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

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

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

Heading Paragraph #

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

[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/.

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 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 $12,240,000 against Sprint Corporation (Sprint 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 Sprint apparently disclosed its customers' location information, without their consent, to a third party who was not authorized to receive it. In addition, even after highly publicized incidents put the Company on notice that its safeguards for protecting customer location information were inadequate, Sprint apparently continued to sell access to its customers' location information for more than a year without putting in place reasonable safeguards—leaving its customers' data at unreasonable risk of unauthorized disclosure.

II. BACKGROUND

A. Legal Framework

4. The Act and the Commission's rules govern and limit telecommunications carriers' use and disclosure of certain customer information. Section 222(a) of the Act imposes a general duty on telecommunications carriers to "protect the confidentiality of proprietary information" of "customers."[7] Section 222(c) establishes specific privacy requirements for "customer proprietary network information" or CPNI, namely information relating to the "quantity, technical configuration, type, destination, *location*, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier" and that is "made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[8] The Commission has issued regulations implementing the privacy

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

[3] *Id.*

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

[5] *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 Sprint

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

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

6. Prior to 2007, the Commission's rules permitted telecommunications carriers to share customers' CPNI with joint venture partners and independent contractors for certain purposes based on a customer's "opt-out approval." This means that a customer is deemed to have consented to a particular use of, disclosure of, or access to CPNI after being given notice of the use, disclosure, or access and not objecting thereto.[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

---

are "telecommunications services." *See* 47 U.S.C. § 332(c)(1); H.R. Conf. Rep. No. 104-458 at 125 (1996) ("This definition [of 'telecommunications service'] is intended to include commercial mobile service.").

[9] *See* 47 CFR § 64.2001 *et seq*.

[10] 47 U.S.C. § 222(c)(1) ("Except as required by law *or with the approval of the customer*, a telecommunications carrier that receives or obtains [CPNI] by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable [CPNI] in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.") (emphasis added).

[11] 47 CFR § 64.2007(b).

[12] *Id.* § 64.2003(k).

[13] *See* 47 CFR § 64.2003(l).

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

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

not change the fact that the risk of unauthorized CPNI disclosures increases when such information is provided by a carrier to a joint venture partner or independent contractor.[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

[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 id.* § 64.2010(b)-(d).

[25] *See id.* § 64.2010(e)-(f).

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

[27] *See id.* at 6959, para. 63 (noting that where there is evidence of an unauthorized disclosure, the Commission "will infer . . . that the carrier did not sufficiently protect that customer's CPNI" and that "[a] carrier then must demonstrate that the steps it has taken to protect CPNI from unauthorized disclosure, including the carrier's policies and procedures, are reasonable in light of the threat posed by pretexting and the sensitivity of the customer information at issue"). This approach, which the Commission articulated in the context of pretexting, is particularly applicable here, where a fundamental issue is whether the Company had reasonable measures to ensure that its customers had in fact consented to the disclosure of their CPNI to 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] *2007 CPNI Order*, 22 FCC Rcd at 6959, para. 64 (citing 47 CFR § 64.2010(a)).

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

remain vigilant in their protection of CPNI.[30] The Commission expected that carriers would employ 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

[30] *2007 CPNI Order*, 22 FCC Rcd at 6945-46, para. 34.

[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 cybersecurity and privacy frameworks which feature instructive practices and guidelines for organizations to reference. The publications can be useful in determining whether particular cybersecurity or privacy practices are reasonable by comparison. The model practices identified in the NIST and other frameworks, however, are not legally binding rules, and we do not consider them as such here. The Federal Trade Commission (FTC) and the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC) also offer guidance related to managing data security risks. *See* NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (Apr. 16, 2018), https://nvlpubs nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (NIST Cybersecurity Framework); NIST, The NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0 (Jan. 16, 2020), https://www.nist.gov/privacy-framework/privacy-framework; FTC, Start with Security: A Guide for Business, Lessons Learned from FTC Cases (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Communications 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.

customer location information, federal civil enforcement authority rests with the Federal Trade Commission, an agency of general jurisdiction.[38]

B. Factual Background

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

11. Sprint provides mobile voice and data services to consumers throughout the United States by enabling consumer mobile phones to make and receive calls or transmit data on Sprint's wireless network.[39] The mobile phones of Sprint subscribers, like those of customers of other carriers, periodically register with nearby network signal towers.[40] In general, wireless carriers use the information generated from this registration activity to ensure proper functioning of its network and to provide the services to which its customers subscribe. Because Sprint knows the location of its network signal towers, Sprint is able to calculate the approximate geographic location of the mobile phones communicating with its towers.[41] This type of location information—which is created even when the customer does not have an active established connection, such as a voice call or data usage—may at times be helpful to consumers. For example, in emergencies, the location of a customer's mobile phone can enable first responders and law enforcement to assist. Location information is also used for non-emergency location-based services, such as roadside assistance, delivery tracking, and fraud prevention.[42] 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.[43]

[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.").

[39] *See* Sprint Corporation, 2017 Annual Report, http://www.annualreports.com/HostedData/AnnualReportArchive/s/NYSE_S_2017.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*).

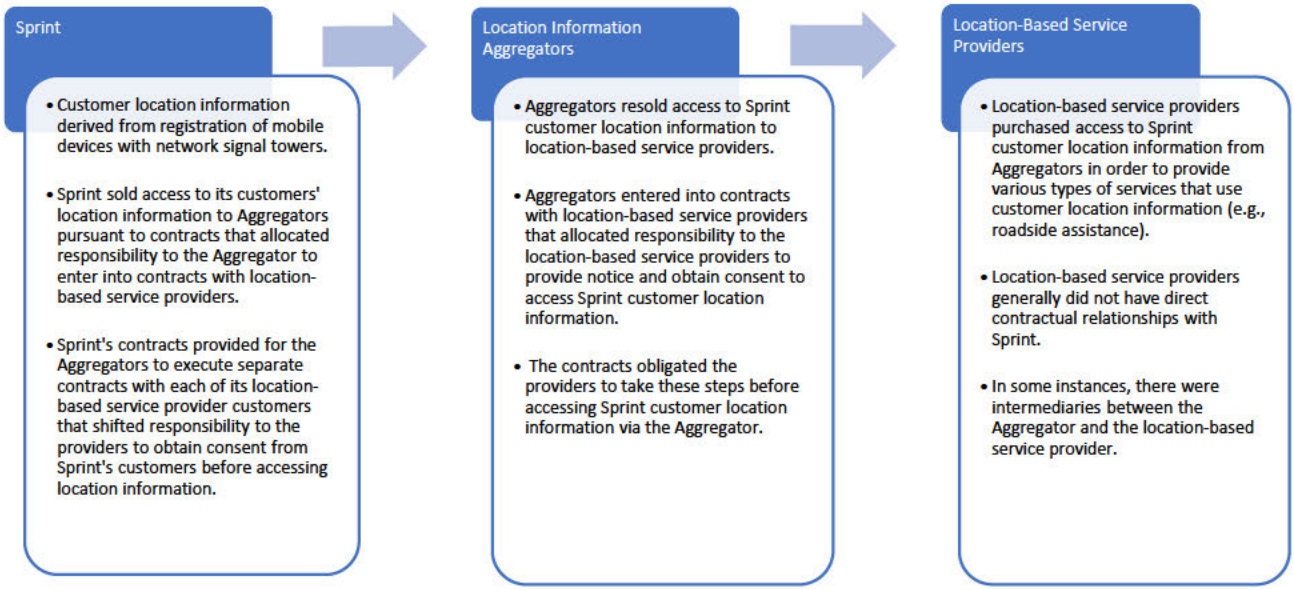
[41] *2012 LBS Report* at 11-12.

[42] Response to Letter of Inquiry from Sprint Corp., to Kristi Thompson, Chief, Telecommunications Consumer Division, FCC Enforcement Bureau, at 1-5, Response to Question 1 (Oct. 16, 2018) (on file in EB-TCD-18-00027700) (LOI Response).

[43] 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.

2. Sprint's Location-Based Services Business Model

12. Until May 31, 2019, Sprint provided location-based service providers access to its customers' location information through a chain of contract-based business arrangements.[44] Sprint 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 "sub-aggregators" or intermediary companies who then resold access to such information to location-based service providers. Sprint had arrangements with two aggregators: LocationSmart and Zumigo (the Aggregators).[45] 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. Sprint apparently sold access to its customers' location information, directly or indirectly, to 86 third parties, including the two Aggregators. The following 77 entities purchased access to Sprint customer location information from LocationSmart: 3Cinteractive;

[44] *See* Response to Supplemental Letter of Inquiry from Sprint Corp., to Kristi Thompson, Chief, Telecommunications Consumer Division, FCC Enforcement Bureau, at 3, Response to Question 1 (Oct. 16, 2018) (on file in EB-TCD-18-00027700) (Supplemental LOI Response).

