question 8.

[136] *Id.*

[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.

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, Verizon may not have it both ways. If Verizon 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 Verizon itself. If not, then Verizon effectively granted those third parties the capability to access the CPNI of its customers without customer approval.

57. In sum, we find that Verizon 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]

---

[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. Verizon 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.

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

C. Verizon Apparently Failed to Take Reasonable Measures to Protect CPNI

58. Verizon 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 about the Securus and Hutcheson breaches exposed serious inadequacies with the safeguards on which Verizon relied to protect its customers' location information. Our investigation shows that Verizon failed to promptly address those inadequacies. We therefore conclude that Verizon 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. Verizon 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. To meet this burden, Verizon offers five general categories of safeguards that it claims collectively amounted to a reasonable attempt to protect customer location information. In general, Verizon relied on the safeguards discussed below both before and after the May 10, 2018, report of the Securus and Hutcheson breaches.

61. *First*, Verizon asserts that it vetted both Aggregators and location-based service providers. This involved examining both the integrity of the entities with whom Verizon shared access to location data,[155] as well as how those entities intended to use the location data of its customers.[156] With respect to vetting, there is at least some evidence that Verizon denied applications that did not meet its vetting criteria.[157] With respect to use cases, Verizon claims that it required each company seeking to participate in its location aggregator program to submit: (i) a detailed description of the applicant's use case; (ii) specific details of how end user notice and disclosures were to be provided and how location information would be used, stored, and shared–including exact notice and disclosure language; (iii) a detailed description of the affirmative, opt-in consent model, including proposed language, call flow, and message interval information; and (iv) a full description of the process for opting out of the proposed service.[158]

---

[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*.

[155] LOI Response at 7-8, Response to Question 4.

[156] *Id*. at 3, Response to Question 1.

[157] For instance, Verizon apparently refused the application of a company called because it failed Aegis's vetting process; specifically, Verizon rejected because ." *See* LOI Response at VZ-0000295, Response to Request for Documents No. 6.

[158] LOI Response at 3, Response to Question 1.

62. Verizon asserts that it would approve only uses that fell within six specific categories of services—for example, roadside assistance and "proximity marketing."[159] Verizon's contracts with the Aggregators, in turn, required that any access to location data be confined to these specific, authorized uses.[160]

63. But the *New York Times* report made clear that the contractual promise to limit the use of location data alone was insufficient to prevent the unauthorized use of such data. For example, Verizon acknowledges that the Securus and Hutcheson incident involved a use that was "not an approved use case in [Verizon's] agreement with LocationSmart."[161] According to Verizon, even a regular audit "did not reveal that Securus was using this data in ways that differed from its use case with LocationSmart."[162] In other words, notwithstanding any contractual obligations imposed on LocationSmart—or attempts to confirm that these protections were honored—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 its contract.

64. *Second*, Verizon asserts that its contracts with Aggregators required that Aggregators and location-based service providers supply notice to and obtain the consent of Verizon's customers prior to sharing any location information.[163] Verizon's contracts with the Aggregators also obligated the Aggregators and location-based service providers to send a record of the consent they received to Verizon.[164] In addition, Verizon claims that it "follow[ed] up by regularly conducting audits through the third party auditor [Aegis]" in order to verify that the location-based service providers obtained customer consent before accessing location information.[165] Verizon explains that Aegis would receive records for each location information request submitted to Verizon and review them on a daily basis.[166]

65. But Verizon should have realized in 2017 that these records were only as reliable as the companies supplying them. As Verizon's 2017 investigation

."[167]

66. *Third*, Verizon offers a host of measures that it used to monitor the performance of Aggregators and location-based service providers. Specifically, according to Verizon, its third-party auditor, Aegis, used "proprietary software and database platforms together with analysis services" and "compared aggregator consent and transaction records with Verizon location platform transaction records to detect and investigate any differences that could indicate non-compliance with prescribed processes or consent requirements."[168] Verizon also claims that it retained Aegis to perform "vetting and ongoing monitoring of companies accessing location information" even after those companies were authorized to obtain location information from Verizon.[169] And though it provides scant detail on the scope and extent

[159] *Id*. at 2, Response to Question 1.

