Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of the Petition of	)	
	)	
Public Knowledge et al.	)	WC Docket No. 13-306
	)	
for Declaratory Ruling that Section 222 of the Communications Act Prohibits Telecommunications Providers from Selling Non-Aggregate Call Records Without Customers' Consent	)	

REPLY COMMENTS
OF
PUBLIC KNOWLEDGE
BENTON FOUNDATION
CENTER FOR DIGITAL DEMOCRACY
CENTER FOR MEDIA JUSTICE
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
For Petitioners

March 4, 2014

Table of Contents

Introduction and Summary

Public Knowledge, Benton Foundation,[1] Center for Digital Democracy, Center for Media Justice, Common Cause, Consumer Action, Electronic Frontier Foundation, Electronic Privacy Information Center, Free Press, New America Foundation's Open Technology Institute, and U.S. PIRG ("Public Knowledge et al.") respectfully submit this reply to comments filed on the Petition for Declaratory Ruling that Section 222 of the Communications Act prohibits carriers from selling non-aggregate call records without customers' consent.[2]

Some commenters in this proceeding would like the FCC to leave it up to the carriers to decide when the law applies to them and when it does not. They argue that Public Knowledge et al. have misread the Communications Act, and that customer information that has been de-identified but that leaves individual characteristics intact is not individually identifiable. In the alternative, they argue that just because no one has come forward to proclaim success at re-identifying the records they share, no one has done so. They also argue that getting third parties to agree not to re-identify records satisfies Section 222.

These arguments are without merit. Congress has legislated on this subject and charged the FCC, not carriers, with determining when and how the law protects telecom customers' private information. Where de-identified customer information is concerned, there is only one reasonable reading of Section 222: de-identified records that leave individual characteristics intact are individually identifiable CPNI. Moreover, it is clear that the de-identified information that carriers share can be re-identified, even though no one has come forward saying that they have succeeded at doing so. Finally, establishing contractual protections

---

[1] 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.

[2] Petition of Public Knowledge et al. for Declaratory Ruling Stating that the Sale of Non-Aggregate Call Records by Telecommunications Providers without Consumers' Consent Violates Section 222 of the Communications Act, WC Dkt 13-306 (Dec. 11, 2013).

for shared private information is not the same as getting customers' consent to share the information in the first place.

Public Knowledge et al. recognize that de-identified call records have value in research applications. Thus, Public Knowledge et al. do not suggest that carriers should be prohibited from using or sharing that information, only that carriers obtain consent as necessary before doing so.

I. The Federal Communications Commission Is Responsible for Implementation of Section 222 of the Communications Act

The Federal Communications Commission has been charged with protecting telecom customers' privacy. Industry commenters would like the Commission to leave it up to carriers to interpret and implement Section 222, and to rely on other government entities to ensure that privacy self-regulation keeps pace with developing technology. But the Commission cannot do this, because it and it alone was charged with implementing Section 222.

A. Carriers Must Not Be Allowed to Determine for Themselves When the Law Applies and When It Does Not

Carriers who filed comments in this proceeding seem to believe that they are are responsible for determining when the law applies to themselves. They suggest that the Commission and public simply trust them, based on avowed commitments to privacy and descriptions of de-identification methods that are vague at best. AT&T calls privacy a "business imperative,"[3] says it "goes to great lengths" to protect customers' privacy,[4] and lists several de-identification methods of which it cryptically "may use one or more" before sharing private information with third parties.[5] Similarly, Verizon refers to "carriers' adoption of a variety of security

[3] Comments of AT&T at 1–2, Petition of Public Knowledge et al. for Declaratory Ruling that Section 222 of the Communications Act Prohibits Telecommunications Providers from Selling Non-Aggregate Call Records Without Customers' Consent, WC Docket No. 13-306 (Jan. 17, 2014).

[4] *Id.* at 2.

