

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

In the Matter of	)	
	)	
Petition Of Public Knowledge For Declaratory	)	
Ruling That Section 222 Of The	)	
Communications Act Prohibits	)	WC Docket No. 13-306
Telecommunications Providers From	)	
Selling Non-Aggregate Call Records Without	)	
Customers' Consent	)	

**COMMENTS OF AT&T**

David L. Lawson  
Alan C. Raul  
James P. Young  
Christopher T. Shenk  
Sidley Austin LLP  
1501 K Street, N.W.  
Washington, D.C. 20005  
(202) 736-8000

James J.R. Talbot  
Gary L. Phillips  
Lori Fink  
AT&T Services, Inc.  
1120 20<sup>th</sup> Street, N.W.  
Washington, D.C. 20036  
(202) 457-3048

*Counsel for AT&T*

January 17, 2014

**TABLE OF CONTENTS**

INTRODUCTION AND SUMMARY .....1

ARGUMENT .....5

I. SECTION 222(c)(1) DOES NOT RESTRICT THE USE OR DISCLOSURE OF ANONYMIZED DATA THAT CONTAIN NO INDIVIDUALLY IDENTIFIABLE CPNI. ....5

II. THERE IS NO MERIT TO PETITIONERS’ FALL-BACK ARGUMENT THAT ALL ANONYMIZED DATA MUST BE DEEMED “INDIVIDUALLY IDENTIFIABLE” BASED UPON THE MERE POSSIBILITY THAT *SOME* DATA, UNDER SOME CIRCUMSTANCES, MIGHT BE “RE-IDENTIFIED.” .....15

CONCLUSION .....20

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

_____	)	
In the Matter of	)	
	)	
Petition Of Public Knowledge For Declaratory	)	
Ruling That Section 222 Of The	)	
Communications Act Prohibits	)	WC Docket No. 13-306
Telecommunications Providers From	)	
Selling Non-Aggregate Call Records Without	)	
Customers' Consent	)	
_____	)	

**COMMENTS OF AT&T**

Pursuant to the Commission's *Notice*,<sup>1</sup> AT&T Services Inc., on behalf of the subsidiaries and affiliates of AT&T Inc. (hereinafter collectively referred to as "AT&T"), respectfully submits these Comments.

**INTRODUCTION AND SUMMARY**

AT&T's privacy policies observe the careful balance that Congress struck in Section 222 of the Communications Act<sup>2</sup> with respect to customer proprietary network information ("CPNI"). The basic parameters of this balance have been well understood throughout the industry for almost two decades, and AT&T has implemented a robust privacy policy and other internal controls that fully comply with Section 222 and ensure that our customers' sensitive personal information remains private. Protecting our customers' privacy is a business

---

<sup>1</sup> Public Notice, *Wireline Competition Bureau Seeks Comment on Petition of Public Knowledge 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, DA 13-2415 (rel. Dec. 18, 2013) ("*Notice*").

<sup>2</sup> 47 U.S.C. § 222.

imperative, and AT&T goes to great lengths to make sure that customers' private data are safe and secure.

Petitioners seek a “declaratory ruling” that would upend this carefully crafted statutory balance by applying restrictions meant only for individually identifiable CPNI to “call records that have been purged of personal identifiers.”<sup>3</sup> Specifically, they seek a ruling that all of the major U.S. wireless carriers' privacy policies facially violate Section 222 on the theory that those policies (quite appropriately) contemplate the possibility that the carrier may use or disclose rigorously anonymized, “de-identified” information that is *not* individually identifiable and that implicates no genuine privacy interest.

Petitioners' interpretation of Section 222 is plainly incorrect. Indeed, their principal statutory argument ignores, and is foreclosed by, the operative statutory language. Section 222(c)(1) instructs a carrier that receives “customer proprietary network information” that it may not (without customer consent or unless otherwise authorized by law) use, disclose or permit access to a specified *subset* of that CPNI, namely, “individually identifiable” CPNI.<sup>4</sup> The Commission must give effect to Congress's use of the phrase “individually identifiable,” and under no plausible reading of the statute could CPNI that has been purged of personal identifiers be considered “individually identifiable.” The Commission's analysis of the Petition should begin and end with Section 222(c)(1). “Individually identifiable” CPNI obviously does not include CPNI that has been *de*-identified and anonymized to protect a customer's privacy, and

---

<sup>3</sup> 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 Docket No. 13-306, at 2 (filed Dec. 11, 2013) (“Petition”).

<sup>4</sup> 47 U.S.C. § 222(c)(1).

Petitioners offer no argument to the contrary grounded in the language or purpose of Section 222(c)(1).