[160] *Id*.

[161] *Id*. at 11, Response to Question 8 (emphasis in original).

[162] *Id*. at 12, Response to Question 8.

[163] *Id.*

[164] *See id*. at 8, Response to Question 5.

[165] *Id*. at 7, Response to Question 5.

[166] *Id*. at 8, Response to Question 6.

[167] LOI Response at VZ-0000295, Response to Request for Documents No. 6.

[168] LOI Response at 8, Response to Question 6.

[169] *Id*. at 3, Response to Question 1.

of this practice, Verizon also asserts that Aegis's monitoring included "secret shopping" the services of location-based service providers "to confirm how a subscriber would be presented with . . . information and test their opt-in process."[170]

67. Yet these measures were demonstrably insufficient, and Verizon's descriptions of them seem to raise more questions than answers. To begin with, the declaration Verizon submitted from John Bruner, President and CEO of Aegis, does not support Verizon's assertion that Aegis compared the records it received from the Aggregators to Verizon location platform records. To the contrary, Bruner's belatedly submitted declaration makes clear that Aegis's daily audits simply compared one set of records provided by an Aggregator to another set of records provided by the same Aggregator.[171] More fundamentally, even if we accept Bruner's representation that ultimately Aegis was able to match 99.95% of all records of location access provided by the Aggregators to the corresponding consent records provided by the Aggregators,[172] matching two sets of information provided by the Aggregator indicates nothing about the validity of the consent records themselves. Yet, Aegis's auditing system appears to have assumed that the location requests and consent records provided by the Aggregators would be legitimate in the first instance, a trustworthy baseline against which to gauge anomalous activity. The ease with which Securus was able to operate an unapproved use case, and with which Hutcheson used that unapproved use case to repeatedly access Verizon customer location information without the customers' consent and without being detected by Verizon, underscores the inadequacy of the Aegis review systems.

68. Moreover, even if we were to credit Verizon's use of the Aegis record reconciliation program as providing some level of assurance that location-based service providers were seeking and receiving consent before accessing customer location information, we would need a more detailed understanding of why the actual audit records created by Aegis after its initial attempt to match consent and access records show an apparently troubling rate of noncompliance, both at a program level and with respect to specific participants in its location-based services program. For example, neither Verizon nor its auditor shed any specific light on why

[173] Nor do they provide any details to explain why during that same time period specific transactions were identified as having "no consent"—that is, there were nearly specific, date-and-time-stamped instances during the first half of 2017 in which Verizon's auditor [174] Indeed, if Aegis was, as Verizon claims, using these reports as "an initial effort to track down how well the Location Aggregators were fulfilling their record-keeping obligations" when it came to Verizon customer consent records,[175] the reports demonstrate that the Aggregators were failing in this regard. Rather than offering any provider-specific details about why Aegis's initial attempts to match the consent and access records provided by the Aggregators failed in so many instances, and so badly for some location-based service providers but not others, Verizon and Aegis resort to broad stroke explanations about the challenges of matching the data sets.[176] Verizon's failure, even in Bruner's late-filed affidavit, to provide a fulsome explanation of Aegis's data reconciliation practice and challenges is particularly striking given that Aegis

[170] Supplemental LOI Response at 22, Response to Question 13.

[171] Bruner Decl. at paras. 3-7.

[172] *Id*. at para. 7.

[173] *See* LOI Response at VZ-0000873, Response to Request for Documents No. 6; Supplemental LOI Response at 20-22, Response to Question 13; Bruner Decl.

[174] *See* LOI Response at VZ-0000866, Response to Request for Documents No. 6; Supplemental LOI Response at 20-22, Response to Question 13; Bruner Decl.

[175] Supplemental LOI Response at 21, Response to Question 13.

[176] Bruner Decl. at para. 5; Supplemental LOI Response at 22, Response to Question 13.

and Verizon both claim that Aegis "looked at trends – such as spikes in the number of 'No Consent' results or significant variations between the results in different periods of time – to identify any potential issues."[177] It also raises further questions about whether Aegis truly investigated such trends and their significance to the integrity of the data and the Verizon location sharing program.

