



May 27, 2016

Ms. Marlene H. Dortch, Secretary  
Federal Communications Commission  
445 Twelfth Street, SW  
Washington, DC 20054

*Via Electronic Filing*

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

Dear Ms. Dortch,

I<sup>1</sup> offer these comments to aid the Commission in properly framing privacy issues called out in the March 31, 2016 NPRM that deal with technical matters. I also address some of the public discourse on these matters that is either misleading or factually wrong.

I conclude that the approach proposed by the NPRM is unlikely to protect anyone's privacy but is quite likely to reduce the potential for meaningful competition in online advertising markets. I suggest a more productive approach that would:

- A) Limit the scope of the FCC's direct rulemaking to such private information that is uniquely visible to Internet Service Providers;
- B) Harmonize rulemaking on private information visible to both ISPs and other Internet services under the common, technology-neutral framework devised by the FTC;
- C) Open a further enquiry on: 1) private information visible to non-ISP Internet services that is hidden from ISPs; and 2) recent developments in the Internet standards process that affect privacy such as [RFC 7844](#) (An Anonymity Profile for DHCPv4 and DHCPv6 Clients), and [RFC 7858](#), (Transmission of DNS Requests over TLS).<sup>2</sup>

### **General Observations**

It appears that the FCC has once again rushed into a rulemaking with incomplete

---

<sup>1</sup> I am an independent network engineering consultant and policy analyst, presently working at the American Enterprise Institute as a Visiting Scholar and at High Tech Forum as editor and founder. These remarks are offered in my personal capacity and do not necessarily represent the opinions of AEI or any client or sponsor. I have previously offered comments in the "Preserving the Open Internet" and "Broadband Industry Practices" dockets, GN 09-191 and WC 07-52 respectively, and offered testimony at the [FCC En Banc Public Hearing on Broadband Network Management Practices in Cambridge on February 25, 2008](#) as an invited technical expert. My CV is available at <http://www.bennett.com/resume.pdf>.

<sup>2</sup> Christian Huitema, "Two Wins for Internet Privacy on the Same Day," *Christian Huitema*, May 18, 2016, <https://huitema.wordpress.com/2016/05/18/two-wins-for-internet-privacy-on-the-same-day/>.

information about the Internet's technical characteristics and about the marketplace for Internet-based service. The NPRM fails to define key terms correctly – such as CPNI – and to even define some terms, such as “privacy”, at all. The NPRM takes a scattershot approach to the issues, asking the same questions multiple times in contexts with no pertinent difference, and failing to provide a coherent taxonomy of the issues.

The end result is a proposed rule that applies different standards to the collection, protection, sale, and use of personal information according to the nature of the industry in which the regulated firm is a participant. This is blatantly discriminatory, unreasonable, corrosive to competition, and unfair to consumers.

Rather than beginning with an overview of the market for personal and private information in order to arrive at a coherent framework, the NPRM “goes legal” from paragraph 6, in which it invokes Section 222. Following that, the NPRM asks a series of questions that seem to be calculated to determine how far it can push the Section 222 authority (which it gave itself by incorrectly classifying Internet services under Title II) in order to serve the interests of a favored industry and to punish a disfavored one.

The NPRM fails to distinguish the personal information ISPs have the ability to see by virtue of their role as providers of Telecommunications Service from the information they may be able to see by virtue of the role as Information Service providers. This conflation is consistent with the theory of Internet service underlying the Commission's 2015 Open Internet Order, a matter currently before the court.

The NPRM is irrational and discriminatory because, in the first instance, it fails to characterize Internet service correctly. It is also flawed because it fails to apply consistent regulations to common behaviors. In the end, the NPRM fails to protect privacy because all the allegedly privacy-damaging activities it seeks to prevent ISPs from performing are but a sliver of the personal information transactions commonly performed by firms the FCC chases not to regulate.