Instead, Petitioners rely solely on a tortured construction that they claim to discern in the “structure” of the Act, which depends on the untenable premise that any customer information that is not “aggregate” under Section 222(h)(2) must be “individually identifiable” CPNI (even if it is in no way individually identifiable).<sup>5</sup> Of course, no court would sustain a statutory interpretation based upon the supposed “structure” of the statute when the effect would be to read an express statutory term like “individually identifiable” out of the statute altogether.

Petitioners misread the “structure” of Section 222. The statute does not say that CPNI is either “aggregate” or otherwise necessarily “individually identifiable.” To the contrary, CPNI and aggregate customer information that is *derived* from CPNI are defined as mutually exclusive categories – aggregate data are not CPNI at all. CPNI, on the other hand, includes both individually identifiable CPNI and non-individually identifiable CPNI. Thus, anonymized customer information, if it is not “aggregate,” is simply CPNI that is not individually identifiable. Such non-individually identifiable information does not become subject to Section 222(c)(1) simply because it is not aggregate.

But even if Petitioners were correct that Congress divided all customer information into aggregate and individually identifiable CPNI, it would still make no sense to classify anonymized data as “individually identifiable” rather than “aggregate.” Aggregate information is expressly defined as (and has always been understood to be) anonymized data, and the privacy-related purposes of the statute are far better served by interpreting “aggregate information” to include all anonymized information (rather than, as Petitioners propose,

---

<sup>5</sup> Petition at 3-4.

subjecting anonymized data that present no privacy concerns to the Section 222(c)(1) individually identifiable CPNI restrictions).

Petitioners' fallback argument fares no better. Petitioners argue that even if their "if it's not aggregate, it must be individually identifiable" formulation is rejected, the Commission should nonetheless deem all anonymized data "individually identifiable" because such data "may be vulnerable" to re-identification (*i.e.*, linking back to individual persons). But Petitioners do not allege (nor could they) that all anonymized data is subject to a risk of re-identification. For that reason alone, the Petition is facially defective: there is no possible basis for the across-the-board declaration Petitioners seek. Rather, the extent of any re-identification risk is a factual question that can only be assessed on a case-by-case basis, because it depends on the specific characteristics of the data set at issue and the ways in which it may be used or disclosed.

For example, the Federal Trade Commission ("FTC") recently found that anonymized data "would not be reasonably linkable to a particular consumer" if (1) the data were shared pursuant to contracts that prohibit re-identification and (2) the data has been properly scrubbed of the types of information that can be used to re-identify the particular person associated with the data.<sup>6</sup> Industry and academic experts have likewise concluded that the potential for re-identification of anonymized data is severely reduced when the data is not made publicly available.

AT&T's own policies illustrate why the Commission must reject Petitioners' position that all anonymized, de-identified data is necessarily subject to grave risk of re-identification and

---

<sup>6</sup> Federal Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policy Makers*, at 21 (March 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> ("Final Report").

must therefore be deemed individually identifiable. Petitioners rely upon anecdotal examples in which weakly anonymized data that included combinations of pseudo-identifiers widely recognized to be susceptible to re-identification was *publicly* released, and it is in that context that legitimate concerns about re-identification have been raised. AT&T, in contrast, does not make anonymized individual customer information publicly available. Moreover, as explained in AT&T's privacy policy and detailed below, when AT&T shares de-identified customer information with other businesses, it requires them to agree that they will handle the information in a secure manner and will not attempt to re-identify or de-anonymize the data. And, unlike the re-identification examples cited by Petitioners, AT&T's anonymized data does not include attributes (such as a combination of gender, location and birth date) that are typically used to re-identify anonymized data. To the contrary, AT&T uses sophisticated masking techniques specifically designed to foil re-identification.

The Petition thus should be denied. There is no basis for the broad declaratory ruling Petitioners seek, and the Commission's existing CPNI rules, orders, and enforcement processes are more than adequate to address any individual situation in which a carrier is alleged to have unlawfully used or disclosed individually identifiable CPNI.

## **ARGUMENT**

### **I. SECTION 222(c)(1) DOES NOT RESTRICT THE USE OR DISCLOSURE OF ANONYMIZED DATA THAT CONTAIN NO INDIVIDUALLY IDENTIFIABLE CPNI.**

Congress struck a careful balance in Section 222, protecting the paramount privacy interests associated with customer information that is identifiable to a particular individual and may therefore be personal and sensitive, while at the same time recognizing the legitimate business and competitive interests in using information that is *not* personally identifiable to better serve customers' needs. The Petitioners seek a sweeping and wholly illegitimate revision

of that statutory framework that would apply prohibitions that Congress intended only for individually identifiable information to “call records that have been purged of personal identifiers.”<sup>7</sup> The language, purposes and structure of Section 222 foreclose that result.