69. *Fourth*, Verizon imposed a variety of information security requirements on the Aggregators to whom it sold access to customer location information—for example, that they prevent unauthorized disclosure of Verizon's data,

[178] But, as Verizon explains, the Company's contractual relationships were with the Aggregators,

[179] In other words, these contractual requirements were largely passed down to the entities responsible for obtaining consent and that used the location information of Verizon's customers through an attenuated chain of downstream contracts. To enforce the requirements, Verizon would have needed to take steps to determine whether they were actually being followed. While Verizon did have measures in place that were designed to monitor compliance by the Aggregators and their location-based service provider customers, Verizon has not sufficiently demonstrated that these measures were appropriate or effective. In fact, evidence in the record indicates that at least as early as August 2017, Verizon had actual knowledge that its consent mechanisms were able to be bypassed by location-based service providers if they submitted false records of consent.[180]

70. Moreover, in the post-incident analysis of Securus's unauthorized location-finding service, Verizon concluded that it failed to detect Securus's activities because its daily audits were unable to detect any differences between the authorized and unauthorized location requests that Securus submitted.[181] This is especially troubling because of the distinctions between the types of "consents" that Securus purported to collect in each program. The authorized Securus program was designed with the sole purpose to "confirm that call recipients were not within a certain distance of [a] prison from which a collect phone call was placed."[182] Under Securus's authorized service, Verizon's customers should have received an audio prompt requesting consent for the caller's location to be tracked in order to complete the call to the prison. In other words, Verizon customers were supposed to provide affirmative consent before Securus could obtain their location information. Not so with Securus's *unauthorized* location-finding service. The unauthorized service did not collect consents from Verizon's customers—just the opposite. When working as intended, Securus's unauthorized program collected electronic copies of legal process asserting a right to obtain location information *without the knowledge or consent of the Verizon customer*. A system allegedly designed to monitor customer consents but that is incapable of detecting its opposite is not a "reasonable measure" to detect unauthorized uses of or access to CPNI.

71. *Fifth and finally*, Verizon claims that it provided only "coarse" location data through its location aggregator program.[183] Verizon explains that this information "would have included the

---

[177] Bruner Decl. at para. 7; Supplemental LOI Response at 22, Response to Question 13.

[178] *See* LOI Response at 7, Response to Question 4; LOI Response at 10, Response to Question 8; LOI Response at VZ-03-0000054-0000057, Response to Request for Documents No. 3 (Verizon-LocationSmart Agreement, ; LOI Response at VZ-03-0000011-0000013, Response to Request for Documents No. 3 (Verizon-Zumigo Agreement,).

[179] LOI Response at 3, Response to Question 1.

[180] *See* .

[181] LOI Response at 12, Response to Question 8.

[182] *Id*. at 11, Response to Question 8.

[183] *Id*. at 4, Response to Question 1; *see also* Supplemental LOI Response at 5-6, Response to Question 2. Verizon states that "[t]he location aggregator program" likewise "generally utilized 'coarse' location information," as well.

customer's approximate latitude and longitude, as well as the error radius and other error information for location queries."[184] But claiming that Verizon only disclosed less accurate customer location information is no defense: Congress declined to distinguish between "coarse" and "fine" location information in section 222—nor do we draw such a distinction in our rules. What is more, Verizon fails to explain how the mere fact that the location data were "coarse," in and of itself, provided a safeguard against unauthorized access or use.

72. In sum, the safeguards implemented by Verizon to protect customer location information against unauthorized use relied heavily on a chain of contractual agreements that delegated operational responsibility down to location-based service providers. Verizon's efforts to ensure compliance with these agreements apparently mainly consisted of analysis of unverified vendor-created consent records. Yet, Verizon was aware of the unreliability of these consent records in 2017.

73. To the extent that Verizon's safeguards relied on trusting Aggregators and location-based service providers to honor their contractual commitments, it is hard to conclude that such trust alone was a reasonable safeguard here—even in the absence of an unauthorized disclosure. This is particularly so in light of the industry's experience with pretexting, which should have apprised Verizon of the high risk that bad actors would attempt to gain unauthorized access to Verizon's customers' CPNI, particularly by trying to find ways around any systems Verizon put in place to authenticate that its customers were actually providing consent to third parties' access to their location information.

