October 13, 2016

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

Re: WC Docket No. 16-106, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services;
WB Docket No. 13-306, 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

Dear Ms. Dortch:

On Tuesday, October 11, Sarah Morris of New America’s Open Technology Institute and I met with Claude Aiken, counsel to Commissioner Clyburn, and Travis Litman, counsel to Commissioner Rosenworcel, in two separate meetings to discuss matters in the above-referenced proceeding. In both meetings, the facts and arguments presented were substantively the same.
**The FCC’s Broadband Privacy Rule Should Not Distinguish Between Sensitive and Non-Sensitive Information**

As we explained in our meetings, OTI continues to be concerned that establishing different levels of privacy protection that turn on the perceived subjective sensitivity of various types of data is not the best solution for consumers, not in line with Section 222 of the Communications Act, and not consistent with the expectations of broadband customers. When consumers sign up for broadband, they expect that their ISP will only use information about their use of the internet to deliver service, and not for other purposes. They certainly don’t expect that they won’t even be asked before their ISP uses or shares information that someone else has decided is “non-sensitive.”

As OTI has previously explained, it would be in administrable and unwise for the FCC to offer less protection to customer information it considers “non-sensitive.” Many consumer advocates have expressed skepticism that BIAS providers could effectively and reliably parse the sensitive from the non-sensitive without in some way examining datasets to determine whether they contain sensitive information. Moreover, sensitive information can be extracted from data that might not immediately appear to be sensitive.

In addition, as OTI has argued in this docket repeatedly, the statute does not contemplate differential treatment for subjective categories of “sensitive” and “non-sensitive” information. OTI also noted that even seemingly innocuous data can sometimes, through analysis, be used to infer other information about those individuals that they would consider highly private. Something that is “non-sensitive” to a majority of people may also nevertheless be sensitive to a minority. In addition, as the Center for Democracy & Technology noted in a recent filing in this docket, “non-sensitive” information may serve as a “lynchpin,” and “could result in a significant privacy

---

1 See Reply Comments of New America’s Open Technology Institute, WC Docket No. 16-106 (July 6, 2016), at 21-27.
2 New America’s Open Technology Institute Notice of Ex Parte, WC Docket No. 16-106 (Oct. 3, 2016), at 3-4.
invasion because the information would facilitate a connection with other, existing pools of information.”

If the FCC nevertheless adopts a broadband privacy framework that relies on distinctions between sensitive and non-sensitive categories of information, as the recently released fact sheet suggests, OTI argued that the FCC should consider customer proprietary information and customer proprietary network information (CPNI) to be sensitive by default. In other words, rather than designating some information as sensitive and assigning everything else to the non-sensitive category, the FCC should do the reverse: enumerate which categories of information are not sensitive, and assign everything else to the sensitive category.

A sensitive-by-default approach would better protect consumers by placing the burden on broadband providers to demonstrate that some categories of information ought to fall in the non-sensitive category. Sensitive-by-default would also help future proof the framework. It may be difficult to anticipate today what type of information will be considered sensitive in a year or several years, but a sensitive-by-default approach ensures that even as technology changes, consumers will remain protected. For example, as facial recognition technology advances, it is becoming more and more clear that photographs of faces may be sensitive information, especially when the context in which a face is photographed includes visual cues regarding the photographed individual’s associations, hobbies, or other aspects of their private life.

In any event, if it adopts a framework that differentiates between sensitive and non-sensitive categories, OTI urged inclusion of MAC addresses, source IP addresses, and traffic data in the sensitive category and clarification that browsing history includes destination IP addresses. OTI also explained that there is absolutely no reason for the FCC to waver on its intention to include browsing history and app usage history in the sensitive category.

---

3 Notice of Ex Parte of Center for Democracy & Technology, WC Docket No. 16-106 (Sept. 29, 2016), at 2.
MAC Addresses

If the FCC is going to draw distinctions between sensitive and non-sensitive categories of information, OTI argued that MAC addresses must be categorized as sensitive. As an initial matter, MAC addresses are CPNI. As OTI explained in comments filed in this docket in May, “This definition clearly captures data such as . . . MAC addresses (‘destination’ and ‘technical configuration’ of use), IP addresses (‘destination’ and ‘location’ of use), and traffic statistics (‘type’ and ‘amount’ of use).”