[45] *See* LOI Response at 2, Response to Question 1; LOI Response at Sprint RD03-000096, Response to Request for Documents No. 3, 2011 Agreement between Sprint Corp., and TechnoCom Corporation d/b/a LocationSmart, at Section 22.11 (A) - Third-Party Developer Privacy Guidance (executed on Feb. 22, 2011, by Mario Proietti, CTO for LocationSmart, and Kevin McGinnis, VP Product, for Sprint Corp.) (Sprint LocationSmart Agreement); LOI Response at Sprint RD03-000134, Response to Request for Documents No. 3, 2013 Agreement between Sprint Corp., and Zumigo Inc., at Section 22.11 (A) - Third-Party Develop Privacy Guidance (executed on Mar. 29, 2013, by Chirag Bakshi, CEO, for Zumigo Inc., and Lisa Small, Sourcing Manager, for Sprint Corp.) (Sprint Zumigo Agreement). Sprint does not contend that its customers consented to these arrangements with the Aggregators.

Securus,

[46] The following 6 entities purchased access to Sprint customer location information from Zumigo: .[47] Additionally, Sprint learned in January 2019 that Zumigo had a seventh client, MicroBilt, that had been receiving Sprint customer location information since 2017 but that had apparently been unknown to Sprint until that time.[48]

14. According to Sprint, it structured its location-based service program in accordance with CTIA's "Best Practices and Guidelines for Location Based Services" (CTIA Guidelines)[49] and contractually required the Aggregators and location-based service providers (which Sprint calls "application developers" or "third-party developers")[50] to comply with those Guidelines.[51]

15. *Sprint's Contracts with the Aggregators.* Pursuant to its contracts with the Aggregators, Sprint provided the Aggregators with access to Sprint's customers' location information and authorized them to share it with sub-aggregators and third-party developers.[52] According to Sprint, subject to certain exceptions not relevant to this investigation, Sprint required customer consent to access or share its customer location information.[53] In describing the types of services that had access to Sprint customer location information through the Aggregators, Sprint describes slightly different notice and consent procedures depending on whether the account holder was a business or an individual and depending on how the user interacted with the application.[54] But, according to Sprint, in all instances, application developers and the Aggregators were "contractually obligated to incorporate conspicuous and stand-alone notice . . . that explains how location information will be accessed, used, stored, disclosed or collected" and that the end user had to "expressly and affirmatively accept the notice before continuing."[55] Also, as Sprint describes it, the Aggregators and developers were required to document the presentation of notice and receipt of consent in each instance and were required to make those records available to Sprint upon

[46] LOI Response at 3-5, Response to Question 3.

[47] *Id.* at 3-5, Response to Question 3.

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

[49] 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. 5, 2020); LOI Response at 1, Response to Question 1.

[50] LOI Response at RD03-000096, Response to Request for Documents No. 3 at Section 22.11 (A), Sprint-LocationSmart Agreement; LOI at RD03-000134, Response to Request for Documents No. 3 at Section 22.11 (A), Sprint-Zumigo Agreement.

[51] LOI Response at 1, Response to Question 1.

[52] LOI at RD03-000096, Response to Request for Documents No. 3 at Section 2, Sprint LocationSmart Agreement); LOI at RD03-000134, Response Request for Documents No. 3 at Section 2, Sprint Zumigo Agreement.

[53] LOI Response at 1, Response to Question 1.

[54] *Id.* at 6, Response to Question 5.

[55] *Id.* at 1, Response to Question 1.

request.[56] In addition, according to Sprint, the Aggregator was contractually obligated to provide the notice record to Sprint before Sprint provided location information to the Aggregator.[57]

16. Sprint did not contract directly with the third-party developers but instead delegated all responsibility to the Aggregators to ensure that the sub-aggregators and application developers complied with "the Aggregator and Third Party Developer obligations" contained in Sprint's contracts with the Aggregators.[58] Among other things, Sprint's agreements with the Aggregators provided for the Aggregators to ensure that the location-based service providers complied with Sprint's privacy policy and consumer protection, marketing, data security laws and regulations in addition to the CTIA Guidelines.[59]

17. Sprint's contracts with the Aggregators established a "Certification" process that required the Aggregators to test the sub-aggregators and location-based service providers' applications to ensure they met Sprint's notice, privacy, and data security requirements.[60] Sprint's contracts with the Aggregators also required the Aggregators to "obtain prior written consent from Sprint 60 days before the use of any [s]ub-[a]ggregator" and gave Sprint sole discretion "to approve or reject each [s]ub-aggregator."[61] The contracts contain no such provision with respect to Aggregators' use of third-party developers.

18. Sprint had broad authority under its contracts with the Aggregators to terminate access to customer location information. Sprint's contract with each Aggregator gave Sprint the right to terminate the agreement for convenience upon 90 days written notice to the Aggregator.[62] Additionally, each contract included a provision that allowed Sprint to terminate the contract with the Aggregator immediately under certain conditions. Specifically, and in relevant part, Sprint could trigger immediate termination if the Aggregator (1) failed to impose required obligations on its location-based service provider clients; (2) failed to comply with the contract terms specifying non-disclosure of sensitive information (such as the location information at issue here); (3) failed to "employ administrative, physical, and technical safeguards . . . that prevent the unauthorized collection, access, disclosure, and use" of information provided by Sprint; (4) failed to ensure that the Aggregator's location-based service provider clients complied with Sprint's customer notice requirements; or (5) negligently or knowingly misrepresented the location-based service provider's service or application.[63] The contracts permitted Sprint to immediately suspend or terminate an Aggregator's access to customer location information for

[56] *Id.* at 6, Response to Question 5.

[57] *Id.*

[58] LOI at RD03-000096, Response to Request for Documents No. 3 at Section 2.2-2.3, Sprint-LocationSmart Agreement; LOI at RD03-000134, Response to Request for Documents No. 3 at Section 2.2-2.3, Sprint-Zumigo Agreement.

[59] LOI at RD03-000096, Response to Request for Documents No. 3 at Section 22.11, Sprint LocationSmart Agreement; LOI at RD03-000134, Response to Request for Documents No. 3 at Section 22.11, Sprint Zumigo Agreement.

[60] LOI at RD03-000096, Response to Request for Documents No. 3 at Section 12, Sprint-LocationSmart Agreement; LOI at RD03-000134, Response to Request for Documents No. 3 at Section 12, Sprint-Zumigo Agreement.

[61] LOI at RD03-000096, Response to Request for Documents No. 3 at Section 2.2, Sprint-LocationSmart Agreement; LOI at RD03-000134, Response to Request for Documents No. 3 at Section 2.2, Sprint Zumigo Agreement.

[62] LOI at RD03-000096, Response to Request for Documents No. 3 at Section 2.2, Sprint-LocationSmart Agreement; LOI at RD03-000134, Response to Request for Documents No. 3 at Section 2.2, Sprint Zumigo Agreement.

[63] LOI at RD03-000096, Response to Request for Documents No. 3 at Section 21, Sprint-LocationSmart Agreement; LOI at RD03-000134, Response Request for Documents No. 3 at Section 21, Sprint-Zumigo Agreement.

reasons that included a breach of the Aggregator's contractual obligations.[64] Sprint also had the right to immediately suspend the transmission of location information by the Aggregator to any sub-aggregator or location-based service provider that Sprint believed was not complying with the obligations that the Aggregators were directed to impose upon them.[65]

19. *Sprint's Contractual Right to Review and Audit*. Pursuant to the terms of its contracts with the Aggregators, Sprint maintained the right to assess compliance with the terms of agreements with Aggregators, and could seek "reports, full and complete access to relevant facilities, books, records, procedures, and information."[66] Sprint's standard contract terms also gave it the right to audit the Aggregators' performance once every 12 months.[67] Sprint also had the right to perform audits at any time as necessary if it had a good faith reason to believe a breach of privacy and security obligations had occurred.[68] Sprint offers no evidence that it exercised any of those contractual provisions before 2018. Sprint does claim that it conducted a legal review of both LocationSmart and Zumigo in 2018 but, citing privilege, refused to specify when each review occurred and refused to provide any information about either of them.[69]

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

20. On May 10, 2018, the *New York Times* reported on security breaches involving Sprint's (and other carriers') practice of selling access to customer location information.[70] Specifically, Securus Technologies, Inc. (Securus), a provider of telecommunications services to correctional facilities throughout the United States, also operated a "location-finding service" that enabled law enforcement and corrections officials to access the location of a mobile device belonging to customers of major wireless carriers, including Sprint, *without* the device owner's knowledge or consent.[71] 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.[72] Securus did not, however, assess the adequacy of the purported legal authorizations submitted by users of its location-finding service.[73]

21. 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.[74]

---

[64] LOI Response at 7, Response to Question 5.

[65] LOI at RD03-000096, Response to Request for Documents No. 3 at Section 14, Sprint-LocationSmart Agreement; LOI at RD03-000134, Response to Request for Documents No. 3 at Section 14, Sprint-Zumigo Agreement.

[66] LOI Response at 7, Response to Question 5; LOI Response at RD03-000096, Response to Request for Documents No. 3 at Section 22.7, Sprint-LocationSmart Agreement; LOI at RD03-000134, Response to Request for Documents No. 3 at Section 22.7, Sprint-Zumigo Agreement.

