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

In the Matter of	)	
	)	
Implementation of the Telecommunications Act of 1996:	)	CC Docket No. 96-115
	)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information	)	
	)	
	)	

DECLARATORY RULING

Adopted: June 27, 2013 **Released: June 27, 2013**

By the Commission: Acting Chairwoman Clyburn and Commissioner Rosenworcel issuing separate statements; Commissioner Pai approving in part, concurring in part and issuing a statement.

I. INTRODUCTION

1. In this *Declaratory Ruling*, we address the real privacy and security risks that consumers face when telecommunications carriers use their control of customers' mobile devices to collect information about their customers' use of the network. Absent carriers' adoption of adequate security safeguards, consumers' sensitive information, such as the numbers a wireless customer has called, the time calls are made, and where the customer was located when he or she made a call, can be disclosed to third parties without consumers' knowledge or consent. The Commission acts now to clarify existing law so that consumers will know that their carriers must safeguard these kinds of information so long as the information is collected by or at the direction of the carrier and the carrier or its designee[1] has access to or control over the information.

2. Technology now allows consumers to use wireless devices that provide powerful computing, as well as communications, capabilities. Carriers, which most often control the initial configuration of these devices, can use their unique position as the provider of the wireless service and the device to configure their customers' devices in ways that will serve their needs as service providers. In particular, carriers can cause the devices to collect information that includes such things as lists of numbers called and calls received and the locations from which calls have been made. While residing on the device, that sensitive information is potentially vulnerable to acquisition by others. It is thus important that the Commission clarify carriers' statutory and regulatory obligations with respect to information that they collect from their customers.

3. The actual risks to consumers of unauthorized disclosure of sensitive information—and the need for Commission action—are demonstrated by the insecure way in which some carriers caused software provided by Carrier IQ, Inc. (Carrier IQ) to be installed on some mobile devices. Carrier IQ's diagnostic software can be installed on a mobile device to provide carriers with information about how

[1] For purposes of this ruling, a "designee" is an entity to which the carrier has transmitted, or directed the transmission of, CPNI or is the carrier's agent.

their network and devices on their network are functioning.[2] In November 2011, a researcher discovered security vulnerabilities that permitted third parties to access the information collected by the Carrier IQ software, resulting in the potential for consumers' location and other data to be accessed and disclosed.[3] This discovery led to calls for an investigation into the overall security of sensitive information throughout the mobile services ecosystem.[4]

4. To clarify these issues, this *Declaratory Ruling* addresses how section 222 of the Communications Act of 1934, as amended (the Act), and the Commission's implementing rules apply to information relating to telecommunications service and interconnected voice over Internet Protocol (VoIP) service that fits the statutory definition of customer proprietary network information (CPNI)[5] when such information is collected by the customer's device, provided the collection is undertaken at the mobile wireless carrier's direction and the carrier or its designee has access to or control over the information.

5. We acknowledge that there may well be good reasons for carriers to collect CPNI on mobile devices, and we are not barring them from doing so. We are simply clarifying that if they choose to do so, they must protect the confidentiality of such CPNI as required by section 222 and may use it only as permitted by law. We take this action so that carriers understand their legal responsibility to protect CPNI collected in this manner just as they must protect CPNI collected and stored in other ways. In this regard, this *Declaratory Ruling* takes into consideration developments in technologies and business practices in the market for mobile communications services and the record developed in response to a Public Notice issued by the Wireline Competition Bureau, Wireless Telecommunications Bureau, and Office of General Counsel in May 2012.[6]

6. The legal issue here arises under 47 U.S.C. § 222. Section 222 establishes the duty of every telecommunications carrier to "protect the confidentiality of proprietary information of, and relating to … customers."[7] Furthermore, a carrier that receives or obtains CPNI by virtue of its provision of a telecommunications service may use, disclose, or permit access to such information only in limited circumstances.[8] The Commission has adopted rules to implement those obligations.[9] The Commission

---

[2] Carrier IQ, *Understanding Carrier IQ Technology: What Carrier IQ Does and Does Not Do* (Dec. 15, 2011), at 2, *available at* http://www.carrieriq.com/documents/understanding-carrier-iq-technology/6461/ (*Understanding Carrier IQ Technology*) (last visited June 26, 2013).

[3] *See id.* at 8.

[4] *See, e.g.,* Letter from The Honorable Al Franken, United States Senate, to Larry Lenhart, President and CEO, Carrier IQ, Inc. (Nov. 30, 2011), *available at* http://www.franken.senate.gov/files/letter/111201_Letter_to_CarrierIQ.pdf.

[5] Section 222 of the Act defines CPNI to mean "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information." 47 U.S.C. § 222(h)(1).

[6] *Comments Sought on Privacy and Security of Information Stored on Mobile Communications Devices*, Public Notice, DA 12-818, 27 FCC Rcd 5743 (2012) (*Mobile Device Privacy and Security Public Notice*); *see* 77 Fed. Reg. 35,336 (2012).

[7] 47 U.S.C. § 222(a).

[8] *See* 47 U.S.C. § 222(c); *see also* 47 C.F.R. §§ 64.2001-.2011.

[9] *See* 47 C.F.R. §§ 64.2001-.2011; *see also, e.g.*, *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061 (1998) (*1998 CPNI*

(continued….)

also has extended application of the CPNI requirements to providers of interconnected VoIP service.[10]

7. We conclude that the definition of CPNI in section 222 and the obligations flowing from that definition apply to information that telecommunications carriers cause to be stored on their customers' devices when carriers or their designees have access to or control over that information. When providers of mobile telecommunications service leverage their control of their customers' mobile devices to collect information that relates to the quantity, technical configuration, type, destination, location, and amount of use of the telecommunications service,[11] that information is "made available to the carrier by the customer solely by virtue of the carrier-customer relationship"[12] and therefore is CPNI. A telecommunications carrier that collects CPNI by virtue of its control over its customer's mobile device is obligated to protect that information by the Act and by the Commission's rules.[13]

8. We do not, at this time, adopt or propose any new rules to apply specific new obligations to carriers that collect CPNI in this manner. Rather, this *Declaratory Ruling* discusses the applicability of existing standards and requirements to this context.

II. BACKGROUND

9. Congress, through the Communications Act, requires communications providers to protect consumers' sensitive personal information to which they have access as a result of their unique position as network operators. Section 222, which became part of the Act in 1996, obligates telecommunications carriers to protect the privacy and security of information about their customers. Its most specific obligations[14] concern CPNI, which includes information about a customer's use of the service that is made available to the carrier by virtue of the carrier-customer relationship. As the Commission has explained, "[p]ractically speaking, CPNI includes information such as the phone numbers called by a consumer; the frequency, duration, and timing of such calls; and any services purchased by the consumer, such as call waiting."[15]

(Continued from previous page)
Order); Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14860 (2002) (*2002 CPNI Order*); Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007) (*2007 CPNI Order*).