74. Setting aside the inadequacy of Verizon's safeguards before disclosure of the Securus and Hutcheson breaches, Verizon was on clear notice that its safeguards were inadequate after the disclosure, and so we focus on the actions that Verizon took, or failed to take, after discovery of that breach. We find that however reasonable Verizon's safeguards might have been from the inception of Verizon's location-based services business model, Verizon has apparently failed to demonstrate that they were reasonable following the disclosure of Securus's unauthorized location-finding service in May 2018. The Securus incident laid bare the fundamental weaknesses of Verizon's safeguards with respect to the third parties to which it entrusted its customers' location information. Nevertheless, Verizon continued to sell access to its customers' location information for months under the same system that had allowed (1) Securus to provide location information in a manner inconsistent with its approved use case, and (2) Hutcheson to easily and improperly access Verizon customers' location information. Specifically, Verizon continued to sell access to for 204 days after the *New York Times* report and to another for a total of 324 days after the report. Relying on demonstrably faulty safeguards in the wake of this incident does not appear to have been reasonable.

75. There are several commonsense measures that Verizon could have taken following the May 2018 *New York Times* article. One obvious reasonable 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. Verizon did so only in part. Verizon ended 3Cinteractive and Securus's access to Verizon customer information on May 11, 2018.[185] But it did not suspend the access of LocationSmart, the Aggregator that had the contractual obligations to monitor Securus and 3Cinteractive's access to Verizon's customer data, for another 324 days (March 30, 2019). Yet the evidence shows that LocationSmart was responsible not only for the unauthorized Securus

Supplemental LOI Response at 5, Response to Question 2. Verizon does not explain how the mere fact that the location data were "coarse," in and of itself, provided a safeguard against unauthorized access or use.

[184] LOI Response at 4, Response to Question 1; *see also* Supplemental LOI Response at 5-6, Response to Question 2.

[185] Supplemental LOI Response at 16, Response to Question 7.

program, but also the demonstration page that LocationSmart apparently created without Verizon's authorization.[186]

76. Another measure would have been to promptly ascertain the full scope and extent of the Securus breach. Verizon notes that it "undertook a review to better understand how this issue could occur despite the contractual, auditing, and other protections in place in the location aggregator program to protect customer location data" following the May 2018 *New York Times* article.[187] But Verizon provided no indication that the review it performed extended beyond investigation of the specific Hutcheson events. Nor is there any indication that Verizon conducted any review to determine whether Hutcheson was the only Securus customer who misused Securus's location-finding service. Accordingly, it is not possible to determine whether (1) the scope of Verizon's investigation was reasonable, or (2) whether Verizon took reasonable steps in response to the discovery of Securus's long-running unauthorized service. Again, it is *Verizon* that bears the burden of demonstrating the reasonableness of its practices in the wake of an unauthorized disclosure.[188] Indeed, there is no evidence that Verizon knows the full impact of Securus's unauthorized access to CPNI even to this day.

77. Another measure Verizon could have taken was to determine whether the Securus incident was an isolated occurrence, or whether it was indicative of a broader vulnerability with Verizon'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 Verizon's contractual safeguards. Again, however, Verizon has offered insufficient evidence to demonstrate that it took adequate 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. Verizon claims that "[u]pon learning of the incident involving Securus . . . Verizon conducted an investigation" into the matter, but the Company fails to provide any details about the scope or strength of that investigation. Verizon merely says that the Company "did not uncover any new incidents in which a Location Aggregator (or its customer) misrepresented that it had customer consent."[189] Securus obtained location information from the Aggregator LocationSmart—but Verizon fails to indicate whether it examined LocationSmart's history of compliance as part of its investigation. Verizon also failed to provide any evidence that it specifically looked into Zumigo's activities, or any of the location-based service providers it served. This failure to investigate is particularly inexcusable in light of the fact that Verizon as early as August 2017 that the location-based service providers could obtain customer location information by misrepresenting that they had customer consent.[190] Verizon chose to structure its aggregator program such that the responsibility for collecting customer consent lay with the location-based service provider, overseen by the Aggregators. The moment Verizon learned that it was possible for the location-based service providers to bypass the system, it was incumbent upon the Company to take steps to determine whether—and to what extent—this was happening.