[5] *Id.* at 19.

controls designed to protect the [de-identified] data," but does not describe those controls concretely.[6] And CTIA endorses a "voluntary" approach to consumer privacy.[7]

But Congress has considered whether or not privacy protections for telecom customers should be left up to self-regulation and decided, indisputably, that they should not. Thus Congress very explicitly delegated the task of protecting CPNI to the FCC. "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."[8]

Additionally, carriers cannot be trusted to maximize customers' privacy when they share records with third parties because they have an incentive not to. Because they benefit from the sale of de-identified records, it is in carriers' best financial interest to make those records attractive and useful to third parties. But as Paul Ohm, former Senior Policy Advisor for the Federal Trade Commission, has observed, "as the utility of data increases, the privacy decreases."[9] Thus, because carriers have a financial incentive to preserve as much utility as possible in the data they share with third parties, they correspondingly have an incentive to apply the least rigorous de-identification methods they believe will enable them to escape liability under Section 222.

If carriers are not motivated to maximize customers' privacy, they will surely fail to irreversibly de-identify private records before sharing them with third parties. Indeed, even when those releasing private data have had all the right incentives to correctly anonymize it, they have often failed to protect against re-identification. For example, in the 1990s a Massachusetts state government agency

---

[6] Comments of Verizon and Verizon Wireless at 7, Petition of Public Knowledge, WC Docket No. 13-306 (Jan. 17, 2014).

[7] Comments of CTIA—The Wireless Association at 15, Petition of Public Knowledge, WC Docket No. 13-306 (Jan. 17, 2014).

[8] Declaratory Ruling, 28 FCC Rcd. 9609, 6, CC Docket No. 96-115 (June 27, 2013).

[9] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701, 1706 (2010), *available at* http://www.uclalawreview.org/pdf/57-6-3.pdf.

released de-identified state employees' hospital records for research. The state government had every motivation to protect the privacy of state employees. Nevertheless, then-graduate student Latanya Sweeney was able to re-identify the records of William Weld, then the governor of the state, with ease.[10] Similarly, when, in 2006, Netflix released a large number of de-identified subscribers' movie ratings as part of a contest, it had every motivation in that context to prevent re-identification (and public outrage). However, researchers quickly demonstrated that individual subscribers could be re-identified within the supposedly anonymized dataset.[11]

Unlike the Massachusetts state government and Netflix in this instance, carriers do not have the right incentives to maximize individuals' privacy when sharing de-identified CPNI with third parties. Congress does not trust the carriers to self-regulate in this area, and has therefore charged the Commission with ensuring that consumer privacy is protected. The Commission must not allow carriers to self-regulate when Congress has decided they should not be allowed to do so.

B. Implementation and Enforcement of the Privacy-Protective Aspects of the Communications Act Are the Sole Domain of the Federal Communications Commission

Several commenters note that other government entities have examined related privacy issues, implying that the Commission should just surrender its privacy jurisdiction and leave all privacy-related policymaking up to the Federal Trade Commission ("FTC") and White House. Verizon asserts that the Petition does not "acknowledge that the FTC has recommended specific reasonable measures to minimize privacy risks with de-identified data."[12] AT&T references the "best

---

[10] *See id.* at 1719–20.

[11] Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, Proc. 2008 IEEE Symp. on Security & Privacy 111 (2008).

[12] Comments of Verizon, *supra* note 6, at 7.

practices" set forth by the FTC.[13] The Future of Privacy Forum explains that "the FTC's proposed privacy framework does not apply to data that has been reasonably anonymized."[14] And CTIA warns the Commission that if it "attempts to paint with too broad a CPNI brush, it risks interfering with a process the White House has said is flexible, efficient, and beneficial to consumers."[15]

The FTC and the White House have indeed both conducted their own privacy proceedings, but neither has endorsed self-regulation to the exclusion of the enactment and enforcement of privacy legislation. On the contrary, both have advocated for new and stronger privacy legislation, which would replace self-regulation in many instances.[16]

Moreover, it would not make sense to apply the FTC's best practices for anonymous data in this context. The FTC's best practices were designed to apply to many different types of data, collected in many different contexts, by many different actors, across many different fields, used and shared for many different reasons. As such, the FTC's best practices were designed to be relevant to companies whose primary business is collecting, using, and/or sharing customer information, and whose customers share personal information voluntarily. In contrast, Section 222

---

[13] Comments of AT&T, *supra* note 3, at 16–17.

