

To: Mr. Tom Wheeler, Chairman, FCC
Ms. Mignon Clyburn, Commissioner
Ms. Jessica Rosenworcel, Commissioner
Mr. Ajit Pai, Commissioner
Mr. Michael O'Rielly, Commissioner

CC: Commission's Secretary, Office of the Secretary, Federal Communications Commission

From: Dr. Paul Vixie, CEO and Chairman, Farsight Security, Inc. <vixie@fsi.io>

Date: May 1, 2016

Subject: Comments on "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," FCC 16-39 (WC Docket No. 16-106),
http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0401/FCC-16-39A1.pdf

Dear Chairman Wheeler and FCC Commissioners Clyburn, Rosenworcel, Pai and O'Rielly:

It is our pleasure to offer Farsight Security's comments on the above captioned Notice of Proposed Rule Making (NPRM).

I. CONTEXT FOR THESE COMMENTS

Our company: Leveraging our deep Domain Name Systems (DNS) expertise, Farsight Security offers real-time Passive DNS solutions that provide critical context to significantly increase the value of prepackaged reputation & threat feeds, and other threat intelligence. The availability of timely and relevant security-related data is the key to establishing tactical superiority in any cyber engagement. The entire Farsight Security organization is focused on increasing the availability, variety, volume, quality, breadth, and relevance of the network telemetry data we deliver. Our coordinated efforts allow our customers to increase the variety and effectiveness of their network protections and countermeasures, which can now often even be deployed before attacks are initiated against them. At Farsight Security, we are committed to finding new ways to secure the world's digital infrastructure while *fully respecting and protecting the privacy of all law-abiding Internet users*. More information about Farsight Security, Inc. can be found online.¹

My background: I am Paul Vixie, the Chief Executive Officer and Chairman of the Board of Farsight Security, Inc. I've previously served as President, Chairman, and Founder of Internet Systems Consortium (ISC), as President of MAPS, PAIX and other businesses, as CTO of Abovenet/MFN, and serve on the boards of several for-profit and non-profit companies.

I have previously served on the ARIN Board of Trustees, including serving as Chairman in 2008 and 2009, and I am a founding member of ICANN Root Server System Advisory Committee (RSSAC) and ICANN Security and Stability Advisory Committee (SSAC). I operated the ISC's F-Root name server for many years, and I am a member of Cogent's C-Root team. I'm also a sysadmin for a leading industry cybersecurity information sharing forum, OpSec Trust.

I've been contributing to Internet protocols and UNIX systems as a protocol designer and software architect since 1980. I wrote Cron (for BSD and Linux), and am considered the primary author and technical architect of BIND 4.9 and BIND 8, and I hired many of the people who wrote BIND 9. I've authored or co-authored a dozen or so RFCs, mostly on DNS and related topics, and wrote *Sendmail: Theory and Practice* (Digital Press, 1994). My technical contributions include DNS Response Rate Limiting (RRL), DNS Response Policy Zones (RPZ), and Network Telemetry Capture (NCAP). I earned my Ph.D. from Keio University for work related to DNS and DNSSEC, and was named to the Internet Hall of Fame in 2014.

This broad technical- and Internet governance-related background, and my roles leading innovative and successful Internet tech companies, gives me an expert's perspective from which to review and comment on the Commission's new proposed privacy rules for Broadband Internet Service Providers.

The remarks below are offered in my capacity as Farsight CEO and Chairman of the Board, and reflect both my own personal perspective on these matters and Farsight Security, Inc.'s official company perspective.

Structure of comments submitted: Because the NPRM is 101 page long (in addition to 32 pages of appendices and 14 pages of Commissioner statements), and has 492 footnotes, and to avoid any ambiguity or confusion, these comments have been **keyed** to the NPRM-provided paragraph numbers. Where necessary, we've included relevant excerpts from each applicable paragraph to help establish context for our remarks.

We have chosen to not address all questions raised in the NPRM. Where we're silent on a particular paragraph or question, please interpret that silence as being reflective of "no comment" rather than either tacit approval or tacit rejection of that material.

Comments on the document are offered in the sequence topics were introduced in the document, rather than according to their importance.

II. COMMENTS

The substantive content in the NPRM begins with definitions, and as is often the case, those definitions are of critical importance to framing and scoping the proposed regulations. We have feedback regarding a number of them.

"Broadband Internet Access Service" (BIAS) defined.

In NPRM **paragraph 29**, BIAS is defined to mean

[a] mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up Internet access service. This term also encompasses any service that the Commission finds to be providing a functional equivalent of the service described in the previous sentence, or that is used to evade the protections set forth in this part.

Transport is, and should be, irrelevant: The proposed definition explicitly includes "wire" or "radio" transport, explicitly excludes dialup Internet access service, and is silent on other transport technology (such as fibre or satellite transport).

We appreciate the regulatory rationale for this specific definition, but believe that the average Internet user would be baffled by your NPRM's scoping. Assume that an Internet user may connect via...

- a cable provider such as Xfinity,
- a DSL service such as CenturyLink,
- an optical fiber provider such as Verizon's FIOS,
- via metro Ethernet,
- through a wireless broadband provider,
- via a satellite Internet service,
- by dialup,
- or by other means.

In all cases, the user accesses the "same" Internet. By differentiating solely based on **transport**, with some connections covered by the draft privacy policies and others not, you're creating an incomplete and inconsistent "patchwork quilt" of privacy protection rather than establishing a trustworthy and fully inclusive bedrock foundation for Internet privacy that protects users wherever and however they may choose to access the Internet. Whether fast or slow, wireline or wireless, fixed or mobile, users of any "mass-market" Internet Access Service (IAS) should be able to have consistent privacy expectations and consistent privacy protections.

Is the "Broadband" In "Broadband Internet Access Service" important? If it is the Commission's intent is to exclude dialup Internet Access Services due to the **low realized speeds of such services**, we'd urge you to explicitly make that clear, and to call out the relevant threshold throughput level for "broadband" Internet Access Service (whether that's 25Mbps down

or something else). Please avoid focusing just on the transport technologies used! It would be kin to a water district regulating drinking water carried in PVC pipe but excluding water carrier in copper or cast iron, and that's crazy talk.

There are BIAS provider-like roles performed by educational institutions, libraries, and other non-commercial ISPs, and their users deserve privacy, too. We also urge the Commission to explicitly recognize the Broadband Internet Access Service-like function performed by some non-"retail" entities, such as K12 schools, colleges, universities, etc. These entities provide ISP-like service for what may be thousands or even tens of users, and as such they should be required to provide BIAS-equivalent privacy protection for their users given their BIAS-like functional role. ("If an organization acts like an BIAS, it should be treated as such.") We urge you to explicitly clarify this point in the final rules.

"Affiliate" defined. In **paragraph 30**, the Commission provides a proposed definition of "affiliate" envisions a business entity that's comparatively **closely tied** to the BIAP:

[...] a person that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with, another person," where the term "own" is defined to mean "to own an equity interest (or the equivalent thereof) of more than 10 percent."

The common understanding of "Affiliates" does not compote with the FCC's definition: These days, "affiliates" (a the term now entrenched in the popular lexicon) are routinely assumed to be **loosely connected independent contractors** who are compensated for their performance in helping to market a product or service online:

- an "rev share" affiliate might get a share of the revenue resulting from customers who subsequently make a purchase
- a "pay per click" (PPC) affiliate might get payments from online advertisers for customers "clicking through" to a product offer page
- a "pay per impression" (PPI) affiliate normally is paid for displaying advertising to visitors surfing his web pages,
- etc.

Using the term "affiliate" as the NPRM currently proposes to do is inconsistent with the colloquial use of that term, and thus risks becoming a potential source of confusion. For clarity, that term should be replaced with a less-ambiguous term more reflective of the relationship the NPRM envisions, such as "subsidiary business" or "co-owned subordinate business" rather than using the vague and overloaded generic term "affiliate."

"Customer" Defined. **Paragraphs 31, 34 and 35** attempts to clarify who is a "customer." The NPRM states that:

We propose to define "customer" to mean 1) a current or former, paying or non-paying subscriber to broadband Internet access service; and 2) an applicant for broadband Internet access service.

Setting aside the fact that merely applying for service (while not actually having consummated that relationship) is taken as being sufficient to trigger "customer" status, there are others who actually use a BIAS provider's services who are NOT clearly covered by that definition.

Broadband Connections Are Routinely Shared: While there is always a single person who is the "subscriber"/"account-holder-of-record" for a commercial ISP, a broadband Internet connection will commonly be shared, used by many users beyond just the single account-holder-of-record:

- In the case of a residential connection, "other users" will often include household members, such a spouse or intimate partner, children, extended family members, visiting friends, etc.
- In the case of a small business (such as a coffee shop) purchasing Internet access for customer use, other users may literally number in the hundreds

-- In the case of a K12 school, university, or public library, any of which may end up acting in an "BIAS Provider"-like capacity, "other users" may include thousands of staff, students, and visitors who are provided access.

Even mere "additional" users should always have a right to privacy online. Additional users are NOT the "subscriber" or "account-holder-of-record" for the connection they're using, but they may nonetheless originate or receive privacy-sensitive information over the Broadband Internet Access Network. Authorized non-subscriber users of a shared network connection deserve the right to control how (or if) their privacy-sensitive data gets collected, shared and used, and any failure to acknowledge that reality undercuts the privacy regime envisioned by this NPRM. We therefore urge the Commission to explicitly recognize the legitimate privacy rights of users other than the account-holder-of-record, even if these other users are merely secondary or occasional network users.

Does "someone" "have" to be "the decider?" As a pragmatic matter, the account-holder-of-record will often be deemed to be the responsible "decision maker" for all who may receive access via the account holder's connection. Those responsibilities including having *de facto* responsibility for unilaterally making privacy-related choices on behalf of everyone using his/her connection. This policy is consistent with the traditional "their network, their rules" approach, sometimes presented as "take it or leave it" terms of use. However, [paragraph 258](#) of the NPRM discusses "take it or leave it" approaches, and proposes to prohibit that approach, at least in the case of any BIAS provider's "take it or leave it" options. How can the Commission prohibit a "take it or leave" regime for BIAS providers, yet implicitly allow it in the case of additional users?

The impossibility of disentangling comingled traffic? Of course, from a technical point of view, given current architectures, it may be difficult or impossible for a provider to distinguish traffic sourced by one user from traffic sourced by another user, particularly if NAT/PAT is employed and if deep packet inspection is forbidden (as the Commission appears to recommend later in the NPRM).

The conservative default option: deliver maximum privacy for ALL users. The realities of current hierarchical network architectures means that there may only be one realistic option when it comes to shared connections and privacy: all users must be assumed to want maximum privacy by default, unless per-person opt-outs from that maximum privacy regime can be technically supported.

Privacy for Legal Persons As Well As Natural Persons? The Commission should also explicitly clarify their intent *vis-a-vis* natural persons vs. legal persons (such as corporations). Is the intent that both legal and natural persons should enjoy the same full measure of privacy protection? (That would certainly be our recommendation).

Specifically Define NON-Customers, Too: We also recommend that the Commission create a bright line definition of who's NOT a "customer" for privacy-related purposes, explicitly declaring that **cyber intruders** and other **unauthorized users** of a BIAS shall **NOT** be considered to be "customers," and as such should have no expectation of privacy, whether from the BIAS provider or from any other party.

Definition of CPNI. The NPRM proposes a definition of "Customer Proprietary Network Information" (CPNI) in the context of BIAS, at [paragraphs 38-47](#) 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**" and "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer or a carrier," except that CPNI "does not include subscriber list information" [emphasis added]

For the purpose of the following discussion, we exclude discussion of billing and subscriber list ("telephone directory") information, and focus solely on the first part of the proposed definition.

In analyzing what's appropriately categorized as CPNI for the purpose of a BIAS provider, we urge the Commission to narrowly define that category of information consistent with:

- The plain meaning of the name for this category of information
- The extent to which the purportedly confidential information is actually non-public and not readily inferable
- The potential for *actual* harm if the nominal CPNI were to be disclosed, and
- The "direction" of the information sharing involved (that information flow must be from the customer to provider, and not vice versa)

We now elaborate on these points:

Root of the term "proprietary information:" The term "proprietary information" has its roots in the word "property," specifically the valuable non-public information of an entity used for competitive advantage. In business, for example, proprietary information might be a secret technique or approach that allows a company to manufacture a product or deliver a service that's better, more economical, or otherwise superior to its competition. By contrast, random facts are not "proprietary information," even if little known.

An example: should "mass market broadband pricing and capacity information" be CPNI? These items are suggested in the NPRM as being examples of CPNI, but even a cursory analysis reveals that the pricing and the data cap levels of mass market broadband products are standardized and widely shared by providers with potential customers and the public at large. As such, that information can hardly be considered to be "non-public." Moreover, no harm to *customer* interests occurs if that information is shared with third parties. Finally, the pricing/data cap information (created by the provider, after all) is shared by the provider to the customer rather than vice versa. Clearly this is an example that fails any reasonable test for being CPNI.