[186] LOI Response at 12-13, Response to Question 10.

[187] *Id*. at 12, Response to Question 10.

[188] *2007 CPNI Order*, 22 FCC Rcd at 6959-60, para. 65.

[189] LOI Response at 12, Response to Question 10. Verizon further states that its investigation uncovered that a "cybersecurity researcher was able to gain access to Verizon customer data through LocationSmart's website via a demonstration page for prospective customers," but the researcher limited his location queries to persons who had given him prior consent. *Id*. at 13, Response to Question 10. According to Verizon, LocationSmart disabled the demonstration page upon learning of the vulnerability. *Id*. It is not clear when this incident took place, nor when LocationSmart learned about the security flaw and fixed it.

[190] *See*

.

78. Yet another measure that Verizon could have taken was to enhance the measures it uses to verify customer consent—for example, by directly confirming with customers that they have actually consented to the use of their location information. After the Securus and Hutcheson incident came to light, Verizon had good reason to doubt the accuracy of the consent records it received from any location-based service provider. As Verizon itself explains, both the Company and its third party auditor, Aegis, failed to detect Securus's unauthorized service because "(i) Securus was using its profile for the approved use case to access location information for unauthorized purposes; (ii) nothing changed in the background check that the auditor maintains for Securus that would have prompted the auditor to question its credibility about following approved use cases; and (iii) the number of requests from Securus was consistent with the number the auditor normally would expect from them."[191] Thus, instead of a consent mechanism that would allow Verizon to confirm that its customers had actually consented to the sharing of their location information, Verizon relied on 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. Verizon's first warning that this was the case came at least as early as 2017 .[192] Yet even after the next warning—the May 2018 *New York Times* report—the Company relied on the original flawed system for months, increasing the risk of further unauthorized access to Verizon's customers' location information. Verizon was demonstrably capable of implementing a location-based services program with a more reliable mechanism for collecting customer consent—Verizon implemented one in 2018 when it launched its Direct Location Services program.[193] And yet Verizon nonetheless continued to sell access to customer location information under its legacy, unreliable system.

79. Finally, the surest safeguard to protect its customers' CPNI was for Verizon to expeditiously terminate its location-based service program. If Verizon could not reasonably safeguard the customer location information that it sold access to, then it should have ceased to sell access to that information. The ease by which Hutcheson accessed location information indicated that the Company lacked visibility into how the location-based service providers were making use of the location information and that Verizon needed to change its practices or terminate its location-based service program. We recognize that Verizon correctly interpreted Hutcheson's actions as a sign of a fundamental weakness in its program. But despite the continuing risk that unauthorized access posed to Verizon's customers, it took the Company 324 days to fully end its program.

80. According to Verizon, it notified the Aggregators in June 2018 that it intended to terminate their contracts "as soon as possible," a little over one month after the publication of the *New York Times* report.[194] But it took Verizon nearly four months before it actually terminated its arrangements with Zumigo, and substantially narrowed them with LocationSmart.[195] During this four month interim, Verizon explains that it (1) stopped authorizing any new uses of location information by the Aggregators or the sharing of such information with any new customers of the Aggregators, and (2) strengthened its transaction verification process to identify anomalies in consent requests that might be indicative of a problem.[196] Ultimately, by the end of November 2018, Verizon terminated all arrangements with Zumigo and nearly all arrangements with LocationSmart and its location-based service customers.[197] Verizon explains that it left in place arrangements with four companies that provided location-based roadside assistance through LocationSmart "for the narrow purpose of providing roadside

[191] LOI Response at 12, Response to Question 8.

[192] *See* .

[193] LOI Response at 9, Response to Question 6.

[194] *Id*.

[195] Supplemental LOI Response at 2, Response to Question 1.

[196] LOI Response at 10, Response to Question 6.

