

DEC 11 2013

FCC Office of the Secretary

Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, DC 20554

In the Matter of the Petition of )  
Public Knowledge et al. )  
for Declaratory Ruling Stating that the Sale )  
of Non-Aggregate Call Records by )  
Telecommunications Providers without )  
Customers' Consent Violates Section 222 of )  
the Communications Act )

RM-\_\_\_\_\_

PETITION FOR DECLARATORY RULING  
OF  
PUBLIC KNOWLEDGE  
BENTON FOUNDATION  
CENTER FOR DIGITAL DEMOCRACY  
CENTER FOR MEDIA JUSTICE  
CHRIS JAY HOOFNAGLE  
COMMON CAUSE  
CONSUMER ACTION  
ELECTRONIC FRONTIER FOUNDATION  
ELECTRONIC PRIVACY INFORMATION CENTER  
FREE PRESS  
NEW AMERICA FOUNDATION'S OPEN TECHNOLOGY INSTITUTE  
U.S. PIRG

Laura M. Moy  
Public Knowledge  
1818 N St, NW  
Suite 410  
Washington, DC 20036  
(202) 861-0020 ext. 106

Filed December 11, 2013

For Petitioners

## Table of Contents

Summary and Background.....	1
I. Non-Aggregate Call Records that Have Been Purged of Personal Identifiers Are Individually Identifiable CPNI Under Section 222 of the Communications Act.....	2
A. In the Context of Section 222 "Individually Identifiable" Means "Not Aggregate" .....	3
B. Information that Has Been "Anonymized" May in Many Cases Be Used to Re-Identify Specific Individuals.....	6
II. AT&T Is in Violation of Section 222 Because It Sells Individually Identifiable Call Records to the C.I.A., Companies, and Other Entities Without Customers' Consent.....	8
III. AT&T, Verizon, Sprint, and T-Mobile Reserve the Right to Unlawfully Sell Pseudonymous Call Records to Third Parties Without Customers' Consent ...	9
A. AT&T Reserves the Right to Share Individually Identifiable CPNI with Companies and Other Entities Without Customers' Consent.....	9
B. Verizon Reserves the Right to Share Individually Identifiable CPNI with Third Parties Without Customers' Consent .....	9
C. Sprint Reserves the Right to Share Individually Identifiable CPNI with Third Parties Without Customers' Consent .....	10
D. T-Mobile Reserves the Right to Share Individually Identifiable CPNI with Third Parties Without Customers' Consent.....	10
IV. Conclusion .....	11

Public Knowledge, Benton Foundation,<sup>1</sup> Center for Digital Democracy, Center for Media Justice, Chris Jay Hoofnagle,<sup>2</sup> Common Cause, Consumer Action, Electronic Frontier Foundation, Electronic Privacy Information Center,<sup>3</sup> Free Press, New America Foundation's Open Technology Institute, and U.S. PIRG (collectively "Public Knowledge, et al.") petition the Commission to clarify that under Section 222 of the Communications Act, "anonymized" or "de-identified" but non-aggregate call records constitute individually identifiable customer proprietary network information ("CPNI"), and must not be sold to or otherwise shared with third parties without customers' consent.

### Summary and Background

Section 222, "Privacy of customer information," was passed as part of the Telecommunications Act of 1996.<sup>4</sup> According to Senator Burns, one of the authors of the 1996 Act, "Section 222 . . . was written to protect consumers' privacy."<sup>5</sup>

---

<sup>1</sup> The Benton Foundation is a nonprofit organization dedicated to promoting communication in the public interest. This Petition reflects the institutional view of the Foundation and, unless obvious from the text, is not intended to reflect the views of individual Foundation officers, directors, or advisors.

<sup>2</sup> Lecturer in Residence, UC Berkeley Law. Hoofnagle petitioned the FCC in 2005 to increase security standards for CPNI, in light of widespread evidence that "private investigators" were accessing CPNI of subscribers on behalf of stalkers and other unauthorized individuals. *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary network Information and other Customer Information; Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information*, Notice of Proposed Rulemaking, 21 FCC Rec 1782 (2006).

<sup>3</sup> The Electronic Privacy Information Center has previously written to the Commission on two separate occasions urging it to investigate Verizon and AT&T, respectively, for violating Section 222 by sharing CPNI with the United States Government. Letter from Electronic Privacy Information Center to Acting Chairwoman Mignon Clyburn (June 11, 2013), *available at* <http://epic.org/privacy/terrorism/fisa/EPIC-FCC-re-Verizon.pdf>; Letter from Electronic Privacy Information Center to Chairman Wheeler (Nov. 15, 2013), *available at* <http://epic.org/privacy/terrorism/fisa/EPIC-FCC-Wheeler-Ltr.pdf>.