First and foremost, the plain language of Section 222(c)(1) places restrictions only on individually identifiable CPNI, which that provision makes equally clear is a subset of CPNI that does not encompass truly anonymized data:

Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains *customer proprietary network information* by virtue of its provision of a telecommunications service 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.<sup>8</sup>

Congress defined the term “customer proprietary network information” broadly to mean “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.”<sup>9</sup> The prohibition in Section 222(c)(1), however, applies only to the “*individually identifiable*” subset of that CPNI.

The Commission must give effect to Congress’s use of the phrase “individually identifiable,”<sup>10</sup> and under no plausible reading of Section 222(c)(1) could CPNI that has been

---

<sup>7</sup> Petition at 2.

<sup>8</sup> 47 U.S.C. § 222(c)(1) (emphasis added).

<sup>9</sup> *Id.* § 222(h)(1)(A). Less relevant here, CPNI also includes “information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.” *Id.* § 222(h)(1)(B).

<sup>10</sup> *TRW Inc. v. Andrews*, 534 U.S. 19, 31 (2001) (discussing the “cardinal principle of statutory construction that a statute ought, upon the whole, to be so construed that, if it can be prevented,

purged of all personal identifiers be considered “individually identifiable.” Congress did not define the phrase “individually identifiable,” and it is a “fundamental canon of statutory construction” that “[w]hen a term goes undefined in a statute, [a court] give[s] the term its ordinary meaning.”<sup>11</sup> In this context, the ordinary meaning of “individually identifiable” is plain: CPNI is “individually identifiable” if a third party recipient using reasonable means could *identify* the *individual* (i.e., the specific customer) associated with that customer information. This follows naturally from both the statute’s purpose of protecting the privacy of sensitive customer information<sup>12</sup> and the definition of the same phrase in other statutes and regulations.<sup>13</sup> Moreover, to the extent that common sense is any guide, which of course it must be, one can turn

---

no clause, sentence, or word shall be superfluous, void, or insignificant”) (internal quotation marks omitted).

<sup>11</sup> *E.g.*, *Perrin v. United States*, 444 U.S. 37, 42 (1979) (“A fundamental canon of statutory construction is that, unless otherwise defined, words will be interpreted as taking their ordinary, contemporary, common meaning”); *Taniguchi v. Kan Pac. Saipan Ltd.*, 132 S.Ct. 1997, 2002 (2012) (“When a term goes undefined in a statute, we give the term its ordinary meaning.”); *Smith v. United States*, 508 U.S. 223, 228 (1993) (“When a word is not defined by statute, we normally construe it in accord with its ordinary or natural meaning.”).

<sup>12</sup> *See, e.g.*, Declaratory Ruling, *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Info. & Other Customer Info.*, 28 FCC Rcd. 9609, ¶ 17 (2013) (“section 222 is calibrated to apply its strongest protections to ‘individually identifiable’ CPNI”) (quotes in original) (“*2013 CPNI Ruling*”).

<sup>13</sup> For example, the very healthcare statute Petitioners cite (at 6 n.18) confirms Congress’s understanding that the term “individually identifiable” refers to information that identifies the subscriber, as opposed to merely identifying information about an anonymous account. In that statute, Congress defined “individually identifiable health information” as information that “identifies the individual.” 42 U.S.C. § 1320d(6). Moreover, the Department of Health and Human Services (“HHS”), which has regulatory and enforcement authority over such healthcare statute, has expressly acknowledged that anonymization is an acceptable methodology to de-identify sensitive medical information. *See* 45 C.F.R. 164.502(d), 164.514(a)-(b); *see also* U.S. Department of Health & Human Services, *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, available at <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveridentities/De-identification/guidance.html#rationale>.

to any dictionary definition of “anonymous” to refute Petitioners’ argument that anonymous information could be individually identifying information.<sup>14</sup>

Courts, to the limited extent they have interpreted this language, confirm this reading. The Sixth Circuit has noted that customer information that has been redacted so that the customer cannot be identified does not raise a disclosure issue under Section 222 “as that section only prohibits disclosure of ‘individually identifiable’ CPNI.”<sup>15</sup> The court noted that whether such disclosure would raise a Section 222 issue would depend on the facts – specifically, whether “there may be customers for which even a redacted contract would contain sufficiently distinctive customer-linked data so that competitors could easily recognize the underlying customer.”<sup>16</sup> This discussion reflects the commonsense reading of Section 222 that the phrase “individually identifiable” refers to the ability of a third party to use the information to identify the specific customer.

For these reasons, the analysis should begin and end with Section 222(c)(1). “Individually identifiable” CPNI obviously does not include CPNI that has been *de*-identified and anonymized to protect a customer’s privacy, and Petitioners offer no argument to the contrary grounded in the language or purpose of Section 222(c)(1). Instead, Petitioners’ entire argument is based on the “structure” of Section 222 – *i.e.*, making inferences about the meaning of Section 222(c)(1) from *other* provisions in the Act that do not even deal with individually identifiable CPNI. In particular, based on the mere existence of Section 222(c)(3), which

---

<sup>14</sup> For example, *Merriam-Webster* online dictionary defines the term “anonymous” as “not named or identified” and “made or done by someone unknown.” *Merriam-Webster Dictionary*, “Anonymous,” available at <http://www.merriam-webster.com/dictionary/anonymous> (last visited Jan. 16, 2014).