[14] Comments of The Future of Privacy Forum at 7, Petition of Public Knowledge, WC Docket No. 13-306 (Jan. 17, 2014).

[15] Comments of CTIA, *supra* note 7, at 15.

[16] *See* White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* 35 (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf ("The Administration urges Congress to pass legislation adopting the Consumer Privacy Bill of Rights."); *Id.* at 36 ("The Administration encourages Congress to follow a similar path with baseline consumer data privacy legislation."); Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* i(2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf ("The Administration and certain Members of Congress have called for enactment of baseline privacy legislation. The Commission now also calls on Congress to consider enacting baseline privacy legislation and reiterates its call for data security legislation.").

was designed only for and applies only to telecom carriers, whose primary business is providing telecom service, not using or sharing customer information, and whose customers have no choice but to share personal information.

Vigorous protection of CPNI does not conflict with other government entities' privacy initiatives. But even if it did, Congress selected the FCC to protect CPNI. The FCC should rely on its unique expert knowledge of carriers, this industry, and the relationship between carriers and customers in applying Section 222.

II. There Is Only One Reasonable Reading of 47 U.S.C. § 222(c)

Several commenters argue that "individually identifiable customer proprietary network information" in the context of Section 222(c) does not include de-identified records.[17] These commenters are incorrect for at least two reasons. First, Congress knows how to create exceptions, and did in fact insert several in Section 222(d), but chose not to except anonymous or de-identified information. Second, under industry commenters' formulation of Section 222, carriers would face more restrictions with respect to aggregate de-identified information than information that is de-identified but not aggregate—an absurd result.

If Congress had wanted to create an exception to Section 222 for de-identified information it would have done so, just as it created other exceptions. Section 222 subsection (d) lists a number of situations in which CPNI is not subject to the restrictions set forth in the rest of the section. But de-identification is not included as an exception.

If de-identified customer records were neither individually identifiable CPNI under 222(c)(1) nor aggregate customer information under 222(c)(3), carriers' use of those records would be even less regulated than their use of aggregate customer information, even though aggregate records are more privacy protective than non-aggregate de-identified records. Section 222(c)(3) requires carriers that use, disclose, or permit access to aggregate customer information other than for purposes described in 222(c)(1) to "provide[] such aggregate information to other carriers or

[17] *See, e.g.*, Comments of AT&T at 8 (arguing that individually identifiable CPNI "does not include CPNI that has been *de*-identified").

persons on reasonable and nondiscriminatory terms and conditions upon reasonable request therefor."[18] Aggregate customer information is "collective data that relates to a group or category of services or customers, from which individual customer identities *and characteristics* have been removed."[19] Because records de-identified in the way described *infra* in Section VI leave intact individual characteristics such as ZIP code, call times and durations, and locations, they are not aggregate. Therefore if carriers were correct that de-identified customer information is not individually identifiable CPNI, they could share such records while escaping Section 222(c)(3). In other words, records from which individual identities had been removed could be shared with third parties with impunity. In contrast, records from which individual identities *and characteristics* had been removed could be shared with third parties only if it were also made available on a nondiscriminatory basis to other carriers and persons. This would truly be an absurd result, and as Sprint points out, interpretations of a statute that would produce absurd results are to be avoided.[20]

There is only one reasonable reading of Section 222. Individually identifiable CPNI and aggregate customer information constitute a dichotomy, and de-identified non-aggregate records fall in the category of individually identifiable CPNI.

III. Carriers Are Sharing De-Identified CPNI that Is Re-Identifiable

Despite what industry commenters claim, there is clear evidence that call detail records de-identified in the way at least one carrier de-identifies them can be re-identified. That there are no publicly available examples of an attacker doing this to ill effect does not mean it has not happened or will not happen. And contractual assurances from recipients of de-identified records not to re-identify them does not change the fact that they can be re-identified.