[10] 47 C.F.R. § 64.2003(o) (defining "telecommunications carrier" or "carrier," for purposes of the CPNI rules only, to include an entity that provides interconnected VoIP service as that term is defined in § 9.3); *see 2007 CPNI Order*, 22 FCC Rcd at 6954-57 ¶¶ 54-59 (2007). The Commission also earlier this month adopted rules modeled on the CPNI rules in order to apply similar protections to Telecommunications Relay Service and point-to-point video services offered by Video Relay Service providers. *See Structure and Practices of the Video Relay Service Program; Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities,* Report and Order and Further Notice of Proposed Rulemaking, FCC 13-82 ¶¶ 155-172 (2013).

[11] 47 U.S.C. § 222(h)(1) (defining "customer proprietary network information"); *see also* § 222(f)(1) (requiring express prior authorization of the customer for the use or disclosure of or access to location information). Subsequent to the adoption of section 222(c)(1), Congress added subsection (f). Section 222(f) provides that, for purposes of section 222(c)(1), without the "express prior authorization" of the customer, a customer shall not be considered to have approved the use or disclosure of or access to (1) call location information concerning the user of a commercial mobile service or (2) automatic crash notification information of any person other than for use in the operation of an automatic crash notification system. 47 U.S.C. § 222(f).

[12] 47 U.S.C. § 222(h)(1).

[13] *See* 47 U.S.C. § 222(a); § 222(c)(1); 47 C.F.R. §§ 64.2001–.2011.

[14] *See 2007 CPNI Order*, 22 FCC Rcd at 6930 ¶ 4 (explaining that "[t]he section 222 framework calibrates the protection of [customer information] from disclosure based on the sensitivity of the information").

[15] *2007 CPNI Order*, 22 FCC Rcd at 6931 ¶ 4.

10. Congress enacted section 222 to "define[] three fundamental principles to protect all consumers. These principles are: (1) the right of consumers to know the specific information that is being collected about them; (2) the right of consumers to have proper notice that such information is being used for other purposes; and (3) the right of consumers to stop the reuse or sale of that information."[16] The Commission's implementation of section 222 to date has focused on rules governing the use and disclosure of CPNI, including the extent to which section 222 permits carriers to use CPNI to render the telecommunications service from which the CPNI was derived,[17] the types of consent that a carrier must obtain for use and disclosure, and safeguards to protect against unauthorized use or disclosure of CPNI.[18] In 2007, the Commission extended application of its CPNI rules to providers of interconnected VoIP service,[19] concluding that the rules would apply whether interconnected VoIP service is a telecommunications service or an information service.[20]

11. The last time the Commission updated its CPNI rules, in 2007, its focus was on the then-increasing practice of "pretexting," which refers to "the practice of pretending 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."[21] The Commission concluded that "pretexters have been successful at gaining unauthorized access to CPNI"[22] and that "carriers' record on protecting CPNI demonstrate[d] that the Commission must take additional steps to protect customers from carriers that have failed to adequately protect CPNI."[23] The Commission therefore imposed security requirements on carriers' disclosure of CPNI to customers over the telephone and online, required that law enforcement and customers be notified of security breaches involving CPNI, and required affirmative customer consent ("opt-in consent") before a carrier could disclose a customer's CPNI to a carrier's joint venture partners or independent contractors for the purposes of marketing communications-related services to that customer.[24]

12. In a Further Notice of Proposed Rulemaking (FNPRM) that accompanied the 2007 order, the Commission suggested that section 222 imposes an obligation on carriers to protect information stored on customers' devices. At that time, the Commission was addressing an emerging security concern: the security of information stored on mobile communications devices, particularly at the time such devices are returned for refurbishment and resale. The Commission sought comment on carriers' practices for erasing customer information in those circumstances and "whether the Commission should

[16] H.R. Conf. Rep. No. 458, 104th Cong., 2d Sess. 204 (1996) (Joint Explanatory Statement of the Committee of Conference); *see also* H.R. Rep. No. 204, 104th Cong., 1st Sess. 91 (1995); *id.* at 90 (explaining that section 222 balances "the need for customers to be sure that personal information that carriers may collect is not misused" with customers' expectation that "the carrier's employees will have available all relevant information about their service").

[17] *1998 CPNI Order*, 13 FCC Rcd at 8080 ¶ 23; 47 C.F.R. § 64.2005.

[18] *See* 47 C.F.R. §§ 64.2009-.2011; *e.g.*, *1998 CPNI Order*, 13 FCC Rcd at 8195-200 ¶¶ 193-202; *2007 CPNI Order*, 22 FCC Rcd at 6933-54 ¶¶ 12-53.

[19] 47 C.F.R. § 64.2003(o) (defining "telecommunications carrier" or "carrier," for purposes of the CPNI rules only, to include an entity that provides interconnected VoIP service as that term is defined in § 9.3).

[20] *See 2007 CPNI Order*, 22 FCC Rcd at 6954-57 ¶¶ 54-59.

[21] *Id.* at 6928 ¶ 1 n.1.

[22] *Id.* at 6934 ¶ 12.

[23] *Id.*

[24] *See id.* at 6929 ¶ 3. Prior to these amendments, carriers could share CPNI with joint venture partners and independent contractors for the purposes of marketing communications-related services after providing only a notice to a customer (i.e., opt-out consent). *Id.* at 6947 ¶ 38.

require carriers to permanently erase, or allow customers to permanently erase, customer information in such circumstances."[25] In response, carriers argued against the appropriateness or the Commission's authority to adopt such a requirement, emphasizing consumers' control of, and the carriers' lack of control of, information residing on consumers' devices. For example, AT&T Inc. commented that "decisions about what personal data to store, or not to store, on a mobile device rest with the consumer. Carriers do not typically have access to such information and play no role in determining what information a consumer chooses to store on mobile devices or how that information is used."[26] Sprint Nextel Corporation commented that "[w]ireless carriers are not well-positioned to guarantee the privacy of customer information stored on devices" because those devices are manufactured by suppliers and "in the physical control and custody of customers."[27] Sprint added that "none of the information (e.g., songs, photographs and address books) stored on a handset is CPNI and thus [it] is not addressed by section 222 of the Act."[28]

13. In May 2012, the Wireline Competition Bureau, the Wireless Telecommunications Bureau, and the Office of General Counsel issued a Public Notice in this docket (the *Mobile Device Privacy and Security Public Notice*) in response to more recent technological and business developments, particularly the growing practice of mobile carriers collecting and storing customer-specific information on their customers' mobile devices using software tools. The Public Notice observed that the comments in response to the 2007 FNPRM, which had emphasized the carriers' lack of control of information stored on communications devices, were out of date, and it sought comment to refresh the record concerning the practices of mobile wireless service providers with respect to information stored on their customers' mobile communications devices.[29]

14. One such software tool has been provided to various carriers by Carrier IQ, Inc.[30] As discussed above, Carrier IQ's diagnostic software can be installed on a mobile device to provide carriers with information about how their network and devices on their network are functioning.[31] Based on specifications determined by the carrier, such information may include dialed phone numbers and calling behavior, location coordinates, and mobile subscriber numbers, among other data elements.[32] In November 2011, a researcher discovered security vulnerabilities that permitted others to access the sensitive information collected by the Carrier IQ software, resulting in the potential for users' location and other data to be accessed and disclosed.[33] In response to congressional inquiries, carriers said that they had been using Carrier IQ's tool in order to enhance their ability to evaluate and improve their network services and to improve the ability of customer-service representatives to assist their customers

[25] *Id.* at 6962 ¶ 72.