[197] Supplemental LOI Response at 2, Response to Question 1.

assistance during the holidays and winter months for public safety reasons" with the expectation that all services would cease by March 30, 2019.[198]

81. We are nonetheless unpersuaded that Verizon acted with a speed that was reasonable in light of the risks involved to customer privacy, public safety, and security. In particular, we are not persuaded by Verizon's argument that "termination . . . had to be completed in careful steps so as not to disrupt beneficial services . . . such as [] fraud prevention and call routing services."[199] But these purported benefits simply assume that customers had in fact consented for such uses—a premise Verizon should not have relied on given its own findings that "

" without the consent of the affected customer.[200] And in that light, we disagree that the benefits that could flow to some consumers were sufficient to justify putting those same consumers—and others—at risk of harm. In the end, Verizon did not fully terminate its arrangements with LocationSmart and four of LocationSmart's location-based service provider customers until March 30, 2019—324 days after revelation of the Securus and Hutcheson breaches.[201]

82. In sum, Verizon apparently did not take any of the reasonable steps described above. Nor has it presented evidence that it took other reasonable measures that might have cured the flaws exposed by the Securus breach. The ease with which Hutcheson accessed location information about any individual of his choosing should have alerted Verizon 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, Verizon placed its customers' location information at continuing risk of unauthorized access through its failure to expeditiously terminate its program or impose reasonable safeguards to protect its customers' location information. For these reasons, we conclude that Verizon 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.[202]

D. Proposed Forfeiture

83. 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."[203] Here, section 503(b)(2)(B) of the Act authorizes us to assess a forfeiture against Verizon of up to $204,892 for each day of a continuing violation, up to a statutory maximum of $2,048,915 for a single act or failure to act.[204] In exercising our forfeiture

---

[198] *Id*.

[199] *See* LOI Response at 9, Response to Question 6; Supplemental LOI Response at 2, Response to Question 1.

[200] *See* .

[201] Supplemental LOI Response at 2, Response to Question 1.

[202] 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").

[203] 47 U.S.C. § 503(b).

[204] *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).

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."[205] 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.[206] 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.[207]

84. 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.[208] Nor has the Commission dealt with the unauthorized disclosure of location information 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*).[209] 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.[210] 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.[211]

85. Neither the *CPNI Cases* nor *TerraCom* are directly on point with the conduct in this case, but nevertheless are helpful in context. We find that Verizon'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. 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*

[205] 47 U.S.C. § 503(b)(2)(E).

[206] 47 CFR § 1.80(b)(8), Note to paragraph (b)(8).

[207] *Id*.

[208] 47 CFR § 1.80(b).

[209] *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).

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

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

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.

86. 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 service 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 along with a $2,500 forfeiture for the second day and each successive day that the violation continued. In other contexts involving consumer protections under the Act and the Commission's rules, the Commission has applied a base forfeiture of $40,000 for a single act.[212] 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.

87. We recognize that Verizon took one reasonable step towards improving its safeguards by terminating Securus and 3Cinteractive's access to Verizon customer location information on May 11, 2018, one day after the *New York Times* report.[213] But that step did not protect customer location information at all from the other entities that had access to it. These included —and constitute 65 separate continuing violations. We find that Verizon apparently did not take reasonable steps to safeguard that CPNI until November 30, 2018[214]—a full 204 days after the *New York Times* report— and until March 30, 2019[215]—324 days after the report— . 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, Verizon'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

	Time Period	Days of Continuing Violation	Base
	June 9, 2018 to November 30, 2018	174	
	June 9, 2018 to March 30, 2019	294	
		Total:	**$32,212,500**

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

[213] Supplemental LOI Response at 16, Response to Question 7.

[214] *Id*. at 2, Response to Question 1.

[215] *Id*. at 16, Response to Question 7.

Accordingly, we find Verizon apparently liable for a forfeiture in the amount of $32,212,500 for its apparent violations of section 222 of the Act and section 64.2010 of our rules.

