

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

In the Matter of	)	
	)	
Implementation of the Telecommunications Act of 1996:	)	
	)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information	)	CC Docket 96-115
	)	
	)	
	)	

**REPLY COMMENTS OF NEW AMERICA FOUNDATION'S OPEN TECHNOLOGY  
INSTITUTE, BENTON FOUNDATION, CENTER FOR MEDIA JUSTICE, FREE  
PRESS, INSTITUTE FOR LOCAL SELF-RELIANCE, MEDIA ALLIANCE, PEOPLE'S  
PRODUCTION HOUSE, AND PUBLIC KNOWLEDGE**

Sarah J. Morris  
Benjamin Lennett  
Open Technology Institute  
New America Foundation  
1899 L Street, NW, 4th Floor  
Washington, DC 20036

July 30, 2012

## I. INTRODUCTION

While various commenters would prefer to rely on the rhetoric proffered in the Commission's 2007 proceeding<sup>1</sup>, their comments reflect the same opacity and blind faith in voluntary behavior to protect privacy, the effectiveness of which has failed to materialize in the five years following the Commission's last assessment of its § 222 obligations. The Commission has an opportunity (and, indeed the statutory directive) to regulate CPNI data collection practices of mobile carriers. New America Foundation's Open Technology Institute, Benton Foundation<sup>2</sup>, Center for Media Justice, Free Press, Institute for Local Self-Reliance, Media Alliance, People's Production House, and Public Knowledge (collectively, "Commenters") offer the following reply comments in the above-captioned dockets outlining the need and statutory basis for Commission action with regard to data stored on mobile devices and collected using applications such as Carrier IQ.

We counter the assertions that the CPNI rules do not extend to data stored on mobile devices and ask the Commission to find that data to be within the purview of § 222. Commenters also point out the unreliability and obvious evasiveness of the justifications offered with regard to this data collection behavior, and we reaffirm our request that "the Commission ... not merely

---

<sup>1</sup> *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007) ("2007 Order").

<sup>2</sup> The Benton Foundation is a nonprofit organization dedicated to promoting communication in the public interest. These comments [or this press release] reflect the institutional view of the Foundation and, unless obvious from the text, are not intended to reflect the views of individual Foundation officers, directors, or advisors.

take the carriers' self-assessments of these practices at face value, given the variety of incentives in play as well as the carriers' inconsistencies in the 2007 proceeding."<sup>3</sup>

Further, Commenters argue that the existence of a concurrent agency proceeding on privacy issues that may or may not fully address mobile privacy issues is not a bar to Commission action on a specific statutory directive. Commenters note that the Commission can and should consider these obligations notwithstanding any other privacy proceedings that may or may not ultimately result in comprehensive reform.

Finally, Commenters reiterate their earlier request that the Commission impose an explicit, opt-in consent requirement for all CPNI data collected by mobile carriers, as well as a requirement that carriers re-disclose their data collection and sharing practices and renew consent from each customer once every six months. Commenters also support the suggestion by other privacy groups that the principles outlined in the White House's recently-released Privacy Report<sup>4</sup> should serve to guide the Commission's development of specific requirements for CPNI.

## **II. EVEN IF NOT ALL INFORMATION STORED ON MOBILE DEVICES IS CPNI, SOME OF IT ALMOST CERTAINLY IS.**

As we have already explained more fully in our initial comments, the fact that information is stored on mobile devices does not prevent that information from falling within the definition of CPNI. Much of the information from mobile devices that is collected by carriers

---

<sup>3</sup> Comments of New America Foundation's Open Technology Institute, Benton Foundation, Center for Media Justice, Chicago Media Action, Free Press, Institute for Local Self-Reliance, Media Alliance, Peoples Production House, Public Knowledge, and The Peoples Channel & Durham Community Media, CC Docket No. 96-115 (July 13, 2012) ("NAF et al Comments") at v.