[26] Comments of AT&T Inc., CC Docket No. 96-115 (July 9, 2007), at 9, *quoted in Mobile Device Privacy and Security Public Notice*, 27 FCC Rcd at 5744.

[27] Comments of Sprint Nextel Corporation, CC Docket No. 96-115 and WC Docket No. 04-36, at 21 (July 9, 2007), *quoted in Mobile Device Privacy and Security Public Notice*, 27 FCC Rcd at 5745.

[28] Reply Comments of Sprint Nextel Corporation, CC Docket No. 96-115 and WC Docket No. 04-36, at 14 (Aug. 7, 2007), *quoted in Mobile Device Privacy and Security Public Notice*, 27 FCC Rcd at 5745 n.9.

[29] *Mobile Device Privacy and Security Public Notice,* 27 FCC Rcd at 5745-46.

[30] *Id.* at 5745.

[31] *Understanding Carrier IQ Technology* at 2.

[32] *See id.* at Exh. B.

[33] *See id.* at 8.

with problems, and that they were doing so in compliance with privacy laws.[34]

15. After the Commission began this proceeding, the Federal Trade Commission (FTC) announced that mobile-device manufacturer HTC America (HTC) had agreed to settle charges that it had "failed to take reasonable steps to secure the software it developed for its smartphones and tablet computers, introducing security flaws that placed sensitive information about millions of consumers at risk."[35] The FTC's complaint charged that HTC had insecurely implemented two logging applications, Carrier IQ and HTC Loggers, creating vulnerabilities that compromised the functionality of devices and sensitive information stored on those devices. For example, according to the consent order, a vulnerability on certain HTC devices would allow any third-party application that could connect to the Internet to intercept information being collected by the Carrier IQ software.[36]

III. DISCUSSION

16. After review of the record in response to the *Mobile Device Privacy and Security Public Notice*, we conclude that there is uncertainty in the industry about obligations to protect CPNI collected by mobile devices. To address that uncertainty, and to ensure that potentially sensitive consumer information is handled appropriately, we issue this ruling declaring that section 222 applies to information that fits the statutory definition of CPNI when such information is collected by the subscriber's mobile device, provided the collection is undertaken at the carrier's direction and that the carrier or its designee has access to or control over that information. By issuing this *Declaratory Ruling*, we do not prohibit such information collection, which may well have beneficial uses for improved network operations, but we make clear that telecommunications carriers are responsible for securing the information and that the Commission will hold carriers responsible for compliance with their statutory and regulatory obligations.

17. We disagree with commenters who claim that section 222 is too rigid or outdated to apply to mobile devices. The relationship between a telecommunications carrier and its customer is one of particular sensitivity, given the special position that a carrier occupies as its customers' gatekeeper to the network, and Congress recognized that special position in enacting section 222. This is no less the case when the information is stored at the carrier's direction on a mobile device. In this regard, we note that Verizon Wireless argues that "precise location information warrants different protections than anonymous or aggregate data" and, therefore, "the extent of notice provided, and necessity or manner of consumer consent, will vary depending on the circumstances."[37] This illustration is fully consistent with

---

[34] *Mobile Device Privacy and Security Public Notice,* 27 FCC Rcd at 5744 & n.7, 5745 & nn. 10-13; Letter from Timothy P. McKone, Executive Vice President, Federal Relations, AT&T Services, Inc., to The Honorable Al Franken, United States Senate (Dec. 14, 2011), *available at* http://apps.fcc.gov/ecfs/document/view?id=7021920018 (AT&T letter to Sen. Franken); Letter from Vonya B. McCann, Senior Vice President, Government Affairs, Sprint Nextel, to The Honorable Al Franken, United States Senate (Dec. 14, 2011), *available at* http://apps.fcc.gov/ecfs/document/view?id=7021920019 (Sprint Letter to Sen. Franken); Letter from Thomas J. Sugrue, Senior Vice President, Regulatory and Legal Affairs, T-Mobile USA, Inc., to The Honorable Al Franken, United States Senate (Dec. 20, 2011), *available at* http://apps.fcc.gov/ecfs/document/view?id=7021920020 (T-Mobile Letter to Sen. Franken).

[35] Federal Trade Commission, *HTC America Settles FTC Charges It Failed to Secure Millions of Mobile Devices Shipped to Consumers*, News Release, Feb. 22, 2013, *available at* http://www.ftc.gov/opa/2013/02/htc.shtm. The FTC investigated HTC pursuant to its authority to prevent persons subject to its jurisdiction "from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a)(2). That authority includes manufacturers of telecommunications equipment but not common carriers subject to the Act, which are addressed by Title II (including section 222) of the Act.

[36] Federal Trade Commission, Agreement Containing Consent Order, *HTC America, Inc.*, File No. 122 3049, at 11, *available at* http://www.ftc.gov/os/caselist/1223049/130222htcorder.pdf.

[37] Verizon Wireless Comments at 9.

our conclusion. Aggregate customer information is not subject to the privacy obligations in section 222(c)(1).[38] Rather, section 222 is calibrated to apply its strongest protections to "individually identifiable" CPNI.[39]

18. We take this action not because the practice of collecting CPNI from customers' mobile devices is inherently improper or to prevent providers from doing so, but because these actions create risks and thus impose reasonable responsibilities on the carriers that engage in such practice. As pointed out by many commenters, collecting customer information from mobile devices can benefit consumers. Although other information in a carrier's network might enable a network operator to become aware that calls are being dropped or that a specific geographic area has poor reception, the mobile device itself is in a better position to collect information about the reason for a dropped call or other failure.[40] Data from mobile devices can also be useful in responding to customer requests for assistance with device, service, and performance issues.[41] It can also help a network operator determine which parts of its network are most in need of improvement and whether particular models of phones are experiencing more problems than others.[42]

19. There are thus legitimate reasons for mobile providers to collect information on their customers' mobile devices. Doing so, however, also creates risks to the privacy and security of consumers' information. In the example that led Commission staff to issue the *Mobile Device Privacy and Security Public Notice*, it appears that at least some smartphones that carriers equipped with the Carrier IQ software were configured in such a way as to store a great deal of sensitive customer information in an insecure manner, creating the possibility that it could be captured by malicious third-party applications.[43] Even to the extent that customers may have known about or consented to the service provider's collection and use of data in this manner,[44] a customer's consent to the collection and use of data to maintain and improve the network would not constitute consent for other use, disclosure, or permission of access (such as storing it in an insecure manner), nor would it negate section 222(a)'s duty to protect proprietary information from unauthorized access or disclosure.