<sup>15</sup> *CMC Telecom, Inc. v. Michigan Bell Telephone Co.*, 637 F.3d 626, 631 (6<sup>th</sup> Cir. 2011).

<sup>16</sup> *Id.*

addresses aggregate customer information, Petitioners reason that: (1) all CPNI must be either “individually identifiable” or “aggregate,” (2) any CPNI that is not “aggregate” therefore must be treated as “individually identifiable,”<sup>17</sup> and (3) anonymized CPNI does not meet the definition of aggregate customer information and therefore it *must* be individually identifiable<sup>18</sup> – even if it cannot be used to identify *any* particular customer.

This mode of statutory construction is specious. Petitioners’ premises do not logically follow from the statutory language, and equally important, courts have repeatedly held that interpretations based on structural arguments that would read a term like “individually identifiable” out of the statute are impermissible where, as here, alternative reasonable interpretations of the statute would give full meaning to all of the words Congress placed in the statute.<sup>19</sup> But even on its own terms, Petitioners’ interpretation fails on at least two grounds.

---

<sup>17</sup> Petition at 4-5. The meat of Petitioners’ statutory analysis is a single sentence: “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).” *Id.* at 5.

<sup>18</sup> *Id.* at 5-6.

<sup>19</sup> *TRW Inc.*, 534 U.S. at 31 (rejecting a proposed interpretation of the statute on the grounds that it would violate the “cardinal principle of statutory construction that a statute ought, upon the whole, to be so construed that, if it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant”) (internal quotation marks omitted); *Duncan v. Walker*, 533 U.S. 167, 174 (2001) (“[W]ere we to adopt respondent’s construction of the statute, we would render the word ‘State’ insignificant, if not wholly superfluous. It is our duty to give effect, if possible, to every clause and word of a statute.”) (internal quotation marks omitted); *Weinberger v. Hyson, Westcott & Dunning Inc.*, 412 U.S. 609, 633 (1973) (rejecting a construction of a statute that “offends the well-settled rule of statutory construction that all parts of a statute, if at all possible, are to be given effect”); *Walters v. Metro. Educ. Enterprises, Inc.*, 519 U.S. 202, 209 (1997) (“Statutes must be interpreted, if possible to give each word some operative effect”); *BedRoc Ltd., LLC v. United States*, 541 U.S. 176, 183 (2004) (“The preeminent canon of statutory interpretation requires us to “presume that [the] legislature says in a statute what it means and means in a statute what it says there”) (internal quotation marks omitted); *Cablevision Sys. Dev. Co. v. Motion Picture Ass’n of Am. Inc.*, 836 F.2d 599, 610 (D.C. Cir. 1988) (rejecting alternative interpretation of a statute, in part, because those “alternatives . .

*First*, Petitioners’ initial premise is incorrect. Contrary to Petitioners’ theory, CPNI and aggregate customer information are mutually exclusive categories, and individually identifiable CPNI is a subset of the broader CPNI category, which includes both individually identifiable CPNI that is subject to the Section 222(c)(1) prohibition and anonymized CPNI that is not. In that regard, as noted above, the statutory definition of CPNI in Section 222(h) is plainly broad enough to include both individually identifiable and anonymized CPNI, because it includes any 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” without regard to whether that information is “individually identifiable” or “aggregate.”<sup>20</sup> Indeed, a number of other provisions in Section 222 use the simple term “customer proprietary network information,” which further confirms that Congress acted with purpose in limiting the prohibitions in Section 222(c)(1) to CPNI that is truly individually identifiable.<sup>21</sup>

---

violate the canon of construction that effect should be given to every word of the statute so that no part is rendered inoperative or superfluous”) (internal quotation marks omitted).

<sup>20</sup> 47 U.S.C. § 222(h)(1)(A).

<sup>21</sup> *Duncan*, 533 U.S. at 173 (“It is well settled that where Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposefully in the disparate inclusion or exclusion.”) (internal quotation marks omitted). Indeed, this is clear from Section 222(c)(1) itself – that provision applies to any telecommunications carrier that “receives or obtains customer proprietary network information” but places restrictions only on that carrier’s use of “individually identifiable customer proprietary network information.” 47 U.S.C. § 222(c)(1); *see also id.* § 222(c)(2) (requiring a carrier to “disclose customer proprietary network information upon affirmative written request by the customer, to any person designated by the customer”); *Id.* § 222(d) (“[N]othing in this section prohibits a telecommunications carrier from using, disclosing, or permitting access to customer proprietary network information obtained from its customers” to perform various functions relating to billing, protection of property, and inbound telemarketing).