What about Service Plan information, including type of service (e.g., cable, fiber, or mobile)? Service plan information is jointly agreed upon between the provider and the customer, and may even be predetermined and non-confidential because a provider might only *offer* a single type of service. Again, there is no functional justification for treating BIAS provider service plan information as CPNI.

Service tier (e.g., speed)? Is that an attribute properly categorized as CPNI? Unlike poorly instrumented or un-instrumented POTS or cellular networks, Internet packet networks are often extensively instrumented by users, and thus are subject to empirical investigation. A researcher or other well-instrumented party can easily acquire information about an ISP customer's realized connection speeds, as has been well demonstrated by projects such as Ookla's SpeedTest.net, and the FCC's own Speed Test App. This is **not** "secret" information. Moreover, because the BIAS provider ultimately controls the speed the customer is allowed to have, the information flow of the nominal CPNI is going in the "wrong" direction, from the provider to the customer, rather than vice versa. Service tier information should NOT be treated as CPNI.

Geo-location? We agree that geo-location data is potentially highly sensitive, however the illusion that if the provider just doesn't "play along" and provide it, that location cannot be determined, is dangerously incorrect. Geo-location can be inferred with reasonable specificity by triangulating network latencies; thus, this is not information that's exclusively available to the provider by virtue of a 'carrier-customer relationship.' As such, it, too, fails to deserve treatment as CPNI.

Media access control (MAC) addresses and "other device identifiers"? Providers will normally only see the layer 2 (MAC) address for the provider/customer-demarkation-point device, typically a combination broadband "router"/wireless access point. The MAC address of that device, like any MAC address, is provided to facilitate creation of layer 2 adjacencies and traffic flow between the provider's switch and the account-holder-of-record's broadband router. Where we disagree with the Commission is in our assessment of the sensitivity of that information. We do NOT agree that knowledge of a customer's MAC address is "proprietary" information (it is basically just a "random fact").

What About IPv6 SLAAC addresses using embedded Modified EUI-64 identifiers: CPNI? As we cast about looking for an instance where MAC addresses are "more than just a random fact," the most promising circumstance is likely the use of modifier EUI-64 identifiers in IPv6 SLAAC (stateless autoconfiguration) addresses. Modified EUI-64 addresses are derived from a MAC addresses, and are mechanically translatable back into a MAC address by simple packet surgery. A description of this process involved in forming a modified EUI-64 address from a MAC address is available in Wikipedia.²

We'd note, however, that privacy-conscious users need not rely on a SLAAC address. They can use an IPv6 privacy address, instead, created precisely to preclude any need or MAC addresses to be potentially shared. As such, it is hard to get very discomfited by the thought of sharing IPv6 SLAAC addresses since no one really needs to use them unless they want to do so.

Source and destination Internet Protocol (IP) addresses? In **paragraph 45** the NPRM states:

We propose to consider both source and destination IP addresses as CPNI in the broadband context. **An IP address is the routable address** for each device on an IP network, and BIAS providers use the end user's and edge provider's IP addresses to route data traffic between them. As such, IP addresses are **roughly analogous** to telephone numbers in the voice telephony context, and the Commission has previously held telephone numbers dialed to be CPNI. Further, our CPNI rules for TRS providers recognize IP addresses as call data information. **IP addresses are also frequently used in geo-location.** As such, we believe that we should consider IP addresses to be "destination" and "location" information under Section 222(h)(1)(A). Similarly, we propose to consider other information in Internet layer protocol headers to be CPNI in the broadband context, because they may indicate the "type" and "amount of use" of a telecommunication service. We seek comment on this proposed interpretation.

First key point: most IP addresses are *assigned by the provider to the customer, whether via DHCP or as a static IP*. As such, that data flows the "wrong way" (from the provider to the customer rather than vice versa) to be considered CPNI.

Second key point: all IP addresses are **not** alike:

Some IP addresses aren't routable. While the proposed definition declares that "An IP address is [a] **routable** address [...]," not all IP addresses are, in fact, routable. RFC4193 IPv6 ULA (unique local address) and RFC1918 IPv4 private address space addresses are, by definition, **not** publicly routable. RFC1918 IPv4 private addresses and RFC4193 IPv6 ULAs should be excluded from any definition of CPNI.

Ditto for the **loopback address block** (127.0.0.0/8): these should be excluded from any definition of CPNI.

Some addresses are only meaningful when combined with other data. For example, dynamic IP addresses (as assigned by a DHCP server) may be used by many different customers over the course of a day. Even the ISP itself requires an IP address PLUS a **time stamp** to be able to accurately map a dynamic IP to the identity of the customer using that IP at a given time. Another example of this phenomena can be seen in the case of so-called "carrier grade NAT" addresses where mapping an IP to a customer requires not just the IP and time stamp, but also the **port number** information. Without an IP address, port number and accurate time stamp, a "carrier grade NAT" IP address cannot be mapped to an individual customer.

A third category of atypical addresses would be those intentionally meant to preserve the user's privacy. The canonical example of this would probably be IPv6 privacy addresses. These addresses are explicitly structured to make it difficult or impossible to persistently track users over time. There is little long term value to considering IPv6 privacy addresses as potential CPNI, either.

Third key point: if a provider is prohibited from "disclosing" a customer's IP address to third parties, how will networking work? Providers need to be able to work with IP addresses for the Internet to work!

We assume (but are only speculating) that you mean to say providers are forbidden from disclosing the fact that a particular IP address is associated with a particular user. If so, however, what about static IP addresses? We think a much more carefully-written description of specific constraints around IP address disclosure should be prepared, if this restriction is needed at all.

Should domain names be considered CPNI? We believe that domain names should **not** be considered CPNI. At **paragraph 46** of the NPRM, the Commission states that:

Similarly, we propose to consider the domain names with which an end user communicates CPNI in the broadband context. Domain names (e.g., "www.fcc.gov") are common monikers that the end user uses to identify the endpoint to which they seek to connect. **Domain names also translate into IP addresses, which we propose to consider CPNI.** We therefore propose to treat domain names as destination and location information. We seek comment on this proposed interpretation. [emphasis added in both paragraphs]

Note that finding domain names to be CPNI depends on the Commission first having found IP addresses to be CPNI. We've already explained why we believe IP addresses to NOT be CPNI, but in the case of DNS, further arguments pertain.

Unlike MAC addresses or IP addresses, at least some of which are employed in providing connectivity to the customer, domain names are able to be totally anonymized by the end user if he or she is concerned about the privacy of that data. For example, some user may create an encrypted VPN tunnel to a third party of their choice, tunneling all their traffic -- including their DNS query and response traffic -- "opaquely" past their BIAS provider to their third party VPN provider. The local BIAS provider would have no ability to decode the traffic flowing over that encrypted tunnel.

If the user elects to share DNS query traffic with their BIAS provider as a matter of convenience, that is certainly their choice, but it should NOT encumber the BIAS providing customer recursive resolver service that's provided as a courtesy.

In the alternative, if DNS query traffic is CPNI, third part providers of recursive resolver capabilities (such as Google's famous 8.8.8.8 and 8.8.4.4) should be subject to the same privacy requirements as pertain to BIAS providers -- but they're not, are they?

What about "traffic statistics" as potential CPNI? In **paragraph 47** of the NPRM, the Commission writes:

We propose to consider traffic statistics to be CPNI pertaining to the "type" and "amount of use" of a telecommunications service. We believe that "amount of use" encompasses quantifications of communications traffic, including short-term measurements (e.g., packet sizes and spacing) and long-term measurements (e.g., monthly data consumption, average speed, or frequency of contact with particular domains and IP addresses). We recognize that modern technology enables easily collecting and analyzing traffic statistics to draw powerful inferences that implicate customer privacy. For example, a BIAS provider could deduce the type of application (e.g., VoIP or web browsing) that a customer is using, and thus the purpose of the communication. Further, traffic statistics can be used to determine the date, time, and duration of use, and deduce usage patterns such as when the customer is at home, at work, or elsewhere. We believe traffic statistics are analogous to call detail information regarding the "duration[] and timing of [phone] calls" and aggregate minutes in the voice telephony context. We seek comment on our proposed interpretation.

What sort of "traffic statistics?" The Commission refers to "traffic statistics," but then proceeds to describe everything from macroscopic measurements (most commonly associated with network flow protocols such as Netflow/Jflow/Sflow), to exceptionally fine-grained packet-level measurements (as might be gleaned from use of a network protocol analyzer such as Wireshark). Alternatively, the Commission might be thinking of something as basic as periodically polling and graphing summary SNMP counters with RRDTool.

The sort of measurements actually being discussed matters to a non-trivial degree.

Encryption can effectively defeat fine-grained measurements. For example, if the Commission's focus is on fine-grained packet-level measurements, the ability of BIAS provider to take those sort of measurements can be **totally derailed through customer use of strong encryption**, assuming the provider is not allowed to intentionally interpose himself as a "man-in-the-middle" (MITM).

Thus, it is not necessary to wrap confidential data in the "tissue paper" of potential statutory "protections" against traffic monitoring when private data can be technically "armored" against fine grained traffic measurements with the use of strong crypto.

In fact, because un-encrypted network traffic can be measured **anywhere along the path that that traffic follows**, relying on local/national privacy policies for "protection" against traffic measurement-related exposures means that international network traffic can still be potentially be measured in up to 195 out of 196 countries worldwide. Being "protected" against the risks of fine-grained traffic measurement by national policy in ~1/2 of 1% of all countries is not very comprehensive indemnification.

Use of other network privacy tools can protect against macroscopic traffic measurement risks, too. For example, customers might elect to use a Virtual Private Network, or, alternatively, Tor (a network privacy tool created with U.S. State Department funding) to defeat metadata analysis and macroscopic traffic measurement analyses.

Polled SNMP traffic. Polled SNMP traffic, often graphed with tools such as RRDTool, represents a different sort of "animal." It is very difficult or impossible to avoid the potential collection of SNMP traffic, but this is one of the coarsest granularity measures that may be collected by a BIAS provider. Collection of SNMP octets in/octets out data allows performance and service availability issues to be resolved. Given the potential choice between "operating one's network blind in order to avoid potentially collecting CPNI, or allowing a provider to collect polled SNMP traffic, we'd recommend allowing collection of SNMP traffic every time.

Broadly, for the reasons outlined above, we believe that "traffic statistics" should NOT be considered CPNI.

Exploration of other potential CPNI. In paragraphs 48-52, the NPRM explores other potential CPNI, including "Port Information," "Application Headers," "Application Usage," and "Customer Premises Equipment."

Port information as potential CPNI (paragraph 49). While novice traffic analysts may assume that traffic on port 80 must be web traffic, that naive misconception lasts only through an analyst's first contact with a real traffic capture.

One result of the widespread use of perimeter firewalls is that "everything" seems to tunnel its traffic over port 80. Port numbers have largely gone from reliable clues to the type of application generating traffic seen on the wire to either:

- Everything over port 80, or
- Everything over a random dynamic port.

Neither of those paradigms make for a very useful analytic framework. Competent analysts normally do deep packet inspection instead of relying on port numbers for potentially misleading hints.

Application headers (e.g., as shared by web browsers) as potential CPNI (paragraph 50). These days, all applications should assume that the network is potentially hostile, encrypting application layer traffic. Assuming that is done, there is no need to consider Application Headers as potential CPNI.

Application usage (e.g., profile of applications) as potential CPNI (paragraph 51). Application usage data shows the relative usage of various applications, either measured by apparent port usage (highly unreliable these days), or measured by a deep packet inspection appliance. To the extent that other measurement traffic isn't CPNI (or is CPNI), "application usage" information should be treated similarly. It's just the compilation of individual measurements, and poses no special considerations meriting special consideration in our opinion.

Customer Premises Equipment (CPE) as potential CPNI (paragraph 52). We would distinguish the single device that actually connects to the BIAS provider's network from other "interior" network devices. For example, for a cable Internet service provider, the relevant single device would be the cable modem attached to the provider's coaxial cable. While those devices may be consumer owned or rented from the provider, the information contained on those devices **SHOULD** be normally considered to be CPNI. Interior devices (to include the customer's broadband router/wireless access point and any computers, tablets, smart phones, servers, printers, etc., downstream thereof) should **NOT** be considered CPNI.

Overly inclusive definition of PII. In the NPRM at paragraph 57, the Commission declares:

"As described in more detail below, consistent with well-developed concepts of what constitutes personally identifiable information in the modern world, we propose to define PII to mean any information that is linked or linkable to an individual."

We believe this definition is unnecessarily overbroad. As written, a score from a bridge tournament would potentially be PII, and even data protected with strong encryption would potentially still constitute "PII."