20. In this *Declaratory Ruling*, we do not reach any conclusions about whether carriers have violated the Act as a result of the Carrier IQ event discussed above. Rather, we issue this *Declaratory Ruling* because there is a need to clarify the obligations of mobile providers when they or their designees collect and have access to or control over sensitive customer information by virtue of their control of customers' devices.

A. Data Collected by Mobile Devices May Be CPNI.

21. We conclude that customer-specific information collected by mobile devices can include

[38] 47 U.S.C. § 222(h)(2) (defining *aggregate information*); § 222(c)(3) (providing that a telecommunications carrier "may use, disclose, or permit access to aggregate customer information other than for the purposes described in paragraph (1)"); *see infra* para. 34.

[39] 47 U.S.C. § 222(c)(1); *see 2007 CPNI Order*, 22 FCC Rcd at 6930 ¶ 4.

[40] CTIA Comments at 1-2; AT&T Comments at 19 ("Indeed, when a device fails to connect at all, the network will not even know of the failure.").

[41] T-Mobile Reply Comments at 5.

[42] AT&T Comments at 19; T-Mobile Reply Comments at 6; ITIF Comments at 3.

[43] Federal Trade Commission, Complaint, *HTC America, Inc.*, File No. 122 3049, at 4-5, *available at* http://ftc.gov/os/caselist/1223049/130222htccmpt.pdf.

[44] *See, e.g.*, CTIA Comments at 2 ("Consumers are well aware of this practice because carriers clearly and conspicuously disclose that they gather this type of information to improve network performance and the user's experience."); AT&T Comments at 20.

information that fits the statutory definition of CPNI. The statute defines CPNI to include the following:

> (A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and
>
> (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier;
>
> except that such term does not include subscriber list information.[45]

22. Application of this definition is straightforward. Information collected by a mobile device can include "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer," such as the telephone numbers of calls dialed and received and the location of the device at the time of the calls — information that is recorded by the Carrier IQ software.[46] The Commission has previously made clear that "CPNI includes information such as the phone numbers called by a consumer [and] the frequency, duration, and timing of such calls."[47] The location of a customer's use of a telecommunications service also clearly qualifies as CPNI.[48]

23. We also conclude that information that a carrier causes to be stored on its customer's device in order to allow the information to be shared with the carrier is "made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[49] This is true whether the carrier itself installs, or directs the installation of, the software that collects the information, and whether the information is shared directly with the carrier or with its designee.[50] A carrier is in a unique position with respect to its customers when it configures a mobile device to collect the information before the device is sold to a customer.[51] This unique position satisfies the "carrier-customer relationship" element of the definition of CPNI.

---

[45] 47 U.S.C. § 222(h)(1). "Subscriber list information" is defined in § 222(h)(3).

[46] *Understanding Carrier IQ Technology* at 9 (stating that recording phone numbers dialed and received "allows a Network Operator to understand both ends of a problem" by, for example, enabling the carrier to determine which customer's device caused a dropped call); *id.* at 4, 11 (explaining the recording and use of location information to diagnose dropped calls or areas with no service).

[47] *2007 CPNI Order*, 22 FCC Rcd at 6931 ¶ 5.

[48] *See* 47 U.S.C. § 222(h)(1)(A) (defining CPNI to include "information that relates to the … location … of a telecommunications service subscribed to by any customer of a telecommunications carrier").

[49] 47 U.S.C. § 222(h)(1)(A).

[50] *See* 47 U.S.C. § 217 (establishing that a common carrier is responsible for the act, omission, or failure of its agent); *see also* Letter from Dale Sohn, President and Chief Executive Officer, Samsung Telecommunications America, LLC, to The Honorable Al Franken, United States Senate (Dec. 14, 2011), at 1, *available at* http://www.franken.senate.gov/files/letter/111214_Samsung_Response_to_Sen_Franken_CarrierIQ.pdf (Samsung Letter to Sen. Franken) ("Pursuant to the carriers' agreements with [Samsung], some of those cellular carriers required Samsung to pre-install Carrier IQ software on some of the devices prior to the sale of those devices to the carrier (and before the sale of the devices to the consumer by the distributor, carrier or its agent)."); CDT Comments at 5-6. To the extent that the relationship between carrier, manufacturer, and customer may be different, this principle may not apply.

[51] This may also be true if a carrier leverages its control of a customer's device to install such a collection capability after the initial sale, such as through a forced update of the operating system or embedded software.

24. We disagree with CTIA's argument that "data stored on mobile devices is not CPNI within the meaning of Section 222 because it is not 'information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service."[52] Although it is certainly true that *some* of the information that carriers have collected and stored on mobile devices is not CPNI,[53] it is equally clear that some of it is.[54] In any event, if the information a carrier collects in the future does not meet the statutory definition, then section 222 will not apply. To reiterate, the Commission is clarifying only that information that meets the definition of CPNI is subject to section 222, just as the same information would be subject to section 222 if it were stored elsewhere on a carrier's network.

25. We also disagree with CTIA and some other commenters' contention that "[n]etwork diagnostic information and other information acquired from wireless devices is not CPNI because it does not contain personally identifiable call data."[55] The examples CTIA cites, such as "data on when and where calls fail" and "the location, date, and time a handset experiences a network event, such as a dialed or received telephone call [or] a dropped call,"[56] do reveal call details, which we conclude do fall within the statutory definition of CPNI.[57]

26. We also do not interpret section 222 or the Commission's rules in the limited way suggested by Verizon Wireless, which contends that the Commission's CPNI rules "are targeted at information related to a telecommunications carrier's provision of telecommunications services available via its network, and at activities and operations relating to a carrier's network and back-office systems."[58] The language of section 222 and the Commission's implementing rules do not specifically exclude information collected on mobile devices. The record developed in response to the Carrier IQ controversy and the subsequent *Mobile Device Privacy and Security Public Notice* demonstrates that carriers can and do exercise control over the wireless devices used to connect to their networks. They can determine, for instance, what CPNI the device will collect, how it will be stored, and when such information will be transmitted back to the carrier, without the customer's specific knowledge or ability to change those parameters in the device settings. Accordingly, the carrier is in a position to protect the privacy and

[52] CTIA Comments at 3.