The NPRM does not live up to the FCC's promise to harmonize ISP privacy regulations with the FTC's technology neutral privacy framework. This judgment is confirmed by the statement of former FTC chairman Jon Leibowitz highlighting some of the many inconsistencies between the NPRM's proposed approach and the FTC framework.<sup>3</sup>

### **A Privacy Taxonomy**

The NPRM would gain a lot of clarity by discarding its scattershot approach in favor of a coherent framework defined by meaningful technical distinctions. For purposes of consistency, we can segregate advertising-relevant information into three categories of visibility:

- A. **Customer Proprietary Network Information (CPNI)** is information necessary to the provision of a telecommunication service. Historically, CPNI can only be

---

<sup>3</sup> Jon Leibowitz, “Re: Protecting the Privacy of Broadband and Other Telecommunications Services, WC Docket No. 16-106” (Davis Polk and Wardwell LLC, May 23, 2016).

seen by networks: Between a caller and a called party on the PSTN, there are no intermediaries but telecommunication networks. CPNI is said to be “made available to the carrier by the customer solely by virtue of the carrier-customer relationship.”

By its nature, information made available to other parties, such as Internet search and advertising services, cannot be CPNI because there is no “carrier-customer relationship” between the parties. Therefore, any information routinely provided to non-carrier parties by carrier customers that is also seen by telecommunication networks must not be CPNI. CPNI, in other words, implies exclusivity because it pertains to the PSTN. The design of the PSTN is centralized, exclusive, and monolithic and there are no parties in the path between caller and called party that are not Telecommunication Services. The Internet obviously has a different structure because it does not provide a PSTN-like service.

Therefore, the strict definition of CPNI must include only such information as is known or knowable *only* by the carrier and the carrier’s customer. Two examples of strict CPNI would be 1) the Medium Access Control (MAC) address of the customer’s home router; and 2) the DHCP parameters sent by by Customer Premise Equipment (CPE) to the carrier’s DHCP server to enable the provisioning of Internet Protocol routing services by the carrier for the customer.

Additional examples of CPNI would include data on the customer’s frequency and intensity of network utilization. CPNI would not include customer location or the IP addresses of the customer’s Internet destinations because such information is known by parties other than the telecommunication provider and the customer.

The MAC address of the customer’s home router roughly corresponds to the telephone number in the PSTN regime, but the analogy is less than perfect. MAC addresses are globally unique, like telephone numbers, but they are not routable as telephone numbers are. IP addresses are fully routable, but they are not persistent as telephone numbers are. MAC addresses assigned to customer equipment other than routers do not travel outside the home and are therefore not useful for advertising purposes.

Hence, the nearest analogy to the phone number in the IP realm is the DHCP transaction that assigns an IP address to the MAC address of a home (or office) router. While there is no direct analogy to DHCP in the PSTN realm, it seems sensible to regard DHCP transactions as CPNI because they serve no purpose beyond facilitating IP routing services and are not known by parties other than networks.

- B. **Common Internet Information (CII)** is information about the customer that is known or knowable by carriers as well as other Internet players such as advertising networks, websites, browsers, operating systems, and transit networks. Such information is broadly shared by Internet users with other parties explicitly

and implicitly because the Internet is an open platform funded chiefly by advertising. CII is the essential input to advertising sales.

The Internet is therefore a very different marketplace than the PSTN, which is funded by subscription fees and provides users with a strong expectation of privacy. Without the sharing of such information the Internet would cease to be the open platform it is today; rather, it would become a platform for subscription-based services and for the kinds of not-for-profit activities permitted by NSFNET's Acceptable Use Policy before the NSFNET was de-commissioned in the mid 1990s.

CII includes such information as Internet Protocol (IP) headers, unencrypted IP payloads, and Domain Name Service (DNS) queries. Unencrypted IP payloads include TCP headers and TCP payloads, which in turn include HTTP headers, commands, and payloads. HTTP, of course, reveals a great deal of information about the user that websites may either conceal or make available to ISPs, transit networks, and network analyzers.

Non-carrier elements of the Internet typically have access to CII without an explicit opt-in by the Internet users. It is discriminatory and inconsistent to require opt-in consent before this commonly-shared data can be accessed by ISPs when opt-out is the standard for non-ISPs.