We suggest that a more balanced approach would follow the line employed by the state of Oregon in SB 601 from the 2015 legislative session.³ We quote from that measure, in effect since the first of this year:

(11) "Personal information" means:

(a) [Means] A consumer's first name or first initial and last name in combination with any one or more of the following data elements, if encryption, redaction or other methods have not rendered the data elements unusable or if [when the data elements are not rendered unusable through encryption, redaction or other methods, or when] the data elements are encrypted and the encryption key has [also] been acquired:

- (A) A consumer's Social Security number;
- (B) A consumer's driver license number or state identification card number issued by the Department of Transportation;
- (C) A consumer's passport number or other [United States issued] identification number issued by the United States; [or]
- (D) A consumer's financial account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to a consumer's financial account[.];
- (E) Data from automatic measurements of a consumer's physical characteristics, such as an image of a fingerprint, retina or iris, that are used to authenticate the consumer's identity in the course of a financial transaction or other transaction;
- (F) A consumer's health insurance policy number or health insurance subscriber identification number in combination with any other unique identifier that a health insurer uses to identify the consumer; or
- (G) Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer.

(b) [Means] Any of the data elements or any combination of the data elements described in paragraph (a) of this subsection [when not combined with] without the consumer's first name or first initial and last name [and when the data elements are not rendered unusable through encryption, redaction or other methods, if the information obtained would be sufficient to permit a person to commit identity theft against the consumer whose information was compromised.] if:

- (i) Encryption, redaction or other methods have not rendered the data element or combination of data elements unusable; and
- (ii) The data element or combination of data elements would enable a person to commit identity theft against a consumer.

Applying this principle to the NPRM's [paragraph 62](#) definition would imply at least the following adjustments:

"We propose that types of PII include, but are not limited to: name; Social Security number; date and place of birth; mother's maiden name; unique government identification numbers (e.g., driver's license, passport, taxpayer identification); physical address; ~~email address or other online contact information; phone numbers; MAC address or other unique device identifiers; IP addresses; persistent online identifiers (e.g., unique cookies); eponymous and non eponymous online identities; account numbers and other account information, including account login information; Internet browsing history; traffic statistics; application usage data; current or historical geo-location;~~ financial information (e.g., account numbers, credit or debit card numbers, credit history); ~~shopping records;~~ medical and health information; the fact of a disability and any additional information about a customer's disability; biometric information; ~~education information; employment information;~~ information relating to family members; race; religion; sexual identity or orientation; ~~other demographic information;~~ and information identifying personally owned titled property (e.g., property, vehicle license plates, ~~device serial numbers~~)."

Some of those exclusions (or non-exclusions) bear elaboration.

- Physical address should be treated as PII because it can be used by stalkers or others to physically harm an individual, and it can be difficult or impossible to "unring the bell" once that information has been disclosed, similarly moving to a new physical address can be disruptive and expensive if possible at all.
- Email addresses or other online contact information: routinely shared by the Internet user; should be "directory information" as allowed by other Federal legislation such as FERPA, but subject to mandatory suppression from directory information by individual request.
- Phone numbers: treat as per email addresses.
- MAC addresses, other unique device identifiers, and IP addresses: previously addressed *supra*.
- Traffic statistics, application usage data, current or historical usage data, geo location data: also previously addressed *supra*.
- Cookies should be encrypted in transit, and managed locally by the user on their browser, likewise Internet browsing history should be managed locally by the user, likewise shopping records
- Education, employment, race, religion, sexual identity or orientation, other demographic information: not relevant to BIAS providers.
- Information identifying personally owned property (e.g., license plates, device serial numbers)." -- protect information required to be provided for titled property (such as homes, cars, etc.), but exclude device serial numbers.

Directory Information Defined To Be PII by the NPRM. The NPRM declares in [paragraph 63](#) that:

Other PII Considerations. Consistent with a widespread understanding of what constitutes PII, we propose

to consider a BIAS customer's name, postal address, and telephone number as PII and, consequently, that they are customer PI protected by Section 222(a) in the broadband context. We recognize that because of the unique history of telephone directory information, the Commission has previously treated such information as not falling within the statutory definition of CPNI in the voice telephony context."

We believe this change is a mistake. This information should continue to be directory information, but subject to mandatory suppression if requested by the customer.

Use or Sharing of Contents of Communications. The NPRM in [paragraph 67](#) states: "We do not think that providers should ever use or share the content of communications that they carry on their network without having sought and received express, affirmative consent for the use and sharing of content. We therefore seek comment on whether there is a need to provide heightened privacy protections to content of communications beyond Section 705 and ECPA, and if there is, what additional protections should be provided."

The contents of communications should be protected by strong encryption, thereby rendering this item moot: if strong encryption is used providers will not be ABLE to use the contents of communications, assuming the provider is not allowed to intentionally interpose himself as a "man-in-the-middle" (MITM).

Definition of Aggregate Customer Proprietary Information. In the NPRM at [paragraph 74](#), the Commission states: "We propose to define aggregate customer proprietary information as collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed. [...] We use slightly different terminology to make clear that our proposed rules addressing the use of aggregate customer information are intended to address the use of all aggregate customer PI and not just aggregate CPNI. [continues]"

We re-emphasize for the record that we would substantially contract the items in-scope as customer proprietary information, particularly with respect to CPNI.

However, that said, aggregated data is not necessarily adequately sanitized/private. For example, assume a statistician collects "aggregated" information about alcohol use at a local high school, and surveys all members of the football team. The results are "aggregated," rather than being reported on a player-by-player basis, but the results show that 100% of the players admitted to illegally consuming alcohol within the last ninety days. This is only the most trivial of examples, but nonetheless one that's sufficient to illustrate that "aggregated" data isn't necessarily adequately de-identified.

Definition of Breach. In the NPRM at [paragraph 75](#), the Commission states: "For purposes of our proposed data breach notification requirements, we propose to define "breach" as any instance in which "a person, without authorization or exceeding authorization, has gained access to, used, or disclosed customer proprietary information." Unlike the "breach" definition in our current Section 222 rules, our proposal does not include an intent element, and it covers all customer PI, not just CPNI."

It is not always easy -- or even possible -- to determine what an intruder has accessed when a computer is breached. Under your definition, if a system with multiple types of data (some covered PI, some not), is accessed, and there's no ability to retrace what the intruder accessed or exfiltrated, how is the *potentially-affected* site to proceed? Does it matter if the accessed data has been encrypted, and the encryption keys were not compromised?

Definition of Customer Premises Equipment (CPE). In [paragraph 79](#) of the NPRM, the Commission endeavors to ensure that their definition of Customer Premises Equipment is appropriate for their revised rules. You state: For example, the existing CPNI rules define the term "customer premises equipment" (CPE) to mean "equipment employed on the premises of a person (other than a carrier) to originate, route, or terminate telecommunications." We seek comment whether we should adopt this definition for purposes of the proposed broadband privacy rules. What would be the scope of covered devices under the statutory definition or any alternatives? Would "premises of a person" include Internet-connected devices

carried outside one's home or office? With large numbers of consumer products becoming networked devices (e.g., thermostats, cars, home appliances, and others), are there particular types of uses, activities, or devices that operate over broadband Internet access service that we should or should not include within the definition of CPE? Are there other terms the Commission should define for the broadband privacy context?

As previously expressed in our comments to [paragraph 52](#):

We would distinguish the single device that actually connects to the BIAS provider's network from other "interior" network devices. For example, for a cable Internet service provider, the relevant single device would be the cable modem attached to the provider's coaxial cable. [...] Interior devices (to include the customer's broadband router/wireless access point and any computers, tablets, smart phones, servers, printers, etc., downstream thereof) should **NOT** be considered CPNI.

This single device should serve as a hard demarcation point between the BIAS provider's network and the customer's network.

Alternative Languages. [Paragraph 83](#) touches upon consumer privacy notices, including mentioning that such notices should "Be completely translated into another language if any portion of the notice is translated into that language." That requirement is insufficient given our increasingly polyglot online population.

We propose that BIAS providers should be required to produce translated versions of required privacy notices in all five official languages of the United Nations. Currently that would imply producing versions in Arabic, Chinese, English, French, Russian and Spanish.

Timing and Placement of Privacy Notices. [Paragraph 87](#) of the NPRM states: "We seek comment on our proposal regarding the timing and placement of privacy notices. We believe that by requiring point-of-sale notices and requiring that notices of a BIAS provider's privacy policies be persistently available through a link on the provider's homepage and through its mobile application, gives providers two existing, user-friendly avenues for providing customers with notice of their privacy policies, while also leaving open a technology-neutral, "functional equivalent" option in the event that future innovations in technology offer new and innovative ways to provide customers with transparency.

At the risk of being deemed rather cynical, few customers likely ever visit their BIAS provider's home page, nor are customers likely to use the provider's mobile application. If they do happen to do so, there's a vanishingly small likelihood that they will take the time to review the provider's privacy policy, particularly if it is long or complex.

If you want people to actually at least visit their provider's privacy page, you'll likely need to offer some incentive for them to do so (and even then, they'll likely just make a *pro forma* pass through the document *en route* to getting their incentive, whatever it may be). "You can lead a horse to water, but you can't make it drink."

Format of Privacy Notices. In **paragraph 91**, the Commission states: "We seek comment on whether we should adopt a standardized approach for BIAS providers' privacy notices in this proceeding. Would a one-size-fits-all approach provide clear, conspicuous, and understandable information?"

We favor a consistent privacy notice format for required elements. We would recommend that that standardized template be allowed to be augmented by additional supplemental material that enhances or clarifies the information included in the template.

Paragraph 91 also mentioned: "The study concluded by suggesting that companies could develop shorter, user-facing privacy notices that specifically emphasize those practices where mismatches exist between a company's actual use and disclosure policies and consumers' expectations."

We support clear and concise privacy notices, and really like a "management-by-exception"-like approach that clearly emphasizes points of departure from normative behaviors.

Accessible Formats. In **paragraph 93** of the NPRM, the Commission stated "What is the best way to ensure that BIAS providers are able to convey this privacy policy information in accessible formats, like ASL?"

We'd note that most deaf or hard of hearing adults who use American Sign Language are usually also able to read written English materials, so there's not necessarily a need to translate privacy policy information into ASL (although please contact the National Association of the Deaf for a definitive statement from the deaf community on this point).

Similarly, you may want to inquire as to accessible formats for the blind, whether that's a screen-reader-compatible written format, a recorded audio format, a printed Braille edition of the policies, or something else.

Marketing of Additional BIAS Offerings In The Same Category of Service. At **paragraph 114**, the FCC states: "We also propose to adopt rules permitting BIAS providers to use customer PI for the purpose of marketing additional BIAS offerings in the same category of service (e.g., fixed or mobile BIAS) to the customer, when the customer already subscribes to that category of service from the same provider without providing the opportunity to provide opt-out or opt-in consent."

This is an incredibly offensive provision that denies consumer any choice or control whatsoever with respect to their BIAS provider. It is very disappointing to see this provision shoe horned into this NPRM.

A customer should NOT be compelled to accept marketing materials from anyone without an ability to control that messaging. We'd strongly support customer choice, and believe that each customer should be asked if they'd like to receive marketing communications at the time they become a customer. The default can be set to "no," or left unmarked by default (requiring the consumer to make an affirmative choice), but should NOT be set to "yes" by default

Disclosure of Geo-Location Information. In **paragraph 116** of the NPRM, the Commission states that: 'Section 222(d)(4) permits providers to use and disclose CPNI to provide "call location information" concerning the user of a commercial mobile service for public safety. We believe that the critical public safety purposes that underlie this provision counsel in favor of applying a similar rule in the broadband context, and that providing customer PI to emergency services, to immediate family members in case of emergency, or to providers of information or database management services for the delivery of emergency services, are uses for which customer approval is implied. We therefore propose to allow BIAS providers to use or disclose any geo-location information, or other customer PI, for these purposes.'

While we realize the good intention behind this proposed provision, we believe that there are important differences between the commercial mobile context and the broadband context. A mobile user might be calling from anywhere while suffering a heart attack or other serious emergency event. Locating that individual can make the difference between successfully saving that person or having the victim die. There may be nothing

except the mobile device's geo-location available as a hint to direct emergency services personnel.

Contrast that with residential (fixed location) broadband service. The user's physical address (and phone number) would be all the customer PI that would typically need to be disclosed for delivery of emergency services, yet in this case, apparently any or all customer PI is "fair game" for disclosure. We urge the Commission to restrict the information shared with emergency service providers to just the customer's physical address and phone number.

We also note that the Commission proposes to release customer PI to "immediate family members in case of emergency." In most cases, we believe that "immediate family members" will already have relevant customer contact information, and it can be difficult or impossible to authoritatively determine who is or isn't an "immediate family member." Providing this sort of exemption invites attempts at pretexting, and circumvention of a lawful desire to simply be let alone, as in spousal abuse cases, contested divorces, bankruptcies, etc.