<sup>4</sup> White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy (2012) *available at* [www.whitehouse.gov/sites/default/files/privacy-final.pdf](http://www.whitehouse.gov/sites/default/files/privacy-final.pdf) ("White House Report")

using applications like Carrier IQ indeed falls clearly within the language of the statute.<sup>5</sup> The language of the statute defines CPNI as “(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.”<sup>6</sup>

Sprint goes to great lengths to point out information it *does collect* that it believes does not fall under the reach of § 222, though its self-assessment hardly serves as representative of all of the information stored on mobile devices that it *can collect* (or, indeed, does actually collect). Moreover, it appears from even the company’s self-assessment that the data they categorize as not CPNI would necessarily include, in addition to the data they list, information that would fall under the definition of CPNI.

For example, it points to “remote diagnostic information” as a category of information that does not fall within CPNI “because it does not relate to the quantity, technical configuration, type, destination, location, or amount of use of a telecommunications service subscribed to by a consumer,” but rather “provides a look at the performance of carrier networks and a consumer’s mobile device during certain events such as dropped calls.”<sup>7</sup> While the company argues otherwise, it seems counterintuitive to the basic understanding of how cellular networks work that such performance assessments would not also necessarily require collection of data such as

---

<sup>5</sup> NAF et al Comments at 2.

<sup>6</sup> 47 U.S.C. § 222(h)(1).

<sup>7</sup> Comments of Sprint Nextel Corporation, CC Docket No. 96-115 (July 13, 2012) (“Sprint Comments”) at 12.

where the consumer was when the dropped call occurred (location), the number to which she was calling (destination), or how long the call lasted (amount of use).<sup>8</sup>

Noting Verizon's expansive collection practices outlined in its privacy policy<sup>9</sup>, EPIC points out that with that information, "mobile carriers are capable of building extensive digital profiles of individual consumers"<sup>10</sup> that "may contain sensitive information about the consumer, including health or financial data and information revealing the individual's exercise of First Amendment rights."<sup>11</sup> This information can be used for a number of reasons besides improving network service or "remote network diagnostics," including behavioral advertising and general marketing purposes.<sup>12</sup>

Moreover, the carriers and their representative organizations argue that information must be "linked to individual users" or contain "personally identifiable call data" to fall within the

---

<sup>8</sup> Sprint also notes later that "[t]he purpose of remote diagnostic data collection is not to analyze individual consumers' usage..." (Sprint Comments at 12-13) Commenters point out that the *purpose* of the collection is irrelevant if the actual data collected falls within the statutory definition of CPNI. *See also* Comments of the Electronic Privacy Information Center and Consumer Watchdog, CC Docket No. 96-115 (July 13, 2012) ("EPIC et al Comments") at 3, noting "[a]lthough mobile carriers claim to collect and store data primarily to improve mobile service to the user, carriers also use and share data for unrelated purposes."

<sup>9</sup> Including "location data, web addresses and search terms, demographic information, amount of usage of the mobile phone, and type of data plan used by the consumer", EPIC Comments at 3, citing *Privacy Policy*, Verizon Wireless, <http://www22.verizon.com/about/privacy/policy/> (last accessed June 21, 2012).

<sup>10</sup> EPIC et al Comments at 3.

<sup>11</sup> *Id.*

<sup>12</sup> *See* Comments of Electronic Frontier Foundation, CC Docket 96-115 (July 13, 2012) ("EFF Comments") at 2, noting that both AT&T and Verizon admittedly use data explicitly for marketing purposes; and EPIC et al comments at 3, where EPIC, citing the White House's Privacy Report, notes that "[m]obile carriers collect, store, and then share data with third parties for use in behavioral advertising, in which information about the consumer's online interests is used to allow companies to target advertisements to the consumer."

definition of CPNI<sup>13</sup>, and that “the data collected from devices is usually device specific, and not consumer specific.”<sup>14</sup> It is impossible to understand how the company that sells the device to the consumer and collects “remote diagnostic data” from it does not, with that device-specific information, thereby know to which consumer that device belongs. Indeed, the carriers would know this information precisely because of the “carrier-customer relationship.”<sup>15</sup>

Perhaps tellingly, neither Verizon nor AT&T make an explicit claim that that the data they collect is not CPNI. Rather, they rely solely on the merits of their own privacy agendas and the existence of concurrent privacy discussions occurring in other venues as reasons that the Commission should not, even if it presumably could, make any new interpretations about the reach of § 222 of the statute. As Commenters explain more fully below, these rationales are no more meritorious than the weak arguments regarding the statute’s applicability in this context.