- C. **Customer Non-Visible Network Information (CNNI)** is information that can only be seen by parties other than ISPs. Such information generally consists of encrypted cookies, payloads encrypted by Transport Layer Security (TLS, AKA "HTTPS"), data streams passed through Virtual Private Networks, onion routers, or other types of secure tunnels.

Browsers, Internet applications, and operating systems have access to a great deal of information regarding the user's interaction with data acquired or shared through network transactions. Browsers, for example, know whether users read web pages all the way to the end because they see mouse clicks and keyboard input. If a user re-reads a paragraph of text, highlights a section, or annotates a document obtained across the Internet, the browser or document reader knows these actions have taken place but the ISP doesn't.

Similarly, if the viewer of a video program pauses, rewinds, skips, fast forwards, or replays a portion of a video stream, the video streaming service knows which scenes in the video program are the objects of these actions. The ISP and transit network can deduce that the user interrupted the program flow, but would not easily know which scenes were affected. These actions are, of course, indications of user interest that have valuable advertising consequences and therefore important privacy implications.

In addition to these three categories of visibility, advertising-related privacy encompasses

several types of information. The chief distinction among information types separates static information that identifies a person or device (an actor) from the activities the actor performs. Information elements in the first category are known as identifiers and information elements in the second category are known as actions or behaviors. Some actions include data that is rightly considered “sensitive” by the FTC framework and some does not. This is a meaningful distinction that should be applied consistently across platforms.

	Visible to ISP		Invisible to ISP	
	CPNI	CII <sup>4</sup>	CNNI with TLS <sup>5</sup>	CNNI with VPN <sup>6</sup>
Identifier	MAC address	Source IP address Destination IP address Domain name Transport protocol IP payload: - Port number - Account name - Application	IP payload: - Port number - Account name - Application	IP payload: - Port number - Account name - Application Destination IP address Domain name Transport protocol
Action	DHCP parameter exchange Periods of inactivity Data volume	Periods of activity DNS lookup <sup>7</sup> Upload Download Video control <sup>8</sup> Purchases <sup>9</sup> Sensitive data	DNS lookup <sup>10</sup> Video control details Purchase details Sensitive data	Access DNS lookup Video action details Purchase details Sensitive data

Table 1: Taxonomy of Private Data by Visibility and Type

Consequently, there is no meaningful difference between the information visible to ISPs and to web services in the common, unencrypted scenario. In the new reality – in which IP payloads are encrypted by TLS or VPNs – there is an enormous difference between the small pool of information available to ISPs and the much larger pool visible to web services. But in no scenario is there any empirical support for the NPRM’s claim that ISPs are in a privileged position with respect to web information.

<sup>4</sup> Without encryption these elements are visible to ISPs and edge services alike.

<sup>5</sup> With TLS encryption these elements are invisible to ISPs.

<sup>6</sup> With VPN encryption these elements are invisible to ISPs

<sup>7</sup> When using third party DNS

<sup>8</sup> Without scene

<sup>9</sup> Without details such as vendor and price

<sup>10</sup> When using third party DNS with IETF standard encryption

The NPRM's assumption that ISPs have privileged access to web activity is not factual.<sup>11</sup> Identifiers that function like UIHD can be added and are added to HTTP data streams by websites as easily as they can be added by ISPs. User identification is a basic function of web cookies, IP addresses, and user account names. And unlike ISP-visible objects, web cookies function across platforms and devices. Users of a particular browser, such as Chrome, access the same cookies across desktops, laptops, tablets, and smartphones, whether connected by wired residential ISPs, business ISPs, or mobile ISPs. So the NPRM's claim that ISPs have greater visibility and control over user web information is the polar opposite of the truth.