Use or Disclosure of CPNI For Cyber Security-Related Purposes. Paragraph 117 of the proposed NPRM states: "In addition, we propose to interpret Section 222(d)(2) to permit BIAS providers to use or disclose CPNI whenever reasonably necessary to protect themselves or others from cyber security threats or vulnerabilities. Section 222(d)(2) permits providers to use CPNI to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services. We believe that this proposal comports with the statute, because cyber security threats and vulnerabilities frequently harm the rights or property of providers, and typically harm users of those services and other carriers through the fraudulent, abusive, or unlawful use of, or subscription to, such services. Furthermore, we note that other statutes explicitly permit particular types of disclosure, which may encompass customer PI. We seek comment on this proposal."

We enthusiastically support this provision.

Protection from Unlawful Robocalls. Paragraph 118: "We also propose to interpret Section 222(d)(2) to allow telecommunications carriers to use or disclose calling party phone numbers, including phone numbers being spoofed by callers, without additional customer consent when doing so will help protect customers from abusive, fraudulent or unlawful robocalls. Month after month, unwanted voice robocalls and texts (together, "robocalls") top the list of consumer complaints we receive at the Commission. At best, robocalls represent an annoyance; at worst they can lead to abuse and fraud. All concerned parties—regulators, providers, and consumer advocates—agree that better call blocking and filtering solutions are critical to helping consumers. To that end, we recently clarified that voice providers may offer their customers call blocking solutions without violating their call completion requirements, and encouraged providers to offer those solutions. We expect that sharing of calling party information to prevent robocalls will benefit consumers. We seek comment on this proposal, and on how well it fits within the framework of 222(d)(2). Is it consistent with customer expectations?"

We also enthusiastically support this provision.

Proposed Marketing Notice and Opt-Out Policy: In paragraph 122-123 of the NPRM, the Commission proposes:

Consistent with this and our existing rules, we propose that, except as permitted above in Part III.C.1.a, BIAS providers must provide a customer with notice and the opportunity to opt out before they may use that customer's PI, or share such information with an affiliate that provides communications-related services, to market communications-related services to that customer.

This approach is similar to the approach taken by our current Section 222 rules, and we believe it is consistent with customers' expectations. However, we invite comment on this approach, specifically on customers' expectations and preferences regarding how their broadband provider may itself use customer PI; and for what purposes it should be allowed to share information with its affiliates subject to

opt-out approval. Given the prevalence of bundled service offerings, do customers expect that their broadband providers could or should themselves use or share the customers' proprietary information with affiliates to market voice, video, or any types of communications-related services tailored to their needs and preferences without their express or implied approval? Or would customers prefer and expect to have their customer PI used or shared with affiliates only after the customers have affirmatively consented to such use or sharing?

Most Americans suffer from marketing fatigue. They're continually tracked and bombarded with advertising. This is empirically demonstrated by things such as the popularity of ad-blocking software for web browsers (e.g., the #1 add-on, of all add-ons for Firefox is "AdBlock Pro").⁴

Given the disproportionate preference of most consumers to NOT receive additional marketing messages, let's avoid being disingenuous: make the default be to NOT allow use of customer PI for ANY marketing purposes unless the customer specifically requests to receive such content.

Don't make millions of customers jump through hoops to confirm their already-obvious preference.

Even the Commission grudgingly concedes (in [paragraph 127](#) of the NPRM) that "We believe that customers desire and expect the opportunity to affirmatively choose how their information is used for purposes other than marketing communications-related services by their provider and its affiliates." That statement is partially correct, but isn't sufficiently inclusive: customers desire and expect the ability to affirmatively choose how their information is used for ALL marketing related purposes. The customer's BIAS provider and its marketing partners do not have, and should not be given, a special exemption from this general rule.

Third Party vs. First Party Disclosures: In [paragraph 130](#) the Commission alleges that: "[...] we believe that the threat to broadband customers' privacy interest from having their personal information disclosed to such entities without their affirmative approval is a substantial one, and there is a greater need to ensure express consent from an approval mechanism for third party disclosure. We seek comment on this analysis, and in particular, the threat to broadband customers' privacy stemming from disclosure of customer information to third parties."

Consistent with our comments in response to [paragraphs 122-123 \(and 127\)](#) *supra*, we believe that customer PI should be subject to a uniform and consistent treatment for all marketing, and that marketing to a customer should only be permitted if the customer explicitly opts-in to receiving such content.

Collection, Use and Disclosure of "Highly Sensitive" Customer Information: In [paragraph 136](#), the Commission discusses it thinking around "highly sensitive" customer information, stating in part:

In particular, we seek comment whether certain types of "highly sensitive" customer information should be used by BIAS providers, even for the provision of the service, or shared with their affiliates offering communications-related services, only after receiving opt-in approval from customers. For example, the FTC has recognized certain types of information as particularly sensitive, including Social Security numbers and financial information, geo-location information, children's information, and health information. Given the highly sensitive nature of such information, customers may have an interest in ensuring that such data is not used without their prior, affirmative authorization. We seek comment on these issues. For example, location-based information—particularly mobile geo-location data—that reveals a customer's residence or current location is particularly sensitive in nature, and consumers may have a keen interest in safeguarding such data out of concerns for both safety and basic privacy. In the voice context, Congress recognized that use of "call location information" should not be "used or disclosed without the "express prior authorization of the customer." How should we consider treatment of location information in the broadband context? Likewise, we seek comment on what steps we could take to ensure knowing consent regarding the customer PI of children. Are there other types of information that we should treat as highly-sensitive and subject to opt-in protection? For example, should practices that involve using or sharing a

customer's race or ethnicity, or other demographic information about a customer be subject to heightened privacy protections? Are there any types of information that BIAS providers should never use for purposes other than providing BIAS services?"

In general, we believe that the best way to control the use and potential misuse, and the possibility of unauthorized disclosure, of highly sensitive information is to not collect it in the first place. Why on earth would a BIAS provider need to know a customer's health information, for example? Or a customer's race or ethnicity? BIAS providers should be required to not solicit or otherwise obtain highly sensitive information about their customers, and if they already have such data, they should be required to delete such information wherever it may be found.

In the event that a BIAS fails to do so and a breach occurs, the Commission should define penalties and liquidated damages that would apply to each and every such unauthorized disclosure of highly sensitive data collected or retained in violation of Commission policy.

When it comes to geo-location information, such information is obviously of highest salience for mobile broadband users, where marketers love to know if a potential customer is near one of their stores. However, we believe that customers already have the ability to grant or withhold geo-location information in the mobile space -- they can allow or deny app access to their smartphone's GPS location information. There is no need for BIAS providers to collect or offer access to geo-location data, except for narrow exceptions relating to E911 locate-and-respond requirements for mobile customers.

Access to Contents of Communications. In [paragraph 137](#) the Commission solicits comment on how to...

[...] treat the content of communication, if we determine that it is covered by Section 222. The content of communications contain a wide variety of highly personal and sensitive information. Congress has also recognized that content of communications should be protected in all but the most exceptional circumstances. In addition to personal privacy implications, provider use of communications content raises competitive issues. A broadband provider may be able to glean competitively sensitive information from the contents of customers' communications. Would such conduct be prohibited under the Commission's general conduct rule prohibiting carriers from unreasonably interfering with or unreasonably disadvantaging end users' ability to select, access, and use broadband Internet access service or the lawful Internet content applications, services, or devices of their choice? We seek comment on whether the use or sharing, including with affiliates, of the content of customer communications should be subject to opt-in approval. We also seek comment on other approaches to the use of the content of customer communications, including how such approaches interact with our treatment of other types of information covered by Section 222.

As we noted in our comments with respect to [paragraph 67](#), the contents of communications should be protected by strong encryption, thereby rendering this item moot: if strong encryption is used providers will not be ABLE to use the contents of communications, assuming the provider is not allowed to intentionally interpose himself as a "man-in-the-middle" (MITM).

E-Pending: In [paragraph 138](#), the Commission asks,

Finally, we seek comment whether customers expect their BIAS providers to treat their PI differently depending on how the provider acquires it, and whether BIAS providers do and should treat such information differently. Should a broadband provider obtain some form of consumer consent before combining data acquired from third-parties with information it obtained by virtue of providing the broadband service?

We strongly oppose use of e-pending and other attempts at data matching. Consistent with our responses to other items in this NPRM, we support requiring affirmative consumer consent prior to targeting customers for marketing, or for

"enhancing" their record with information obtained from third parties. BIAS providers do not need to build a dossier for each of their customers!

Soliciting Customer Approval for Disclosure of Customer PI. In **paragraph 140** of the NPRM, the Commission states:

To ensure that customers provide meaningful approval, we propose to require BIAS providers to solicit customer approval—subsequent to the point-of-sale—when a BIAS provider first intends to use or disclose the customer’s proprietary information in a manner that requires customer approval. To ensure that customers’ approval is fully informed, we propose to require BIAS providers to notify customers of the types of customer PI for which the provider is seeking customer approval to use, disclose or permit access to; the purposes for which such customer PI will be used; and the entity or types of entities with which such customer PI will be shared. We seek comment on this approach.

In considering this approach, we repeat that customers are continually inundated with marketing, and generally want less of it. It is thus key to consider not just the details of what message gets sent, and when, but what happens if the customer is silent and fails to respond. That is the overarching issue when it comes to notice and consent: how are non-responses handled? We believe that unless a consumer affirmatively OPTS-IN, they must be presumed to not be interested, and be treated as having OPTED-OUT.

The Commission goes on to say:

Is there other information that a provider should be required to share as part of receiving opt-out or opt-in consent for the use or disclosure of customer information? For example, should a provider be required to share information about the arrangements it has made with third parties for the use of customer PI? If so, what information should they be required to share? We also seek comment on whether providers should be required to provide a link to the provider’s privacy policy notice or other information when seeking approval for the use or sharing of customer PI.

Full disclosure should be made about the arrangements that the provider has made with the third party. In particular, such a policy should address:

- Confirmation that participation is voluntary, and no consequences will be associated with any decision to not participate
- Disclosure of the compensation received by the provider in exchange for providing the customer's PI
- The financial benefit, if any, to the customer other than "discounts" or other savings if a purchase is made
- The type of product that will be promoted to the customer by the third party
- How that product will be promoted
- Whether the customer's record will be "enhanced" with e-pended data obtained from third parties
- The true identity of the third party to whom the data is being shared, including the third party company's name, the name of its senior-most company officer, the company's street address, web address, telephone number, the email address of its privacy officer, the length of time it has been in business and any/all other names by which it has been known
- Details of any incidents in which the company or the company's principles having been disciplined by the FTC, FCC, or other federal, state, local or international criminal justice, regulatory or consumer protection agencies
- Whether the third party is being licensed to use the customer's contact information once, or perpetually
- Whether the third party has the right to retransfer, resell, or otherwise provide the customer's details to still other entities
- How the customer can revoke their permission for use of their information, both for the third party and any subsequent recipients of their information
- The customer's recourse if any of the preceding is inaccurate or disregarded, resulting in the customer receiving unauthorized communications.

That information should remain available for at least three years from a publicly-accessible web site, indexed by major search engines (e.g., there shall be no use of robots.txt or other measures in an attempt to block search engine processing of that page).

Documenting Use and Disclosure of Customer PI. In [paragraph 149](#), the Commission states:

In order to ensure that the requisite approval is clearly established before the use or disclosure of customer PI, and also that the approval can be demonstrated after the use or disclosure, we propose to require BIAS providers to document the status of a customer's approval for the use and disclosure of customer PI, and we seek comment on that proposal. We base our proposal on the existing rules governing safeguards on the use and disclosure of customer PI for voice telecommunications services. Specifically, we propose requiring BIAS providers to (1) maintain records on customer PI disclosure to third parties for at least one year, (2) maintain records of customer notices and approval for at least one year, (3) adequately train and supervise their personnel on customer PI access, (4) establish supervisory review processes, and (5) provide prompt notice to the Commission of unauthorized uses or disclosures. With these proposed rules, we seek to promote consumer confidence that BIAS providers are adequately protecting customers' PI, to provide clear rules of the road to BIAS providers about their obligations, and to maintain consistency with existing legal requirements and customer expectations. Are there any other or different requirements that we should adopt in order to ensure that providers document their compliance with our customer consent requirements? Should we require BIAS providers to file an annual compliance certification with the Commission, as is required under the current Section 222 rules? Are there alternative approaches to safeguard customers' proprietary information and boost customer confidence in the privacy of their customer PI that we should consider?

We support requiring detailed recordkeeping to document affirmative expression of customer opt-in choices. All records described in this part should be kept for a minimum of three years, not just one. Records retained should include the address from which the consent was solicited and received, including in the case of email messages, the full headers for such messages, and in the case of web-based approvals, the connecting IP and the value of all normally available web header fields⁵ in an effort to identify anomalous/spoofed "opt-in" campaigns.

