U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE

July 9, 2018

TO: Members, Subcommittee on Communications and Technology

FROM: Committee Majority Staff

RE: Hearing entitled "Protecting Customer Network Proprietary Information in the Internet Age."

I. INTRODUCTION

The Subcommittee on Communications and Technology will hold a hearing on July 11, 2018, at 10:15 a.m. in 2322 Rayburn House Office Building. The hearing is entitled "Protecting Customer Proprietary Network Information in the Internet Age."

II. WITNESSES

- Hance Haney, Senior Fellow, Discovery Institute;
- Robert McDowell, Senior Fellow, Hudson Institute; former Commissioner, Federal Communications Commission; and
- Laura Moy, Deputy Director, Georgetown Law Center on Privacy and Technology.

III. BACKGROUND

Under Section 222 of the Communications Act, telecommunications carriers must protect the confidentiality of customer proprietary network information (CPNI).[1] When enacting this provision in 1996, Congress recognized the importance of protecting the privacy of customers when using the primary method for communications at the time: telecommunications networks. In the 22 years since the enactment of Section 222, the ways that consumers choose and are able to communicate has changed dramatically. Consumers still use networks to communicate, but instead of primarily relying on the telecommunications network, they increasingly use social networks like Facebook, Google, or Snapchat to communicate. These social networks often offer consumers the ability to communicate and make calls via apps, but unlike traditional cell phone calls, calls made via the apps might not intersect with the telecommunications network at all. Even though consumers might not be using telecommunications networks in the same way today as they were in 1996, one thing remains unchanged: consumers are still providing personal information when communicating on other types of networks. Today's hearing will discuss the various entities that have access to information that is regulated as CPNI when it is held by a telecommunications provider.

[1] 47 U.S.C. § 222.

Regulatory Framework Under Section 222

By enacting Section 222, Congress established a specific statutory scheme governing access to and protection of CPNI in a way that Congress felt "balance[d] both competitive and consumer privacy interests with respect to CPNI."[2] Section 222 ensures "(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."[3] Section 222(a) imposes a duty on all telecommunications carriers to protect the confidentiality of their customers' "proprietary information."[4] Section 222(c) imposes restrictions on telecommunications carriers' use and sharing of CPNI without customer approval, subject to certain exceptions.[5] The statute focuses on customers' notice, choice, and control over their personal, proprietary information and delegates authority to the Federal Communications Commission (Commission) to promulgate rules under the statute. The Commission's rules currently include requirements for telecommunications providers under the Commission's Title II jurisdiction for transparency, choice, data security, and data breach notification.

Since Section 222 was enacted by Congress over 20 years ago, the Commission has implemented the statutory CPNI requirements by adopting privacy rules for telecommunications carriers.[6] As the telecommunications market evolved and new telecommunications entities obtained access to sensitive customer data, the Commission extended the applicability of its Section 222 privacy rules. For example, in 2007, the Commission added customer authentication and data breach notification requirements to its Section 222 rules to curb the practice of "pretexting," where entities were improperly accessing and selling details of residential telephone calls.[7] At that same time, the Commission extended Section 222 CPNI protections to interconnected VoIP to ensure consumers' privacy interests are protected whether making a phone call over traditional telephony or voice over the Internet. In 2013, the Commission extended its CPNI rules to mobile devices. Specifically, the Commission clarified that telecommunications carriers who use their control of customers' mobile devices to collect information about their customers' use of the network (such as the time a call was made or where the customer was located when the call was placed), must safeguard that information under

[2] Joint Explanatory Statement of the Committee of Conference, 104th Cong., 2d Sess. at 205.
[3] Joint Explanatory Statement of the Committee of Conference, 104th Cong., 2d Sess. at 204.
[4] 47 U.S.C. § 222(a)
[5] 47 U.S.C. § 222(c)(1).
[6] *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) Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14860 (2002).
[7] *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, CC Docket No. 96-115, WC Docket No. 04-36, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007).

Section 222's rules so long as the information is collected by or at the direction of the carrier and the carrier or its designee has access to or control over the information.[8]

While the Commission has in the past acted to update its Section 222 rules to continue to protect consumers in the face of an evolving telecommunications market, the rules under the statute can only stretch so far. For instance, when the Commission extended CPNI protections to facilities-based and interconnected VoIP providers in 2007, the same protections applied to details involving a consumer's private phone conversation on a VoIP phone service as would apply if making the call over a traditional wireline network. Interconnected VoIP service enables users, over their broadband connections, to receive calls that originate from the public switched telephone network (PSTN) or other VoIP users, and to terminate calls to the PSTN.[9] Extending these CPNI requirements to interconnected VoIP providers is just one of the Title II-like obligations that the Commission has applied to VoIP providers without classifying those services as telecommunications services or information services under the Communications Act.

However, CPNI protections currently do not extend to messaging and calling services that do not touch the PSTN, such as WhatsApp (a messaging and VoIP service owned by Facebook) or Google Voice (a messaging and VoIP service owned by Alphabet Inc.). This means that a consumer who calls someone from their smartphone using an app interface is not guaranteed to have the same level of privacy protections as if the consumer makes the call using their wireless cell service, which does rely on the PSTN. This distinction takes on critical importance as more and more consumers communicate using free apps that mimic phone calls, but since the app is not making the call over the telephone network, consumers do not have the same CPNI protections attached to the app-based call. Even when the Commission temporarily extended CPNI privacy requirements to broadband Internet access providers when they were classified as telecommunications services,[10] consumers' personal information was still not protected at the same level when making a call via an over-the-top app as they would if they made a phone call using their wireless cellular plan. Although the Commission temporarily required broadband providers to comply with CPNI rules, the Commission did not have jurisdiction over the third party app provider—so the app provider was not required to protect the consumer's information in the same way that the broadband provider was.