### **Commercial Value of User Activity Information**

The core issue that underlies the NPRM is the structure of the marketplace for web preference data. By discarding the goal of harmonizing ISP data practices with the FTC framework, the NPRM seeks to exclude ISPs from full participation in this market. Thus, the mantra "competition, competition, competition" is not operative in this context. Rather, incumbent suppliers of advertising, web analytics, and preference data retain a privileged position. Consequently, the status quo remains intact and consumers are denied the benefits that come from competition.

The chief goal of advertisers is the presentation of ads to potential customers in such a way as to influence buying decisions. Therefore, advertisers seek to create preference models for Internet users that will allow them to align ads with users' interests.

Preference models are often very crude. In my experience, Internet purchases over a certain dollar value from Amazon following a Google search will automatically cause advertisers to show me ads for the item I just purchased for a week or more. In fact, simply searching Google for shopping information and then visiting websites that show up in Google web search or shopping search will elicit ads for as much as two weeks.

In some instances, the very vendor who sold us an item will continue to show ads for said item following the purchase. This is a system failure that extracts fees from vendors and enriches advertising networks in an unreasonable way, of course. This privacy enquiry will go down as a failure if it makes such unproductive (and annoying) ads more common.

Access to CII does not have to be an anarchic free-for all, but the policies that govern its collection and use should be consistent across the board. The NPRM's claim that ISPs are uniquely capable of harvesting CII is not factual and therefore can't be used as a justification for disparate regulation of firms with access to CII.

---

<sup>11</sup> See Tom Wheeler, "Statement of Chairman Tom Wheeler Re: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106." (Federal Communications Commission, March 31, 2016), "Our ISPs handle all of our network traffic. That means an ISP has a broad view of all of its customers' unencrypted online activity – when we are online, the websites we visit, and the apps we use. If we have mobile devices – and I have had a mobile device since 1983 – our providers can track our physical location throughout the day in real time. Even when data is encrypted, our broadband providers can piece together significant amounts of information about us – including private information such as a medical condition or financial problems – based on our online activity" and NPRM ¶39 on UIHD.



The question that the NPRM should have asked, but didn't, concerns the market conditions necessary for the development of interest-based advertising. Quite simply, the NPRM should have asked what policies should be applied to ISPs to hasten the rise of accurate interest-based advertising for users who want it. The related question, of course, is what policies will prevent those who don't want interest-based advertising from seeing it.

By choosing for us, the NPRM has the prevention side of the equation covered, but that's not the reality that Internet users inhabit. We understand that trading personal information can open up new venues and new services to us. We want to be empowered to choose the paths we want, not those that the NPRM dictates to us.

### **The Research Value of User Activity Information**

Nearly as importantly, the technology known as "Big Data" takes a hit as well. By adopting a discriminatory approach predicated on paranoia, the NPRM delays the Big Data revolution that will ultimately improve our lives by allowing researchers, scientists, and public policy analysts insight into developing trends. The NPRM's dismissal by omission of the benefits and requirements of Big Data – and the related issues of anonymization, aggregation, and protection of large data sets – is deeply disturbing. The term "big data" is relegated to the footnotes of the NPRM and only mentioned once in the main text.<sup>12</sup>

I'm not going to offer a treatise on the benefits and hazards of Big Data – the NPRM's unreasonably short time line precludes thoughtful discussion – but I will mention the term and suggest that the NPRM can be greatly improved by recognizing the opportunity it represents.

### **Specific Questions**

The NPRM seeks comment on some 500 questions but fails to allow time for thoughtful and reasonable replies because, apparently, the author already knows the correct answers. Many of the questions can be answered quickly and sensibly by simply applying the taxonomy provided in Table 1. I provide the following non-exhaustive list of definitions by way of illustration.

¶20 asks whether the FCC needs to provide additional protection to sensitive data by invoking Section 222. Sensitive data falls outside the CPNI category and therefore should be governed the same way for all parties with access to it.

¶24 asks whether ISPs of different technology types should be harmonized. But the more intelligent question is whether all platforms should be harmonized. The answer to that question is yes.

---

<sup>12</sup> See NPRM ¶36, "At least some of the concerns we identified above in regard to BIAS customers are not unique to BIAS; voice customers in today's world of big data face similar issues related to the protection of their own private information when they apply for and after they have terminated service."