Customer Choice and Small Providers: In [paragraph 151](#), the Commission asks:

We seek comment on ways to minimize the burden of our proposed customer choice framework on small BIAS providers. In particular, we seek comment on whether there are any small- provider-specific exemptions that we might build into our proposed approval framework. For example, should we allow small providers who have already obtained customer approval to use their customers' proprietary information to grandfather in those approvals? Should this be allowed for disclosure to third parties? Should we exempt providers that collect data from fewer than 5,000 customers a year, provided they do not share customer data with third parties? Are there other such policies that would minimize the burden of our proposed rules on small providers? If so, would the benefits to small providers of any suggested exemptions outweigh the potential negative impact of such an exemption on the privacy interests of the customers who contract for the provision of BIAS with small providers? Further, were we to adopt an exemption, how would we define what constitutes a "small provider" for purposes of that exemption?

We support treating all BIAS providers, large or small, the same.

Use and Disclosure of Aggregate Customer PI. In **paragraph 153**, the Commission describes its perspective on aggregate customer information, stating that:

Because of the complexity of the issues surrounding aggregation, de-identification, and re-identification of the data that BIAS providers collect about their customers, we propose to address separately the use of, disclosure of, and access to aggregate customer information. Consistent with reasonable consumer expectations, existing best practices guidance from the FTC and NIST, and Section 222(c)(3)'s treatment of aggregate CPNI, we propose to allow BIAS providers to use, disclose, and permit access to aggregate customer PI if the provider (1) determines that the aggregated customer PI is not reasonably linkable to a specific individual or device; (2) publicly commits to maintain and use the aggregate data in a non-individually identifiable fashion and to not attempt to re-identify the data; (3) contractually prohibits any entity to which it discloses or permits access to the aggregate data from attempting to re-identify the data; and (4) exercises reasonable monitoring to ensure that those contracts are not violated. We also propose that the burden of proving that individual customer identities and characteristics have been removed from aggregate customer PI rests with the BIAS provider.

If properly-aggregated/anonymized, aggregated/anonymized data should be able to be freely and safely shared, a premise the Commission explicitly agrees with in **paragraph 155**, *infra*.

As such, we believe that the extensive program of determinations and oversight envisioned in this section should not be necessary.

We do recommend **more specific guidance** about the types of aggregation or anonymization that will meet the expectations of the Commission. For example, the Commission might establish a safe harbor around data sharing if a BIAS provider is sharing:

- IPv4 Netflow data and the BIAS provider sanitizes IPv4 network flow data by having the low order 11 bits of each unicast IPv4 address zeroed before that data is released (this is the Internet2 IPv4 research Netflow sanitization standard)
- IPv6 Netflow data and the BIAS provider sanitizes IPv6 network flow data by having the low order 80 bits of each unicast IPv6 address zeroed before that data is released (again, this is the Internet2 standard for this type of data)
- DNS query and response data if the query and response data is solely limited to cache miss traffic collected **above** caching recursive resolvers, and those recursive resolvers service a minimum aggregation pool of at least 200 users per day.
- Some types of data, such as BGP routing table snapshots or route updates and withdraw data, may be inherently aggregated and require no sanitization or special data collection considerations whatsoever

Similar privacy-preserving sanitization safe harbor standards can and should be developed and shared by the Commission for other data collection types as well.

Paragraph 155 goes on to state:

Recognizing that aggregate, non-identifiable customer information can be useful to BIAS providers and the companies they do business with, and not pose a risk to the privacy of consumers, Section 222(c)(3) permits telecommunications carriers to use, disclose, or permit access to aggregate customer information—collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed—without seeking customer approval. Our proposed rule expands this concept to include all customer PI, and imposes safeguards to

ensure that such information is in fact aggregated and non-identifiable, and that safeguards have been put in place to prevent re-identification of this information.

We support the existing policy that permits "telecommunications carriers to use, disclose, or permit access to aggregate customer information—collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed—without seeking customer approval."

We do NOT believe additional safeguards are needed or should be imposed, absent evidence that problems exist with the existing aggregated data regime.

"Not Reasonably Linkable." In [paragraphs 157-159](#), the Commission states that

In order to protect the confidentiality of individual customers' proprietary information, the first prong of our approach would require providers to ensure the aggregated customer PI is not reasonably linkable to a specific individual or device. Our proposal recognizes that techniques that once appeared to prevent re-identification of aggregate information have increasingly become less effective. It is also consistent with FTC guidance which recommends that companies take reasonable measures to ensure that the data is de-identified, and recommends that this determination should be based on the particular circumstances, including the available methods and technologies, the nature of the data at issue, and the purposes for which it will be used.

We seek comment on this proposal. Are the factors identified by the FTC well-suited to determining whether a BIAS provider has taken reasonable measures to de-identify data? Are there other factors that we should expect providers to take into account? Should we provide guidance on what we mean by linked and linkable information? NIST defines linked information as "information about or related to an individual that is logically associated with other information about the individual," and linkable information as "information about or related to an individual for which there is a possibility of logical association with other information about the individual." Should we adopt either or both of these standards? Are there other approaches we should use to decide whether information is reasonably linkable? For example, HIPAA permits covered entities to de-identify data through statistical de-identification, whereby a properly qualified statistician, using accepted analytic techniques, concludes that the risk is substantially limited that the information might be used, alone or in combination with other reasonably available information, to identify the subject of the information.

We seek comment on alternative approaches to this prong and the comparative merits of each possible approach. We also seek comment whether we should require BIAS providers to retain documentation that outlines the methods and results of the analysis showing that information that it has treated as aggregate information has been rendered not reasonably linkable.

We do not believe the Commission should impose additional regulation around "linkability" except to explicitly affirm specific technological measures or collection architectures that are sufficient to merit safe harbor status, as previously described in response to [paragraph 153](#).

Public Commitments. In [paragraph 160](#), the Commission states:

Prong two of our proposal would require BIAS providers to publicly commit to maintain and use aggregate customer PI in a non-individually identifiable fashion and to not attempt to re-identify the data. Such public commitments would help ensure transparency and accountability, and accommodate new developments in the rapidly evolving field of privacy science. This prong and the next are consistent with FTC guidance and the Administration's draft privacy bill recommending that companies publicly commit not to re-identify data and contractually prohibit any entity with which a company shares customer data from attempting to re-identify it. We seek comment on this proposal. Would this requirement help ensure

that providers are protecting the confidentiality of customer PI? How could or should a BIAS provider satisfy the requirement to make a public commitment not to re-identify aggregate customer PI? For example, would a statement in a BIAS provider's privacy policy be sufficient?

"Public commitments are mere theater. Commission investigations with sanctions against violators would speak far more loudly and far more credibly than the most earnest of BIAS provider "pinkie promises"⁶ to be good.

Limits on Other Entities. In [paragraph 161](#), the Commission suggests that:

The third prong of our proposal would require providers to contractually prohibit any entity to which the BIAS provider discloses or permits access to the aggregate customer data from attempting to re-identify the data. This proposal presents a modern approach to the difficulties of ensuring the privacy of aggregate information, recognizing that businesses are often in the best position to control each other's practices. Researchers have argued that such contractual prohibitions are an important part of protecting consumers' privacy, because making data completely non-individually identifiable may not be possible or even desirable. We recognize that the categories of what can potentially be reasonably linkable information will continue to evolve, and we believe these contractual provisions provide a critical layer of privacy protection that remains constant regardless of changes in the technology."

Contractual prohibitions imposed on third parties may prevent them from conducting the sort of analyses that Commission is worried might occur, but can that prohibition be meaningfully enforced by aggrieved customers against subsequent downstream recipients of their data? That is, assume:

- A BIAS provider sells aggregated customer PI to third party provider "A," receiving contractual commitments from "A" as envisioned by the Commission.
- Third party provider "A" now in turn resells a version of that data to third party provider "B," again with contractual commitments between "A" and "B" consistent with the Commission's intent
- Third party provider "B" in turn resells part of that data to third party provider "C," perhaps with full, limited, or no contractual protections -- things are hazy, as they often are when two many links need to get followed.

If an employee of "C" misuses that data, and successfully de-anonymized it somehow, do we really believe that the adversely affected customers, the BIAS provider, or any other party will realistically be able to collect damages from "C" or force "C" to cease and desist? We suppose this is a hypothetical possibility, but we believe likely a very remote one.

We are candidly skeptical of the value of this provision unless aggrieved customers have a private right of action against any/all downstream recipients of the data, particularly if those recipients are international entities.

Reasonable Monitoring. In [paragraph 162](#), the Commission goes on to state that

Related to the requirements for prong three, the fourth prong of our approach requires BIAS providers to exercise reasonable monitoring of the contractual obligations relating to aggregate information and to take reasonable steps to ensure that the if compliance problems arise they are immediately resolved. This prong is a logical outgrowth of the previous prongs, and it is consistent with the 2012 FTC Privacy Report. We seek comment regarding the types of monitoring and remediation steps BIAS providers should be required to take to ensure that entities with which they have shared aggregate customer PI are not attempting to re-identify the data. What potential burdens and benefits would arise from this proposal?

"Monitoring" the uses to which aggregated data is put will be impossible. We think the commission may even know this - we see a suggestion that you know what you'd like, but have no idea how to practically accomplish that. We share your bewilderment on this point.

Monitoring individual level data is possible through things such as inclusion of trap accounts, but aggregate level data, by definition, strips away the possibility of doing that sort of thing.

Alternatives. In **paragraph 163**, the Commission offers an alternative, specifically:

Alternatively, we seek comment whether we should develop a list of identifiers that must be removed from data in order to determine that "individual customer identities and characteristics have been removed." If we take such an approach, should it replace all, a portion of, or be in addition to our current proposal? HIPAA incorporates such a standard, and under this approach, a covered entity or its business associate may de-identify information by removing 18 specific identifiers. Under HIPAA, the covered entity must also lack actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information. We are aware of criticisms that the approach taken by HIPAA no longer provides the levels of protection previously assumed. One legal scholar, for example, argues that "[t]he idea that we can single out fields of information that are more linkable to identity than others has lost its scientific basis and must be abandoned." Are such concerns valid? Were we to adopt a similar standard to that in HIPAA, what categories of identifiers would be relevant in the broadband context? And, given the wide variety of customer data to which BIAS providers have access by virtue of their provision of BIAS, is such a list even feasible? Is it likely that any list developed would be rendered obsolete by technological developments in the data re-identification field? How could we best ensure that the categories we identify remain adequate to prevent aggregate customer PI from being re-identified? Should we adopt a catch-all to address evolving methods of de-identification and re-identification of aggregate customer PI, and if so, how would such a process work? We also seek comment whether, if we were to pursue such an approach, we should also adopt an "actual knowledge" standard, as HIPAA includes. How would the Commission enforce such a standard, and would it encourage willful ignorance on the part of broadband providers?

Re-iterating themes we've previously mentioned, we believe the keys to effectively managing the privacy of BIAS customer data privacy are:

- Minimizing the amount of private data intentionally collected in the first place
- Encouraging/deploying encryption to protect the contents of all communications
- Protecting customer PI against all marketing uses by default, subject solely to affirmative customer opt-in
- Requiring providers to leave a trail of detail around marketing partnerships, discoverable through simple search engine queries, in the event abuses occur
- Defining anonymization and aggregated data sharing regimes whose adoption the FCC is willing to incent with safe harbor protections

Risk Management Practices, Training, Authentication, And Other Measures: In **paragraph 169**, you state:

[...] we propose to require BIAS providers to protect the security and confidentiality of all customer proprietary information from unauthorized uses or disclosures by adopting security practices calibrated to the nature and scope of the BIAS provider's activities, the sensitivity of the underlying data, and technical feasibility. To ensure compliance with this obligation, we propose to require BIAS providers to, at a minimum, adopt risk management practices, institute personnel training practices, adopt customer authentication requirements, identify a senior manager responsible for data security, and assume accountability for the use and protection of customer PI when shared with third parties. In addition, we seek comment on whether we should also include data minimization, retention, and destruction standards in any data security regime we adopt. Finally, we seek comment on harmonizing the data security requirements for BIAS providers and those for voice providers, and on adopting harmonized data security requirements for cable and satellite providers.

We've already explained that we believe that data shared with third parties may be effectively impossible for a BIAS to control post-sharing. Let us now consider the other measures mentioned in [paragraph 169](#):

-- "[...] we propose to require BIAS providers to, at a minimum, adopt risk management practices,"

Risk management cannot magically eliminate technical security risks or prevent privacy breaches. In fact, adoption of risk management practices has led to poor outcomes so often that it has become the subject of popular parody videos such as "Host Unknown presents: Accepted the Risk," see <https://www.youtube.com/watch?v=9IG3zqvUqJY>

The fundamental challenge, of course, is that everyone has limited resources. If there's only so much budget available, and you have to spend it standing up a formal compliance-oriented risk management program, that's money that's not available to be spent on actual technical security measures.