---

[18] 47 U.S.C. § 222(c)(3) (2012).

[19] 47 U.S.C. § 222(h)(2) (2012) (emphasis added).

[20] Comments of Sprint Corp. at 3, Petition of Public Knowledge, WC Docket No. 13-306 (Jan. 17, 2014) (citing Report and Order, 20 FCC Rcd. 14242, n.43 (Aug. 23, 2005)).

A. Call Detail Records De-Identified in the Way at Least One Carrier De-Identifies Them Can Be Re-Identified

Although the carriers have not disclosed their de-identification techniques, at least one carrier shares records that have been de-identified in a way that leaves them vulnerable to re-identification. A research paper co-written by researchers at AT&T Research describes the contents of de-identified call detail records ("CDRs") used for the research, presumably obtained from a carrier that is most likely AT&T:

> **Anonymized CDR Contents**: . . . The CDRs contain information about two types of events involving these phones: voice calls and text messages. In place of the phone number, each CDR contains an anonymous identifier consisting of the 5-digit billing ZIP code and a unique integer. Each CDR also contains the starting time of the voice or text event, the duration of the event, the locations of the starting and ending cell towers associated with the event, and an indicator of whether the phone was registered to an individual or a business. It is important to note that we collect CDRs for these phones wherever in the US they travel, not only when they contact cell towers within their billing ZIP codes.[21]

Although these CDRs are referred to as "anonymous," they plainly retain enough individual characteristics to re-identify specific customers. It is easiest to see how location information in the form of cell tower coordinates could inform a re-identification attack. Indeed, researchers have demonstrated that as many as 60 percent of users can be re-identified from supposedly de-identified CDRs using

---

[21] Sibren Isaacman et al., *Identifying Important Places in People's Lives From Cellular Network Data*, Proc. 9th Int'l Conf. on Pervasive Computing 133, 135 (2011), *available at* http://www2.research.att.com/~varshavsky/papers/isaacman11places.pdf.

publicly available information such as census records.[22] Another group of researchers demonstrated that 95 percent of phone users can be uniquely identified using only four cell site locations.[23]

Even if location information were not included in de-identified call records, re-identification attacks could take advantage of customers' ZIP codes and the times and durations of calls and text messages.

B. Those with the Skills and Motivation to Re-Identify De-Identified Records Have No Motivation to Reveal Success in Doing So

Some commenters point out that there are no publicly known examples of an attacker successfully re-identifying de-identified customer records. For example, Verizon calls on the Commission to do nothing to protect customer privacy in de-identified CPNI "absent specific facts proving" that current anonymization methods are inadequate.[24] AT&T declares that "Petitioners provide no legitimate basis for their speculation that data anonymized . . . could or would be re-identified."[25]

Of course there are no known examples of de-identified customer records being re-identified, because those who would re-identify such records would not reveal that they had done so. If it benefited an attacker to re-identify de-identified records obtained from a carrier, it would also benefit that attacker to continue to

---

[22] Hui Zang & Jean Bolot, *Anonymization of Location Data Does Not Work: A Large-Scale Measurement Study, in* Proceedings of the 17th Annual International Conference on Mobile Computing and Networking 145 (2011), *available at* http://www.cse.ohio- state.edu/~prasun/mobicom11/accepted/mobicom2011-paper128.pdf.

[23] Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen, & Vincent D. Blondel, *Unique in the Crowd: The Privacy Bounds of Human Mobility*, Sci. Rep., Vol. 7, Article 1376, 1 (2013), *available at* http://www.nature.com/srep/2013/130325/srep01376/pdf/srep01376.pdf. The authors noted that the outside information needed to match de-identified location information to real people "could come from any publicly available information, such as an individual's home address, workplace address, or geo-localized tweets or pictures." *Id.* at 2.

[24] Comments of Verizon, *supra* note 6, at 8.

[25] Comments of AT&T, *supra* note 3, at 16.

receive additional records de-identified in the same way. Revealing success in re-identification would jeopardize the attacker's ability to continue to obtain the same type of records.