A great deal of private information can be learned about a customer from a MAC address. Ranges of MAC addresses are assigned to single device manufacturers, so an individual MAC address may tell an observer what company manufactured a specific device. OTI explained that in the case of a company that manufactures only one type of device, the MAC address may tell an observer what kind of connected device the customer owns. In some cases, an observer can draw inferences about attributes or interests of the customer based on the customer’s devices. For example, MAC addresses beginning with 84-77-78 are assigned to a company called Cochlear Limited, which only makes hearing assistance devices. MAC addresses beginning with 24-E5-AA are assigned to Philips Oral Healthcare, which only makes oral care products.

OTI also explained that the type of information that can be learned from MAC addresses is increasing as the Internet of Things expands, and connected devices with MAC addresses proliferate both in number and in kind. For example, connected devices available today already include:

- Wi-Fi-enabled physical buttons for ordering goods,
- Wi-Fi-enabled baby monitors,

---

5 47 U.S.C. § 222(h)(1)(A) defines customer proprietary network information as “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.”
6 Comments of New America’s Open Technology Institute, WC Docket No. 16-106 (May 27, 2016), at 20.
7 See http://standards-oui.ieee.org/oui/oui.txt
9 See http://standards-oui.ieee.org/oui/oui.txt
10 http://www.usa.philips.com/c-m-pe/dental-professionals/about-us
• Wi-Fi-enabled garage door openers,\textsuperscript{13}
• Wi-Fi-enabled door locks,\textsuperscript{14}
• Wi-Fi-enabled coffee makers,\textsuperscript{15}
• Wi-Fi-enabled crock pots,\textsuperscript{16}
• Bluetooth-enabled baby onesies,\textsuperscript{17}
• Wi-Fi-enabled mattress covers,\textsuperscript{18}
• Bluetooth-enabled sex toys,\textsuperscript{19}
• Bluetooth-enabled menstrual cups,\textsuperscript{20}
• Wi-Fi-enabled children’s toys,\textsuperscript{21}
• Wi-Fi-enabled pet feeders,\textsuperscript{22} and
• Bluetooth-enabled thermometer pacifiers.\textsuperscript{23}

For a customer with many connected devices, much can be learned about their private life by inferring what kinds of devices they have based on MAC addresses. Much more may be learned by analyzing (likely in an automated way) timing, volume, and patterns of traffic to and from those devices. MAC addresses of Wi-Fi-enabled devices may be exposed to ISPs because many consumers use ISP-provided routers to set up their home Wi-Fi networks, and those ISP-provided routers may provide ISPs with visibility into network-connected devices. However, it is possible that MAC addresses could also be an issue even with Bluetooth-enabled devices, particularly on mobile broadband.

\textsuperscript{12} https://www.motorolastore.com/mbp854connect.html.
\textsuperscript{13} http://shop.garageio.com/collections/frontpage.
\textsuperscript{14} http://remotelock.com/products/smartlocks/.
\textsuperscript{16} http://www.crock-pot.com/slow-cookers/wemo-enabled-smart-slow-cooker/crock-pot-6-quart.-smart-slow-cooker-with-wemo/SCCPWM600-V1.html
\textsuperscript{17} http://mimobaby.com/product/.
\textsuperscript{18} http://www.postscapes.com/wifi-mattress-cover-luna/.
\textsuperscript{19} https://www.kiiroo.com/teledildonics/.
\textsuperscript{22} http://www.feedandgo.com/pet-feeder/.
\textsuperscript{23} https://www.pacif-i.io/.
An entity with visibility into the home networks and connected devices of its customers could learn information about interpersonal relationships between multiple customers by tracking MAC addresses or other device identifiers across multiple locations. For example, in a region where a single provider supplies all or most broadband connections to homes, that provider—which can likely view, log, and use MAC address information—would be well-positioned to draw inferences regarding relationships between multiple customers who live in separate homes, by observing when the MAC addresses of known devices converged in a single location (for example, away from home, but in the home of another customer served by the same provider), and when they parted ways.