Compliance cannot be allowed to "starve" or deprecate technical security.

-- "[...] institute personnel training practices,"

We suggest that the Commission clarify whether they mean a security awareness program, a true security training program, or in-depth security education (including perhaps mandating formal professional development through participation in security certification programs).⁷ The options are substantially different in terms of number of individuals trained and the depth of the training delivered.

It is also worth noting that many well respected figures in the cyber security industry are rightfully skeptical of security training. For example, well regarded security expert and cryptographer Bruce Schneier has stated:⁸

Should companies spend money on security awareness training for their employees? It's a contentious topic, with respected experts on both sides of the debate. I personally believe that training users in security is generally a waste of time, and that the money can be spent better elsewhere. Moreover, I believe that our industry's focus on training serves to obscure greater failings in security design.
[article continues]

-- "[...] adopt customer authentication requirements,"

We strongly support improved customer authentication practices. We will comment further on this below.

-- "[...] identify a senior manager responsible for data security,"

We also support this recommendation, provided the manager has both the responsibility *and* the authority and budgetary/staff resources required to take required actions. Having a "senior manager responsible for data security," but without the authority, staff and budget to do the job means the he or she has merely been hired to be an ablative scapegoat when security catastrophes inevitably occur.

-- "[...] and assume accountability for the use and protection of customer PI when shared with third parties."

We have discussed the practical limitations to this recommendation earlier in this document.

-- "[...] data minimization,"

We strongly support efforts at data minimization.

-- "[... data] retention,"

We will not be offering recommendations relating to data retention, except to recognize the tension that exists between data retention (the more data you retain, the greater the potential exposure if there's a breach) and the desirability of having Netflow and similar archives for incident assessment and cyber forensic purposes.

-- "[... data] destruction standards"

We recommend the Commission consider adopting NIST 800-88r1, "Guidelines for Media Sanitization"⁹ as its default standard in this area. See also the NSA/CSS guidance related to this area.¹⁰

"... not to specify technical measures for implementing [...] the data security requirements[...]" In **paragraph 176** of the NPRM, the Commission states that:

In order to allow flexibility for practices to evolve as technology advances, while requiring the regulated entities to install protocols and safeguards that are available and economically justified, we propose not to specify technical measures for implementing the data security requirements outlined below. This follows the regulatory approaches taken at other federal agencies. We believe this approach will encourage BIAS providers to design security measures that can easily adapt to new and different technologies. We seek comment on this approach.

We applaud the Commission's proposed course of NOT dictating technical solutions. There often isn't "one and only one" path that will work for all providers in all circumstances.

At the same time, we would urge you to provide a reasonable portfolio of illustrative options that meet the Commission's standards, and which, if adopted, offers safe harbor to BIAS providers for that particular requirement. This approach, while providing flexibility for experts, can help to steer the less knowledgeable toward proven options and minimize their anxiety when it comes to evaluating and selecting solutions.

Employee Training. In **paragraph 185**, the Commission elaborates on its thinking about required training, stating:

We also propose to require BIAS providers to protect against unauthorized uses or disclosures of customer PI by training their employees, agents, and contractors that handle customer PI on the data security measures employed by the BIAS provider and by sanctioning any such employees, agents, or contractors for violations of those security measures. Data security training is well recognized as a key component of strong data security practices. A training requirement is a well-established part of the Commission's treatment of CPNI for voice providers. The Commission adopted a personnel training safeguard as part of its original 1998 CPNI rules, requiring that carriers train all employees with access to customer records as to when they can and cannot access CPNI and that they maintain internal procedures for managing employees that misuse CPNI. In its data security consent orders, the Enforcement Bureau has also adopted training requirements to help "ensure that consumers can trust that carriers have taken appropriate steps to ensure that unauthorized persons are not accessing, viewing or misusing their personal information." We seek comment on our proposal and our rationale.

As discussed in conjunction with **paragraph 169**, above, we suggest that the Commission clarify whether they mean to establish a requirement for security awareness program, a true security training program, or in-depth security education (including perhaps mandating formal professional development through participation in security certification programs). The options are substantially different in terms of number of individuals trained and the depth of the training delivered.

It is also worth noting that many well respected figures in the cyber security industry are rightfully skeptical of security training. For example, well regarded security expert and cryptographer Bruce Schneier has stated:

Should companies spend money on security awareness training for their employees? It's a contentious topic, with respected experts on both sides of the debate. I personally believe that training users in security is generally a waste of time, and that the money can be spent better elsewhere. Moreover, I believe that our industry's focus on training serves to obscure greater failings in security design.
[article continues]

Training Program Topical Coverage and Duration/Frequency. Looking at NPRM [paragraph 187](#), we see the Commission state that:

The existing training programs required by the HIPAA and GLBA rules do not specify all the topics that must be included under the training program, nor do they mandate the frequency or length of training. We seek comment whether we should follow this approach or provide further clarifications on the training process. We also seek comment whether we should require training be done on an annual basis or with some other specified frequency, or establish a minimum frequency. Are there additional entities to which these training requirements should apply?

We recommend that the Commission define the objectives and the minimum/essential topics that required training should cover, and the categories of individuals it expects to receive training, should the Commission elects to mandate training for BIAS providers. If BIAS providers are left to "guess" or "work it out themselves," coverage and training outcomes will likely be inconsistent. Providers will also likely need to devote substantial effort or expense to working out syllabi and instructional material. If all BIAS providers are expected to provide cyber security training covering the same topics, we suggest that the Commission should partner with industry training partners to develop appropriate materials that can be provided to BIAS providers at little or no cost.

Robust Customer Authentication. In [paragraph 191 \(continuing through paragraph 192\)](#) of the NPRM, it is stated that:

To honor customers' rights to access their personal information while ensuring that BIAS providers comply with their duty to safeguard confidential customer data, we propose to require BIAS providers to adopt robust customer authentication requirements. We seek comment on whether we should require providers to use, at a minimum, a multi-factor authentication before granting a customer access to the customer's PI or before accepting another person as that customer's designee with a right to access a customer's PI. We also propose to require BIAS providers to notify customers of account changes to protect against fraudulent authentication attempts. Relatedly, we also seek comment on the methods by which consumers should be allowed to access their customer PI and whether we should adopt rules requiring BIAS providers to correct inaccurate customer PI.

We strongly support the Commission's proposed requirement to require strong authentication to protect customer PI. Strong authentication should be required for **both** customer access, **and** for provider employee access.

The Commission also specifically asked if multifactor authentication should be required. Yes, it should, however there's more to identity management than just multifactor authentication -- for example, identity proofing should also be addressed. We recommend that the Commission officially adopt NIST 800-63-2¹¹ LOA-3 as the minimum level of assurance required for access to customer PI.

Types of Multifactor Authentication. In [paragraphs 193-194](#), the Commission states that:

-- "We do not currently propose to require BIAS providers to adopt multi-factor authentication or, more granularly,

specific types of multi-factor authentication methods, because we recognize that there is no perfect and permanent approach to customer authentication. Technology develops over time."

If the Commission fails to require multifactor authentication, that choice speaks louder than any written policy about the extent to which the Commission is serious (or NOT serious) about BIAS customer privacy. Doing nothing, because "something" might be less than perfect, is a recipe for disaster. As is often said, "The perfect is the enemy of the good." It is true that many multifactor solutions aren't perfect, but most are still better than just plain old passwords. If a revolutionary discovery yields tremendous improvement in multifactor authentication technology, the Commission can always revise its requirements accordingly.

-- "We seek comment on the advantages and disadvantages of requiring multi-factor authentication. Are there security risks associated with multi-factor authentication that we should take into account?"

The risks associated with multifactor authentication depend on the type of multifactor authentication employed. For the purpose of this discussion we assume that most multifactor authentication schemes will use a plain old password plus either:

- Something the user has (like a cryptographic hard token, or a linked smart phone), or
- Some biometric property associated with the user (such as their finger print or a voice sample)

In the first case, the biggest risk is inaccessibility: the user may lose or not have their second factor device with them, and as a result they may be unable to log in, potentially for days or more if they need to request a replacement token from their provider. This risk can be managed through a variety of backup mechanisms, including production of backup codes (those codes can be produced in advance, and carried for use in case the primary multifactor authentication device is lost, ruined, or forgotten), or things like phone-a-friend proxy authentication schemes. Duo Security¹² is an example of a multifactor company that is popular in the higher education space¹³ in part because of the options it offers to manage lock-out risk. An analysis of other factors that may deter adoption of multifactor authentication (albeit in a higher education context) is also available.¹⁴

In the second case, the biometric case, the biggest challenge is the lack of ubiquitous and interoperable sensor deployment. For example, assume you might want to try fingerprints as a biometric characteristic. Some laptops and some smart phones offer fingerprint readers, but many others do not, and the ones that do have support are typically not interoperable from one vendor to another. The best option in the biometric space may be voice based solutions, since everyone has access to a phone even if their laptop doesn't support voice.

-- "How would consumers be affected by a multi-factor authentication requirement?"

In a nutshell, consumers would likely be inconvenienced. Having to do multifactor, even something as simple as hitting "yes" or "no" on a smart phone, Duo Security style, is still not as easy as just logging in with a plain old password, particularly if you save your passwords in a password manager.

-- "What would be the additional costs imposed on BIAS providers and/or consumers?"

The cost of multifactor solutions vary from provider to provider, just like the cost of dinner. As an example, however, the Duo Security solution previously mentioned, has public pricing at <https://duo.com/pricing>

The pricing that pertains for colleges and universities that are part of InCommon, a popular higher education identity management consortia, can be seen at <http://www.incommon.org/duo/fees.html>

Additional costs will also be associated with multifactor integration with existing identity management systems, and with customer support.

-- "If a cell phone number or email address is used to provide new information after authentication, how can the provider be certain that neither has been compromised?"

Cell phones and email accounts normally are secured against unauthorized users with passwords or PINS. Of course, you could always recursively deploy multifactor authentication on those devices as well, although some may eventually find that becomes a bit "over the top" or "silly" and we'd concur with their assessment.

-- "Are there customers that would not be able to take advantage of a multi-factor authentication process based on lack of access to specific types of technology? If so, what alternatives should be available, and should we require providers to make these alternatives available?"

One option would be to allow self-enrollment. Then, if a customer doesn't want the security associated with multifactor, or they lack some required technology, they could simply not use multifactor authentication. (Users are adults, and should be allowed to make choices about their own lives, including the protection of their PI, even if those choices may be unwise.)

Phone-based multifactor solutions, however, should work for virtually *all* users, via one or another of:

- proprietary solutions such as the smart phone-based Duo Push application ("hit yes to login or no to reject"),
- a soft token app running on a smart phone (emulating a classic hardware RSA-style cryptographic token, e.g., "copy the displayed six or eight digit number generated by your phone to finish logging in"), works even if the user has limited connectivity
- traditional SMS-based messaging ("we've sent a special numeric code to your phone; enter the number we sent you to continue")
- or even via simple voice phone calls ("You're attempting to login to your account at broadband provider Foo. Hit any key if you'd like to proceed, or hang up to reject this attempt"), etc.

Another hypothetical option would be for the Commission to issue PKI smart cards to all interested Americans, either in classic credit-card form (similar to the CAC/PIV cards the government currently issues to government employees and the military), or in a plug-and-go USB format. This would have the advantage of providing a potential LOA-4 credential, too.

-- "Would a multi-factor authentication requirement unduly burden small providers?"

Not necessarily. There are third party outsourced identity management providers who can deliver the required technical capabilities.

-- "How would a multi-factor authentication regime work for interactions that are off-line, i.e., in-person access to customer PI via a face-to-face interaction at the BIAS provider's regional offices or via a telephone call?"

In the face-to-face scenario, the provider can inspect and verify government issued ID, such as a driver's license or passport, the provider need not rely on multifactor authentication.

In the customer-calls-the-provider scenario, the provider can either call the customer back at a phone number that the customer has pre-established as trusted, or the provider can ask the customer for the same info that would normally be requested directly by the provider's web site ("please tell me the code that's currently shown on your fob")

- "Are there specific issues with respect to multi-factor authentication and customers with disabilities that we should take into account?"

Classic "copy the six or eight digit number from your cryptographic token" solutions obviously poses a problem for the blind, but audio options can be a good reasonable accommodation.

Audio solutions are obviously a problem for the deaf and hard of hearing, but visual methods can work well for them.

Other robust methods of customer authentication. Paragraph 195 of the NPRM states:

- "We seek comment on other robust methods of customer authentication. FTC guidance encourages "[c]ompanies engaged in providing data for making eligibility determinations [to] develop best practices for authenticating consumers for access purposes," and highlights the security work of the private sector such as Payment Card Institute Data Security Standards for payment card data, the Better Business Bureau, and the Direct Marketing Association that developed and implemented best practices for authenticating consumer accounts."

