



September 20, 2016

Ms. Marlene H. Dortch  
Secretary  
Federal Communications Commission  
445 12 Street, SW  
Washington, DC 20554

**Re: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106**

Dear Ms. Dortch:

The Internet Commerce Coalition (ICC) files this Ex Parte letter in response to arguments presented in this proceeding<sup>1</sup> by a subset of privacy groups in an Ex Parte letter filed on September 7, 2016 (“Privacy Groups September 7 Ex Parte”), which mirror arguments made by Professor Paul Ohm in his Ex Parte letter of July 28, 2016 (“Ohm Ex Parte”), and in a similar Ex Parte filed by the Open Technology Institute on behalf of other privacy advocates on September 12, 2016 (collectively, “the Ex Parte Filings”). All these Ex Parte Filings oppose rules that, like the White House and FTC Privacy Frameworks, set different standards for sensitive data and “data that does not pose a risk to consumers.”<sup>2</sup>

Nothing submitted by these parties – or any other commenter – provides a valid rationale for the FCC to depart from the well-established and successful sensitivity-based analysis used for many years by the FTC and endorsed by the Administration for determining when an opt-in consent requirement is appropriate. As described in the FTC 2012 Privacy Report<sup>3</sup> and the 2012 White House Privacy Report,<sup>4</sup> this approach has been successful at protecting consumers in a way that allows innovation to flourish. And, as explained herein, this sensitivity-based approach is consistent with well-established Internet sector compliance practices, and does not involve the open-ended, subjective analysis that the three Ex Parte Filings posit.

---

<sup>1</sup> *In re* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, *Notice of Proposed Rulemaking*, FCC 16-39, WC Docket No. 16-106 (2016).

<sup>2</sup> Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, WC Docket No. 16-106, at 9 (May 27, 2016) (“FTC Comments”).

<sup>3</sup> *Protecting Consumer Privacy in an Era of Rapid Change*, Federal Trade Commission (2012) (“FTC Privacy Staff Report”).

<sup>4</sup> *Consumer Data Privacy In a Networked World: A Framework for Protecting Privacy and Promoting Innovation In the Global Digital Economy*, The White House (2012) (“White House Privacy Report”).

First, the contention that Section 222 of the Communications Act reflects a Congressional judgment that all information handled by telecommunications carriers is sensitive flies in the face of the plain language of the statute. Professor Ohm asserts that “the design of the statute makes clear that all covered information is intrinsically sensitive.”<sup>5</sup> However, Congress defined consumer proprietary network information (CPNI) as a narrow subset of the data that telecommunications carriers receive from customers, *not* all such data,<sup>6</sup> and imposed privacy obligations only on a subset of that subset – “individually identifiable” CPNI.<sup>7</sup> Section 222 also distinguishes between different types of CPNI in that it imposes greater privacy protection for location data and automatic crash notification data than for other CPNI.<sup>8</sup> These and other commenters who defend the FCC’s proposed rules fail to mention that Section 222 expressly excludes from the statute’s privacy protections “subscriber list information.” This information is not confidential even though subscriber list information is information that carriers receive from customers.<sup>9</sup> These commenters also ignore that, as the Commission stated in its NPRM, Section 222 includes aggregate customer information as CPNI, but allows for less restrictive use and disclosure of aggregate information than other CPNI,<sup>10</sup> and has *never* included information like customer billing address.<sup>11</sup>

In the Internet context, “subscriber list information” is directly analogous to information such as IP addresses, MAC address, customer home and address information that are widely available across the Internet ecosystem or in the phone book. However, this broad range of widely available, non-sensitive information would be swept into the proposed new category of “customer proprietary information” (CPI). The proposed definition of CPI is far broader than the specific categories of information that are defined as CPNI in Section 222(h).

The more general, related contention that Congress “tends not . . . to draw fine lines based on levels of sensitivity of information” and instead to regulate all information in a sector the same way when it enacts a sectoral privacy statute, is substantively incorrect.<sup>12</sup> In fact, all three statutory examples that the Privacy Groups September 7 Ex Parte rely upon actually prove the opposite. First, the Electronic Communications Privacy Act treats the contents of communications and subscriber list information very differently, recognizing that the privacy interest in subscriber list information is lower than that in contents of communications.<sup>13</sup> Second, the Family Educational Rights and Privacy Act treats “education records” as sensitive and regulates them under a very different opt-in regime than “directory information,” which may

---

<sup>5</sup> Ohm Ex Parte at 4.

<sup>6</sup> 47 U.S.C § 222(h).