<sup>4</sup> Pub. L. No. 104-104, 110 Stat. 56, 148 (1996), *available at* <http://www.gpo.gov/fdsys/pkg/PLAW-104publ104/pdf/PLAW-104publ104.pdf>.

The primary effect of Section 222 is to severely restrict what phone carriers can do with their customers' private information. Under Section 222, a carrier may not use, disclose, or permit access to a customer's individually identifiable CPNI without that customer's consent except to provide service or comply with the law.<sup>6</sup>

Despite these restrictions, phone carriers regularly share—or reserve the right to share—customers' records in an “anonymized” form with third parties. For example, the privacy policies of all four major mobile carriers (AT&T, Verizon, Sprint, and T-Mobile) state that they may share supposedly “anonymized” or “de-identified” customer information with third parties.<sup>7</sup> In addition, the *New York Times* recently reported that AT&T has been selling call records to the C.I.A.<sup>8</sup> AT&T reportedly attempts to anonymize call records before sharing them with the C.I.A. by “masking” several digits of Americans' phone numbers.

But as this Petition argues, “anonymized” or “de-identified” call records still constitute individually identifiable CPNI under Section 222. Therefore, phone carriers violate Section 222 when they disclose or even use those records internally for any reason other than those narrowly set forth under Section 222.

**I. Non-Aggregate Call Records that Have Been Purged of Personal Identifiers Are Individually Identifiable CPNI Under Section 222 of the Communications Act**

Phone carriers' records of their customers' phone calls constitute CPNI under Section 222 of the Communications Act. The definition of CPNI includes “information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any

---

(footnote continued)

<sup>5</sup> *Protecting Consumers' Phone Records: Hearing Before the Subcomm. on Consumer Affairs, Prod. Safety, and Ins. of the S. Comm. on Commerce, Sci., and Transp.*, 109th Cong. 6 (2006) (statement of Sen. Conrad Burns, Member, S. Comm. on Commerce, Sci., and Transp.).

<sup>6</sup> 47 U.S.C. § 222.

<sup>7</sup> See *infra* at Section III.

<sup>8</sup> Charlie Savage, *C.I.A. Is Said to Pay AT&T for Call Data*, *N.Y. Times*, Nov. 7, 2013, available at <http://www.nytimes.com/2013/11/07/us/cia-is-said-to-pay-att-for-call-data.html>.

customer of a telecommunications carrier.”<sup>9</sup> And as the D.C. Circuit acknowledged in *National Cable & Telecommunications Association v. F.C.C.*, this “encompasses customers’ particular calling plans and special features, the pricing and terms of their contracts for those services, and details about who they call and when.”<sup>10</sup>

Even when carriers have “anonymized” or “de-identified” call records by removing personal identifiers from them they still constitute individually identifiable CPNI for at least two reasons. First, under Section 222, all CPNI that is not aggregate is individually identifiable, as such records can be linked to a single person. Second, what carriers refer to as “anonymized” records may not be anonymous at all. “Anonymization” is a complex procedure that has become the focus of top computer scientists.<sup>11</sup> The carriers’ methods of “anonymization,” as reported in the media may be vulnerable to “re-identification,” that is, a process that reveals the true identities of individuals in an allegedly “anonymous” dataset. Re-identification is now well understood in both the legal<sup>12</sup> and computer science literature,<sup>13</sup> and can be executed by non-technically trained people.

**A. In the Context of Section 222 “Individually Identifiable” Means “Not Aggregate”**

Both the structure of Section 222 and the definition of “aggregate customer information” indicate that under this Section, “individually identifiable” means “not aggregate.”<sup>14</sup> Thus CPNI is individually identifiable under Section 222 if it is granular enough to retain the characteristics of individual customers.

---

<sup>9</sup> 47 U.S.C. § 222(h)(1)(A).

<sup>10</sup> 555 F.3d 996, 997 (D.C. Cir. 2009).

<sup>11</sup> See, e.g., Latanya Sweeney, *k-anonymity: a model for protecting privacy*, 10 Int’l J. on Uncertainty, Fuzziness and Knowledge-based Sys. 557 (2002); Arvind Narayanan, *Posts on Reidentification*, 33 Bits of Entropy, <http://33bits.org/tag/re-identification/> (last visited Dec. 10, 2013).