At the same time, CPNI does not include “aggregate customer information.” Contrary to Petitioners’ contention, aggregate customer information is not a subset or “narrow carve-out category of CPNI.”<sup>22</sup> CPNI, by definition, is information that is made available to the carrier by “any customer” or “a customer,”<sup>23</sup> and is thus information associated with a single customer (although it may not be individually identifiable to a specific customer if it has been anonymized to eliminate personal identifiers). Aggregate customer information, by contrast, is not defined in terms of CPNI, but is instead defined as “collective data that relates to a *group or category* of services or customers.”<sup>24</sup> In essence, Congress created a category of information *derived* from CPNI that is not itself CPNI.<sup>25</sup> This interpretation is further confirmed by the structure of the statute. Where Congress intended to define separate independent categories, it did so explicitly by providing separate definitions (*i.e.*, CPNI, Aggregate Information, and Subscriber List Information). But where Congress intended to refer to a subset of one of those general categories, it did so using modifiers to the general category (*e.g.*, “individually identifiable CPNI” versus simply “CPNI”). To be sure, the merits of the Petition do not turn on whether aggregate customer information is or is not CPNI, because regardless of how that issue is resolved, Petitioners have no answer to the dispositive fact that anonymized, de-identified call

---

<sup>22</sup> Petitioner at 5.

<sup>23</sup> 47 U.S.C. § 222(h)(1)(A) & (B).

<sup>24</sup> *Id.* § 222(h)(2) (“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>25</sup> *See, e.g.*, Second Report and Order and Further Notice of Proposed Rulemaking, *In re Implementation of the Telecommunications Act of 1996*, 13 FCC Rcd. 8061, ¶ 149 (rel. Feb. 26, 1998) (“when CPNI is *transformed* into aggregate customer information, carriers . . . are free to use the aggregate CPNI for whatever purpose they like”) (emphasis added) (“1998 CPNI Order”).

records fall within the definition of CPNI, but they do not comprise the individually identifiable subset of CPNI that is the only category of CPNI to which Section 222(c)(1) applies.

Given their misreading of these various provisions, however, Petitioners miss the true import of Section 222(c)(3). Section 222(c)(3) is not in a definitional yin-and-yang with Section 222(c)(1), in which “individually identifiable” and “aggregate” establish the universe of possibilities. Rather, the principal purpose of Section 222(c)(3) is to impose special duties with respect to aggregate customer information on local exchange carriers – *i.e.*, a LEC “may use, disclose, or permit access to aggregate customer information other than for purposes described in paragraph (1) only if it provides such aggregate information to other carriers or persons on reasonable and nondiscriminatory terms and conditions upon reasonable request therefor.”

In this respect, the statute’s approach to governing customer information makes sense, because it reflects Congress’s effort to promote the varied purposes of Section 222. Congress enacted Section 222 in 1996 “to balance both competitive and consumer privacy interests with respect to CPNI.”<sup>26</sup> Since Section 222 attempts to balance the customer’s interest in privacy, the carrier’s legitimate business interests in using the information to better serve customers, and the need to promote competition, Sections 222(c)(1) and (c)(3) are best viewed as two specific marketplace interventions at the two extremes of this spectrum. With respect to individually identifiable CPNI, the customer’s privacy interests are paramount, and Section 222(c)(1) therefore places careful limits on the carrier’s ability to use, disclose or provide access to such information.<sup>27</sup> With respect to aggregate customer information, by contrast, which by definition is both collective and anonymized, Congress’s concerns about LECs’ lingering market position

---

<sup>26</sup> *1998 CPNI Order* ¶ 3 (quoting Joint Statement of Managers, S. Conf. Rep. No. 104-230, 104th Cong., 2d Sess., 1 (1996) at 205).

<sup>27</sup> *See 2013 CPNI Ruling* ¶ 17 (“section 222 is calibrated to apply its strongest protections to ‘individually identifiable’ CPNI”).

become paramount, and Section 222(c)(3) requires LECs that make certain uses of aggregate information to share it with requesting competitors on reasonable terms and conditions. But these two provisions do not cover the waterfront – these provisions leave intact the category of CPNI that is neither aggregate nor individually identifiable and which is therefore not subject to the Section 222(c)(1) restrictions.

*Second*, even if Petitioners were correct that all customer information is either aggregate or individually identifiable CPNI, anonymized call records surely fit into the “aggregate” category more readily than they do in the “individually identifiable” category. There is no plausible construction of “individually identifiable” that includes anonymized, de-identified information that cannot be identified to a specific customer. “Aggregate customer information,” in contrast, is defined as collective data relating to groups of customers or services “from which individual customer identities and characteristics have been removed.”<sup>28</sup> Since the anonymized information at issue is by definition CPNI from which individual customer identities (*i.e.*, customer name) and characteristics (*e.g.*, address, social security number) have been removed, the language of both Section 222(c)(1) and 222(c)(3) overwhelmingly indicate that even if CPNI were, as Petitioners claim, limited to “individually identifiable” and “aggregate,” anonymized data would necessarily be classified as “aggregate.”