MAC addresses indisputably can reveal information about customers’ private lives and activities. Under no circumstances should the FCC be swayed by arguments some parties have made that MAC addresses should be classified as non-sensitive and afforded a lesser level of protection.

**IP Addresses**

Similar to MAC addresses, OTI argued that both source and destination IP addresses are sensitive. First, source IP address can disclose accurate geolocation information. There are sites that provide specifically this service. For instance, [www.iplocation.net](http://www.iplocation.net) allows anyone to put in any IP address and it will provide geolocation data from several geolocation providers. The FCC should ensure that its final rule allows it to enforce against the use and disclosure of source IP addresses, which can accurately locate a person, without opt-in consent.

OTI also urged the FCC to clarify in its final rule that destination IP addresses constitute browsing history, and therefore are sensitive information subject to an opt-in consent requirement prior to non-service-related uses and disclosures.

**Traffic Metadata**

OTI argued that traffic metadata, such as the time and volume of a customer’s use of their connection, must be considered sensitive information as well. OTI pointed out that this information is classic CPNI, because it clearly “relates to the quantity,

---

24 There are several other services, including www.ip2location.com and www.ipfingerprints.com.
technical configuration, type, destination, location, and amount of use of a telecommunications service.” In addition, information about when and how much a customer uses their connection can be analyzed to determine when the customer is home and when they are not (i.e. location), as well as when they are asleep and when they are awake. Information about the volume of traffic on the network can be analyzed to deduce what a customer is doing (e.g. streaming a movie). And changes in routine traffic patterns could indicate that a customer is on vacation, has become unemployed, or has experienced a change in family status. Traffic metadata may also tell an observer when a customer has guests in their home, and when those guests leave.

Web Browsing and App Usage Histories

OTI also urged the FCC to stand firm on its intent to categorize web browsing and app usage histories as sensitive. In at least two recent filings in this proceeding, Google and marketing associations argued — incredibly — that this information somehow falls into the non-sensitive category. But the sites visited and apps used by consumers plainly include information that consumers would want and expect to receive the highest level of protection. As OTI has previously explained,

Domain names, of course, can expose intimate details about the subscriber’s health (plannedparenthood.org), finances (acecashexpress.com, particularly if accessed before each payday), political views (joinnra.nra.org), and many other sensitive attributes. A subscriber’s history of domain name lookups could also be used to more accurately predict certain attributes about a subscriber like gender, age, race, income range, and employment status.

---

25 Google argued that web browsing history is not sensitive. See Letter from Austin Schlick to Marlene Dortch, WC Docket No. 16-106 (Oct. 3, 2016), at 1 (“Calls by some parties in this proceeding to extend an opt-in consent requirement to all web browsing information are unjustified.”). Several marketing associations, who rely on the ability to mine browsing histories to intrude on people with targeted advertising, argued similarly. See Letter from Am. Advertising Federation et al. to Marlene H. Dortch, WC Docket No. 16-106 (Oct. 10, 2016), at 3.

Google, of all parties, is well aware that browsing history can be used to infer deeply private information about individuals; indeed, Google is among the lead developers of the technology that facilitates this type of analysis. For example, a 2011 patent application filed by Google for “estimating user demographics” explains how browsing history may be used “to estimate the demographics” of an Internet user. That application further defines “demographics” to include a number of characteristics that many—if not most—customers would consider private:

- demographics data may include a user’s age, gender, race, ethnicity, employment status, education level, income, mobility, familial status (e.g., married, single and never married, single and divorced, etc.), household size, hobbies, interests, location, religion, political leanings, or any other characteristic describing a user or a user's beliefs or interests.

Another patent application filed by Google explains that browsing history can be used to learn location information about an individual. Thus Google is actively developing the very technology that can mine browsing history to reveal information about consumers’ financial status, familial status, age, and location. Other ISPs, for their part, are likely capable of the same type of inference based on browsing history.