Thus the fact that there are no publicly known examples of an attacker re-identifying de-identified CPNI obtained from a carrier does not mean it has not happened. Moreover, the Commission need not wait for a clear example of harm resulting from carriers violating customers' privacy before it acts to protect privacy and prevent harm.

C. A Contractual Obligation Not to Re-Identify Data Does Not Make that Data Anonymous

Several commenters explain that when they do share de-identified customers' records with third parties, they require those third parties to agree not to re-identify the records.[26] But this fact has no bearing on whether or not de-identified records constitute individually identifiable CPNI. Whether or not data is individually identifiable is a different question than whether or not others have agreed contractually not to re-identify it.

Furthermore, no matter how well constructed it is, a contract cannot create ironclad assurance that the recipient of de-identified customers' records will not re-

---

[26] Comments of Verizon, *supra* note 6, at 7 ("Contractual provisions can further restrict how business partners can use or share information by, for example, prohibiting a partner from using the data for its own purposes or from attempting to re-identify the data, mandating the use of data protection measures, including encryption and use restrictions and prohibitions, and by providing audit rights and detailing other remedies."); Comments of Future of Privacy Forum, *supra* note 14, at 11 ("When appropriate administrative safeguards (*e.g.*, access controls and restrictions, contractual data use restrictions, and data deletion protocols) are used in conjunction with sophisticated anonymization techniques, reidentification 'remains a relatively difficult task,' and 'in the vast majority of cases, de-identification will protect the privacy of individuals.'"); Comments of AT&T, *supra* note 3, at 18 ("AT&T's Privacy Policy makes clear that the use of anonymized individual consumer data that may be provided to third parties in connection with our External Marketing & Analytics program will be limited to preparing aggregate reports; that those third parties must agree not to attempt to identify any person using this information, and that the data will be securely protected.").

identify or share them. The recipient could breach the contract; doing so is not a crime and may sometimes be in a party's best interest.[27] The recipient could have no intention of ever breaching the contract, but host or transfer the data in a manner that is not secure, allowing a malicious attacker to intercept it. And even if the recipient has the best intentions and guards the data carefully and securely, the recipient itself—and the data it holds—could later be acquired by a different company that has different motivations and intentions.

Any time customer data is shared with a third party, carriers should require the recipient to commit under contract to protect customers' privacy. But such contracts do not exempt carriers from the restrictions that otherwise apply to individually identifiable CPNI under Section 222.

IV. Carriers that Wish to Use or Share Individually Identifiable CPNI for Valuable Research Must Obtain Customers' Consent First

Several commenters note that call records are critical to valuable research. For example, Future of Privacy Forum notes, "The societal value of anonymized data is immense, and anonymization is integral to a wide range of business models."[28] Information Technology & Innovation Forum discusses "[d]ata innovation" and notes that "[a]dvances in computing technology are unlocking opportunities to collect and analyze data in ways never before possible."[29]

But Public Knowledge et al. have not suggested and are not suggesting that carriers never use or share individually identifiable CPNI for valuable research. Public Knowledge et al. ask only that carriers uphold their obligation to obtain customers' consent first.

---

[27] *See* Oliver Wendell Holmes, *The Path of the Law*, 10 Harv. L. Rev. 457, 462 (1897) ("The duty to keep a contract at common law means a prediction that you must pay damages if you do not keep it,—and nothing else.").

[28] Comments of Future of Privacy Forum, *supra* note 14, at 11.

[29] Comments of Information Technology & Innovation Forum at 6, Petition of Public Knowledge, WC Docket No. 13-306 (Jan. 17, 2014).

V. Conclusion

For the foregoing reasons, Public Knowledge et al. urge the Commission to dismiss comments opposing the Petition. Section 222 protects the privacy of telecom customers, who have no choice but to share highly private information about themselves in order to obtain service. The Commission should grant the Petition and clarify that the protections of Section 222 extend to records that have been purged of personal identifiers but that leave individual characteristics intact.

Respectfully submitted,

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

By:

/s/

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

Filed: March 4, 2014