¶27 asks a series of 10 questions on regulations and processes for ISP regulation. The answers to these questions are present in the current FTC Privacy Framework. As the the FCC has previously declared an intent to harmonize with the FTC framework, the only issue with these 10 questions is simply how to harmonize them. It's worth noting that the FTC approach includes a process element that seems to have escaped the NPRM's notice.

It's not enough to impose regulations from on high that capture the regulator's imperfect understanding the Internet marketplace. Because the Internet is a dynamic system (unlike the PSTN), Internet regulations are closely coupled with multi-stakeholder process. The same process that applies to the FCC's favored enterprises should apply to disfavored ones, the ISPs.

¶34 asks if customers and consumers are the same. The focus of personal data is the person and the firms who collects the data, not the firms that provides first mile connectivity but collect and distribute no personal information, such as employers and coffee shops.

¶38-40 seek a new definition of CPNI, which I provided in my discussion of the privacy taxonomy. CPNI is not a bludgeon to be used arbitrarily.

¶41 incorrectly classifies geolocation, IP addresses, and domain names as CPNI. This is irrational because this information is available to websites and other Internet applications by the nature of the Internet. Without the sharing of IP addresses there is no communication across the Internet.

¶42 seeks to create a rationale for classifying service characteristics such as "type of service (e.g., fixed or mobile; cable or fiber; prepaid or term contract), speed, pricing, and capacity (including information pertaining to data caps)" as CPNI. But some of these properties are easily discoverable by websites because they're commonly communicated by browsers to web servers, others (such as speed) are easily discoverable, and the remainder (wired or wireless, data limits) are important for tailoring purposes by web services. Netflix used its estimates of data limits to control streaming speeds, for example. So why does the NPRM go on this fishing expedition when any restriction on this information only makes the Internet less functional? And no, these parameters are not CPNI.

¶44 quite imaginatively equates MAC addresses with International Mobile Station Equipment Identity (IMEI): "A MAC address uniquely identifies the network interface on a device, and thus uniquely identifies the device itself (including the device manufacturer and often the model); as such, we believe it is analogous to the IMEI mobile device identifier in the voice telephony context." Unfortunately, this analogy overlooks the function and visibility of MAC addresses.



Unlike IMEI, MAC addresses can be randomized by non-technical users as their only function is to identify sources and destinations within a local area network.<sup>13</sup> Unlike IMEI, MAC addresses do not travel outside the local network. The only MAC address the ISP sees is the one assigned to the home router. If the home router is supplied by the ISP, the MAC addresses currently in use by non-randomizing devices are visible, but they are not communicated upstream.

MAC addresses are not device identifiers in any case; they are interface identifiers, and any computer with both an Ethernet and a Wi-Fi interface has more than one MAC address. And the NPRM's claim that "...BIAS providers use MAC addresses to route data packets to the end user..." is simply not correct. MAC addresses are non-routable, and all routing decisions are made on the basis of the IP address.

So the router's Ethernet MAC address is CPNI but the MAC addresses of other devices are not.

¶45 corrects the error of ¶44 by declaring IP addresses "routable addresses." Bravo. But it goes downhill from there, declaring the IP addresses used by web services to answer user requests CPNI that presumably cannot be shared with web services without affirmative consent by the ISP customer. This will not work.

The additional presumption that IP header signals "the "type" and "amount of use" of a telecommunication service" is absurd. The IP header simply indicates a protocol type necessary for proper treatment of the payload embedded in the IP datagram as well as fragmentation information necessary for reassembly by the receiving host. This information has nothing to do with any service type; the service is IP routing regardless of the header content. The IP header also contains information that is meant to be used for service differentiation (the IntServ and DiffServ fields) but the Open Internet order declares service differentiation presumptively unlawful. If such information were permitted, the service endpoint would need to use it in order to communicate with the ISP customer, so it can't very well be considered CPNI.