<sup>7</sup> 47 U.S.C. § 222(c)(1).

<sup>8</sup> 47 U.S.C § 222(f)(1) and (2).

<sup>9</sup> 47 U.S.C. § 222(h)(3).

<sup>10</sup> 47 U.S.C § 222(c)(3).

<sup>11</sup> *Implementation of the Telecommunications Act of 1996, Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information, Order on Reconsideration and Petitions for Forbearance*, 14 FCC Rcd 14409 ¶¶ 9, 146 (1999) (affirming that “a customer’s name, address, and telephone number are not CPNI”).

<sup>12</sup> Ohm Ex Parte at 4.

<sup>13</sup> Compare, e.g., 18 U.S.C. § 2511 with 18 U.S.C. § 2703(c).

be disclosed with notice and opt-out.<sup>14</sup> Third, under the Health Information Portability & Protection Act (HIPAA), some forms of first party marketing communications to covered entity patients are exempt from HIPAA's opt in requirement for marketing, thus undermining the argument that all patient data is treated the same.<sup>15</sup> Furthermore, noticeably absent from the chosen sample of sectoral laws in the three Ex Parte filings is a list of U.S. sectoral privacy laws that treat some information collected by an industry sector as sensitive and subject to an opt-in, and other information as not sensitive and subject to an opt-out or implied consent. For example, the Gramm-Leach-Bliley Act regulates sensitive financial information, allows sharing of non-public personal information held by financial institutions with third parties subject to notice and opt-out, and exempts disclosures of that information to affiliates from the opt-out requirement.<sup>16</sup> However, it bars disclosure of personally identifying account number or other account access codes to unaffiliated third parties.<sup>17</sup>

Of course, as the FTC's comments explain,<sup>18</sup> the generally-applicable FTC privacy framework varies by sensitivity of information, as do all the State breach notification laws. The bottom line is that an approach that does *not* make distinctions based on data sensitivity would be a major departure from the overwhelming body of U.S. privacy law. It would even be inconsistent with the EU privacy framework, which most of the privacy advocate commenters typically hold up as a model that the U.S. should emulate.<sup>19</sup>

In an attempt to dismiss the sensitivity-based distinction made by the FTC, the White House, and the vast majority U.S. privacy laws, the three Ex Parte Filings argue that sensitive information is virtually impossible to define effectively because it must be evaluated in context for each customer. Specifically, they all invoke the *Doe v. Netflix, Inc.*<sup>20</sup> class action complaint for the proposition that de-identified data may still be considered sensitive by some customers and requires a highly subjective, case-by-case sensitivity determination that would require a searching examination of data regarding each consumer.<sup>21</sup> The information at issue in this case was made publicly available and was freely manipulated by researchers trying to identify users and establish that the data was sensitive.<sup>22</sup>

This example is very far afield. ISPs are not making large swaths of customer data publicly available for researchers to analyze as they wish. To the contrary, ISPs are subject to

---

<sup>14</sup> Compare 20 U.S.C. § 1232g(a)(1) & (2) with (a)(5).

<sup>15</sup> 45 CFR § 164.508(a)(3). Under HIPAA there are many first party communications that would be considered "marketing" under other statutes but that are expressly excluded from the definition. 45 C.F.R. § 164.501.

<sup>16</sup> 15 U.S.C. § 6802(a) & (b).

<sup>17</sup> 15 U.S.C. § 6802(d).

<sup>18</sup> FTC Comments at 23.

<sup>19</sup> European Union General Data Protection Regulation, Reg. 2016/679. *See also* FTC Comments at 23 n. 94 ("This approach is also consistent with existing international frameworks, such as the OECD Privacy Guidelines, which distinguish between sensitive and non-sensitive information.").

<sup>20</sup> N.D. Cal. 2009.

<sup>21</sup> Ohm Ex Parte at 4.

<sup>22</sup> Future of Privacy Forum Ex Parte, Sept. 12, 2016, *Observations About the Federal Communication Commission's Privacy Rulemaking in Light of Universal De- Identification Guidance, Methodologies, and Practices*, by Khaled El-Emam, PhD at 11.

internal compliance controls and have been subject to privacy enforcement by regulators and presumably will be subject to enforcement under the eventual final rule.