[53] We reject any suggestion that we refrain from applying section 222 to information that meets the statutory definition just because some information collected in the same manner does not meet the statutory definition. *See, e.g.*, AT&T Comments at 10-11 ("It would thus not be in the public interest for the Commission to develop a new set of balkanized regulations or declaratory rulings for the small percentage of data stored on mobile devices that falls within the Commission's purview."). Doing so could leave a gap in the privacy and security obligations where section 222, by its terms, applies, leaving consumers unprotected.

[54] *See* New America Foundation Reply Comments at 3-6. We find 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. The Commission has never before created such a comprehensive list of CPNI, and we have had no indication that the absence of such a list has caused any significant confusion in the industry. Thus we do not decide today whether or under what circumstances "the locations where customers have problems accessing the network" qualifies as CPNI, *see* CTIA Comments at 8, though we note that location information in particular can be very sensitive customer information.

[55] CTIA Comments at 7.

[56] CTIA Comments at 8.

[57] *See* ITIF Comments at 2 (arguing that the Commission should "continue to limit its authority" to types of information that carriers have historically been able to access about their customers, such as "the amount and type of services used, the destination of communication, the location of the customers, and technical information about the devices used").

[58] Verizon Wireless Comments at 7.

security of information collected in that manner. We therefore decline to limit the "carrier-customer relationship" element of the definition of CPNI to exclude information that resides on devices.

27. The fact that CPNI is on a device and has not yet been transmitted to the carrier's own servers also does not remove the data from the definition of CPNI, if the collection has been done at the carrier's direction.[59] CPNI is defined as information that is *made available to the carrier*;[60] even if that information has not yet been transmitted from the mobile device to the carrier, the configuration of the device has made the information available to the carrier. Nor do we read the language in paragraph (c)(1), which imposes obligations on a telecommunications carrier "that receives or obtains [CPNI] by virtue of its provision of a telecommunications service," as excluding information that has not yet been transmitted to the carrier's back-office systems. We reach this conclusion for two independent reasons: First, that provision does not limit a carrier's obligations to CPNI that it has received.[61] Second, we conclude that information stored on a customer's device at the carrier's direction for the purpose of transmitting it to the carrier or its designee (and accessible to or controlled by the carrier or its designee) has, for this purpose, been obtained by the carrier.[62] Such information is under the carrier's control for all practical purposes, and the statutory obligations should and do apply.[63] We also note that subsection (a)'s obligation to protect customer information is not limited to CPNI that the carrier has obtained or received.[64] This statutory obligation provides independent support for requiring carriers to secure the CPNI that they have caused to be stored on a customer's device.[65]

28. We recognize that not all of the information collected on mobile wireless devices is CPNI. Some of the information that software such as the Carrier IQ agent can record does not pertain to a telecommunications service or might otherwise not relate to the quantity, technical configuration, type, destination, location, or amount of use of a telecommunications service, as required by the statutory

[59] *See Mobile Device Privacy and Security Public Notice*, 27 FCC Rcd at 5746 (observing that the phrase "'that is made available to a carrier by the customer solely by virtue of the carrier-customer relationship' … on its face could apply to information collected at a carrier's direction even before it has been transmitted to the carrier" and seeking comment on that analysis).

[60] 47 U.S.C. § 222(h)(1)(A) (defining CPNI to include "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship").

[61] A carrier that receives or obtains CPNI by virtue of its provision of a telecommunications service has obligations as to all "individually identifiable customer proprietary network information." 47 U.S.C. § 222(c)(1). Congress could have limited the obligations imposed by paragraph (c)(1) to the CPNI that the carrier has received or obtained by referring to "such CPNI," but it did not.

[62] *See Black's Law Dictionary* 1078 (6th ed. 1990) (defining "obtain" as "[t]o get hold of by effort; to get possession of; to procure; to acquire, *in any way*") (emphasis added).

[63] *See* CTIA *ex parte* presentation at 1 (June 19, 2013) ("CPNI requirements only apply to carriers if a carrier directed or caused CPNI to be on a mobile device and that the carrier has access to that CPNI.").

[64] *See* 47 U.S.C. § 222(a) (requiring "[e]very telecommunications carrier … to protect the confidentiality of proprietary information of, and relating to, … customers").

[65] *See, e.g.*, *2007 CPNI Order*, 22 FCC Rcd at 6943 ¶ 27 ("In conjunction with the general rulemaking authority under the Act, section 222(a), which imposes a duty on '[e]very telecommunications carrier … to protect the confidentiality of proprietary information,' provides ample authority for the Commission to require carriers to report CPNI breaches to law enforcement …." (footnote omitted)); *id.* at 6952 ¶ 48 ("[A]ll CPNI constitutes sensitive information that is protected under the Communications Act and our rules."); *id.* at 6959 ¶ 64 & n.198 (citing subsection (a) in support of the expectation that carriers will "take every reasonable precaution to protect the confidentiality of proprietary or personal customer information").

definition of CPNI.[66] In addition, modern mobile operating systems enable consumers to install applications developed by third parties that can collect sensitive personal information. Such third-party applications may raise privacy concerns. They are, however, generally beyond the scope of section 222 and our rules. For example, third-party applications might collect the same or different kinds of data,[67] some of which might be CPNI if collected at the carrier's direction; where such information is not collected by or at the direction of a carrier or its agent, it is not "made available to the carrier … by virtue of the carrier-customer relationship."[68] Furthermore, information stored on a mobile device that is not under the carrier's control and not intended to be transmitted to the carrier or otherwise not accessible by the carrier, as may be the case with a contact list or call log, is not CPNI because it is not "made available to the carrier,"[69] even if it would otherwise satisfy the definition of CPNI if made available to the carrier.

B. Telecommunications Carriers Have Statutory Obligations to Protect CPNI That They Collect on a Mobile Device.

29. We do not, at this time, adopt or propose any new rules governing the protection, use, or disclosure of individually identifiable CPNI that carriers collect by virtue of their control of customers' mobile devices. Rather, this *Declaratory Ruling* removes uncertainty about whether the obligations that already exist under the statute and our rules apply to CPNI collected in this manner. For example, section 222(a) of the Act provides that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to … customers,"[70] and section 222(c)(1)'s restriction on "disclos[ure]" of "individually identifiable" CPNI would appear to make carriers liable for inadvertent disclosures.[71] Such obligations apply equally to CPNI that carriers collect via their customers' devices.