[67] Supplemental LOI Response at 6, Response to Question 5; LOI at RD03-000096, Response to Request for Documents No. 3 at Section 29.7, Sprint-LocationSmart Agreement; LOI at RD03-000134, Response to Request for Documents No. 3 at Section 29.7, Sprint-Zumigo Agreement.

[68] Supplemental LOI Response at 6-7, Response to Question 5.

[69] LOI Response at 9, Response to Question 11; Supplemental LOI Response at 11, Response to Question 10.

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

[71] *Id.*

[72] *Id.*

[73] *Id*.

[74] *Id.*

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.[75] 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.[76]

22. Sprint does not deny the existence of the Securus location-finding service nor the abuse of that system by Hutcheson. Instead, Sprint explains that Securus apparently misrepresented to 3Cinteractive (a sub-aggregator of LocationSmart) and LocationSmart the purpose for which it was accessing information.[77] According to Sprint, Securus had represented to 3Cinteractive and LocationSmart that it was using Sprint's customer location information only to geolocate Sprint customers who received collect calls from inmates at correctional institutions.[78] In fact, Sprint explains its failure to detect Securus's activities as the result of Securus's misrepresentations to 3Cinteractive and LocationSmart about the purpose(s) for which Securus used Sprint's customer location information.[79] Sprint is unequivocal in saying that Securus was not authorized to use its customer location information in support of ongoing criminal investigations.[80]

23. On May 17, 2018, Sprint terminated Securus's access to the Company's customer location information.[81] According to Sprint, Securus has declined to provide Sprint with information about its access to Sprint's customer location information for any purpose other than locating the recipients of collect calls from prison phones.[82] As a result, Sprint has not identified the scope of unauthorized activity, nor determined how many other individuals like Hutcheson may have abused their access to the Securus service. Sprint claims that it "has not discovered any confirmed incidents involving unauthorized access to Sprint [c]ustomer [l]ocation [i]nformation by Securus, Securus' correctional institution customers, other [location-based service providers], or other third parties."[83] Evidence obtained by the Enforcement Bureau, however, indicates that Hutcheson unlawfully accessed the location information of at least 18 Sprint customers.[84]

24. On May 25, 2018, Sprint suspended sharing customer location information with LocationSmart after confirming that data sharing through LocationSmart and 3Cinteractive "had occurred for an unknown and unapproved purpose."[85] This suspension effectively terminated access to Sprint

[75] *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.

[76] *See* Complaint, *William T. Cooper et al. vs. Sheriff Cory Hutcheson*, Case: 1:17-cv-00073 (E.D. Mo. May 8, 2017).

[77] LOI Response at 8, Response to Question 8.

[78] *Id*.

[79] *Id.*

[80] *See* Securus Technologies Location-based Services (LBS) White Paper (Feb. 21, 2018) (on file in EB-TCD-18-00027704).

[81] Supplemental LOI Response at 10, Response to Question 7.

[82] LOI Response at 9, Response to Question 12.

[83] Supplemental LOI Response at 12, Response to Question 11.

[84] *See* Department of Justice Evidence Records (on file in EB-TCD-18-00027700).

[85] LOI Response at 7, Response to Question 6.

wireless customer location information for LocationSmart and the 77 entities that purchased access through LocationSmart.

25. On June 20, 2018, Sprint "moved to terminate," as Sprint describes it, its contracts with both Aggregators.[86] According to Sprint, it terminated LocationSmart's contract immediately on June 20, 2018.[87] Also according to Sprint, it provided the 90-day notice of termination to Zumigo on June 20, 2018 that the then-existing agreement would terminate on September 18, 2018.[88]

26. At the same time, in June 2018, Sprint began formalizing a "[Location-Based Services] Methods & Procedures" protocol (Methods & Procedures) to "complement" the contract protections for future Aggregators and location-based services.[89] These Methods & Procedures were finalized in August 2018.[90] Sprint points to several obligations that provided more specific direction than was in the Aggregator contracts.[91] For example, unlike the Aggregator contracts, the Methods & Procedures required Aggregators to submit reports to Sprint that provided detailed information about all companies (including aggregators and sub-aggregators) that used Sprint customer location information. The reports also had to include detailed information about how the Sprint customer location information was or would be used.[92] Sprint's Methods & Procedures also provided expanded internal guidance on what information it could seek in auditing its location-based services partners, including reviewing compliance with notice and consent requirements; reviewing a list of companies to which the Aggregator provides location services; reviewing the Aggregator's process for validating companies receiving location data; reviewing the Aggregator's partners methods and procedures related to privacy; and reviewing the Aggregator's privacy and security training for location-based services customers.[93] Sprint asserts in particular that the new obligations on the Aggregators "included a requirement for an independent third-party audit of the Location Aggregators on their privacy and data security practices."[94] Sprint does not explain how, or whether, the Methods & Procedures auditing and review process differed from the audits that Sprint had the right to conduct under the original contracts.

27. On or around August 23, 2018, Sprint re-launched its aggregator location-based services program. Specifically, Sprint executed two new agreements with LocationSmart to permit that Aggregator to access Sprint customer location information to serve two specific location-based service providers: (1) ;[95] and (2)

[86] *Id.*

[87] Letter from Sean Olsen, Manager, Contract Administration, Sprint Corp., to Mario Proietti, CEO, Masoud Motamedi, President, TechnoCom Corporation/Locaid d/b/a LocationSmart (June 20, 2018) (on file in EB-TCD-18-00027700).

[88] LOI Response at RD03-000180, Response to Request for Documents No. 3.

[89] LOI Response at 7, Response to Question 6.

[90] *Id.*

[91] Supplemental LOI Response at 6-8, Response to Question 4.

[92] *Id.* at 6, Response to Question 4.

[93] *Id.*at 7, Response to Question 4.

[94] *Id.* at 6-7, Response to Question 4.

[95] Supplemental LOI Response at 3, Response to Question 1; LOI Response at Sprint RD03-000001, Response to Request for Documents No. 3, 2013 Agreement between Sprint Corp., and TechnoCom Corporation d/b/a LocationSmart (executed on Aug. 24, 2018, by Masoud Motamedi, President for LocationSmart and Sean N. Olson, Manager, Contracts, for Sprint Corp.).

."[96] The new LocationSmart agreements allowed LocationSmart to obtain Sprint customer location information for 90 days, with monthly renewal up to one year.[97]

28. On September 18, 2018, Sprint's contract with Zumigo terminated.[98] On October 16, 2018, Sprint renewed its previously terminated contract with Zumigo in its entirety—meaning that all of Zumigo's prior location-based service provider clients again had access to Sprint's customer location information.[99] According to Sprint, it decided to revive its agreements with Zumigo and LocationSmart because "Sprint customers were seriously impacted by the lack of [location-based] services that had been provided by Location Aggregators, particularly for roadside assistance or compliance with certain state requirements."[100]

29. On January 8, 2019, *Motherboard* published an article titled "I Gave a Bounty Hunter $300. Then He Located Our Phone."[101] The article alleged that access to customer location information was sold and resold, with little or no oversight, within the bail bonds industry, and that this led to consumers being tracked without their knowledge or consent.[102] To illustrate the practice, the article described how a "bounty hunter" paid by *Motherboard* used his contacts in the bail bonds industry to access the location of a T-Mobile user's mobile phone.[103] The bounty hunter reportedly received the information from an employee of a bail bonds company that was a customer of MicroBilt, a credit reporting and consumer finance company.[104] MicroBilt, in turn, was a customer of Zumigo, an Aggregator that received customer location information from Sprint and the other major wireless carriers.[105]

30. Sprint does not deny that MicroBilt, acting as Zumigo' s customer, received Sprint customer location information. But Sprint claims that it was unable to "identify any record of Zumigo obtaining Sprint's prior written consent before using MicroBilt as a sub-aggregator."[106] According to Sprint, the Company only became aware that Zumigo was providing location-based services to MicroBilt through media reports.[107] Sprint concedes that it was unable to verify whether Sprint's own credentialing process had been followed with respect to MicroBilt, and that Sprint had no information about whether MicroBilt complied with Sprint's notice-and-consent processes.[108] According to Sprint, Zumigo contended that Vice Media, a MicroBilt customer, intentionally provided fraudulent information to, and

[96] Supplemental LOI Response at 3, Response to Question 1; LOI Response at Sprint RD03-000032, Response to Request for Documents No. 3, 2013 Agreement between Sprint Corp., and TechnoCom Corporation d/b/a LocationSmart, (executed on Aug. 28, 2018, by Masoud Motamedi, President for LocationSmart and Sean N. Olson, Manager, Contracts, for Sprint Corp.).

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

[98] LOI Response at RD03-000180, Response to Request for Documents No. 3.

[99] LOI Response at RD03-000183, Response to Request for Documents No. 3.

[100] LOI Response at 7-8, Response to Question 6.

[101] Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone*, Motherboard (Jan. 8. 2019), https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-MicroBilt-zumigo-tmobile.