In our opinion, the work of these other parties is not directly applicable. For example, in the payment card case, the PCI-DSS is really best know as establishing standards for networks collecting payment card data, they do not focus on robust authentication per se (note that debit cards, for example, are already inherently multifactor, combining either a magnetic stripe card + PIN or a smartcard + PIN).

We believe that the FCC would be best served by tracking NIST's NSTIC (National Strategies for Trusted Identities in Cyberspace) work.¹⁵

- "Further, NIST's cybersecurity standards recommend authentication standards based on risk models, noting that "the level of authentication required for online banking is likely to differ from that required to access an online magazine subscription." We seek comment on application of these authentication practices and standards to the relationship between BIAS providers and their customers, as well as the benefits and drawbacks of adopting any of these methods as requirements in the broadband context.

A good first step would be to clarify the tasks that are being secured between BIAS providers and customers: Access/updates to customer contact and billing information? Network access? Customer email? Cryptographic key material (ability to upload or access PGP/GPG keys, for example)?

Most common customer transactions will not rise to the risk level of an irrevocable wire transfers, for example. The most innovative use of risk-based methods is likely RELAXING required authentication requirements when the customer is coming from a known system, on a previously seen IP address, at a reasonable time, for low-risk services. This approach, which ensures that multifactor doesn't get overused or become a cause of friction, is a worthwhile approach, however our understanding is that it is also a *patent-encumbered* approach. See for example <http://www.google.com/patents/US20050097320> ("System and method for risk based authentication")

One potential downside to risk-based approaches is that the user does not have an absolutely consistent user authentication experience (e.g., sometimes they may need to provide a second factor, sometimes they may not). This can result in user "surprise" when the second factor is needed, perhaps in particularly inconvenient circumstances. For example, perhaps a user is virtually "never" prompted to demonstrate possession of a cryptographic hard token at home, but then, while traveling for work and NOT carrying that token, they need to use it while in Europe. If the token had been required each and every time, the user would be more likely to remember to have it with them when traveling than if it is only rarely needed.

- "Are there any authentication methods being used that we should discourage or even prohibit because they are outdated, present their own privacy or data security risks, are unworkable for people with certain types of disabilities,

or for other reasons?"

Efforts at deploying PKI-based methods have always been hugely painful, and pose special challenges in a mobile broadband environment. It is very tempting to suggest that discouraging or prohibiting PKI-based solutions be considered, but then there's the reality that it is one of the rare approaches that will let an entity get to LOA-4.

From the POV of the disabled, approaches that require the transcribing of multiple digits from one device to another can be a problem for the blind. Strictly-timed authentication mechanisms may be a problem for those with limited fine motor skills.

-- "For example, do authentication methods that rely on additional, less mutable, personal information, such as fingerprints or other biometric information, raise particular concerns in the case of a breach of that personal information or other scenarios? Would BIAS providers need to employ additional safeguards to secure this authentication-specific information? Should our rules prohibit BIAS providers from requiring their customers to provide biometric information as part of any authentication scheme?"

It is true that you "can't reset your fingerprints" if your biometric data is breached. However, if state of the art biometric readers are employed, it should be quite difficult for stolen biometric data to be worked into a usable fake prosthetic overlay -- having possession of someone's biometric data isn't like having possession of their password, you don't just "punch in" stolen biometric data.

On the other hand, some biometrics (such as automated facial recognition) can be employed against you without your knowledge or consent. Having authoritatively matched a person's face to their identity once, that identification can be repeatedly performed thereafter, whether the customer wants it to be done or not. This is an example of the biggest risk of biometrics: involuntary identification rather than impersonation.

We would suggest prohibiting the collection and storage of biometric information for those under the age of 21, and making any submission of biometric information opt-in, and optional, only.

Passwords: required? In [paragraph 196-197](#). "We also seek comment on whether we should require password protection. Our existing voice rules rely on authenticating customers based on a password the customer must establish before seeking to obtain call-detail information over the telephone or via online access. These measures were implemented to address the problem of pretexting, where parties pretend to be a particular customer or other authorized person in order to obtain access to that customer's call detail or other private communications records.

However, given the frequency with which passwords are compromised due to phishing attacks, password database leaks, and reuse of passwords across multiple websites and service offerings, we have concerns whether a password is a sufficient safeguard when a customer requests access to customer PI over a customer-initiated phone call or via online access in the broadband context. We seek comment generally on the efficacy of password authentication in this context. If commenters agree that password protection should be part of a robust customer authentication mechanism, should we prescribe additional requirements, such as mandating the use of secret questions or character limitations on passwords? Or should we establish a particular standard with respect to password protection and leave it up to the provider to determine the best way to meet that standard?"

We just discussed multifactor, didn't we? Adoption of multifactor authentication should dramatically reduce the phishing problem, in our opinion.

Passwords are simultaneously not enough, and too painful for customers and providers to rely on. However, even in the multifactor case, passwords typically remain part of the package (e.g., they're routinely half of what needs to be supplied as part of a multifactor login.

For verbal use, we suggest consideration be given to passphrases, rather than passwords. It is a lot easier to

tell a call center operator "I like maple syrup and butter on my Belgian waffles" than it is to read off a strong password such as pound sign capital H lowercase x exclamation point four nine caret capital P eight lowercase d at sign lower case f"

For online access, encourage end users to take advantage of password safes. They allow users to employ strong unique passwords without going crazy.

When thinking about passwords, be sure to consider the authentication system **as a whole**: password reset mechanisms are often the weakest link, leveraging either a secondary email account (which may be compromised), or "security questions" which are either impossible to remember or trivially easy to guess or research on social media.

Customer notifications. In [paragraph 203](#), the Commission states: "We also propose to require BIAS providers to notify customers when someone has unsuccessfully attempted to access the customer's account or change account information. Providing such notice will alert the customer of possible data breach attempts. We seek comment on this proposal. Might it risk additional customer notice fatigue? Do the benefits outweigh the burdens?"

Automated tools make it trivial for attackers to try to brute force a customer's account. Should customers be notified of that? What can they do, having learned this, other than worry or potentially set a stronger password for their account?

We'd argue that the right thing for a provider to do would be to limit attack traffic *per source.* That is, if a provider sees N failed logins during time T from a given IP address or address block, block that source for an automatic period of time. This is the sort of scalable approach that system administrators routinely implement with anti-brute forcing tools. One nice discussion of authentication brute forcing counter measures can be seen in the Dragon Research Group "SSH Password Authentication: Threats and Countermeasures."¹⁶

Do NOT use the approach of N failed login attempts against a particular account "locks" that *account* -- this is a perfect way of conducting a denial of service attack against your own customers: any mischief maker or enemy can lock out thousands of customers at will.

Other safeguards and security practices. In [paragraph 215](#) the NPRM states, "In addition to the safeguards we propose above, we seek comment on whether there are other safeguards that BIAS providers should employ to protect against reasonably anticipated unauthorized use or disclosure of customer PI by the BIAS provider, its employees, agents, and contractors. For example, we seek comment on whether restricting access to sensitive data; setting criteria for secure passwords; segmenting networks; requiring secure access for employees, agents and contractors; and keeping software patched and updated would be useful security measures to reduce the probability of threats. If so, should we require them? If not, what other security measures should we consider?"

Restricting access to sensitive data is good. Moreover, log the access that takes place, by whom, from where, and for what purpose. Adequate logs can go a long way toward discouraging insider misuse.

Strong passwords are also good, but multifactor authentication with strong passwords are even better.

Use virtual private networks or IPsec throughout.

Keeping ALL software patched is critically important, which is why we recommend Windows systems be scanned with Secunia CSI or PSI (depending on their ownership/usage). Likewise, unneeded software should be removed, and the number of network services running kept to a minimum.

Other recommended measures:

- Employ centralized syslogging.
- Monitor critical files against unauthorized changes with something like Tripwire.
- Install hardware/software firewalls immediately in front of the employee's device.
- Encrypt all network traffic.
- Collect 1:1 network flow traffic.
- Scan all systems with Nessus or the equivalent.
- Ensure all systems are backed up.
- Ensure all systems employ whole disk encryption
- Cable down or cradle down all systems to protect against theft.

Encryption. In **paragraph 216**, the FCC asks: "In addition we seek comment whether we should require or encourage BIAS providers to use standard encryption when handling and storing personal information. The FTC established best practices for maintaining industry-standard security, SSL encryption among them, which it considers to be a "reasonable and appropriate" step to secure user data. Should we mandate that customer PI be encrypted when stored by BIAS providers?"

Encryption should be used to secure data in transit and at rest. We hope that your reference to "SSL" is meant to refer generically to https encryption, since SSL is actually an insecure protocol -- you really want to be using TLS 1.2 rather than any version of the now-historical SSL. Self-signed certificates should be disallowed. Providers should be required to demonstrate correct configuration by means of third party TLS web evaluation tools such as <https://www.ssllabs.com/ssltest/> (happy to see that the FCC's own web site gets an "A" grade on that tester)

Beyond use of TLS for web traffic, interactive logins by employees should be via ssh (rather than telnet), and file transfers should be via sftp or scp (rather than ftp), using ssh preshared keys.

Hard disks should be protected with full disk encryption.

Databases should be protected with passive row-level encryption whenever possible.

All employee traffic should be protected with IPsec, either via a VPN or through a native IPsec deployment.

Email should be protected with DKIM and DMARC, DNS traffic should be protected with DNSSEC, and route announcements should be protected with RPKI, too.

Factors to consider when thinking about safeguards. In **paragraph 218** the Commission states: "We believe that Section 222(a) requires BIAS providers to, at a minimum, consider these factors when designing their safeguards to protect the confidentiality, integrity, and security of customer PI, and we seek comment on the inclusion of these factors and whether there are additional factors that we should consider. [...]"

The textbook security objectives are normally confidentiality, integrity, and availability in the enterprise case. Did the Commission intentionally exclude availability? We believe availability to be fully on par with the other objectives mentioned for a utility-like service such as broadband service. A desire for security must NOT be allowed to potentially degrade availability.

What might be done to improve availability? Well thing like:

- Local loop path diversity and redundancy
- Better power protection (more local power feeds, better backup generators with more fuel on hand and more frequent testing)
- More emphasis on disaster recovery and business continuity planning
- Hardening facilities against easily understood low tech threats such as vandalism involving gun fire,¹⁷ and more-complex high tech threats such as space weather¹⁸ and electromagnetic pulse attacks¹⁹

Unrestricted Data Collection. In **paragraph 224** the NPRM states: "We seek comment on the effect of unrestricted data collection practices on data security, as well as the relationship to the concept of privacy-by-design. If we do adopt rules restricting the types of data BIAS providers can collect, will there be negative societal consequences? For example, data collected in conjunction with other online services has yielded services such as spam filters that use a variety of data for "machine learning." Are there particular types of customer data, such as health information, that a provider should be prohibited from collecting? Could such a requirement be implemented and operationalized without undue burden? Is it possible for a BIAS provider to reasonably distinguish between types of data that it collects such that it could comply with such a requirement?"

We urge you to distinguish between information about **customers** (including things such as their race, religious preferences, or health information) that have nothing to do with cyber security, VS. information about **network traffic, system configurations, and similar areas** where that information can be of critical importance to resisting attacks and preventing compromised systems and networks. This is a simple "bright line" that any provider should be able to easily maintain.

Spam filtering, for example, is a distinct challenge, and one where the Commission should do all it can to support anti-spam technology development and deployment, including facilitating the prosecution of those who would attempt to spam customers notwithstanding existing legal and technical anti-spam efforts.

Data destruction. In **paragraph 231** the NPRM states "We seek comment on whether we should adopt data destruction requirements and, if so, how sensitive data should be disposed of when it is no longer needed. Should we follow the model laid out by the Fair and Accurate Credit Transactions Act (FACTA), which requires the proper disposal of information contained in consumer reports and records? Under the FTC disposal rule, which implements FACTA with respect to companies under the FTC's jurisdiction, companies must "tak[e] reasonable measures to protect against unauthorized access to or use of [consumer] information in connection with its disposal." The rule offers a non-exhaustive list of such reasonable measures that includes burning, pulverizing, or shredding paper so that they are unreadable and cannot be practicably reconstructed and destroying or erasing electronic media such that it cannot be practicably read or reconstructed. Should we take a similar approach here? Several states have also enacted laws regarding the disposal of records that contain personal information. Should we look to any such state laws for guidance?"