More fundamentally, the three Ex Parte Filings' argument also ignores that Internet companies, including ISPs and many others, have routinely implemented special privacy and security protections for sensitive data under threat of enforcement under the FTC's well-established privacy framework. For example, they avoid using sensitive data (such as health or children's information, social security numbers, and precise geolocation data) to target advertising or market to consumers on the basis of sensitive data categories, unless opt-in consent is obtained. This distinction is a key part of the Digital Advertising Alliance and Network Advertising Initiative self-regulatory frameworks, programs in which Internet companies, including ISPs participate. Participants are subject to enforcement, by government regulators and industry regulatory bodies, such as the Better Business Bureau, if they fail to comply with program requirements.<sup>23</sup> The suggestion in the three Ex Parte Filings that the FCC could not enforce a sensitivity-based privacy restriction that defines sensitive data elements ignores the enforcement of the FTC framework and many sectoral privacy laws, as well as the enforceable industry codes that have successfully incorporated this approach for many years.

The three Ex Parte Filings offer a second, flawed argument that in order to respect the boundaries of each customer's subjectively defined sensitivities, ISPs would need a surveillance program in order to identify those sensitivities.<sup>24</sup> Again, this is simply not true. Under legal requirements that pre-date the Open Internet Order and compliance under widely adopted Internet advertising self-regulatory frameworks, Internet companies – including ISPs – do nothing of the sort. And they would certainly not need to conduct surveillance under final rules that limited opt-in consent to sensitive data. If the final rules adopted by the FCC are consistent with the FTC framework, ISPs, as they do today, would exclude sensitive data categories from data used for advertising or marketing unless it is collected with the informed, opt-in consent of that user. This easily resolves the quandary that these commenters posit. Indeed, neither the FTC framework nor any of many federal privacy statutes that distinguish between sensitive and non-sensitive data require the sort of contextual, customer-specific analysis that the Ex Parte Filings suggest is required.

The Ex Parte Filings' assertions that opt-in consent will be easy to obtain are also similarly incorrect.<sup>25</sup> As the Internet Commerce Coalition explained in its Reply Comments, this argument rests entirely on an example in a very different context – check overdraft protection – and ignores the proposed rules' rigid requirements for providing notice and obtaining opt-in consent that would provide ISPs with far less latitude to obtain opt-in consent.<sup>26</sup> The Ex Parte Filings ignore the practical reality that when consumers fail to opt in, they often do so not by

---

<sup>23</sup> See, e.g., IAB Tech Lab Content Taxonomy, at <https://www.iab.com/guidelines/iab-quality-assurance-guidelines-qag-taxonomy/> (last visited Sept. 16, 2016) (providing a standardized taxonomy of websites for advertisers to use, among other things, to identify sensitive versus non-sensitive websites).

<sup>24</sup> Ohm Ex Parte at 4.

<sup>25</sup> Ohm Ex Parte at 5; Privacy Groups September 7 Ex Parte at 4.

<sup>26</sup> Proposed Rule § 64.7001.

considered choice, but because they do not wish to take the time needed to make a choice and they do not fully internalize the social costs of their non-choice.<sup>27</sup> Furthermore, obtaining, cataloguing, and tracking opt-in consents that applied to the huge range of data elements included in the NPRM's sweeping definition of CPI would be cumbersome for ISPs and consumers alike. Finally, the notion that consumers will opt-in if the benefits are truly significant is belied by numerous studies showing that consumers often do not opt-in *regardless* of the benefits of doing so.<sup>28</sup>

These parties' arguments against the well-established sensitivity-based data distinctions in U.S. privacy law in no way undermine the comments and recommendations of the FTC, an expert agency on privacy, that the final FCC rules should reserve opt-in privacy and heavy information security obligations for sensitive data. A sensitivity-based data distinction approach is not unworkable, as these filings try to argue, but rather something that is well established in U.S. privacy law, widely implemented by companies, and successfully enforced by regulators. The FTC recognizes that a failure to distinguish between non-sensitive and sensitive data could impede beneficial uses of data that consumers may prefer because, for example, of service innovations and lower costs. The FCC should follow this well-established and effective privacy approach in the final rules.

Respectfully submitted,

/s/ **Jim Halpert**

Jim Halpert  
Sydney White  
Counsel to Internet Commerce Coalition

---

<sup>27</sup> US Telecom Ex Parte, May 27, 2016, *An Economic Analysis of the FCC's Proposed Regulation of Broadband Privacy* by Joshua D. Wright at 14.

<sup>28</sup> *E.g.*, Comments of AT&T Services, Inc., WC Docket No. 16-106, at 52-53 (May 27, 2016); Comments of Comcast Corp., WC Docket No. 16-106, at 26, 48-49 (May 27, 2016); Comments of the National Cable & Telecommunications Association, WC Docket No. 16-106, at 79-80 (May 27, 2016).