30. The Commission has made clear that carriers must "take[] reasonable precautions to prevent the unauthorized disclosure of a customer's CPNI."[72] To the extent that a carrier's failure to take reasonable precautions renders private customer information unprotected or results in disclosure of individually identifiable CPNI, we believe that a violation of section 222 may have occurred. Any decision would depend on the facts and circumstances in a particular case.[73]

31. Some commenters note that third-party applications commonly store personal data on mobile devices and that wireless carriers have no ability to restrict the ability of those applications to

---

[66] For example, according to Carrier IQ, its software is capable of recording information that pertains to the device's access of the carrier's data network, web URLs visited in a browser, and applications installed and used. *See Understanding Carrier IQ Technology* at Exh. B; *see also* AT&T Comments at 10 ("Section 222 applies by its express terms only to telecommunications carriers. It does not apply to information service providers or other non-carrier entities, nor does it apply to telecommunications carriers when they are not acting in their capacity as such.").

[67] *See* CDT Comments at 7-8 (noting that other entities are capable of acquiring similar information).

[68] 47 U.S.C. § 222(h)(1)(A).

[69] 47 U.S.C. § 222(h)(1)(A).

[70] 47 U.S.C. § 222(a).

[71] *See* 47 U.S.C. § 222(c)(1).

[72] *See 2007 CPNI Order*, 22 FCC Rcd at 6959-60 ¶¶ 63-66; *see also* 47 C.F.R. § 64.2010(a) ("Telecommunications carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI.").

[73] *2007 CPNI Order*, 22 FCC Rcd at 6959-60 ¶¶ 63-66. In this regard, we note that the Commission has said, for example, that it "expect[s] a carrier to encrypt its CPNI databases if doing so would provide significant additional protection against the unauthorized access to CPNI at a cost that is reasonable given the technology a carrier already has implemented." *Id.* at 6959 ¶ 64.

access data stored on a mobile device.[74] To the extent that is true, it imposes an obligation on carriers to ensure that, if they choose to collect or store CPNI on a device and have access to or control over that data, they take reasonable precautions to protect it from unauthorized access and disclosure by such third-party applications, whether by storing the CPNI in a location or form that it is protected or otherwise.

32. Section 222 does not require mobile carriers to protect their customers against all possible privacy and security risks related to non-CPNI on a mobile device, including risks created by third-party applications. The openness of modern smartphones and the ability that they provide consumers to install applications that they desire has produced tremendous benefits.[75] While those benefits also come with risks to the privacy and security of consumers' information, those are risks that other parties may have a responsibility to address or that consumers might assume by their use of such applications.

33. We also reiterate that section 222(c)(1) allows a telecommunications carrier to use, disclose, or permit access to this 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."[76] A carrier thus may use, disclose, or permit access to such information "to initiate, render, bill, and collect for telecommunications services" or "to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services."[77] These provisions should allow a carrier that collects CPNI from customers' devices to use that information to assess and improve the performance of its network and to provide information to customer-support representatives without the customer's specific approval.[78] Verizon Wireless, for example, argues that "it is legitimate for service providers to use diagnostic tools to ensure network performance, provided they employ adequate data security protections."[79] We do not prohibit such practices. Our rules also allow a wireless provider to "use, disclose, or permit access to CPNI derived from its provision of CMRS, without customer approval, for the provision of CPE and information service(s)."[80]

34. Furthermore, as noted above,[81] neither section 222 nor the Commission's implementing rules restrict carriers' use of aggregate customer information. The statute defines "aggregate customer

[74] *See, e.g.*, CTIA Comments at 4-5; Verizon Wireless Comments at 2-4.

[75] *See generally* Federal Communications Commission, *Location-Based Services: An Overview of Opportunities and Other Considerations* (May 2012), *available at* http://www.fcc.gov/document/location-based-services-report; *see also* Roger Entner, Recon Analytics, *The Wireless Industry: The Essential Engine of U.S. Economic Growth* (May 2012), *available at* http://reconanalytics.com/wp-content/uploads/2012/04/Wireless-The-Ubiquitous-Engine-by-Recon-Analytics-1.pdf.

[76] 47 U.S.C. § 222(c)(1).

[77] 47 U.S.C. § 222(d)(1), (2).

[78] *See generally* 47 C.F.R. § 64.2005 ("Use of customer proprietary network information without customer approval."). Commenters emphasize that this use of network diagnostic information collected from wireless devices benefits consumers. *See, e.g.*, CTIA Comments at 8.

[79] Verizon Wireless Comments at 8; *see also id.* at 9 (arguing that "certain uses of information would not warrant customer consent, such as information used for monitoring network performance; many other types of more sensitive uses, however, would warrant notice and consent," though also arguing that "[b]est practices or codes of conduct … are the best methods for addressing these issues").

[80] 47 C.F.R. § 64.2005(b)(1); *see 1999 CPNI Order*, 14 FCC Rcd at 14430-35 ¶¶ 39-47 (finding that the phrase "services necessary to, or used in, the provision of such telecommunications service" includes customer-premises equipment and certain information services).

[81] *See supra* para. 17.

information" to mean "collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed."[82] It makes clear that a telecommunications carrier is not subject to the CPNI restrictions in using, disclosing, or permitting access to aggregate customer information.[83] For example, the Commission has said that carriers are free to use aggregate information "to assist in product development and design, as well as in tracking consumer buying trends, without customer approval."[84] Accordingly, a carrier may store or use aggregate information collected from customers' devices without violating section 222.[85] The exception for aggregate customer information and the other exceptions in section 222(d) do not, however, remove the obligations of a telecommunications carrier to protect the confidentiality of CPNI and to prevent unauthorized use, disclosure, or access.[86]

C. This *Declaratory Ruling* Is Consistent With Other Privacy Regimes.

35. CTIA argues that the Stored Communications Act (SCA), adopted as part of the Electronic Communications Privacy Act in 1986,[87] "confirms the lack of Commission authority in this area because it gives wireless providers broad authority to access and use their customers' information for network diagnostic purposes."[88] But an examination of the provisions cited by CTIA shows that the SCA poses no conflict: The SCA is a general criminal prohibition on voluntary disclosure of customer records; its exceptions carve certain disclosures out of that general prohibition. For example, the SCA's provision that appears to allow a provider to divulge records "to any person other than a governmental entity"[89] cannot reasonably be understood as authority for unlimited disclosure of personal information. Rather, it is an exception only to the general criminal prohibition on voluntary disclosure, as the structure of 18 U.S.C. § 2702 makes clear.[90] Furthermore, its provision allowing a provider to divulge records pertaining to its service "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service"[91] is consistent with section 222's provisions allowing a carrier to disclose CPNI in its provision of the telecommunications service from which it is derived or services necessary to, or used in, the provision of such service,[92] "to initiate, render, bill, and collect for

[82] 47 U.S.C. § 222(h)(2).

[83] 47 U.S.C. § 222(c)(3). For a local exchange carrier, such use of aggregate customer information is subject to a requirement that it provide the information on a nondiscriminatory basis to other persons upon reasonable request. *Id.*; *see 1998 CPNI Order*, 18 FCC Rcd at 8165-71 ¶¶ 143-153.