[102] *Id.*

[103] *Id.*

[104] *Id.*

[105] *Id.*

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

[107] *Id.*

[108] *Id.*

paid a rogue employee of, a state-licensed bail bond agency to process the mobile number.[109] This, Sprint claims, was not an approved use of the location information by MicroBilt and violated the end-user agreement with the bail bond company.[110] According to Sprint, the Company demanded that Zumigo provide additional information and details concerning the relationship between Zumigo and MicroBilt, but Zumigo did not respond to those requests.[111] On January 9, 2019, Sprint terminated its contract with Zumigo.[112]

31. On May 31, 2019—or 386 days after the *New York Times* reported on the Securus location-finding service, as well as the abuse of that service by Hutcheson—Sprint terminated all contracts to provide location-based services to the Aggregators.[113]

32. *Commission Investigation*. The Enforcement Bureau launched an investigation in May 2018 immediately following the *New York Times* report of unauthorized location tracking involving Securus. The Bureau issued a Letter of Inquiry (LOI) to Sprint 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.[114] The Bureau requested additional information and documents from Sprint in 2019.[115] Sprint submitted responses to the Bureau's initial and supplemental LOIs, as well as approximately 2,500 pages of responsive documents concerning its sale of access to its customer location information to third parties.[116]

III. DISCUSSION

33. We find that Sprint 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.

34. 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."[117] In particular, we find that for more than a year after Sprint became aware of Securus's unapproved location-finding service—and thereby had notice that Sprint's contractual arrangements with location-based service providers did not ensure compliance with Sprint's privacy and CPNI obligations—the Company's continued reliance on such attenuated contractual arrangements and

[109] Supplemental LOI Response at 2-3, Response to Question 1.

[110] *Id.*

[111] *Id.* at 9, Response to Question 5.

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

[113] *Id.* at 11, Response to Question 7.

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

[115] Supplemental Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to Maureen Cooney, Head of Privacy, Office of Privacy, Government Affairs, Sprint Corp. (Apr. 8, 2019) (on file in EB-TCD-18-00027700) (Supplemental LOI).

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

[117] 47 CFR § 64.2010(a).

ineffective monitoring tools apparently did not meet the reasonableness requirement of section 64.2010(a).

A. Customer Location Information Constitutes CPNI

35. 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.

36. 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."[118] 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."[119]

37. The customer location information at issue here meets these two criteria. *First*, it relates to the location of a telecommunications service, i.e., Sprint's commercial mobile service.[120] The location data was derived from the wireless mobile devices of Sprint'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. Sprint is therefore providing telecommunications service to these customers whenever it is enabling the customer's device to send and receive calls—regardless of whether the device is actively in use for a call. This view finds ample support in Commission precedent, including the *2013 CPNI Declaratory Ruling*, which indicates that the policy considerations remain the same throughout a consumer's use of a mobile device, including the entire process through which the device stands ready to make or receive a call.[121]

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

39. Sprint asserts that the customer location information it shares with Aggregators and

---

[118] 47 U.S.C. § 222(h)(1)(A) (emphasis added).

[119] *Id.* § 222(h)(1)(A) (defining "customer proprietary network information").

[120] *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").

[121] *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).

location-based service providers, "does not reveal any call details or contain any information regarding a network event" and therefore is not CPNI.[122] We disagree. Location information generated and collected by carriers while a phone is in standby mode (i.e., while a phone is on, but not actively in use during a call) is not 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.

40. 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. 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.[123] 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.

41. Next, Sprint seeks refuge in the *2013 CPNI Declaratory Ruling*, in which the Commission addressed the applicability of our CPNI rules to situations in which "such information is collected by the customer's device."[124] Sprint appears to claim that because the Commission identified certain customer location information—such as when calls fail, "network events" including dropped, received, and dialed calls, and other location information that reveal call details—as CPNI, the Commission implicitly found that any other customer location information is not CPNI.[125] This argument fails for the simple fact that the Commission went out of its way to disclaim any such intent. It "f[ou]nd no reason at this time to set out a comprehensive list of data elements that pertain to a telecommunications service and satisfy the definition of CPNI and those data elements that do not," observing that it "has never before created such a comprehensive list of CPNI, and [it] ha[d] had no indication that the absence of such a list has caused any significant confusion in the industry."[126] That statement is no surprise given that the entire purpose of the *2013 CPNI Declaratory Ruling* was to address a different subject—whether "information . . . that fits the statutory definition of customer proprietary network information" must be protected when collected by a customer's mobile device.[127]

42. Sprint's next argument is that the downstream services that rely on customer location information—like roadside assistance services—are "'information services,' the provision of which does not require approval for use, disclosure or access.'"[128] And Sprint points out that section 64.2005(b)(1) of our rules states that "[a] wireless provider may use, disclose, or permit access to CPNI derived from its

[122] LOI Response at 5, Response to Question 4.

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

[124] *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, 9610, para. 4 (2013) (*2013 CPNI Declaratory Ruling*).

[125] LOI Response at 5, Response to Question 4.

[126] *2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9617, para. 24 n.54.

[127] *Id.* at 9610, para. 4.

[128] Supplemental LOI Response at 3, Response to Question 2.

provision of CMRS, without customer approval, for the provision of . . . information service(s)."[129] But that rule does not save Sprint here. Sprint of course is *not* the entity providing the information service; instead, Sprint is the carrier selling access to its customers' location information. And if we were to take Sprint's apparent reading—that section 64.2005(b)(1) allows carriers to sell access to customer information without their consent to *any* information service provider—there would be nothing left of the statutory protections. The exception would swallow the rule. So it's no surprise that the Commission took a much narrower reading when it adopted this rule that the exception is limited to the use or disclosure of CPNI for that same wireless provider to provide *its own* information service to *that same* customer.[130] In other words, section 64.2005(b)(1) does not authorize a wireless carrier to sell access to CPNI to anyone without customer approval and thus it does not cover Sprint's conduct here.

43. To the extent Sprint is attempting to argue that it is acting as an information service provider when it is selling access to its customers' location information, we again disagree. The definition of CPNI does not depend on the amount of use of telecommunications services relative to a carrier's other service offerings nor the classification of the service that initiated the request for the carrier's location data. Although Sprint (or others) might also provide non-common-carrier services to the same customer, Sprint has its relationship with the customer because the customer has chosen Sprint to be its provider of telecommunications service—that is, by virtue of the carrier-customer relationship. We reject Sprint's overly narrow reading of this common-sense meaning of the statute, which would have the perverse effect of eliminating the statutory protections of the most sensitive types of CPNI contrary to the clear intent of Congress.

44. Sprint's last tack is to argue that its disclosure of customer location information does not reveal any call details or contain any information regarding a network event and does not provide information regarding a customers' use of a telecommunications service.[131] In making this assertion, Sprint 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. Sprint's own internal training documents seem to acknowledge as much. A June 2018 training presentation, for example, notes that, with respect to the delivery of voice calls and data services, "[m]obile service has always required network awareness of device location to appropriately route communications."[132] We find Sprint's arguments unpersuasive, particularly in light of the more straightforward reading of the statutory text.

45. 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,[133] also apply to that customer location information.

[129] 47 CFR § 64.2005(b)(1); *see also* Supplemental LOI Response at 4, Response to Question 2.

[130] *Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, 14432-33, paras. 42-43 (1999).

[131] LOI Response at 5, Response to Question 4; Supplemental LOI Response at 3, Response to Question 2.

[132] LOI Response at Sprint RD02-000001, Response to Request for Documents No. 2, Sprint, *Privacy Protection and Location Based Services* at 4 (June 2018).

[133] 47 CFR § 64.2003(g).

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

46. Sprint 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.[134] 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.[135]

47. The evidence reflects that Hutcheson used the Securus service to obtain the location information of Sprint customers. Sprint 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 Sprint customer consent for the disclosures. The evidence shows that between 2014 and 2017, at least 18 Sprint customers' location information was disclosed to Hutcheson, via Securus, without the customers' consent.[136] Notwithstanding the misconduct of Hutcheson, each such disclosure constitutes a violation of section 222(c)(1) of the Act and section 64.2007 of the Commission's rules for which Sprint is responsible.

48. Sprint 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, Sprint explains that notwithstanding the customer notice and authorization requirements it imposed on LocationSmart (and that LocationSmart then imposed on 3Cinteractive and Securus), Securus misrepresented to 3Cinteractive and LocationSmart the purpose for which it was collecting customer location information, which was limited to geolocation for called parties for collect calls places by prison inmates.[137] In doing so, Securus operated an unapproved location-finding service through which Hutcheson and other law enforcement personnel could access location information without providing notice to, or obtaining consent from, the relevant Sprint customers.[138]

49. We find these arguments unavailing. Sprint 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, Sprint. The restrictions on the use and disclosure of CPNI in section 222 of the Act expressly apply to "telecommunications carriers."[139] 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).[140] Apart from a few exceptions not relevant here,[141] section 222 allows a telecommunications carrier to use CPNI for

[134] 47 U.S.C. § 222(c)(1). There are exceptions in circumstances not relevant here.

[135] 47 CFR § 64.2007(b). There are exceptions in circumstances not relevant here.