### **III. ACTIVITY IN OTHER AGENCIES SHOULD NOT PRECLUDE THE COMMISSION FROM EXERCISING ITS OWN STATUTORY AUTHORITY TO REGULATE CPNI.**

Carriers claim because the NTIA is in the initial stages of its multistakeholder process to develop “a code of conduct to provide transparency about how mobile application providers of interactive services handle personal data,” the Commission should not or cannot move forward with its own analysis of its § 222 obligations. Commenters disagree with this claim and instead

---

<sup>13</sup> “Network diagnostic information and other information acquire from wireless devices is not CPNI because it does not contain personally identifiable call data.” Comments of CTIA – The Wireless Association, CC Docket 96-115 (July 13, 2012) (“CTIA Comments”) at 7, citing to Sprint’s 2007 comment in this docket; *see also* Sprint Comments at 12. Note also that this characterization is not even a correct reading of the plain language of the statute – while the statute does include the phrase “individually identifiable customer proprietary network information” in its explanation of the privacy requirements imposed on carriers in § 222 (c)(1) (not, however, in the § 222 (h)(1) definition of CPNI), nowhere does it use either phrase used by Sprint or CTIA.

<sup>14</sup> Sprint Comments at 12.

<sup>15</sup> 47 U.S.C. § 222 (h)(1)(A).

argue that the Commission can and should consider these obligations notwithstanding any other privacy proceedings that may or may not ultimately result in comprehensive reform.

The carrier claim ignores the fact that the Commission, in this limited context, is not only the agency best suited to regulate CPNI, but also the agency given explicit, statutory direction to do so. In other words, the carriers ask the Commission to refrain from fulfilling its statutory directive to protect consumer's privacy with respect to CPNI, based on the possibility that another agency without a specific statutory mandate may develop guidelines to address the issue.

Moreover, the statute recognizes the “many players in the wireless ecosystem,”<sup>16</sup> makes distinctions about the variety of data collected, and specifically holds that CPNI collected by phone service providers deserves a heightened level of protection. Thus the statute correctly recognizes the complexities of the ecosystem and, in accounting for those complexities, imposes obligations on one group of actors and not others.

In addition and importantly, carriers have a unique relationship with consumers and operate in a market that is neither fully competitive nor suited to allow consumers to easily make changes among wireless service providers. Customers who have a problem with the way that their mobile service provider is handling their CPNI (to the extent that they are aware of the ways that their provider is handling their CPNI) have no real market recourse, so it is important to provide consumers with adequate disclosure as to how that data is handled, and to impose any additional necessary requirements to ensure that, at any rate, the data is afforded the highest degree of protection possible, as contemplated by the statute.

---

<sup>16</sup> See Comments of Verizon Wireless, CC Docket No. 96-115 (July 13, 2012) (“Verizon Comments”) at 2.

**IV. RELYING ON VOLUNTARY INDUSTRY COOPERATION IS INADEQUATE, AND THE COMMISSION SHOULD MODIFY ITS EXISTING CONSENT AND DISCLOSURE REQUIREMENTS AND ADOPT AN EXPLICIT, OPT-IN CONSENT REGIME FOR ALL CPNI.**

While carriers and trade associations claim that carriers are taking steps to protect consumer privacy, they are vague with the details of those assertions. For example, TechAmerica states in its initial comments that “certainly over the last five years companies throughout the mobile ecosystem have made a concerted effort to take steps towards identifying, evaluating, and addressing privacy as products and services are being created and deployed,”<sup>17</sup> it provides no details about those “concerted efforts.”

Rather, the very emergence of Carrier IQ and the opaque ways in which it is being used make it clear that those efforts, if they are occurring, are inadequate to give consumers knowledge and control to ensure that their data is being protected. As Electronic Frontier Foundation notes:

Carrier IQ was deployed in such a way that the average user would not know that it existed, and information about the use of Carrier IQ was ultimately revealed through independent security researcher analysis. Even if this type of software is well known in the industry and the research community, the general public knew little about it. It’s not clear that this issue and its bearing on consumer privacy would otherwise come to light...<sup>18</sup>

Thus, it is clear that whatever industry representatives might assert, additional protections are needed to ensure that consumers are “given meaningful notice and choice with respect to service providers’ collection of usage-related information on their devices.”<sup>19</sup> Commenters therefore

---

<sup>17</sup> Comments of TechAmerica, CC Docket No. 96-115 (July 13, 2012) (“TechAmerica Comments”) at 4.