¶47's traffic statistics are easily visible at any point on the Internet: transit networks have them, web services have them, and it's impossible to diagnose and manage network devices without them.

¶48-55 go on another fishing expedition to prevent ISPs from sharing information that is freely shared by other Internet services. These paragraphs take a memo published by CDT in January as gospel and misconstrue the nature of (1) port information; (2) application headers; (3) application usage; and (4) CPE information.<sup>14</sup> Ports are properties of transport protocols such as TCP and UDP.

---

<sup>13</sup> Huitema, "MAC Address Randomization in Windows 10," *Christian Huitema*, December 31, 2015, <https://huitema.wordpress.com/2015/12/31/mac-address-randomization-in-windows-10/>.

<sup>14</sup> Richard Bennett, "CDT's Diagram Muddies the Waters," *High Tech Forum*, accessed May 27, 2016, <http://hightechforum.org/cdts-diagram-muddies-the-waters/>. Center for Democracy and Technology,

As the ISP service is IP transport, ports have no significance for the telecommunication service. Ports harmonize transport streams to processes in the end user and end service computers, and information processing activity that has no telecommunication significance. Treating matters local to computer operating systems as CPNI makes no technical sense given that at least one of the cooperating operating systems is not controlled by an ISP customer.

The information discussed in ¶48-55 is encrypted by websites that choose to use TLS encryption and by users who employ VPNs, so it's only visible to ISPs when users choose services that share it. WebMD shares ports and application header with ISPs, but high reputation medical websites such as MayoClinic.org do not. Customer choice of websites plays a significant role here.

¶59 asks about harmonizing old and new CPNI rules, ignoring the larger and more important problem of harmonizing new CPNI rules with the FTC framework. If the FCC sticks to the real problem, new regulations for old telephone service are unnecessary. The same can be said of the PII discussion in ¶60-66.

¶67 seems to be confused about the fact that the IP payload details discussed in the previous (¶48-66) paragraphs relate to the “content of customer communications.” There is no need to ask the same questions multiple times.

Internet users have fundamentally different expectations about privacy than PSTN users do. The Internet is fundamentally a medium for publishing: Users offer status updates and comments to Facebook with the expectation of being seen by anonymous other users. To do the things we do on the Internet over the PSTN, we would need to dial random numbers and deliver canned messages as robo-callers do. Rather than attempting to shoehorn the Internet experience into the PSTN model, the FCC should recognize the unique nature of the Internet and treat it accordingly.

Section III.A.8, *Defining Opt-Out and Opt-In Approval*, engages in legal maneuvers based on the NPRM's faulty use of CPNI to justify a different consent standard to CII than the FTC requirements. Opt-in should be used to secure access to sensitive data, not to data that is commonly shared by default in a system that allows customers to withdraw implied consent at any time. The approach taken in ¶69-70 is discriminatory, unfair, and inconsistent with prevailing norms and customer expectations.

Similarly, Section III.A.9, *Defining Communications-Related Services and Related Terms* proposes to use Section 222 to limit ISP access to personal information. ¶71-73 have the same flaws as the preceding section.

---

“Applying Communications Act Consumer Privacy Protections to Broadband Providers,” n.d., [https://cdt.org/files/2016/01/2016-01-20-Packets\\_Layers\\_fnl.pdf](https://cdt.org/files/2016/01/2016-01-20-Packets_Layers_fnl.pdf).

As other commenters have observed, ¶74-77 misconstrue the FTC approach to aggregate PI.<sup>15</sup>

¶79 apparently seeks to impose special ISP-like restrictions on the use of information by customer-owned equipment: “Would “premises of a person” include Internet-connected devices carried outside one’s home or office?” This is a peculiar question. Premises are particular physical locations, and not all locations are within the FCC’s jurisdiction; other countries, for example. I have to question the assumption that Title II should apply to all devices a US customer owns, regardless of their location. This ill-considered paragraph should be deleted.