[136] *See* Department of Justice Evidence Records (on file in EB-TCD-18-00027700).

[137] LOI Response at 8, Response to Question 8.

[138] *Id.*

[139] 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).

[140] *See* 47 U.S.C. § 222(c)(1).

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

other purposes only where "required by law or with the approval of the customer."[142] 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.

50. 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.[143] 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.[144] 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 notification of *the carrier's* request."[145] This was necessary in part "because a carrier is no longer in a position to personally protect the CPNI once it is shared."[146]

51. 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.[147] 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."[148] In other words, a carrier cannot avoid its statutory obligations by assigning them to a third party.

52. 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.[149] 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,'"[150] 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

[142] *Id.* § 222(c)(1).

[143] *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).

[144] *2007 CPNI Order*, 22 FCC Rcd at 6928-29, para. 2.

[145] 47 CFR § 64.2003(k) (defining "opt-in approval") (emphases added).

[146] *2007 CPNI Order*, 22 FCC Rcd at 6948, para. 39.

[147] 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. Sprint does not appear to argue that situation is present here.

[148] 47 U.S.C. § 217.

[149] *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).

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

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.[151] 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."[152]

53. At bottom, Sprint may not have it both ways. If Sprint was relying on third parties to satisfy its obligations to obtain consent, then it is as liable for those third parties' failures as it would be if they had been the failures of Sprint itself. If not, then Sprint effectively granted those third parties the capability to access the CPNI of its customers without customer approval.

54. In sum, we find that Sprint 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.[153]

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

55. Sprint apparently violated section 222 of the Act and section 64.2010 of our CPNI Rules by failing to take reasonable measures to discover and protect against attempts to gain unauthorized access to its customers' location information.[154] The May 10, 2018 *New York Times* report on the Securus and Hutcheson breaches exposed serious inadequacies with the safeguards on which Sprint relied to protect its customers' location information. Our investigation shows that Sprint failed to promptly address those inadequacies. We therefore conclude that Sprint apparently failed to take reasonable measures in a timely fashion to protect its customers' CPNI following that report.

56. 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.[155] 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.[156]

57. Sprint thus bears the burden of demonstrating that the measures it took to safeguard CPNI were reasonable both before and after the Securus and Hutcheson breach. And yet, Sprint's responses suggest it took a somewhat haphazard approach to compliance. In general, Sprint relied on the same safeguards discussed below both before and after the May 10, 2018, report of the Securus and Hutcheson breach.

58. *First*, the primary and seemingly exclusive measure that Sprint took to safeguard the location data of its customers was to impose certain privacy-related obligations on Aggregators, who in

[151] *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).

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

[153] 47 U.S.C. § 222(c)(1); 47 CFR § 64.2007(b).

[154] 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.").

[155] *2007 CPNI Order*, 22 FCC Rcd at 6959-60, para. 65.

[156] *Id.*

turn were contractually obligated to impose privacy safeguards on location-based service providers.[157] Among other things, Sprint established a "Certification" process that required the Aggregator to test the sub-aggregators and location-based service providers' applications to ensure they met Sprint's notice, privacy, and data security requirements.[158] Sprint's contracts with the Aggregators also required the Aggregators to meet Sprint's certification requirements and to receive written approval from Sprint prior to providing any sub-aggregator/location-based service provider access to Sprint's customer location information.[159] After a sub-aggregator and location-based service provider had been certified, the Aggregator had an ongoing responsibility to ensure that sub-aggregators and location-based providers were in compliance with Sprint's notice, privacy, and CPNI obligations.[160] These obligations included the requirements (1) that location-based service providers comply with a number of privacy guidelines, including the CTIA Guidelines, and (2) that location-based service providers supply notice to and obtain the express, affirmative consent of customers prior to sharing any location information."[161]

59. At least before the *New York Times* report, these contractual safeguards apparently represented the whole of Sprint's efforts to safeguard its customers' location data. Sprint's contracts with the Aggregators strove to ensure that responsibility for complying with these safeguards rested with the Aggregators—and not with Sprint.[162] But the Securus and Hutcheson breaches demonstrated that these contractual safeguards—particularly as implemented by Sprint—were insufficient to prevent misuse. In particular, notwithstanding Sprint's contract with LocationSmart, LocationSmart's contract with 3Cinteractive, and 3Cinteractive's contract with Securus (a contract that Sprint was not a party to) for the use of Sprint's customer location information, 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 and without Sprint's knowledge.

60. *Second*, Sprint's responses to the Enforcement Bureau's inquiries make much of its right to police compliance with the contractual safeguards described above. For example, Sprint notes that its "contracts have maintained the right to audit performance of [its contractual safeguards], which includes seeking reports, full and complete access to relevant facilities, books, records, procedures, and information to assess compliance."[163] Sprint notes that it had the right to perform these audits annually or

[157] LOI Response at RD03-000096, Response to Request for Documents No. 3 at Section 5.1 (A), Sprint-LocationSmart Agreement; LOI Response at RD03-000134, Response to Request for Documents No. 3 at Section 5.1 (A), Sprint-Zumigo Agreement.

[158] LOI at RD03-000096, Response to Request for Documents No. 3 at Section 12, Sprint-LocationSmart Agreement; LOI at RD03-000134, Response to Request for Documents No. 3 at Section 12, Sprint-Zumigo Agreement.

[159] LOI Response at RD03-000096, Response to Request for Documents No. 3 at Section 2.2, Sprint-LocationSmart Agreement; LOI Response at RD03-000134, Response to Request for Documents No. 3 at Section 2.2, Sprint-Zumigo Agreement.

[160] LOI Response at RD03-000096, Response to Request for Documents No. 3 at Section 2.4 and 5.1, Sprint-LocationSmart Agreement; LOI Response at RD03-000134, Response to Request for Documents No. 3 at Section 2.4 and 5.1, Sprint-Zumigo Agreement.

[161] *See generally* LOI Response at Sprint RD03-000096, Response to Request for Documents No. 3, LocationSmart Agreement, Section 22.11 (Third-Party Developer Guidance).

[162] For example, Section 22.3 of Sprint's contract with LocationSmart, entitled "Safeguards," states that the "Aggregator is fully responsible for any unauthorized collection, access, disclosure, and use of, and access to, Sprint Information." LOI Response at RD03-000108, Response to Request for Documents No. 3, Sprint-LocationSmart Agreement, Section 22.3; *see also id.* Sprint-LocationSmart Agreement, Section 22.9 (Indemnification).

[163] Supplemental LOI Response at 6, 10, Response to Questions 4, 6.

whenever it had "a good faith reason to believe a breach of privacy obligations occurred."[164] And Sprint boasts of a long list of topics that such an audit could explore, including (1) documentation of consent; (2) compliance with CTIA Guidelines; (3) the list of companies to whom an Aggregator provides location data; (4) privacy practices of an Aggregator and its partners; and (5) the purposes for which location data is shared with recipient companies.[165]

61. Yet there is no evidence that Sprint ever conducted such an audit prior to the May 2018 *New York Times* report. In fact, there is no evidence that Sprint ever policed the Aggregators' access and use of customer location information in any meaningful way. For example, Sprint provides no evidence that it attempted to verify consent records at all prior to the May 2018 *New York Times* report.[166] And though Sprint apparently conducted at least two limited legal reviews and "commissioned an independent security audit" in 2019 of its policies and practices related to disclosing location information to third parties, it has refused to provide the results of those assessments.[167] In sum, Sprint's contractual rights to police compliance were apparently never exercised and largely meaningless.

62. *Third*, Sprint emphasizes that it structured its location-based service program in accordance with CTIA's "Best Practices and Guidelines for Location Based Services" (CTIA Guidelines) and required the Aggregators and location-based service providers to comply with the CTIA Guidelines, which call on location-based service providers to provide notice and receive consent to use and share customer location information.[168] Those guidelines focus on best practices for notice and consent by location-based service providers. But they do not include best practices recommendations for carriers that sell access to their customers' location information to location-based service providers. For example, they do not offer guidance to carriers on how to assure that location-based service providers comply with a contractual obligation to access location information only after furnishing proper notice and receiving customer consent.

63. In sum, the safeguards implemented by Sprint to protect customer location information against unauthorized use relied almost entirely on a chain of contractual agreements that effectively delegated operational responsibility down to location-based service providers. What limited power Sprint had to verify or otherwise demand compliance, it did not appear to exercise. And it had almost no other visibility into or apparent awareness of how the location data it sold was used or protected. While business relationships often rely on trusting a counterparty to honor its contractual obligations, it is hard to conclude that such trust alone was a reasonable safeguard here—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 Sprint of the high risk that bad actors would attempt to gain unauthorized access to Sprint's customers' CPNI, particularly by trying to find ways around any contractual safeguards Sprint put in place to authenticate that its customers were actually providing consent to third parties' access to their location information.

---

[164] *Id.* at 5-6, Response to Question 4; *see also* LOI Response at RD03-000096, Response to Request for Documents No. 3 at Section 22.7, Sprint-LocationSmart Agreement

[165] Supplemental LOI Response at 7-8, Response to Question 4; *see also* LOI Response at RD03-000096, Response to Request for Document No. 3 at Section 22.7, Sprint-LocationSmart Agreement.