<sup>18</sup> EFF Comments at 5.

<sup>19</sup> *Privacy and Security of Information Stored on Mobile Devices*, Public Notice, CC Docket No. 96-115 (rel. May 25, 2012) (“Public Notice”) at 4, *See also* EPIC et al Comments at 6-7, noting that “[c]onsumers are concerned about the use of their data, but they frequently do not understand the extent to which their data is collected and shared,” and that “even informed users

reiterate our request that the Commission require carriers to disclose collection and sharing practices of CPNI to consumers and to obtain explicit, opt-in consent prior to that collection and sharing. Additionally, Commenters further ask the Commission to require carriers to renew that disclosure and consent once every six months.<sup>20</sup>

Commenters note, however, that this opt-in consent requirement and the requirement for subsequent renewals are not *sufficient* to protect the privacy of consumers' CPNI data. Rather, we see this requirement as merely the first step. EFF, quoting a UC-Berkeley study of the use of mobile phones and privacy notes that “transparency about how mobile data is collected and used, along with robust user controls and procedural and technical privacy safeguards, may be necessary to avoid backlash against programs that rely on mobile data.”<sup>21</sup> EFF, along with EPIC, further calls on the Commission to consider the following consumer rights as they evaluate the carriers' obligations: individual control; focused data collection; transparency; respect for context; security; and accountability.<sup>22</sup> Commenters strongly support these principles and urge the Commission to consider them while developing the specifics of its requirements for carriers – in the context of a consent and disclosure regime, as well as any other additional requirements, such as the imposition of limits to the length of time a carrier can store certain types of data.

For example, an opt-in consent regime in the context of these principles should require carriers to disclose their collection practices in a transparent, detailed way that acknowledges

---

are deprived by carriers of meaningful choice in regard to the collection, storage, and use of their data.”

<sup>20</sup> NAF et al Comments at 9-10; *see also* EPIC et al Comments at 10, asking the Commission to “require carriers to obtain, at the time of collection, consent to share a consumer’s data with third parties.” Commenters clarify, however, that we would extend this requirement to *all* CPNI collected by carriers, and not limit it merely to the sharing of that data with third parties.

<sup>21</sup> EFF Comments at 6, quoting Berkeley Report at 3.

<sup>22</sup> *Id.* at 3.

“mobile phone characteristics, including small screens and privacy risks, when providing notice to consumers.”<sup>23</sup> That regime should also limit the amount of time a carrier can retain consumer information, even after it has received consent. This practice would improve privacy vulnerabilities and guard against potential security breaches,<sup>24</sup> and would discourage carriers themselves from misusing large logs of sensitive consumer data.

## V. CONCLUSION

For the reasons outlined above, Commenters urge the Commission to recognize that data stored on mobile devices falls within the purview of § 222 and that it has the authority to regulate collection and distribution collection practices that implicate that data. Commenters also disagree with the submissions from the carriers and other industry representatives that the NTIA multistakeholder process should preclude the Commission from acting on its statutory mandate. Further, Commenters reaffirm our request that the Commission impose an explicit, opt-in consent requirement that is developed with consideration of the principles outlined in the White House’s Privacy Report to ensure that consumers are given adequate information about carrier data collection and sharing practices and that they are able to give meaningful consent to those practices. Finally, Commenters ask the Commission to require that mobile carriers re-disclose and renew customer consent once every six months to ensure that those practices continue to conform to customer values.

---

<sup>23</sup> *Id.* at 13.

<sup>24</sup> *See* EPIC et al Comments at 17. “Reduction and regulation of the amount of data collected and the period that data is retained will greatly reduce the amount of data vulnerable to those who would misuse it, both within and without the carrier. Such reductions are necessary because of the almost-daily occurrence of security breaches.”