<sup>12</sup> Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2010).

<sup>13</sup> See articles cited *supra* note 11.

<sup>14</sup> According to the *Oxford English Dictionary*, “aggregate” is defined as “Constituted by the collection of many particles or units into one body, mass, or amount; collective, whole, total.” In the legal context, aggregate is defined as,

(continued on next page)

The structure of Section 222 sets forth individually identifiable and aggregate as the only two categories of CPNI, indicating that these terms are dichotomous; all CPNI is either aggregate or individually identifiable (not aggregate). Section 222 subsection (c) reads as follows:

(c) Confidentiality of customer proprietary network information

(1) Privacy requirements for telecommunications carriers

Except as required by law or with the approval of the customer, a telecommunications carrier . . . shall only use, disclose, or permit access to *individually identifiable customer proprietary network information* in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.

....

(3) Aggregate customer information

A telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service *may use, disclose, or permit access to aggregate customer information other than for the purposes described in paragraph (1)*. A local exchange carrier may use, disclose, or permit access to aggregate customer information other than for purposes described in paragraph (1) only if it

---

(footnote continued)

“Composed of many individuals united into one association.” *aggregate*, adj. and n., Oxford English Dictionary (3d ed. 2012), available at <http://www.oed.com/view/Entry/3932>.

provides such aggregate information to other carriers or persons on reasonable and nondiscriminatory terms and conditions upon reasonable request therefor.<sup>15</sup>

The presentation of aggregate customer information in paragraph (3) as contrasting with individually identifiable CPNI in paragraph (1) indicates that all CPNI is either individually identifiable (and subject to the restrictions on use and sharing) or aggregate (and not subject to the restrictions). Thus CPNI will be considered individually identifiable unless it is aggregate.<sup>16</sup>

The definition of "aggregate customer information" also indicates that CPNI that is not aggregate is individually identifiable. First, aggregate information is defined in the statute, whereas individually identifiable is not. This suggests that aggregate information is a narrow carve-out category of CPNI, whereas individually identifiable information is broader. Second, the text of the definition is telling:

The term "aggregate customer information" means collective data that relates to a group or category of services or customers, from which individual customer identities *and characteristics have been removed*.<sup>17</sup>

For information to be considered aggregate, both individual customer identities *and characteristics* must have been removed. The definition refers to both, indicating that both are sensitive. Thus a dataset from which customers' names and phone numbers have been removed but in which individual characteristics have been left

---

<sup>15</sup> 47 U.S.C. § 222(c) (emphasis added).

<sup>16</sup> Importantly, "individually identifiable" is distinguishable from "personally identifiable." Individually identifiable records need only pertain to a single person, and that person's identity need not be actually known. For instance, some would argue that a telephone number itself does not identify a person, but rather a household. The careful choice of the phrase "individually identifiable" instead of "personally identifiable" is a signal from Congress that records that reference a single account are protected, even if the owner or user of the account is not personally identified.

<sup>17</sup> 47 U.S.C. § 222(h)(2) (emphasis added).

intact does not meet the definition of aggregate customer information and is individually identifiable.

Non-aggregate call records that contain individual characteristics—such as the call detail record of an individual customer—are individually identifiable CPNI. This remains the case even after a carrier has “anonymized” or “de-identified” the records by removing some personally identifying details. As long as individual customer characteristics remain intact in call records, they are not “aggregate” under Section 222 and are therefore individually identifiable CPNI.

**B. Information that Has Been “Anonymized” May in Many Cases Be Used to Re-Identify Specific Individuals**

Even if “individually identifiable” were interpreted to mean personally identifiable, “anonymized” call records must still fall into this category because in many cases sufficient information remains in anonymized records to link them back to individual people.<sup>18</sup>

When a carrier purges individual identities from a set of call records but leaves individual characteristics (such as incoming and outgoing calls, call times, and call durations) intact, the records are not anonymous at all; they are pseudonymous. Someone looking at the call records of John Doe can still see all the calls that Doe made; they simply do not know Doe’s real name. Unlike truly anonymous aggregate records from which all individual characteristics have been removed, pseudonymous records can be connected to a specific individual at any point in time. If someone discovers Doe’s true identity in the future, it will retroactively affect records about Doe that have already been collected.<sup>19</sup>

---

<sup>18</sup> Similarly, under the Health Insurance Portability and Accountability Act, “individually identifiable health information” includes not only information “that identifies the individual,” but also information “with respect to which there is a reasonable basis to believe the information can be used to identify the individual.” 45 C.F.R. § 160.103.