Petitioners’ contrary interpretation – that Congress intended to distinguish between “collective” and “individual” customer records, whether they had been anonymized or not – finds no support in the statute. Indeed, Petitioners’ notion that all that matters for privacy purposes is whether the data are arranged as individual records or grouped “collectives” is completely unconnected to any purpose of Section 222, would serve no legitimate consumer

---

<sup>28</sup> 47 U.S.C. § 222(h)(2).

privacy goal, and would, in fact affirmatively harm consumers by depriving them of the beneficial uses of anonymized data.

Even if this were a close call, First Amendment considerations would require the rejection of Petitioner’s implausibly expansive view of “individually identifiable” customer information. A broad reading of “individually identifiable” that would limit a carrier’s ability to share information based on thin arguments resting on misuse of canons of construction or invoking hypothetical conduct that might or might not be technically or contractually possible (*see* Section II, *infra*) raises serious First Amendment problems. “It has long been an axiom of statutory interpretation that where an otherwise acceptable construction of a statute would raise serious constitutional problems, the Court will construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress.”<sup>29</sup> Under *Central Hudson Gas & Electric Corporation v. Public Service Commission of New York*,<sup>30</sup> even where a restriction serves to advance a substantial government interest, that restriction must be “narrowly drawn,” and cannot “completely suppress information when narrower restrictions on expression would serve [the government’s] interest as well.”<sup>31</sup> The Court recently reaffirmed the close scrutiny given to restrictions on commercial speech, even in the face of countervailing public concerns like privacy.<sup>32</sup> The Commission itself has acknowledged that its CPNI rules “fall under the First

---

<sup>29</sup> *Public Citizen v. United States Dep’t of Justice*, 491 U.S. 440, 466 (1989) (internal quotation marks omitted).

<sup>30</sup> 447 U.S. 557, 564-65 (1980).

<sup>31</sup> *Id.* The Supreme Court has also noted in *United States v. Playboy Entertainment Group, Inc.*, 529 U.S. 803, 827 (2000), that limits on speech must be “the least restrictive means for addressing a real problem.” In that case, the Court also emphasized that the First Amendment cannot be skirted just because a statute may restrict “speech [that] is not very important.” *Id.* at 826.

<sup>32</sup> *Sorrell v. IMS Health, Inc.*, 131 S. Ct. 2653 (2011) (striking down a law designed, in part, to protect medical privacy as violating the First Amendment). *See also ACLU v. Alvarez*, 679 F.3d

Amendment,”<sup>33</sup> and it has already been forced to modify its CPNI rules and “lessen[] the regulatory burden of various CPNI safeguards” in order to reflect First Amendment rights.<sup>34</sup> The same principles apply here: interpreting the Act to restrict the use and disclosure of anonymized, de-identified information would be unconstitutional given that anonymization is available as a more narrowly tailored method for protecting customers’ legitimate privacy interests.

In short, the Petitioners’ request for a sweeping declaratory order must be denied. The trigger for regulation under Section 222(c)(1) is and must remain whether the CPNI is “individually identifiable,” and call records that have been purged of all personal identifiers are not – by definition – individually identifiable.

**II. THERE IS NO MERIT TO PETITIONERS’ FALL-BACK ARGUMENT THAT ALL ANONYMIZED DATA MUST BE DEEMED “INDIVIDUALLY IDENTIFIABLE” BASED UPON THE MERE POSSIBILITY THAT SOME DATA, UNDER SOME CIRCUMSTANCES, MIGHT BE “RE-IDENTIFIED.”**

Petitioners’ fall-back argument is that “anonymized” call records must in all cases be considered “individually identifiable,” because “in many cases sufficient information remains in anonymized records to link them back to individual people.”<sup>35</sup> The argument fails because the mere possibility that, under some circumstances, it may be technically possible to re-identify

---

583, 604 (7th Cir. 2012) (granting a preliminary injunction against a broad reading of Illinois’ anti-eavesdropping statute on First Amendment grounds).

<sup>33</sup> See Federal Communications Commission, Press Release, *FCC Releases Order Clarifying Rules for Use of Customer Proprietary Network Information* (Sept. 3, 1999), [http://transition.fcc.gov/Bureaus/Common\\_Carrier/News\\_Releases/1999/nrcc9064.txt](http://transition.fcc.gov/Bureaus/Common_Carrier/News_Releases/1999/nrcc9064.txt) (implementing decision in *U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1238-39 (10th Cir. 1999), holding that a regulation designed to protect consumer privacy by requiring customer opt-in to marketing communications violated the First Amendment because, even if the regulation materially advanced privacy goals, it was not narrowly tailored).