[166] LOI Response at 7, Response to Question 5; LOI Response at Sprint RD03-000178, Response to Document Request No. 3, Letter from Sean Olsen, Manager, Contract Administration, Sprint, to Masoud Motamedi, President, TechnoCom Corporation/Locaid d/b/a LocationSmart (May 25, 2018). That said, Sprint notified LocationSmart that it was exercising its contractual right to an audit in the wake of receiving an inquiry from Senator Ron Wyden.

[167] LOI Response at 9, Response to Question 11; Supplemental LOI Response at 11-12, Response to Question 10.

[168] LOI Response at 1, Response to Question 1; Supplemental LOI Response at 9, Response to Question 5. *See also* Supplemental LOI Response at 7, Response to Question 4 (listing "[r]eviewing the aggregators compliance with CTIA's Guidelines of [Location Based Services] Best Practices" as a basis for audit by Sprint).

64. Setting aside the inadequacy of Sprint's safeguards before disclosure of the Securus and Hutcheson breaches, Sprint was on clear notice that its safeguards were inadequate after the disclosure, and so we focus on the actions that Sprint took, or failed to take, after discovery of that breach. We find that Sprint has apparently failed to demonstrate that its safeguards were reasonable following the disclosure of Securus's unauthorized location-finding service in May 2018. The Securus incident laid bare the fundamental weaknesses of Sprint's safeguards with respect to the third parties to which it entrusted its customers' location information. Although Sprint moved to suspend the program while it investigated the Securus breach, Sprint soon reconstituted its contractual relationships with both LocationSmart and Zumigo with a few ostensibly new safeguards. In other words, for 386 days after that incident came to light, Sprint continued to sell access to its customers' location information to multiple entities under essentially the same system that had allowed (1) Securus to provide location information in a manner inconsistent with its authorized uses of location data and (2) Hutcheson to easily and improperly access Sprint customer location information. Relying on demonstrably faulty safeguards in the wake of this incident does not appear to have been reasonable.

65. There are several commonsense measures that Sprint could have taken following the May 2018 *New York Times* article. One obvious measure would have been to identify the companies involved in the Securus breach and terminate their access until it could verify that these companies had properly safeguarded its customers' location data. In this respect, Sprint took the reasonable step of suspending access for all three companies involved in the breach—Securus, 3CInteractive, and LocationSmart—on May 25, 2018. This decision had the collateral consequence of also suspending service for another 75 entities that had relied on LocationSmart for access.

66. But three months later, Sprint undermined this step by reinstating LocationSmart (and two of its customers) into the program. And while such reinstatement may have been reasonable if Sprint had completed some significant review to determine that LocationSmart's access was no longer a threat to its customers, that was not apparently Sprint's reasoning. Instead it decided to revive its agreements with Zumigo and LocationSmart because "Sprint customers were seriously impacted by the lack of [location-based] services that had been provided by Location Aggregators, particularly for roadside assistance or compliance with certain state requirements."[169]

67. Another measure would have been to promptly ascertain the full scope and extent of the Securus breach. Sprint does allege that it "conducted a legal review of the allegations presented in Senator [Ron] Wyden's letter of May 8, 2018" to the Company.[170] But because Sprint declined to provide the details of this audit to the Commission's Enforcement Bureau, it is impossible for us to conclude that (1) the scope of the investigation was reasonable, or (2) that Sprint took reasonable steps in light of its audit findings, which Sprint has likewise refused to provide to the Bureau. Again, it is *Sprint* that bears the burden of demonstrating the reasonableness of its practices in the wake of an unauthorized disclosure.[171]

68. The weakness of Sprint's arguments that its contract-based model provided reasonable protection of CPNI is further underscored by Sprint's inability to compel Securus to cooperate with Sprint's investigation into unauthorized access to its customers' location information. Sprint notes that Securus "decline[d] to provide details" about its unauthorized location-finding service to Sprint.[172] As a result, the full impact of Securus's unauthorized access to CPNI apparently remains unknown to Sprint even to this day. Similarly, after subsequent news reports, Sprint attempted to obtain additional

[169] LOI Response at 7-8, Response to Question 6.

[170] *Id.* at 9, Response to Question 11.

[171] *2007 CPNI Order*, 22 FCC Rcd at 6959–60, para. 65.

[172] Supplemental LOI Response at 10, Response to Question 7.

information about the relationship between MicroBilt and its Aggregator, Zumigo.[173] Here, too, Sprint admits that its attempts to get relevant information were unsuccessful, because Zumigo ignored Sprint's questions.[174] Whatever a company's justification for denying or ignoring Sprint's requests for information, the refusals are further evidence of the fact that Sprint disclosed CPNI to third parties over which it had little or no control or authority.

69. Another measure Sprint could have taken was to determine whether the Securus incident was an isolated occurrence or whether it was indicative of a broader vulnerability with Sprint'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 Sprint's contractual safeguards. Sprint failed to demonstrate that it ever did so. Again, Sprint states that its legal department "conducted a legal review of the allegations" that Senator Wyden raised in a May 2018 letter to Sprint, but refused to provide details on the basis of attorney-client privilege.[175] Similarly, the Enforcement Bureau requested copies of all documents relating to any investigations or review of Sprint's customer location information-sharing practices; Sprint refused to provide them, again citing privilege. In sum, Sprint failed to provide any evidence showing that it sought to uncover other unauthorized programs, abuses in its authorized programs, or other weaknesses in its oversight of access to customer location information.

70. To the extent that Sprint did investigate, this investigation apparently failed to uncover that MicroBilt was a purchaser of access to Sprint's customer location information—a fact that Sprint did not discover until the publication of the *Motherboard* article more than six months after the *New York Times* article.[176] Although Sprint was not the carrier whose customer location was implicated by the article, Sprint reviewed its own sharing of data and determined—apparently for the first time—that it was sharing location data with MicroBilt, a company that apparently disclosed location information to its own corporate customers, which included members of the bail bonds industry.[177] In fact, MicroBilt had been a customer of Zumigo since 2017, receiving Sprint's customer location information, yet Sprint had no records or information about MicroBilt.[178] This means that six months after the Securus incident had demonstrated serious flaws in Sprint's safeguards to protect CPNI, and for four months after Sprint updated its security protocols with new Methods & Procedures, a company completely unknown to Sprint was collecting and selling Sprint's customers' location data without Sprint even knowing.

71. Yet another measure that Sprint could have taken was to enhance the measures it used 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, Sprint had good reason to doubt the efficacy of its contractual protections. As Sprint itself explains, Securus apparently made misrepresentations to 3Cinteractive and LocationSmart regarding the purpose for which it was accessing information.[179] Even Sprint's new Methods & Procedures protocol established after the May 2018 *New York Times* article failed to meaningfully address Sprint's failure to verify customer consent. Among other things, these Methods & Procedures (1) revised Sprint's internal management practices regarding location-based services; (2) created a process for Sprint to review and

[173] *Id.* at 9, Response to Question 5.

[174] *Id.*

[175] LOI Response at 9, Response to Question 11.

[176] Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone,* Motherboard (Jan. 8. 2019), https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-MicroBilt-zumigo-tmobile.

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

[178] Supplemental LOI Response at RD01-000030, Response to Request for Documents No. 1, (E-mail from Chirag Bakshi, CEO, Zumigo, to Mike Cole, Lyndi Long, Sprint Corp. (Jan. 29, 2019, 13:57).

[179] LOI Response at 8, Response to Question 8.

approve new location-based service providers (rather than merely vetting the Aggregators); and (3) expanded internal guidance on how frequently Sprint should audit these companies and what information those audits could seek, including whether Aggregators complied with their obligation to document consent by end users.[180] But these new policies failed to address key weaknesses with Sprint's location-based services program, and there is little evidence that Sprint actually followed through with these policies in a way that had any meaningful impact. For example, Sprint's apparent intention to audit whether Aggregators complied with their contractual obligation to document consent would not have served as a substitute for Sprint *itself* verifying and reviewing customer consent prior to providing access to its customers' location data. While audits may root out noncompliance, they may detect it long after an unauthorized disclosure has taken place. And even so, there is little evidence that Sprint followed through with its new initiative to conduct audits.