<sup>19</sup> See Arvind Narayanan, *There is No Such Thing as Anonymous Online Tracking*, The Center for Internet and Society, (July 28, 2011, 12:38 PM), <https://cyberlaw.stanford.edu/node/6701>.

Not only are pseudonymous records at risk of being linked back to a specific individual, pseudonymous records often contain sufficient information to discover the true identity of the person whose records they are. For example, even if several digits of Doe's phone number and the phone numbers of all other domestic customers are masked in a call log for Doe's cell phone but international phone numbers are not,<sup>20</sup> and Doe's mother lives overseas, one can easily figure out who Doe is by spotting the frequent calls to his mother.

Much has been written about the ease with which records claimed to be "anonymous" can be reconnected to specific people using widely available tools and information.<sup>21</sup> In 2000, Latanya Sweeney—who was recently appointed Chief Technologist of the Federal Trade Commission—demonstrated that individuals can easily be identified even without any of the pieces of information traditionally thought of as personal. She found that "87% of the US population can be uniquely specified by knowledge of his or her 5-digit ZIP code of residence, gender, and date of birth."<sup>22</sup> More recently, researchers at the University of Texas at Austin succeeded in using publicly available information to identify Netflix subscribers in a dataset of movie ratings from which personal identifiers had been removed. "Removing identifying information is not sufficient for anonymity," the researchers explained.<sup>23</sup> And earlier this year, researchers used a dataset of "anonymized" location data from an unidentified mobile phone carrier to demonstrate that 95 percent of individual users could be uniquely identified using just four location data

---

<sup>20</sup> Based on the report in the *New York Times*, this is likely how AT&T anonymizes the records it sells to the C.I.A. Savage, *supra* note 8.

<sup>21</sup> See Daniel J. Solove, *Understanding Privacy*, 117-128 (2008); Ohm, *supra* note 12.

<sup>22</sup> Latanya Sweeney, Abstract, *Uniqueness of Simple Demographics in the U.S. Population* (Carnegie Mellon Univ., Lab. for Int'l Data Privacy 2000), available at <http://www.citeulike.org/user/burd/article/5822736>.

<sup>23</sup> Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, in *Proceedings of the 2008 IEEE Symposium on Security and Privacy* 111, 118 (2008). Professor Narayanan is now at Princeton.

points.<sup>24</sup> Indeed, reidentification is now a widely-known risk in all data intensive industries, as demonstrated by AOL's release of supposedly anonymous search records in 2006 that resulted in identification of specific individuals and the things for which they searched.<sup>25</sup>

Given the increasing ease with which datasets purged of personally identifying information can be re-identified, pseudonymous non-aggregate call records must be considered individually identifiable CPNI even if "individually identifiable" is interpreted to mean personally identifiable. This is especially so if identifying details pertaining to international calls are not removed from the records.

## II. AT&T Is in Violation of Section 222 Because It Sells Individually Identifiable Call Records to the C.I.A., Companies, and Other Entities Without Customers' Consent

On November 7, the *New York Times* reported that AT&T sells "a huge archive of data on phone calls" to the C.I.A. for more than \$10 million a year.<sup>26</sup> According to the article, the call logs that AT&T provides to the C.I.A. include records of international calls with one end in the United States. In these cases AT&T "masks" several digits of the American phone number. Again, however, merely obscuring personal identifiers is not sufficient to turn individually identifiable CPNI protected under Section 222 into unprotected aggregate information. The records AT&T sells to the C.I.A. are pseudonymous records that leave individual characteristics intact and may contain information that can be used to re-identify individual people. AT&T is therefore in violation of Section 222 of the Communications Act for the sale of individually identifiable CPNI to the C.I.A. without customers' consent.

---

<sup>24</sup> Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen, & Vincent D. Blondel, *Unique in the Crowd: The Privacy Bounds of Human Mobility*, 3 *Sci. Rep. (Article 1376)* 1 (2013), available at <http://dx.doi.org/10.1038/srep01376>.

<sup>25</sup> Michael Barbaro & Tom Zeller Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, *N.Y. Times*, Aug. 9, 2006, available at <http://www.nytimes.com/2006/08/09/technology/09aol.html>.

<sup>26</sup> Savage, *supra* note 8.