<sup>34</sup> Federal Communications Commission, Press Release, *FCC Clarifies Rules for Use of Customer Proprietary Network Information* (Aug. 16, 1999), [http://transition.fcc.gov/Bureaus/Common\\_Carrier/News\\_Releases/1999/nrcc9064.txt](http://transition.fcc.gov/Bureaus/Common_Carrier/News_Releases/1999/nrcc9064.txt).

<sup>35</sup> Petition at 6.

certain types of anonymized data does not mean that *all* anonymized data is subject to this same risk. Petitioners provide no legitimate basis for their speculation that data anonymized by AT&T and used or shared by AT&T under its Privacy Policy could or would be re-identified. Nor could they. To the extent AT&T shares anonymized individual information outside the company, it is done in a manner designed to prevent re-identification. Importantly, AT&T approaches anonymization in a manner consistent with best industry practices, such as described in the framework developed by the Federal Trade Commission (“FTC”), and by experts in the field specifically to address concerns related to preventing re-identification of anonymized data.

Even Petitioners concede that re-identification is not a significant risk for *all* anonymized data.<sup>36</sup> Thus, by Petitioner’s own admission, whether there is a significant risk that any particular anonymized data could be re-identified depends on (1) the characteristics of the specific data set at issue and (2) the nature and circumstances of how and to whom anonymized data was made available. For example, posting poorly anonymized data on a public website is much more likely to present re-identification risks than providing data that has been anonymized pursuant to sophisticated techniques to a reputable organization subject to contractual prohibitions against re-identification and limitations on further use and disclosure. Consequently, there is no basis for the Commission to issue the declaratory ruling Petitioners seek that would prohibit use and disclosure of all anonymized data.

Notably, the FTC has collected a vast record addressing issues related to re-identification of anonymous data, and has issued a Final Report containing the “final privacy framework [that] is intended to articulate best practices for companies that collect and use consumer data,”<sup>37</sup> and

---

<sup>36</sup> *Id.* (conceding that only in “many cases” there may be “sufficient information . . . in [the] anonymized records to link them back to individual people”).

<sup>37</sup> Final Report at vii.

in particular addressing “the ability to re-identify ‘anonymous’ data.”<sup>38</sup> “Under the final framework,” the FTC determined that “a company’s data would not be reasonably linkable to a particular consumer or device to the extent that the company implements” certain “significant protections for the data.”<sup>39</sup> Specifically, these protections include: (1) the “company must take reasonable measures to ensure that the data is de-identified,” meaning that “the company must achieve a reasonable level of justified confidence that the data cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, computer, or other device” and (2) “if a company makes such de-identified data available to other companies – whether service providers or other third parties – it should contractually prohibit such entities from attempting to re-identify the data” and “exercise reasonable oversight to monitor compliance with these contractual provisions and take appropriate steps to address contractual violations.”<sup>40</sup>

Academic experts have likewise emphasized that denying public access to anonymized individual data – as AT&T does – is a highly effective means to prevent re-identification. Referring to the instances of re-identification relied upon by Petitioners, these academic experts point out that “[n]one of these publicized attacks, however, have occurred using nonpublic

---

<sup>38</sup> *Id.* at 18.

<sup>39</sup> *Id.* at 20-21.

<sup>40</sup> *Id.* at 21. *See also, e.g.*, Ann Cavoukian & Khaled El Emam, *Dispelling Myths Surrounding De-identification: Anonymization Remains A Strong Tool for Protecting Privacy*, at 1, 6 (2011), *available at* <http://www.ipc.on.ca/images/Resources/anonymization.pdf> (“[C]ontrary to what has been suggested in recent articles, re-identification of properly de-identified information is not in fact an ‘easy’ or ‘trivial’ task” and “the evidence indicates that there are few cases in which properly de-identified data have been successfully reidentified.”); Information Commissioner’s office, *Anonymisation: Managing Data Protection Risk, Code of Practice*, at 7 (2012), *available at* [http://ico.org.uk/for\\_organisations/data\\_protection/topic\\_guides/~/\\_media/documents/library/Data\\_Protection/Practical\\_application/anonymisation-codev2.pdf](http://ico.org.uk/for_organisations/data_protection/topic_guides/~/_media/documents/library/Data_Protection/Practical_application/anonymisation-codev2.pdf). (the United Kingdom’s Information Commissioner’s Office finding that “the effective anonymization of personal data is possible, desirable, and can help society make rich data resources available whilst protecting individuals’ privacy”).

databases,” and “[e]xperts . . . agree that organizations reduce privacy risk by restricting access to a de-identified dataset to only trusted parties.”<sup>41</sup> These experts have concluded that “[n]on-publicly disclosed datasets have a lessened risk of re-identification than publicly disclosed datasets due to the added protection of administrative controls.”<sup>42</sup>

AT&T applies these (and other) safeguards to anonymized data. 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.<sup>43</sup> In addition, AT&T gives its customers tools that provide them with choices about the extent to which their data is shared.<sup>44</sup> AT&T’s contracts also typically include auditing provisions that enable AT&T to confirm compliance with these contract provisions, as well as a requirement that the third party delete the information, render it unusable or unrecognizable or return it to AT&T upon request or at the end of the contract period.