72. Yet the January 8, 2019, *Motherboard* report on its success purchasing customer location information that was disclosed to MicroBilt[181] perfectly illustrates the vulnerability that remained in Sprint's aggregator program. The evidence shows that MicroBilt had been a customer of Zumigo since 2017 and had been receiving Sprint's customer location information from 2017 until early January 2019. Internal correspondence documents from Sprint employees show the Company, in response to an e-mail inquiry from the author of the *Motherboard* article, scrambling to determine who MicroBilt was and whether or how it was getting access to Sprint customer location information.[182] Sprint apparently lacked information about MicroBilt to the point that Sprint company employees had to request information about the company from the CEO of Zumigo.[183]

73. And, as the *Motherboard* article demonstrated, purchasing customer location information provided by a carrier to MicroBilt was not a difficult thing to do—nor did it appear to be difficult for *Motherboard* to unearth the vulnerability. At the time, Zumigo was operating under the supposedly more robust Methods & Procedures protocol implemented in August 2018. Those so-called "improved" safeguards nonetheless failed to (1) detect the presence of an apparently unauthorized location-based service provider able to submit requests via Zumigo or (2) prevent that entity from obtaining Sprint's customer location information without consent.[184]

74. Finally, the surest safeguard to protect its customers' CPNI would have been for Sprint to expeditiously terminate its location-based service program. Sprint asserts that it immediately acted to

[180] Supplemental LOI Response at RD01-000001, Response to Request for Documents No. 10, (*Sprint Location Based Services (LBS) – Product Management Methods and Procedures* (Aug. 8, 2018). *See also* Supplemental LOI Response at 5-7, Response to Question 4.

[181] Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone*, Motherboard (Jan. 8. 2019), https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile.

[182] Supplemental LOI Response at RD01-000239-000242, Response to Request for Documents No. 1 (E-mail from Mark G. Clancy, Exchange Administrative Group, Sprint, to Craig A. Baker, IT, Sprint Corp. (Jan. 31, 2019, 13:16)). *See also* Supplemental LOI Response at RD01-000244, Response to Request for Documents No. 1.

[183] LOI Response at RD01-000016-000018, Response to Request for Documents No. 1.

[184] A category of the NIST Cybersecurity Framework's "Recover" Core Function is to improve based on past experience. *See* NIST Cybersecurity Framework at 43 (improvements mean that "response activities are improved by incorporating lessons learned from current and previous detection/response activities"). *See also* NIST, *Special Publication 800-137, Information Security Continuous Monitoring* (*ISCM*) *for Federal Information Systems and Organizations*, at vi (Sept. 2011), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf (discussing "information security continuous monitoring," which involves "maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions," as a critical component of an organization's cyber risk management framework).

terminate its contracts with both LocationSmart and Zumigo.[185] But that is not the case. Sprint may have terminated its contract with LocationSmart on June 20, 2018, but it signed a new one on August 23. And while Sprint terminated its contract with Zumigo September 18, 2018, it then revived that contract on October 16, reinstating the former agreement "in full force and effect as if [it] had never been terminated."[186] In other words, Sprint apparently resumed business as usual after a short lapse. In reality, it was not until the following year—2019—and the discovery that Sprint had been disclosing customer information to a location-based service provider it was not even aware of that Sprint finally decided to shut down its flawed location-based service program.[187]

75. Sprint apparently did not take any of these reasonable steps. Nor has it presented evidence that it took other reasonable measures that might have cured the flaws exposed by the Securus and MicroBilt breaches. The ease with which Hutcheson accessed customer location information about any individual of his choosing should have alerted Sprint to its lack of visibility into how the location-based service providers were making use of the location information that it was entrusting to the Aggregators and that it needed to change its practices or terminate its location-based service program. Sprint adopted limited security measures and audit provisions that did not meet this burden. The allegedly enhanced Methods & Procedures that Sprint implemented in August 2018 were likewise ineffective to either detect or protect against unauthorized attempts to gain access to location information and did not solve the systematic flaws in Sprint's program. After learning of Hutcheson's practices, Sprint 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 Sprint apparently failed in its obligation under section 222 and our rules to have reasonable measures in place to discover and protect against attempts to gain unauthorized access to its customers' CPNI.[188]

D. Proposed Forfeiture

76. Section 503(b) of the Act authorizes the Commission to impose a forfeiture against any entity that "willfully or repeatedly fail[s] to comply with any of the provisions of [the Act] or of any rule, regulation, or order issued by the Commission . . . ."[189] Here, section 503(b)(2)(B) of the Act authorizes us to assess a forfeiture against Sprint of up to $204,892 for each day of a continuing violation, up to a statutory maximum of $2,048,915 for a single act or failure to act.[190] In exercising our forfeiture authority, we must consider the "nature, circumstances, extent, and gravity of the violation and, with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such

[185] LOI Response at 7, Response to Question 6.

[186] LOI Response at Sprint RD03-000183, Response to Request for Documents No.3, Sprint-Zumigo Amendment No. 2, at Sec. III.

[187] *See* Supplemental LOI Response at 11, Response to Question 7.

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

[189] 47 U.S.C. § 503(b).

[190] *See* 47 U.S.C. § 503(b)(2)(B); 47 CFR § 1.80(b)(2). These amounts reflect inflation adjustments to the forfeitures specified in section 503(b)(2)(B) ($100,000 per violation or per day of a continuing violation and $1,000,000 per any single act or failure to act). The Federal Civil Penalties Inflation Adjustment Act of 1990, Pub. L. No. 101-410, 104 Stat. 890, as amended by the Debt Collection Improvement Act of 1996, Pub. L. No. 104-134, Sec. 31001, 110 Stat. 1321, requires the Commission to adjust its forfeiture penalties periodically for inflation. *See* 28 U.S.C. § 2461 note (4). The Enforcement Bureau announced the Commission's inflation-adjusted penalty amounts for 2020 on December 27, 2019. *See Amendment of Section 1.80(b) of the Commission's Rules, Adjustment of Civil Monetary Penalties to Reflect Inflation*, Order, DA 19-1325 (EB 2019).

other matters as justice may require."[191] In addition, the Commission has established forfeiture guidelines; they establish base penalties for certain violations and identify criteria that we consider when determining the appropriate penalty in any given case.[192] Under these guidelines, we may adjust a forfeiture upward for violations that are egregious, intentional, or repeated, or that cause substantial harm or generate substantial economic gain for the violator.[193]

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

78. 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 Sprint'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.

79. In contrast to the *CPNI Cases*, *TerraCom* addressed a situation of similarly serious threats to privacy—albeit in the context of a different part of section 222. *TerraCom* dealt with exposure of personal information—not CPNI—and the Commission proposed penalties based on language in

[191] 47 U.S.C. § 503(b)(2)(E).

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

[193] *Id*.

[194] 47 CFR § 1.80(b).

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

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

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

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.

80. Apparent Violations of Section 222 of the Act and Section 64.2010 of the Commission's Rules. The violations in this case were continuing in nature, extending each day that the Company's location-based services operated in the apparent absence of reasonable measures to protect CPNI. We propose a base forfeiture of $40,000 for the first day of such a violation and a $2,500 forfeiture for the second day and each successive day that the violation continued. In other contexts involving consumer protections under the Act and the Commission's rules, the Commission has applied a base forfeiture of $40,000 for a single act.[198] We find that the base forfeiture we propose is appropriate (1) to provide a meaningful distinction between the violations in this case and those of other cases involving less egregious facts; and (2) to provide consistency with other consumer protection cases involving serious harm to consumers. We find this base forfeiture appropriately deters wrongful conduct and reflects the increased risk consumers face when their information is not secured in a timely manner.

81. We recognize that Sprint took one reasonable step towards improving its safeguards by suspending Securus, 3Cinteractive, and LocationSmart's access to Sprint customer location information on May 25, 2018, two weeks after the *New York Times* report.[199] But that step did not protect customer location information at all from the other 8 entities (Zumigo and its customers) that had access to it through September 18, 2018, and then again from October 16, 2018 to January 9, 2019—a total of 216 days. Nor did that safeguard against unauthorized access by LocationSmart itself or by its two customers during the 281 days in which Sprint reinstated their access (from August 23, 2018 until May 31, 2019). 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, Sprint'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 *New York Times* report, and apply a base forfeiture of $40,000 for the first day of such violation and a $2,500 forfeiture for the second day and each successive day the violation continued. These calculations are set forth in Table 1 below:

Table 1: Calculation of Base Forfeiture Penalty

Number of Entities	Time Period	Days of Continuing Violation	Base
8	June 9, 2018 to September 18, 2018 and October 16, 2018 to January 9, 2019	186	$4,020,000
3	August 23, 2018 to May 31, 2019	281	$2,100,000
		Total:	**$6,120,000**

Accordingly, we find Sprint apparently liable for a forfeiture in the amount of $6,120,000 for its apparent violations of section 222 of the Act and section 64.2010 of our rules.

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

[199] LOI Response at 7.

82. Apparent Violations of Section 222(c)(1) of the Act and Section 64.2007(b) of the Commission's Rules. Although we find that Sprint apparently violated the Act and our rules for its unauthorized disclosures of CPNI to Hutcheson, the one-year statute of limitations bars any forfeiture for those violations.[200] We thus instead exercise our discretion to admonish Sprint for its unauthorized disclosures of CPNI to Hutcheson.[201]

83. Unlike other federal agencies,[202] the Commission's authority to propose a monetary forfeiture for violations by a common carrier such as Sprint is statutorily limited to the one-year period before issuance of the associated notice of apparent liability.[203] In this case, Hutcheson's unauthorized access to Sprint customer location information ceased by April 2017, when he was arrested by the FBI and state law enforcement authorities. Thus, the statute of limitations on these violations ran out in April 2018, one month before the unauthorized disclosures even came to light in the May 2018 *New York Times* report. As the Act states and courts have affirmed, the countdown clock on the Commission's statutory deadline for action begins when a violation *occurs*, rather than when it is discovered.[204] Accordingly, we are prohibited by statute from imposing a forfeiture penalty when the underlying violation occurred years ago, as was the case with Sprint's unauthorized disclosures to Hutcheson.