88. Apparent Violations of Section 222(c)(1) of the Act and Section 64.2007(b) of the Commission's Rules. Although we find that Verizon 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.[216] We thus instead exercise our discretion to admonish Verizon for its unauthorized disclosures of CPNI to Hutcheson.[217]

89. Unlike other federal agencies,[218] the Commission's authority to propose a monetary forfeiture for violations by a common carrier such as Verizon is statutorily limited to the one-year period before issuance of the associated notice of apparent liability.[219] In this case, Hutcheson's unauthorized access to Verizon 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.[220] Accordingly, we are prohibited by statute from imposing a forfeiture penalty when the underlying violation occurred years ago, as was the case with Verizon's unauthorized disclosures to Hutcheson.

90. Upward Adjustment. Given the totality of the circumstances, and consistent with the Commission's *Forfeiture Policy Statement*,[221] 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. Based on its investigation

Verizon knew as early as 2017 that relying on consent records from location-based service providers was not a successful way to protect customer location information from misuse.[222] Yet it continued to rely on an audit mechanism that compared consent records provided by Aggregators to those

[216] *See* 47 U.S.C. § 503(b)(6)(B).

[217] *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).

[218] 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 . . . .").

[219] *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 Verizon on May 3, 2019. As a result, we may assess penalties for conduct going as far back as May 3, 2018.

[220] *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").

[221] *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).

[222] *See* .

same Aggregators' records of location requests: a mechanism that provided little—if any—value in ascertaining whether, in any given instance, the customer had actually consented. Moreover, even those audit records produced by Verizon raise troubling questions about the integrity of the data that Verizon and its auditor Aegis were receiving from the Aggregators. Those records appear to show a troubling rate of noncompliance—including nearly transactions in the first half of 2017 for which its auditor could not find consent records on its first attempt.[223] But rather than considering whether these deficiencies were symptomatic of serious problems with its audit approach, Verizon seeks to brush them off largely as a matter of faulty recordkeeping that it viewed as inevitable.[224] Other evidence of breaches likewise should have reinforced for Verizon that, rather than a consent mechanism that would allow Verizon to confirm that its customers had actually consented to the sharing of their location information, Verizon was using a system that required it to rely on the unverified representations of third parties that had proven unreliable. Verizon failed to adequately appreciate and meaningfully respond to that wide array of evidence of missing or unreliable consent records, instead continuing to sell access to customer location information under its apparently faulty legacy system. This warrants a substantial upward adjustment.

91. 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 Verizon 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.

92. We find that an upward adjustment of 50% above the $32,212,500 base forfeiture, or the amount of $16,106,250, is justified in these circumstances, will protect the interests of consumers, and deter entities from violating the Commission's rules in the future.[225]

93. 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 $48,318,750, for Verizon's apparent willful and repeated violations of section 222 of the Act,[226] as well as section 64.2010 of the Commission's rules.[227]

IV. REQUESTS FOR CONFIDENTIALITY

94. Verizon 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.[228] With respect to the particular information set forth in this Notice of Apparent Liability, we conclude that there is a significant

[223] *See* LOI Response at VZ-0000866, Response to Request for Documents No. 6; Supplemental LOI Response at 20-22, Response to Question 13.

[224] Supplemental LOI Response at 22, Response to Question 13; Bruner Decl. at para. 5.

[225] *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).

[226] 47 U.S.C. § 222.

[227] 47 CFR § 64.2010.

[228] Verizon requested confidential treatment of only a limited amount of information in its responses to the Letters of Inquiry sent by the Enforcement Bureau and, in subsequent correspondence, further narrowed its request. As is relevant here, Verizon currently seeks confidential treatment with respect to (1) the specific terms of its contracts with LocationSmart and Zumigo; (2) the names of the location-based service providers that received Verizon customer location data, and (3) details of audits and investigations Verizon undertook. Letter from David Haga, Associate General Counsel, Verizon Communications, to Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau (Feb. 21, 2020) (on file in EB-TCD-18-00027698).

public interest in revealing this information to the public by publicly releasing an unredacted version of this *Notice*. We further conclude that this interest outweighs whatever competitive harms to Verizon and others might result from the disclosure of this information, and therefore partially deny Verizon's request.