Types of Information Protected Under Section 222

Section 222 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

[8] *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, 28 FCC Rcd 9609, 9618, para. 27 (2013) (*2013 CPNI Declaratory Ruling*).
[9] 47 C.F.R. § 9.3.
[10] *See, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, 31 FCC Rcd 13911 (2016).

by a customer of a carrier; except that [CPNI] does not include subscriber list information.[11] The Commission has not established a full list of factors that do or do not satisfy the statutory definition of CPNI; however, the Commission has detailed certain information that it considers to be CPNI. These data elements include call detail records (such as "the number called [or the phone number placing the call], and the time, location or duration of any call")[12] and any services purchased by the customer.[13] Following the Commission's, *2013 CPNI Declaratory Ruling*, information that a telecommunications carrier causes to be collected or stored on a customer's device, including customer premises equipment (CPE) and mobile stations, also meets the statutory definition of CPNI.[14]

Congress provided a few narrow exceptions for the type of information protected under Section 222. Congress provided an exception from the definition of CPNI for "subscriber list information," which includes the "listed names of subscribers of a carrier and such subscribers' telephone numbers, addresses, or primary advertising classifications."[15] At the time Congress enacted Section 222, phone books were a mainstay, so this exception seems to have served to preserve the publication of telephone books as a business model, rather than an indication that names and addresses are not a type of information deserving of protection.[16] Congress also created a narrow exception for "aggregate customer information,"[17] which is "collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed."[18] The Commission's Section 222 rules reflect these exceptions and give less protection to information when individually identifiable characteristics and identities have been removed.

Entities With Access to Information Protected Under Section 222

When Congress enacted Section 222, the common belief was that only telecommunications carriers had access to the sensitive information categorized as CPNI. However, recent developments in the marketplace have shown that is no longer the case. As indicated above, in 2013, the Commission took action to prevent third parties from accessing confidential call data stored on consumer's mobile phones via diagnostic software. While the Commission was able to extend its existing CPNI rules since the carriers were in charge of collecting and had control over the information, the Commission does not have the authority to protect consumers' information in other contexts.

Outside of the scope of telecommunications carriers, other entities in the Internet ecosystem have access to data that would otherwise be protected under the CPNI rules. For

[11] 47 U.S.C. § 222(h)(1).
[12] 47 CFR § 64.2003(d).
[13] 47 CFR § 47 CFR § 64.2003(e).
[14] *See, 2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9618, para. 27.
[15] 47 U.S.C. § 222(h)(3).
[16] S. Conf. Rep. No. 104-230 at 205 (1996) ("The subscriber list information provision guarantees independent publishers access to subscriber list information at reasonable and nondiscriminatory rates, terms and conditions from any provider of local telephone service.").
[17] 47 U.S.C. § 222(c)(3).
[18] 47 U.S.C. § 222(h)(2).

example, edge providers such as Facebook and Google provide messaging and voice services to their users. Facebook Messenger allows users to "connect across the world with voice and video calls for free" [19] and Google Voice assigns users "a free phone number for life" that they can use to "text, call, and check voicemail – all from one app."[20] WhatsApp, owned by Facebook, also offers its users the option for voice and video calls.[21] These apps all use the Internet connection on the user's mobile phone, rather than the user's cell phone plan, to connect users on a call. Consumers are increasingly using these apps to communicate because they do not have to worry about cutting into their cell plan's voice minutes, especially when traveling outside of their normal coverage plan area, but they might still incur charges if they access these apps using the data provided by their cell plan. Regardless of the charges incurred when using the apps, consumers do need to worry about how these apps are securing the call information obtained via the in-app calls. Unlike mobile phone calls made using a cell plan, calls made from a mobile phone using an app do not impose any requirements on the app provider to safeguard sensitive information, such as caller and recipient phone numbers, locations, or the frequency, duration, and timing of calls.

Recent news reports have indicated that non-telecommunications carriers, such as edge providers, may also have access to CPNI information.[22] It was reported that, "if you granted permission to read contacts during Facebook's installation on Android a few versions ago—specifically before Android 4.1 (Jelly Bean)—that permission also granted Facebook access to call and message logs by default."[23] Because Android's application programming interface (API) at that time was structured in a way that liberally divulged information from the device, users who gave permission for Facebook to view their contacts also gave Facebook permission to view all call records made by the phone, even outside of the Facebook app, which is considered CPNI. This raises questions as to who else may have information covered under CPNI rules, and whether yesterday's conception of consumer proprietary network information makes sense in today's communications landscape.

Additional Privacy Protections Enforced by the Commission

In addition to giving the Commission the ability to protect the customer information collected by telecommunications companies, Congress also gave the Commission authority to require cable and satellite providers to protect the privacy of subscribers to their service. Congress incorporated Section 631 into the Communications Act to protect the privacy of cable subscribers,[24] and Section 338(i)[25] protects the proprietary information of satellite subscribers.

---

[19] *See*, https://www.messenger.com/features#hdcalls
[20] *See*, https://voice.google.com/about
[21] *See*, https://www.whatsapp.com/features/
[22] *See*, https://arstechnica.com/information-technology/2018/03/facebook-scraped-call-text-message-data-for-years-from-android-phones/
[23] *Supra*, note 23.
[24] *See* 47 U.S.C. § 551.
[25] 47 U.S.C. § 338(i).

IV. STAFF CONTACTS

If you have any questions regarding this hearing, please contact Tim Kurth or Robin Colwell of the Committee Staff at (202) 225-2927.