84. Upward Adjustment. Given the totality of the circumstances, and consistent with the Commission's *Forfeiture Policy Statement*,[205] we also conclude that a significant upward adjustment is warranted. The responsibility for safeguarding the location information of its customers rested squarely on the Company, making it highly culpable. To start, we find Sprint's apparent decision to simply trust the Aggregators and their location-based service provider customers even after the *New York Times* report confounding.[206] *For one*, the Company apparently had no history of internally reviewing and approving third-party proposals for using Sprint's customer location information before the Company actually

[200] *See* 47 U.S.C. § 503(b)(6)(B).

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

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

[203] *See* 47 U.S.C. § 503(b)(6)(B). Notwithstanding the one-year statute of limitations, the Enforcement Bureau can and frequently does enter into agreements with the targets of investigations in order to pause the statute of limitations while an investigation is underway. These agreements are commonly referred to as "tolling agreements." In this investigation, the Enforcement Bureau entered into a tolling agreement with Sprint so that we may assess penalties for conduct going as far back as May 13, 2018.

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

[205] *Commission's Forfeiture Policy Statement and Amendment of Section 1.80 of the Rules to Incorporate the Forfeiture Guidelines*, Report and Order, 12 FCC Rcd 17087 (1997) (*Forfeiture Policy Statement*), *recons. denied*, Memorandum Opinion and Order, 15 FCC Rcd 303 (1999).

[206] We note that our base forfeiture already accounts for Sprint's decision to suspend and terminate its initial contract with LocationSmart and its location-based service provider customers. For these purposes we focus on Sprint's actions with respect to the entities that had access to Sprint customer location information during the time in question.

disclosed that data. So it is unsurprising that at least one location-based service provider, MicroBilt, had access to Sprint customer information without Sprint's knowledge. *For another*, the Company apparently never internally reviewed consumer consent records. So it is again unsurprising that Hutcheson was able to forge such consent records (and submit documents not even purporting to be such records) and gain access to Sprint's customer location information for four years. *For yet another*, the Company apparently never exercised its right to audit the Aggregators' practices before 2018. So it is yet again unsurprising that more than one location-based service provider was using customer location information for improper purposes.

85. What is more, 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 Sprint 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.

86. We find that an upward adjustment of 100% above the $6,120,000 base forfeiture, thereby doubling the total to $12,240,000, is justified in these circumstances, will protect the interests of consumers, and deter entities from violating the Commission's rules in the future.[207]

87. Therefore, after applying the *Forfeiture Policy Statement*, section 1.80 of the rules, and the statutory factors, we propose a total forfeiture of $12,240,000 for Sprint's apparent willful and repeated violations of section 222 of the Act[208] and section 64.2010 of the Commission's rules.[209]

IV. REQUESTS FOR CONFIDENTIALITY

88. Sprint 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.[210] With respect to the particular information set forth in this Notice of Apparent Liability, we conclude that there is a significant 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 Sprint and others might result from the disclosure of this information, and therefore partially deny Sprint's request.

89. 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.[211] At the outset, we find a strong public interest in the public knowing Sprint's practices with

[207] *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).

[208] 47 U.S.C. § 222.

[209] 47 CFR § 64.2010.

[210] On February 21, 2020, Sprint withdrew its request for confidential treatment with respect to several categories of information but, as is relevant to the information contained in this Notice, specifically continued to request confidential treatment for the names of the location-based service providers to which the two Aggregators provided Sprint customer location information. Letter from Maureen Cooney, Head of Privacy, Office of Privacy, Sprint Corp., to Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau (Feb. 21, 2020) (on file in EB-TCD-18-00027700).

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

respect to the location-based services and customer location information at issue, including to whom the carrier provided access to such information. This conclusion is further supported by both the sensitivity of the location data 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 Sprint's practices posed to their location data. We further find that the benefits of revealing the information contained in this Notice greatly outweigh any private interest Sprint or others may have in keeping confidential the entities with whom Sprint shared customer location data. This is all the more true given that Sprint argues that it required these entities to provide conspicuous notice and obtain affirmative consent from Sprint's customers for the sharing of their location data.[212] Thus, the identity of these entities should already be widely known and was required by Sprint to be divulged to its affected customers. And to the extent that Sprint'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 Sprint to keep these identities hidden from, among others, the very customers whose private location information was shared for the commercial benefit of these entities.

90. Because Sprint'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 Sprint or a relevant third party to file a petition for reconsideration;[213] 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).[214] If, after 10 business days, Sprint or a relevant third party has not filed a petition for reconsideration or sought a judicial stay with regard to this partial denial of Sprint's confidentiality request, the material will be made publicly available.[215]

V. ORDERING CLAUSES

91. Accordingly, **IT IS ORDERED** that, pursuant to section 503(b) of the Act[216] and section 1.80 of the Commission's rules,[217] Sprint Corporation is hereby **NOTIFIED** of this **APPARENT LIABILITY FOR A FORFEITURE** in the amount of twelve million, two hundred forty thousand dollars ($12,240,000) for willful and repeated violations of section 222 of the Act[218] and section 64.2010 of the Commission's rules.[219]

92. **IT IS FURTHER ORDERED** that Sprint Corporation is hereby **ADMONISHED** for its apparent violations of section 222(c) of the Act[220] and section 64.2007 of the Commission's rules.[221]

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).

[212] LOI Response at 6, Response to Question 5.

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

[214] *Cf.* 47 CFR § 0.459(g).

[215] *See* 47 CFR § 0.455(g).

[216] 47 U.S.C. § 503(b).

[217] 47 CFR § 1.80.

[218] 47 U.S.C. § 222.

[219] 47 CFR § 64.2010.

[220] 47 U.S.C. § 222(c).

[221] 47 CFR § 64.2007.

93. **IT IS FURTHER ORDERED** that, pursuant to section 1.80 of the Commission's rules,[222] within thirty (30) calendar days of the release date of this Notice of Apparent Liability for Forfeiture, Sprint Corporation **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 93-94 below.

94. Sprint Corporation 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),[223] 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:[224]

- 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).[225] For additional detail and wire transfer instructions, go to https://www.fcc.gov/licensing-databases/fees/wire-transfer.
- Payment by credit card must be made by using the Commission's Fee Filer website at https://apps.fcc.gov/FeeFiler/login.cfm. To pay by credit card, log-in using the FRN captioned above. If payment must be split across FRNs, complete this process for each FRN. Next, select "Pay bills" on the Fee Filer Menu, and select the bill number associated with the NAL Account – the bill number is the NAL Account number with the first two digits excluded – and then choose the "Pay by Credit Card" option. Please note that there is a $24,999.99 limit on credit card transactions.
- Payment by ACH must be made by using the Commission's Fee Filer website at https://apps.fcc.gov/FeeFiler/login.cfm. To pay by ACH, log in using the FRN captioned above. If payment must be split across FRNs, complete this process for each FRN. Next, select "Pay bills" on the Fee Filer Menu and then select the bill number associated to the NAL Account – the bill number is the NAL Account number with the first two digits excluded – and choose the "Pay from Bank Account" option. Please contact the appropriate financial institution to confirm the correct Routing Number and the correct account number from which payment will be made and verify with that financial institution that the designated account has authorization to accept ACH transactions.

95. 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

[222] 47 CFR § 1.80.

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

[224] 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.

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

Street, SW, Room 1-A625, Washington, DC 20554.[226] 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.

96. 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.[227] 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.

97. 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.

98. **IT IS FURTHER ORDERED**, pursuant to section 0.459(g) of the Commission's rules,[228] that the Requests for Confidential Treatment filed by Sprint Corporation in this proceeding **ARE DENIED IN PART**, to the extent specified herein.

99. **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 Mr. Jorge Gracia, Sprint Corporation, c/o Maureen Cooney, Head of Privacy, Office of Privacy, Sprint Corporation, 12502 Sunrise Valley Drive, Reston, VA 20196, and Mr. John Roche, Perkins Coie LLP, 700 Thirteenth Street, N.W., Washington, DC 20005-3960.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

[226] *See* 47 CFR § 1.1914.

[227] 47 CFR §§ 1.16, 1.80(f)(3).

[228] 47 CFR § 0.459(g).

STATEMENT OF
CHAIRMAN AJIT PAI

Re: *Sprint Corporation*, File No.: EB-TCD-18-00027700.

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: *Sprint Corporation*, File No.: EB-TCD-18-00027700.

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: *Sprint Corporation*, File No.: EB-TCD-18-00027700.

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: *Sprint Corporation*, File No.: EB-TCD-18-00027700.

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.

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

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.

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

[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.

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 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

[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*,

number of aggregator contracts cannot be squared with our core mission today – to vindicate harmed consumers first and foremost.

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-

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).

[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.

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 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.