### Conclusion

This analysis merely covers a part of the definitions section of the NPRM, and much mischief follows. The definitions are sufficiently defective that the remainder of the NPRM does not warrant detailed examination. The NPRM incorrectly construes the boundary between legitimate CPNI, Common Internet Information, and information hidden from ISPs.

This misconstruction appears to stem from reports conveyed to the Commission by advocates for strict regulation of ISP privacy practices and loose regulation of Internet advertising networks and other services such as search, email, operating systems, mobile platforms, analytics, and browsers.

One such report is *What ISPs Can See* by Upturn.<sup>16</sup> Upturn claims that “truly pervasive encryption on the Internet is still a long way off” in order to urge the Commission to adopt relatively permanent restrictions on ISPs that would probably persist long after truly pervasive Internet encryption is the norm.

It even argues that the fact that 70% of Internet traffic is already encrypted doesn’t undercut its assertion because data volume doesn’t equate to some other measurement of information flow such as the existence of rarely visited websites. According to this rubric, a tree in a forest where nobody goes makes a sound even if it doesn’t fall.

This is not the correct way to examine pervasiveness. As the NPRM points out, Internet users have choices. If WebMD chooses not to encrypt its medical information website but MayoClinic.org does, consumers of medical information have a choice about encryption.

Similarly, if Google, Amazon, Facebook, and Netflix choose to encrypt – as they do – then consumers of search, shopping, social networks, and video streaming have a choice. If privacy is valuable to consumers, as it sometimes is, then there is no crisis on the Internet of today that should strangle the Internet of tomorrow under a mountain of red tape and discriminatory regulation.

---

<sup>15</sup> Leibowitz, “Re: Protecting the Privacy of Broadband and Other Telecommunications Services, WC Docket No. 16-106.”

<sup>16</sup> Upturn, “What ISPs Can See,” March 2016, <https://www.teamupturn.com/reports/2016/what-isps-can-see>.

Internet of Things devices are often lax about security and encryption. But this is a new ecosystem that has not fully matured, so present conditions are no indication of future performance. Even within this sector firms are beginning to use security as a marketing point: Apple touts the ability of its HomeKit ecosystem to “Securely control your home right from the palm of your hand.”<sup>17</sup> In order to receive HomeKit certification, device manufacturers must demonstrate an above-average degree of security:

*When they positioned themselves for a bid to gain significant traction in the smart home/home automation market Apple put a heavy emphasis on security as that is one of the primary concerns consumers have in regard to putting network-enabled devices in their home: be it light bulbs, security cameras, or thermostats.*

*As such, both to fend off real threats and the imagined threats that keep consumers awake at night, Apple significant security upgrades in the HomeKit platform that far surpass the simple (or even non-existent) security protocols found on other home networking hardware. Where many companies fail to secure their products at all or use simple 128-bit encryption, all HomeKit certified hardware includes a dedicated security co-processor paired with 3072-bit keys and the very secure Curve25519 key exchange system (which is an encrypted key exchange system layered over the already strong 3072-bit key itself).*

*If a device is missing the requisite hardware, keys, and Apple certification then it simply isn't eligible to join your house's HomeKit universe.<sup>18</sup>*

The increasing security of the Internet will resolve the visibility problems the NPRM assumes to be permanent features of the Internet. In fact, this is likely to happen long the court challenge that will inevitably result from the NPRM is resolved.

As long as technology is increasingly protecting privacy and ISPs have less ability to perceive sensitive user data than advertising networks, browsers, and other platforms do, there is no rational justification for adopting a one-sided privacy framework.

The FCC should scale back its definition of CPNI and harmonize its privacy regulations with those of the FTC.

---

<sup>17</sup> Apple, “iOS 9 - HomeKit,” accessed May 28, 2016, <http://www.apple.com/ios/homekit/>.

<sup>18</sup> Jason Fitzpatrick, “HTG Explains: Why Does Apple’s HomeKit Require All New Hardware?,” *How-To Geek*, October 26, 2015, <http://www.howtogeek.com/232235/htg-explains-why-does-apples-homekit-require-all-new-hardware/>.