AT&T applies robust techniques and safeguards to protect against re-identification of anonymized data. AT&T approaches each anonymization use case based on the unique facts applicable to the situation, first identifying the types of data included in a particular data use case that could be used to identify an individual, and then assessing the appropriate anonymization techniques given the proposed use. For example, a data set may include “personal identifiers”

---

<sup>41</sup> Yianni Lagos & Jules Polonetsky, *Public vs. Nonpublic Data: The Benefits of Administrative Controls*, 66 Stan. L. Rev. Online 103, 104 (2013), available at <http://www.stanfordlawreview.org/online/privacy-and-big-data/public-vs-nonpublic-data>.

<sup>42</sup> *Id.* at 109.

<sup>43</sup> AT&T Privacy Policy, available at <http://www.att.com/privacy>.

<sup>44</sup> *See, e.g., id.* (providing instructions and links to allow customers to opt-out of various marketing uses of their data).

that identify or reasonably could be used to identify an individual. To avoid re-identification, AT&T may use one or more of several methods, including deleting personal identifiers/characteristics from the data set, generalizing attributes so that many in the group share the same value (*e.g.*, all ZIP codes generalized to a county, or all phone numbers generalized to area code) and hashing or otherwise obfuscating the attribute (*e.g.*, replacing the identifier with a random string of characters that has no connection to the original information).

A data set may also include “quasi identifiers,” which are attributes that by themselves do not identify an individual but, in combination, may lead to re-identification. A frequently cited example of a quasi identifier set is the combination of gender, date of birth, and ZIP code (indeed, the re-identification examples relied on by Petitioners contained this set of data, or something very similar). To avoid re-identification, AT&T employs anonymization techniques that generalize or otherwise disrupt/perturb or destroy the relationship between quasi identifier attributes to protect against re-identification. For example, all ZIP codes could be generalized to the first three digits, and all ages generalized to within a decade.<sup>45</sup>

On this record, there is no basis whatsoever to grant Petitioners’ request for a declaratory ruling prohibiting the disclosure of any anonymized data. Petitioners have not identified a single instance of AT&T, or any other carrier, having disclosed anonymized data that was subsequently re-identified.<sup>46</sup> Instead, Petitioners rely upon isolated examples of non-telecommunications-

---

<sup>45</sup> AT&T also has strict policies aimed specifically at protecting CPNI. *See* AT&T, Customer Proprietary Network Information (CPNI), <http://www.att.com/gen/privacy-policy?pid=2566> (last visited Jan. 16, 2014).

<sup>46</sup> Public Knowledge cites a New York Times article in which it is asserted that AT&T has provided the Central Intelligence Agency (“CIA”) with certain call records in which several digits of the phone number are “masked.” *See* Petition at 8 (citing Charlie Savage, “*C.I.A. Is Said to Pay AT&T for Call Data*,” N.Y. Times, Nov. 7, 2013). A public Commission proceeding is obviously not an appropriate forum to debate allegations regarding national security-related matters that, if substantiated, would likely be classified. In any event, the

related data sets that were publicly released and that failed to implement robust administrative and technical safeguards to protect against re-identification.

### CONCLUSION

For the foregoing reasons, the Commission should deny the Petition.

Respectfully submitted,

/s/ James J.R. Talbot

David L. Lawson  
Alan C. Raul  
James P. Young  
Christopher T. Shenk  
Sidley Austin LLP  
1501 K Street, N.W.  
Washington, D.C. 20005  
(202) 736-8000

---

James J.R. Talbot  
Gary L. Phillips  
Lori Fink  
AT&T Services, Inc.  
1120 20<sup>th</sup> Street, N.W.  
Washington, D.C. 20036  
(202) 457-3048

*Counsel for AT&T*

January 17, 2014

---

article's own description of the alleged arrangement makes clear that the "masked" call records alleged to have been provided are not "individually identifiable," inasmuch as the article states that if the CIA wishes to identify the customer at issue it must ask the Federal Bureau of Investigation to use its own authority under other statutes to compel disclosure of further information (which would then be governed by the provision in Section 222(c)(1) permitting disclosure of even individually identifiable CPNI if "required by law"). *See also, e.g.,* 18 U.S.C. sec. 2709(a) ("A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section").