[84] *1998 CPNI Order*, 13 FCC Rcd at 8169 ¶ 149.

[85] *See* AT&T Comments at 20 n.56.

[86] 47 U.S.C. § 222(a), (c)(1).

[87] 18 U.S.C. §§ 2701-2712.

[88] CTIA Comments at 3; *see id.* at 10-11.

[89] 18 U.S.C. § 2702(c)(6).

[90] If the SCA were read as authorizing unlimited disclosure of personal information notwithstanding other provisions of law, as CTIA appears to be suggesting, it would nullify section 222 in nearly all respects, not just in the context of CPNI collected by mobile devices. It clearly does not do so. Courts have confirmed that section 222 restricts the use, disclosure, and permission of access to CPNI. *See National Cable & Telecommunications Ass'n v. FCC*, 555 F.3d 996 (D.C. Cir. 2009) (upholding the Commission's opt-in requirement for disclosure of CPNI to a carrier's joint-venture partner or independent contractor for the purposes of marketing communications-related services to that customer).

[91] 18 U.S.C. § 2702(c)(3).

[92] 47 U.S.C. § 222(c)(1).

telecommunications services,"[93] and "to protect the rights or property of the carrier."[94] Finally, we observe that section 222 was enacted in 1996, ten years after the SCA,[95] and therefore CTIA's suggestion that the SCA should carry more weight than the later-enacted statute has no merit.[96]

36. Several commenters urge the Commission to allow industry-developed best practices and codes of conduct to determine the applicable obligations in this context. Doing so, they say, would result in more consistency across related industries and technologies and would enable more flexible approaches.[97] For example, ATIS describes the work of some of its committees that focus on network security, reliability, and privacy. Its Network Reliability Steering Committee has developed Best Practice 8-8-8769, which "notes that service providers should protect such information against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data" and "note that policies for personal information protection should be clearly identified and enforced."[98] The National Telecommunications and Information Administration (NTIA) currently is leading a multistakeholder process, the goal of which is "to develop a code of conduct to provide transparency in how companies providing applications and interactive services for mobile devices handle personal data."[99] The process emerged from a February 2012 framework issued by the White House, sometimes referred to as the Privacy Blueprint, which set forth a "consumer privacy bill of rights" and envisioned a multistakeholder process to specify how its principles would apply in particular business contexts. The framework urged Congress to provide the FTC and state attorneys general with specific authority to enforce those rights.[100] It noted that companies choosing to adopt a code of conduct would be subject to enforcement by the FTC under that agency's authority to prevent deceptive acts or practices as well as its unfairness jurisdiction.[101] The FTC's authority, however, does not extend to common carriers.[102]

37. The Commission has statutory responsibilities to enforce the Communications Act, and, although we welcome these other complementary initiatives, none of them is a substitute for the Commission fulfilling its statutory role. Section 222 provides the Commission with a clear directive to protect the privacy of consumers utilizing the communications infrastructure, and the Commission's rules

[93] 47 U.S.C. § 222(d)(1).

[94] 47 U.S.C. § 222(d)(2).

[95] *See* Telecommunications Act of 1996, Pub. L. No. 104-104, § 702, 110 Stat. 56, 148-49 (adding new section 222 to Title II of the Communications Act of 1934).

[96] *See FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 133, 143 (2000) ("[T]he meaning of one statute may be affected by other Acts, particularly where Congress has spoken subsequently and more specifically to the topic at hand."); CTIA Comments at 10 & n.30 (citing *FDA v. Brown & Williamson Tobacco Corp.*) (noting that the meaning of one statute may be affected by others, particularly subsequent enactments).

[97] *See, e.g.*, CTIA Comments at 5-6; Consumer Electronics Association Comments at 11-13; AT&T Comments at 8-13; ITIF Comments at 4.

[98] ATIS Comments at 3; *see* Protection of Personally Identifiable Information (PII), NRIC Best Practice No. 8-8-8769, *available at* http://www.atis.org/bestpractices/BPDetail.aspx?num=8-8-8769.

[99] *See* National Telecommunications and Information Administration, *Privacy Multistakeholder Process: Mobile Application Transparency*, *available at* http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency. We note that this first multistakeholder process is focused on developers of mobile applications and not on the obligations of telecommunications carriers.

[100] The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 2012) (*White House Privacy Blueprint*), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[101] *See id.* at 27 & n.32.

[102] *See* 15 U.S.C. § 45(a)(2); *see also supra* para. 15 & n.35.

implementing section 222 are longstanding, well-known, and judicially tested.[103] The nature of the communications marketplace has changed since the Commission's last pronouncement on CPNI, and thus we act here to affirm our commitment to fulfilling our statutory directive to ensure that carriers are protecting consumer information to which they have access because of their unique position as the gatekeeper to their customers' access to the network. By this *Declaratory Ruling*, we clarify that we will apply section 222 and our rules to the type of CPNI described herein to avoid a potential gap in consumers' privacy protections.

IV. ORDERING CLAUSES

38. Accordingly, IT IS ORDERED, pursuant to sections 1, 4, 201, 222, and 303(r) of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 154, 201, 222, 303(r), and section 1.2 of the Commission's rules, 47 C.F.R. § 1.2, that this *Declaratory Ruling* in CC Docket No. 96-115 IS ADOPTED.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

[103] *See National Cable & Telecommunications Ass'n v. FCC*, 555 F.3d 996 (D.C. Cir. 2009).

STATEMENT OF
ACTING CHAIRWOMAN MIGNON CLYBURN

Re: *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115.

Protecting consumer privacy is a key component of our mission to serve the public interest. Changes in technology and market practices have raised many new concerns when it comes to privacy. But today's action affirms the Commission's commitment to the protection of wireless consumers by clarifying the FCC's customer proprietary network information – or CPNI – policies.

Consumers rightfully expect that private information -- for example, numbers called, the times of those calls, and the locations from which a customer makes those calls -- will be safeguarded, whether it's retained on their mobile device, or in a carrier's back-office system. That is why this declaratory ruling clarifies that a carrier has "received or obtained" CPNI when the carrier causes that information to be stored on the device and it or its designee has access to or control over that information. Carriers should be responsible for safeguarding the customer information that they collect wherever it's stored. Today's decision ensures that it will be.

It is also worth noting what this Declaratory Ruling does not do. It does not affect third-party app developers or apps that customers might install from an app store. It does not prohibit carriers from collecting information needed to improve networks. In fact, we recognize the benefits of such data collection. However, while there can be benefits to carrier data collection using customers' devices, the fact that such sensitive information is stored on each subscriber's mobile device emphasizes the need to ensure such information is protected. Also, we do not require carriers to implement any particular type of protection. Instead, we allow them to choose their own method of safeguarding CPNI, as long as it provides appropriate protection against unauthorized access. I do want to make clear, however, that if a carrier fails to protect CPNI, the Commission stands ready to use its enforcement authority, including its authority to order forfeitures.