### **III. AT&T, Verizon, Sprint, and T-Mobile Reserve the Right to Unlawfully Sell Pseudonymous Call Records to Third Parties Without Customers' Consent**

Because, as explained above, call records that have been purged of personal identifiers but that leave individual customers' characteristics intact are individually identifiable CPNI under Section 222, they are protected under that section. While Public Knowledge, et al are unable to determine whether or not carriers currently sell information in this form to third parties without customers' consent, several major carriers reserve the right to do so. Doing so would violate Section 222.

#### **A. AT&T Reserves the Right to Share Individually Identifiable CPNI with Companies and Other Entities Without Customers' Consent**

According to AT&T's own privacy policy, AT&T "may share" both "anonymous" and aggregate data "with other companies and entities." To render data "anonymous," AT&T "remove[s] data fields . . . that can reasonably be used to identify you" and also "use[s] statistical techniques and operational controls to anonymize data."<sup>27</sup> Under Section 222, AT&T can share aggregate data with other companies and entities without customers' consent, but the non-aggregate data it refers to as "anonymous" is still protected as individually identifiable CPNI. AT&T thus reserves the right to share this information to companies and other entities without customers' consent, in violation of Section 222.

#### **B. Verizon Reserves the Right to Share Individually Identifiable CPNI with Third Parties Without Customers' Consent**

Like AT&T, Verizon's own privacy policy states that Verizon may share both "anonymous" and aggregate data with third parties.<sup>28</sup> Under Section 222, any non-

---

<sup>27</sup> *AT&T Privacy Policy FAQ*, AT&T, <http://www.att.com/gen/privacy-policy?pid=13692> (last visited Dec. 10, 2013).

<sup>28</sup> *Privacy Policy: Full Privacy Policy*, Verizon, <http://www.verizon.com/about/privacy/policy/> (last visited Dec. 10, 2013).

aggregate data that Verizon refers to as “anonymous” is still protected as individually identifiable CPNI. Verizon thus reserves the right to share this information with third parties without customers’ consent, in violation of Section 222.

**C. Sprint Reserves the Right to Share Individually Identifiable CPNI with Third Parties Without Customers’ Consent**

Sprint’s privacy policy also says that it “may share information that is de-identified or in an aggregated form that does not directly identify you” to third parties.<sup>29</sup> Under Section 222, any non-aggregate data that Sprint refers to as “de-identified” is still protected as individually identifiable CPNI. Sprint thus reserves the right to share this information with third parties without customers’ consent, in violation of Section 222.

**D. T-Mobile Reserves the Right to Share Individually Identifiable CPNI with Third Parties Without Customers’ Consent**

T-Mobile’s privacy policy states, incorrectly, that CPNI “is a subset of Personal Information” which “does not include ‘de-identified,’ ‘anonymous,’ or ‘aggregate information.’”<sup>30</sup> T-Mobile’s policy also says that it “may provide third-party advertisers with aggregated or anonymous, de-identified, demographic or similar data.”<sup>31</sup> Under Section 222, any non-aggregate data that T-Mobile refers to as “anonymous” is still protected as individually identifiable CPNI. T-Mobile thus reserves the right to share this information with third parties without customers’ consent, in violation of Section 222.

---

<sup>29</sup> *Sprint Corporation Privacy Policy*, Sprint, <http://www.sprint.com/legal/privacy.html> (last visited Dec. 10, 2013).

<sup>30</sup> *T-Mobile Privacy Policy*, T-Mobile, <http://www.t-mobile.com/company/website/privacypolicy.aspx#fullpolicy> (last visited Dec. 10, 2013).

<sup>31</sup> *Id.*

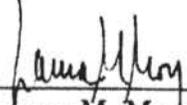
#### IV. Conclusion

For the foregoing reasons, Public Knowledge et al. ask the Commission to issue a declaratory ruling that 1) under Section 222 of the Communications Act, non-aggregate call records that have been purged of personal identifiers but that leave customers' individual characteristics intact are protected as individually identifiable CPNI, and 2) phone carriers including AT&T, Verizon, Sprint, and T-Mobile must not sell such records without customers' consent.

Respectfully submitted,

Public Knowledge  
Benton Foundation  
Center for Digital Democracy  
Center for Media Justice  
Chris Jay Hoofnagle  
Common Cause  
Consumer Action  
Electronic Frontier Foundation  
Electronic Privacy Information Center  
Free Press  
New America Foundation's Open  
Technology Institute  
U.S. PIRG

By:

  
\_\_\_\_\_  
Laura M. Moy  
Public Knowledge  
1818 N St, NW  
Suite 410  
Washington, DC 20036  
(202) 861-0020 ext. 106

For Petitioners  
Filed: December 11, 2013