PUBLIC NOTICE

Federal Communications Commission
445 12th St., S.W.
Washington, D.C. 20554

News Media Information 202 / 418-0500
Internet: http://www.fcc.gov
TTY: 1-888-835-5322

DA 12-818
May 25, 2012

COMMENTS SOUGHT ON PRIVACY AND SECURITY OF INFORMATION STORED ON MOBILE COMMUNICATIONS DEVICES
CC Docket No. 96-115

Comment Date: 30 days after publication in the Federal Register
Reply Comment Date: 45 days after publication in the Federal Register

In this Public Notice, the Wireline Competition Bureau, Wireless Telecommunications Bureau, and Office of General Counsel jointly solicit comments regarding the privacy and data-security practices of mobile wireless service providers with respect to customer information stored on their users' mobile communications devices, and the application of existing privacy and security requirements to that information. Since the Commission last solicited public input on this question five years ago, technologies and business practices have evolved dramatically. The devices consumers use to access mobile wireless networks have become more sophisticated and powerful, and their expanded capabilities have at times been used by wireless providers to collect information about particular customers' use of the network—sometimes, it appears, without informing the customer. Service providers' collection and use of this information may be a legitimate and effective way to improve the quality of wireless services. At the same time, the collection, transmission, and storage of this customer-specific network information raise new privacy and security concerns.

Section 222 of the Communications Act of 1934, as amended, establishes the duty of every telecommunications carrier to "protect the confidentiality of proprietary information of, and relating to … customers."[1] Further, every carrier must protect "customer proprietary network information" (CPNI) that it receives or obtains by virtue of its provision of a telecommunications service and may use, disclose, or permit access to such information only in limited circumstances.[2] The Commission is charged with enforcing those obligations.[3]

---

[1] 47 U.S.C. § 222(a).

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

[3] *See, 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 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*).

In 2007, the Commission updated its rules implementing these statutory obligations to address the practice of "pretexting"[4] and to reaffirm that carriers are responsible for taking all reasonable steps to protect their customers' private information.[5] At the same time, the Commission adopted a Further Notice of Proposed Rulemaking to address another emerging privacy issue: the obligations of mobile carriers to secure the privacy of customer information stored in mobile communications devices.[6] Although the Commission's particular focus in 2007 was on carriers' duty to erase customer information on mobile equipment prior to refurbishing the equipment, the issue of customer information on mobile devices has recently gained greater prominence. In particular, carriers recently have acknowledged using software embedded or preinstalled on wireless devices to collect information about the performance of the device and the provider's network.[7]

Comparing the record collected by the Commission five years ago to the publicly available facts today highlights the need to refresh our record. In response to the 2007 *Further Notice*, AT&T Inc., for example, emphasized consumers' control of the information residing on their devices, stating:

> [D]ecisions 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. Indeed, in some respects, mobile communications devices are becoming more like computers, laptops, personal digital assistants and other devices that permit customers to store their information. In the same vein that consumers erase information stored on those devices, (or shred paper copies of bills or other documents that contain personal information), consumers are necessarily in the best position to know what data they have stored on their mobile devices and to take responsibility for

---

[4] *2007 CPNI Order*, 22 FCC Rcd at 6928 ¶ 1. "Pretexting" is "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." *Id.* at 6928 ¶ 1 n.1.

[5] *See id.* at 6959-60 ¶¶ 63-66; *see also* 47 C.F.R. § 64.2010(a) (requiring telecommunications carriers to "take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI").

[6] *See 2007 CPNI Order*, 22 FCC Rcd at 6962 ¶ 72.

[7] *See* 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). *See generally* Sen. Franken Statement on Responses from Carrier IQ, Wireless Carriers, and Handset Manufacturers (Dec. 15, 2011), *available at* http://www.franken.senate.gov/?p=press_release&id=1891 (last visited May 24, 2012).

> safeguarding and erasing that information before disposal or recycling the device.[8]

Sprint similarly stated in 2007 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."[9]

In recent months, it has become clear that these submissions are badly out of date. Mobile carriers are directing the collection and storage of customer-specific information on mobile devices. In response to questions from Congress concerning its use of "Carrier IQ" software, AT&T explained that it gathers customer-specific data as an "enhance[ment of] its network reporting capabilities" and to collect information about its network from the perspective of its users' devices, "a view that cannot be obtained from the network alone."[10] Answering the same questions, Sprint identified a "legitimate need to deploy and use diagnostic software in the maintenance and operation of [Sprint's] services" and described how Sprint worked with the software vendor to customize data collection for Sprint's devices and network.[11] T-Mobile likewise stated that it uses software on its customers' mobile devices to "assist[] T-Mobile in improving our customers' wireless experience by capturing and analyzing a narrow set of data related to some of the most common issues our customers experience."[12] The data collected in this manner may be shared with a third party for purposes of network diagnostics or improving customer care.[13]

---

[8] Comments of AT&T Inc., CC Docket No. 96-115 (July 9, 2007), at 9, *available at* http://apps.fcc.gov/ecfs/document/view?id=6519559163.

[9] Comments of Sprint Nextel Corporation, CC Docket No. 96-115 and WC Docket No. 04-36, at 21 (July 9, 2007), *available at* http://apps.fcc.gov/ecfs/document/view?id=6519548080; *see also* Reply Comments of Sprint Nextel Corporation, CC Docket No. 96-115 and WC Docket No. 04-36, at 14 (Aug. 7, 2007) ("Importantly, 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."), *available at* http://apps.fcc.gov/ecfs/document/view?id=6519610194.