In sum, today's Declaratory Ruling demonstrates that, while technology and consumer behavior evolve, we will continue to exercise our statutory authority to protect consumers. I would like to thank my colleagues for their support of the item, as well as the tireless efforts of Sean Lev, Jennifer Tatel, Douglas Klein, and other members of the Office of General Counsel, for presenting us with such an important item.

STATEMENT OF
COMMISSIONER JESSICA ROSENWORCEL

Re: *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115.

It has been over six years since the Commission last updated its customer proprietary network information (CPNI) rules. Think about that. Our last major decision was released before the introduction of the iPhone. Before any one of us thought it was normal to tap on a screen—any screen—and expect an Internet-enabled response based on the swipe of a finger. Before streaming any video in our palms and laps was even imaginable. Before the applications economy grew to provide 500,000 new jobs. It was a long time ago.

In the intervening years, several trends have collided to make the values that inform our CPNI rules both more important and more complicated.

First, connection is no longer merely convenient. We live in an age of always-on connectivity. We are a nation with more wireless phones than people. One in three adults now has a tablet computer. Our commercial and civic lives are migrating online with ferocious force and speed. Simply put, the opportunity to opt out of this new digital age is limited. Its advances are too bountiful, they save us time and money, and they inform and support all aspects of modern life.

Second, it used to be that the communications relationship was primarily between a customer and his or her carrier. But the number of third parties participating in our digital age connections and transactions has multiplied exponentially. Dial a call, write an e-mail, make a purchase, post an online update to a social network, read a news site, store your family photographs in the cloud, and you should assume that service providers, advertising networks, and companies specializing in analytics have access to your personal information. Lots of it—and for a long time. Our digital footprints are hardly in sand; they are effectively in wet cement.

Third, the monetization of data is big business. The cost of data storage has declined dramatically. The market incentives to keep our data and slice and dice it to inform commercial activity are enormous. They are only going to grow.

Going forward, I think the Commission needs to take note of these trends. They are the impetus, I believe, for last year's Administration blueprint for consumer data privacy in the 21st Century. It is a blueprint I support.

But against this background, we also need to do simple things at the Commission, like enforce our rules.

To this end, in Section 222 of the Communications Act, Congress sought to guard consumers by defining CPNI rights in their relationship with their telecommunications carriers: the right to know what information is being collected about them; the right to get notice when information is being used for other purposes; and the right to be able to stop the reuse or sale of that information. Today's decision advances these principles. It clarifies that our CPNI rules and obligations apply to information that carriers cause to be stored on their customer's devices, like wireless phones. As a result, carriers may only use and disclose such information consistent with our rules. This means wireless carriers must protect CPNI data from unauthorized disclosure and inform subscribers in the event of a security breach.

However, it is also important to be clear about what our decision does not do. Our CPNI

protections at issue in this decision involve carriers. They do not apply to the manufacturers of wireless phones. They do not apply to the developers of operating systems.

So let's be honest. Consumers can be confused by these distinctions. But the scope of this proceeding and Section 222 are limited. So I hope the agency can be proactive and help consumers better understand the different ways their personal data may be collected on a mobile phones, what rules apply, and how they can protect themselves. Furthermore, I think we should take on this task in cooperation with our colleagues at the Federal Trade Commission. Because consumers should not have to be network engineers to understand who is collecting their data and they should not have to be lawyers to determine if their information is protected. We should strive to simplify privacy policies across all platforms and aim for more consistency. But in the interim, it is also essential we enforce our rules. That is what we do here and that is why I am pleased to support this declaratory ruling.

STATEMENT OF
COMMISSIONER AJIT PAI
APPROVING IN PART AND CONCURRING IN PART

Re: *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115.

The privacy of Americans' phone records is a topic that has been in the news quite a bit lately. But this morning, the Commission tackles a small piece of this subject that hasn't made the headlines. In today's Declaratory Ruling, we seek to clarify both when data stored on a mobile device constitutes customer proprietary network information (CPNI) and when carriers must protect such CPNI pursuant to section 222 of the Communications Act.

I want to start by thanking my colleagues for their willingness to incorporate many of my suggestions into the item and especially commend Chairwoman Clyburn for her leadership, which was critical in reaching this result. I had serious concerns with the original version of this item. But over the last several days, substantial changes to the Declaratory Ruling have largely allayed those concerns. Therefore, I am voting this morning to approve in part and concur in part.

Four factors are critical to my decision. *First*, I agree that there is no "mobile device exception" to either section 222 or our CPNI rules. If information is covered by the statutory definition of CPNI set forth in section 222(h)(1), then it is CPNI, regardless of whether it is located on a mobile device.

Second, today's Declaratory Ruling is limited in scope. It only applies to information that is both: (1) collected by or at the direction of the carrier; and (2) may be accessed or controlled by the carrier or its designee. If a carrier is not responsible for the collection of certain data, then it may not be held responsible for protecting that data. Likewise, if a carrier doesn't have access to or control over information, then it is not obligated to safeguard it.

Third, the Commission provides carriers with maximum flexibility in carrying out their statutory responsibilities with respect to CPNI stored on mobile devices. In today's item, we do not opine on various practices and hypotheticals in the absence of a fully developed factual record and concrete set of facts. Given the complex and quickly evolving technologies at issue, this restraint is wise.

Fourth, and perhaps most important, this Declaratory Ruling does not seek to hold carriers liable for compliance with voluntary codes of conduct under section 201(b) of the Communications Act. I believe the Commission should welcome the development of private-sector solutions to some of the challenges facing the industry. Imbuing such codes of conduct with the force of law, however, would have precisely the opposite effect. Carriers, of course, would be worse off if we changed the meaning of "voluntary" in "voluntary codes of conduct." But consumers ultimately would be worse off too; if we effectively ensure that no good deed goes unpunished, the industry will be less likely to take joint, consumer-friendly action of its own accord.

To be sure, I do not agree with every legal theory set forth in today's item. That's why I am concurring in part. Specifically, I do not join the item's discussion of section 222(c)(1) and in particular its claim that the provision makes a carrier responsible for CPNI that it has neither received nor obtained. On the whole, however, I believe that today's Declaratory Ruling arrives at a reasonable result, one that is fair to both consumers and carriers.

Finally, I would like to thank Sean Lev, Jennifer Tatel, and Doug Klein of the Office of General Counsel as well as Michele Ellison, Dave Grimaldi, and Louis Peraertz in the Office of the Chairwoman

for their hard work on this item, including the fruitful discussions that led to this happy outcome. This item might not receive the same media attention as other recent issues related to privacy, but you deserve public recognition for your efforts.