In addition to inferring demographics and location information from browsing history, it is not difficult to imagine how one could use browsing history to guess whether a particular customer is pregnant, is struggling to pay rent, is out of work, is a child, or is a domestic violence victim. There can be no question that browsing history does not belong in the “non-sensitive” category.

For similar reasons, app usage history is also sensitive. Just as browsing history can be used to learn an extensive amount about a person, app usage history can reveal similar information. Of particular concern are location, health, finance, and related apps. But even when apps do not obviously deal with information that falls into these

---

28 Id.
categories, the mere fact of their use by an individual could reveal information that individual wishes to keep private. To provide just a few examples, some apps available for download include:

- FERZU - social network for furries and furfans,
- Spring - photo editing tools to help users appear taller,
- Insomnia Cookies - in-app cooking ordering at any time of day or night,
- Surge - gay dating and chat,
- History of Nazism - exactly what it sounds like, and
- Guardian Rape Alert - when active, transmits location and an audio feed to a trusted third party if the user pulls the headphone cable out of their device.

The FCC Should Not Allow Merely De-Identified Data to Be Used and Shared Without Permission

As OTI has argued in the past, supposedly de-identified customer information should only be regulated separately from customer proprietary information or individually identifiable customer proprietary network information if it meets the statutory definition of aggregate customer information under 47 U.S.C. § 222, that is, “collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.” Thus, information that has merely been pseudonymized (i.e. purged of datapoints typically considered to be personally identifying, but with the data largely left intact) would not meet the definition of aggregate customer information for two reasons: because it

32 “Furries” are people who are interested in anthropomorphic animals. Many are involved in furry-related roleplaying, including in a sexual context. See George Gurley, Pleasures of the Fur, Vanity Fair (Mar. 2001), http://www.vanityfair.com/culture/2001/03/furries200103.
would not be “collective data,” and because it would not have been purged of individual customer “characteristics.” BIAS providers would not be barred from using pseudonymized information or information that otherwise has been de-identified in a manner that does not meet the definition of aggregate customer information, they would simply need to obtain their customers’ affirmative opt-in consent to use such data for non-service-related purposes.

OTI argued that if the FCC allows the free and unfettered use of supposedly de-identified data, this will become the exception that swallows the rule. As one of the few areas where ISPs would need no customer consent (which is, again, contrary to the statute’s language), ISPs will attempt to force all data collection into the de-identified category without regard for the real and probable privacy harms that result from the public release and re-identification of that information.

If the FCC is going to apply a lower level of privacy protection to supposedly de-identified customer information, it must create some mechanism for oversight of ISPs’ de-identification methods. The public and the FCC should be able to scrutinize de-identification methods to ensure that they adequately protect consumer privacy.

Pay for Privacy

The FCC should ensure that pay-for-privacy plans, particularly those where the price differential is unreasonable, can be challenged through at minimum an enforcement action. This is particularly important in the context of financially vulnerable consumers, where the pay-for-privacy plan could become a constructive conditioning of service based on particular privacy options, which the rules supposedly will prohibit. In other words, a privacy-protective plan that cost an extra $100 per month might as well not exist, because no one would be able to take advantage of it. A lesser privacy premium might be more affordable, but may still render privacy a non-option for individuals and families with limited or no discretionary income.

Even if it is not going to promulgate specific pay-for-privacy restrictions or prohibitions, the FCC should signal that some pay-for-privacy plans could violate the obligation that ISPs obtain customers’ consent (i.e. consent conditioned on an unaffordable premium is not consent at all) and the statutory prohibition against unjust and unreasonable practices in § 201(b).
Conclusion

For the reasons OTI and other public interest advocates have outlined, the FCC should steer clear of a broadband privacy framework that offers less protection for information deemed “non-sensitive.” But if the FCC does decide to go with this framework, it should treat CPNI as sensitive by default and narrowly cabin any non-sensitive category. In no case should MAC addresses or browsing history fall into the narrow non-sensitive category.

Respectfully submitted,

/s/
Laura M. Moy
Institute for Public Representation
Georgetown University Law Center
600 New Jersey Avenue, NW
Suite 312
Washington, DC 20001
(202) 662-9547

Counsel for New America’s Open Technology Institute