[10] AT&T Letter to Sen. Franken at 1; *see also id.* at 5 (stating that this activity is covered by provisions in its privacy policy, wireless customer agreement, and end user licensing agreement that AT&T "collect[s] network, performance, and usage information from our network and customer devices").

[11] Sprint Letter to Sen. Franken at 1.

[12] T-Mobile Letter to Sen. Franken at 1-2.

[13] *See* Carrier IQ, Understanding Carrier IQ Technology: What Carrier IQ Does and Does Not Do (Dec. 15, 2011), at 13, *available at* http://www.carrieriq.com/documents/understanding-carrier-iq-technology/6461/ (last visited May 24, 2012) (stating that Carrier IQ hosts servers on behalf of some customers, while other customers host servers in their own data centers); AT&T Letter to Sen. Franken at 3 (stating that AT&T hosts its own servers); Sprint Letter to Sen. Franken at 2 (stating that data is transmitted to Carrier IQ servers); T-Mobile Letter to Sen. Franken at 4-5 (stating that data is stored on dedicated servers by Carrier IQ and its subcontractors).

Commission staff has itself inquired into practices of mobile wireless service providers with respect to information stored on their customers' mobile communications devices.[14] The staff's inquiry has focused on possible harms to consumers and on what service provider obligations, if any, apply or should apply under section 222 and other provisions of law within this Commission's jurisdiction.

In light of these developments, we now seek to refresh the record in this docket concerning the practices of mobile wireless service providers with respect to information stored on their customers' mobile communications devices. How have those practices evolved since we collected information on this issue in the 2007 *Further Notice*? Are consumers given meaningful notice and choice with respect to service providers' collection of usage-related information on their devices? Do current practices serve the needs of service providers and consumers, and in what ways? Do current practices raise concerns with respect to consumer privacy and data security? How are the risks created by these practices similar to or different from those that historically have been addressed under the Commission's CPNI rules? Have these practices created actual data-security vulnerabilities? Should privacy and data security be greater considerations in the design of software for mobile devices, and, if so, should the Commission take any steps to encourage such privacy by design? What role can disclosure of service providers' practices to wireless consumers play? To what extent should consumers bear responsibility for the privacy and security of data in their custody or control?

Specifically with respect to section 222, we seek comment on the applicability and significance in this context of telecommunications carriers' duty under section 222(a) to protect customer information. Further, the definition of CPNI in section 222(h)(1) includes information "that is made available to a carrier by the customer solely by virtue of the carrier-customer relationship," a phrase that on its face could apply to information collected at a carrier's direction even before it has been transmitted to the carrier. We seek comment on this analysis. We further seek comment on which, if any, of the following factors are relevant to assessing a wireless provider's obligations under section 222 and the Commission's implementing rules, or other provisions of law within this Commission's jurisdiction, and in what ways:

- Whether the device is sold by the service provider;
- Whether the device is locked to the service provider's network so that it would not work with a different service provider;
- The degree of control that the service provider exercises over the design, integration, installation, or use of the software that collects and stores information;
- The service provider's role in selecting, integrating, and updating the device's operating system, preinstalled software, and security capabilities;
- The manner in which the collected information is used;
- Whether the information pertains to voice service, data service, or both; and

[14] The staff's inquiry has included not only a specific examination of mobile wireless service providers' practices with respect to information stored on their customers' mobile communications devices, but also a broad review of so-called "location-based services" used in wireless communications. *See* Location-Based Services: An Overview of Opportunities and Other Considerations, Federal Communications Commission Staff Report, at 6 (rel. May 25, 2012).

- The role of third parties in collecting and storing data.

Are any other factors relevant? If so, what are these other factors, and what is their relevance? What privacy and security obligations should apply to customer information that service providers cause to be collected by and stored on mobile communications devices? How does the obligation of carriers to "take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI"[15] apply in this context? What should be the obligations when service providers use a third party to collect, store, host, or analyze such data? What would be the advantages and disadvantages of clarifying mobile service providers' obligations, if any, with respect to information stored on mobile devices—for instance through a declaratory ruling? What are the potential costs and benefits associated with such clarification?

Pursuant to sections 1.415 and 1.419 of the Commission's rules, 47 C.F.R. §§ 1.415, 1.419, interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS). *See Electronic Filing of Documents in Rulemaking Proceedings*, 63 FR 24121 (1998).

- Electronic Filers: Comments may be filed electronically using the Internet by accessing the ECFS: http://apps.fcc.gov/ecfs/.

- Paper Filers: Parties who choose to file by paper must file an original and one copy of each filing. If more than one docket or rulemaking number appears in the caption of this proceeding, filers must submit two additional copies for each additional docket or rulemaking number.

  Filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.

  - All hand-delivered or messenger-delivered paper filings for the Commission's Secretary must be delivered to FCC Headquarters at 445 12th St., SW, Room TW-A325, Washington, DC 20554. The filing hours are 8:00 a.m. to 7:00 p.m. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes and boxes must be disposed of before entering the building.

  - Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9300 East Hampton Drive, Capitol Heights, MD 20743.

  - U.S. Postal Service First-Class, Express, and Priority mail must be addressed to 445 12th Street, SW, Washington, DC 20554.

[15] 47 C.F.R. § 64.2010(a).

People with Disabilities: To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice), 202-418-0432 (tty).

This is a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules.[16] Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with rule 1.1206(b). In proceedings governed by rule 1.49(f) or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (e.g., .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

For further information, contact Lisa Hone, Wireline Competition Bureau, at (202) 418-1500, Melissa Tye, Wireless Telecommunications Bureau, at (202) 418-0600, or Douglas Klein, Office of General Counsel, at (202) 418-1720.

-FCC-

[16] 47 C.F.R. §§ 1.1200 *et seq.*