95. 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.[229] At the outset, we find a strong public interest in the public knowing Verizon's practices with respect to the location-based services and customer location information at issue, including to whom the carrier provided access to such information; the steps the Verizon took or failed to take to safeguard this information; and the extent to which any such information was improperly disclosed or otherwise put at risk. 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 Verizon's practices posed to their location data. We further find that the benefits of revealing the information contained in this *Notice* greatly outweigh whatever competitive harms to Verizon might result from its competitors or business partners knowing its policies and the actions it took regarding the disclosure of its customers' location data. We likewise find that the public interest greatly outweighs any private interest Verizon or others may have in keeping confidential the entities with whom Verizon shared customer location data. This is all the more true given that Verizon argues that it required these entities to obtain affirmative consent from Verizon's customers for the sharing of their location data.[230] Thus, the identity of these entities should already be widely known and was required by Verizon to be divulged to its affected customers. And to the extent that Verizon'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 Verizon to keep these identities hidden from, among others, the very customers whose private location information was shared for the commercial benefit of these entities.

96. Because Verizon'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 Verizon or a relevant third party to file a petition for reconsideration;[231] if any party avails itself of this opportunity, we will continue to withhold the information from public inspection until we have ruled on the petition(s).[232] If, after 10 business days, Verizon or a relevant third party has not filed a petition for reconsideration or sought a judicial stay with regard to this partial denial of Verizon's confidentiality request, the material will be made publicly available.[233]

---

[229] *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. § 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).

[230] LOI Response at 2-3, 5, 7.

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

[232] *Cf.* 47 CFR § 0.459(g).

[233] *See* 47 CFR § 0.455(g).

V. ORDERING CLAUSES

97. Accordingly, **IT IS ORDERED** that, pursuant to section 503(b) of the Act[234] and section 1.80 of the Commission's rules,[235] Verizon Communications is hereby **NOTIFIED** of this **APPARENT LIABILITY FOR A FORFEITURE** in the amount of forty-eight million, three hundred and eighteen thousand, seven hundred and fifty dollars ($48,318,750) for willful and repeated violations of section 222 of the Act[236] and section 64.2010 of the Commission's rules.[237]

98. **IT IS FURTHER ORDERED** that Verizon Communications is hereby **ADMONISHED** for its apparent violations of section 222(c) of the Act[238] and section 64.2007 of the Commission's rules.[239]

99. **IT IS FURTHER ORDERED** that, pursuant to section 1.80 of the Commission's rules,[240] within thirty (30) calendar days of the release date of this Notice of Apparent Liability for Forfeiture, Verizon Communications **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 102-103 below.

100. Verizon Communications 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),[241] 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:[242]

- 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).[243] 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.

[234] 47 U.S.C. § 503(b).

[235] 47 CFR § 1.80.

[236] 47 U.S.C. § 222.

[237] 47 CFR § 64.2010.

[238] 47 U.S.C. § 222(c).

[239] 47 CFR § 64.2007.

[240] 47 CFR § 1.80.

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

[242] 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.

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

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

101. 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.[244] 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.

102. 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.[245] 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.

103. 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.

104. **IT IS FURTHER ORDERED**, pursuant to section 0.459(g) of the Commission's rules,[246] that the Requests for Confidential Treatment filed by Verizon Communications in this proceeding **ARE DENIED IN PART**, to the extent specified herein.

[244] *See* 47 CFR § 1.1914.

[245] 47 CFR §§ 1.16, 1.80(f)(3).

[246] 47 CFR § 0.459(g).

105. **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 Craig Silliman, Executive Vice President and Chief Administrative, Legal, and Public Policy Officer, Verizon Communications, c/o David Haga, Associate General Counsel, Verizon Communications, 1320 N. Courthouse Rd., 9th Floor, Arlington, VA 22201.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

STATEMENT OF
CHAIRMAN AJIT PAI

Re: *Verizon Communications*, File No.: EB-TCD-18-00027698.

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: *Verizon Communications*, File No.: EB-TCD-18-00027698.

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: *Verizon Communications*, File No.: EB-TCD-18-00027698.

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: *Verizon Communications*, File No.: EB-TCD-18-00027698.

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.