We support appropriate data destruction standards. As previously mentioned, we recommend that the Commission look to NIST 800-88r1, "Guidelines for Media Sanitization"²⁰ as its default standard in this area. See also the NSA/CSS guidance related to this area.²¹

Breach Notification Standards. In **paragraph 237**, the Commission states that 'We seek comment on under what circumstances BIAS providers should be required to notify customers of a breach of customer PI. For consistency and to minimize burdens on breached entities, we look to other federal statutes and other jurisdictions as a basis for determining when it is appropriate to notify, or not notify, consumers of a breach of customer PI. Various state regulations employ a variety of triggers to address this challenge. We seek comment on whether some of these state requirements would also effectively serve our purpose. For example, some states do not require disclosure if, after an appropriate investigation, the covered entity determines that there is not a reasonable likelihood that harm to the consumers will result from the breach. Should we require breach reporting based on the likelihood of misuse of the data that has been breached or of harm to the consumer? If so, how would broadband providers, and the Commission, determine the likelihood of misuse or harm? If we adopted such a standard, is it necessary to clarify what is meant by "misuse" or "harm"? Is it necessary to also require the provider to consult with federal law enforcement when determining whether there is a reasonable likelihood of harm or misuse?'

When it comes to data breaches, some entities may do all they can to avoid notifying users, even in the face of overwhelming evidence that an intrusion occurred. We recommend that you AVOID adopting a standard that requires a probable showing of harm, or definitive evidence that exfiltration occurred. We recommend a four part test:

- 1) It is more likely than not that an intrusion or other unauthorized disclosure took place, or the device was not under the control of its authorized user (e.g., it was lost or stolen). For the avoidance of doubt, if a third party assessor is employed, and they believe an intrusion or loss of control incident occurred, this requirement shall be satisfied.
- 2) Customer PI was on the device or system
- 3) The private information was not securely encrypted and thus inaccessible notwithstanding the intrusion or loss of control
- 4) The intruder or unauthorized user had access to the data (e.g., they succeeded in logging in to the account that had the sensitive information, or they obtained administrator credentials ("root" access on a Unix system).

If a system is lost or stolen and the circumstances associated with that loss cannot be definitively ascertained, the assumption should be made that the data on the system **has been breached** (e.g., if it isn't know if the laptop was encrypted, or it isn't know how far "into" the system the intruder may have gotten).

Deep Packet Inspection. In [paragraph 264](#), the Commission states "We seek comment whether the use of DPI for purposes other than providing broadband services, and reasonable management thereof, should be prohibited or otherwise subject to a heightened approval framework. DPI involves analyzing Internet traffic beyond the basic header information necessary to route a data packet over the Internet. DPI is used by network operators to gather information about the contents of a particular data packet, and may be used for reasonable network management, such as some tailored network security practices. In addition, DPI has been used by network providers in order to serve targeted advertisements. DPI has also been used by network providers to identify and block specific packets."

Deep packet inspection is a potentially valuable tool, however, if network traffic is encrypted as it should be, it should be generally infeasible. We recommend that the Commission render this issue moot by requiring providers to encrypt traffic whenever possible.

Deep Packet Inspection for Marketing Purposes. In [paragraphs 265-266](#), we see that 'The FTC has found that the use of DPI by Internet service providers for marketing purposes raises unique privacy concerns. Noting that broadband providers are uniquely situated as a "gateway" to the Internet, the FTC has found that "ISPs are thus in a position to develop highly detailed and comprehensive profiles of their customers—and to do so in a manner that may be completely invisible." The 2012 FTC Privacy Report also noted that switching costs and a lack of competitive options for broadband service may inhibit consumers' ability to avoid these practices, should they wish to do so. As a result, the FTC voiced "strong concerns about the use of DPI for purposes inconsistent with an ISP's interaction with a consumer," and called for express consumer consent requirements, or more robust protections, as a precondition for their use. We seek comment whether BIAS providers' use of DPI for purposes other than providing broadband services, or as required by law, should be prohibited. Should such practices be subject to either the opt-out or opt-in requirements we have proposed above, or heightened approval requirements? For what purposes do broadband providers engage in DPI? What would be the benefits and drawbacks of prohibiting the use of DPI for purposes other than providing BIAS? What would be the costs to consumers and BIAS providers of such a prohibition?'

Providers should be forbidden from employing DPI for marketing-related purposes. Any other use of DPI should be fully disclosed to customers in thorough detail as part of the customer's privacy policy, including what's collected, how that information is collected, why that information is needed, how long that information is retained and under what circumstances that information is shared with third parties.

Persistent Tracking Technologies. In [paragraphs 268-270](#) the Commission states 'We seek comment whether the use of persistent tracking technologies should be prohibited, or subject to opt-out or opt-in consent. Under our proposed rules, certain types of information used in persistent tracking technologies, such as unique identifiers, would be considered both

CPNI and PII. The use of persistent tracking technologies may allow network operators to obtain detailed insight into their customers' Internet usage. For example, UIDH, injected by carriers into the HTTP header of a data packet, allow BIAS providers to repackage and use customer data for targeted advertising purposes. Unlike cookies, which are located in a web browser and may be controlled locally, UIDH are injected by carriers at the network level, thereby preventing customers from removing them directly. The Enforcement Bureau recently entered into a consent decree with a carrier that used UIDH without obtaining informed consent from its customers. As part of the Consent Decree, the carrier paid a fine and agreed to obtain opt-in approval from its customers before sending UIDH to third-party websites. We seek comment on what other technologies can be used by BIAS providers to track broadband users and their devices, either by storing information (e.g., cookies), collecting partially unique information (e.g., fingerprinting) or associating information at the network level (e.g., UIDH). Do these technologies pose a privacy risk to BIAS customers and, if so, what are the best ways to protect customers' private information and enhance customer control? We seek comment on whether the use of persistent tracking technologies may expose BIAS customers to unique privacy harms, and as such, whether the Commission should prohibit BIAS providers from employing such practices to collect and use customer PI and CPNI. Alternatively, should the use of persistent tracking technologies be subject to opt-in or opt-out consent? Do customers understand how BIAS providers are using this technology such that notice and the opportunity to approve such uses is "informed"? How do BIAS providers use the information gleaned from such technologies? What are the benefits to customers of such technology, if any? What would be the benefits and drawbacks to prohibiting such practices, or subjecting their use to opt-in or opt-out approval? Under what authority could the Commission prohibit BIAS providers' deployment of such technologies? Does the use of such technology violate BIAS providers' duty to protect the confidentiality of customer information, with or without customer approval? Does it violate any other provisions of the Communications Act?'

We oppose all use of persistent tracking technologies and recommend that the Commission ban their use, with the exception that providers may allow users to login, and having done so, have different access than an unlogged-in customers.

In the alternative, if persistent tracking technologies cannot be banned outright, they should only be allowed on an opt-in basis after full disclosure of their deployment and implications.

Industry Framework. Paragraph 280: "[...] They also contend that any such rules should not apply to any information that has been de-identified, aggregated, or does not otherwise identify a known individual."

We support such a standard.

Continuing in *paragraph 282:* "[...] the Industry Framework specifies that consumers need not be given a choice when their information will be used for product or service fulfillment, fraud prevention, compliance with law, responses to government requests, network management, first-party marketing, and affiliate sharing where the affiliate relationship is reasonably clear to consumers. [...] We seek comment on these proposals."

We support the quoted framework excerpt EXCEPT for:

- "responses to government requests:" a court order, subpoena or similar legal paperwork must be presented; a simple government "ask" is not procedurally sufficient
- "first-party marketing:" ANY marketing use should require the customer to have first opted-in; the assumption should be that marketing communications are NOT wanted by default
- "affiliate sharing where the affiliate relationship is reasonably clear to consumers" -- like first-party marketing, any marketing communication can only proceed if the customer has affirmatively opted-in.

Privacy Enhancing Tools and Techniques: In **paragraph 284** the Commission reports that: "[...] Public Knowledge also recommends that we prohibit BIAS providers from interfering with customers' privacy enhancing tools and techniques, such as blocking tracking software or clearing it from caches."

We urge the Commission to distinguish between two categories of privacy enhancing tools and techniques:

- Passive privacy enhancing tools and techniques such as blocking tracking software should NOT be interfered with; customers should be allowed to employ countermeasures against attempts to track them.
- Active anonymization techniques (such as use of Tor) should also be permitted, however a customer should be held responsible for what come out of his or her network address. Such a standard will help to ensure that the worthy goals of anonymization projects such as Tor are facilitated, while also ensuring that exit nodes are configured in ways that minimize abuse such as email spam.

Public Knowledge's Recommendations Around DPI. In **paragraph 285** the Commission states that "The PK Framework also includes recommendations on two particular practices: deep packet inspection and differential privacy protections based on discounts or other inducements. With regard to deep packet inspection, the PK Framework suggests that consent to use or disclose CPNI does not mean consent to use or disclose communications content. Public Knowledge further recommends that we prohibit "any provider under any circumstances from using DPI or other tools to view the content of subscriber traffic."

Appropriate adoption of encryption should render this debate moot, however, for the sake of argument, if encryption were to suddenly become impossible, we'd OPPOSE a blanket ban on DPI since it might potentially be interpreted as banning things like spam, phishing or malware filtering.

EPIC Framework recommendations. In **paragraph 287** the Commission states: "EPIC Framework. [...] Third, the EPIC Framework recommends we promote privacy enhancing technologies such as "Do Not Track" mechanisms. Fourth, the EPIC Framework argues that all Internet-based service providers obtain opt-in consent for the use or disclosure of consumer data."

We support these recommendations.

III. Process Notes

Too Long! The length and level of detail involved in this NPRM was (and is!) daunting. It basically covers all topics directly or tangentially related to privacy. At 147 pages (including appendices and Commissioner statements), and 492 footnotes, it is just *too long*. We suspect that many potential individual commenters, including those who may have strong feelings about privacy-related issues, may be inhibited from commenting by the sheer breadth of this inquiry and the myriad questions it raises. Asking **many** questions is an excellent strategy if you want to hear **few** answers, but we find it hard to believe that that was the Commission's intent. Nonetheless, we believe this NPRM has intimidated many potential commentators into stunned silence, and thus has missed the mark. Many who might have commented simply won't bother because you've asked for too much, even for a topic as important as this one.

We suggest that you'd get a broader range of responses, and likely more thoughtful responses, if you focused on just a single area or perhaps two or three areas, rather than trying to run one omnibus/marathon process that attempts to encompass "all things privacy" with topics ranging from:

- Personally identifiable information
- Data sharing and anonymization
- Data breach prevention and response
- Online tracking and marketing
- Opt-in vs. opt-out permission management
- Identity management and authentication, including multifactor authentication

- Deep packet inspection (DPI)
- Privacy-enhancing tools
- Security best practices for providers
- etc.

We applaud your enthusiasm, but this NPRM went too far. We urge any future Commission NPRMs where the Commission wants broad input to be no more than 20% of the size of this one.

Avoid Asking The Same Question Multiple Times: Perhaps due to the length and breadth of this NPRM, we noticed numerous occasions when the same topic was raised multiple times. This repetition adds unnecessarily to the length of the NPRM and complicates the work of commentators. Unless this was done intentionally as a sort of "consistency" or "validity" check, please avoid asking the same question multiple times in the same solicitation.

Please also consider numbering each individual question to simplify the response process, rather than embedding multiple questions in a single numbered paragraph.

If there are superficially similar questions with subtle but important difference between two questions, please emphasize those differences or compare/contrast the similar questions so commentators can understand any subtle but important differences that may genuinely exist.

IV. Conclusion

Thank you for the opportunity to comment on these proposed rules. Farsight Security, Inc., stands ready to address any follow up comments or questions you may have.

¹ <http://www.farsightsecurity.com/>

² https://en.wikipedia.org/wiki/IPv6_address#Modified_EUI-64

³ <https://legiscan.com/OR/text/SB601/id/1242304/Oregon-2015-SB601-Enrolled.pdf>

⁴ <https://addons.mozilla.org/en-US/firefox/extensions/?sort=users>

⁵ https://en.wikipedia.org/wiki/List_of_HTTP_header_fields

⁶ https://en.wikipedia.org/wiki/Pinky_swear

⁷ <http://csrc.nist.gov/groups/SMA/ate/>

⁸ https://www.schneier.com/blog/archives/2013/03/security_aware_1.html

⁹ <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>

¹⁰ https://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/

¹¹ <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf> at PDF page 8.

¹² <https://duo.com/>

¹³ You can see a list of nearly a hundred universities or university systems that have standardized on Duo as a multifactor solution at <http://www.incommon.org/duo/subscribers.html>

¹⁴ "Multi-Factor Authentication: Do I Need It, Should I Get Started? [And If I Do Need It, Why Aren't Folks Deploying It?]," <https://www.stsauer.com/joe/global-summit-mfa/global-summit-mfa.pdf>

¹⁵ <http://www.nist.gov/nstic/>

¹⁶ <https://www.dragonresearchgroup.org/insight/sshpwauth-tac.html>

¹⁷ https://en.wikipedia.org/wiki/Metcalf_sniper_attack

¹⁸ <http://www.bbc.com/news/science-environment-29525154>

¹⁹ <http://www.empcommission.org/>

²⁰ <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>

²¹ https://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/