Federal Communications Commission
Office of Legislative Affairs
Washington, D.C. 20554

Office of the Director

June 29, 2016

The Honorable Charles E. Grassley
Chairman
Committee on the Judiciary
United States Senate
224 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Grassley:

Enclosed please find responses to Questions for the Record submitted for Chairman Tom Wheeler regarding his appearance before the Subcommittee on Privacy, Technology and the Law on May 11, 2016 at the hearing entitled "Examining the Proposed FCC Privacy Rules."

If you have further questions, please contact me at (202) 418-0095.

Sincerely,

Michael Dabbs
Director

Enclosure

Attachment I - Additional Questions for the Record

The Honorable Jeff Flake

1. **Has the FCC performed any preliminary cost-benefit analysis of (1) the need for its proposed privacy rule and (2) the impact of its proposed privacy rule?**

    a. **If so, please provide my staff with any results of these analyses.**
    b. **If not, why not?**
        i. **Does the FCC intend to undertake any preliminary cost-benefit analysis before promulgating its privacy rule?**
        ii. **If not, what other actions does the FCC intend to take in order follow the "General Principles of Regulation" suggested in Executive Order 13,563, "Improving Regulation and Regulatory Review"? ("Our regulatory system … must take into account benefits and costs, both quantitative and qualitative.")**

    Response: The FCC has not performed a preliminary cost-benefit analysis of the need for or impact of the proposed privacy rules. We welcome comments on the relative costs and benefits, both quantitative and qualitative, of the proposed rules and any alternatives for which commenters advocate. Additionally, the NPRM seeks comment on ways to reduce any burden from the proposed rules on small providers of broadband internet access services ("BIAS").

    The FCC intends to consider any comments on the relative costs and benefits of the proposed rules and any alternative rules proposed. Regarding what actions the FCC intends to take to follow the principles suggested in Executive Order 13563, to the extent that this Executive Order applies requirements to independent agencies, we have taken steps to act consistently with the principles articulated within.

2. **Has the FCC identified any concrete examples of abuses, harms or risks that have been associated with BIAS providers regarding online privacy?**

    Response: In March 2016, the Enforcement Bureau ("EB") settled its investigation into Verizon's alleged failure to inform, or accurately inform, Verizon customers of its insertion of unique identifier headers ("UIDH" or so-called "super-cookies") into consumers' mobile internet search traffic, as well as Verizon's alleged failure to obtain customer consent to use UIDH. UIDH was inserted into consumer's internet search traffic to facilitate targeted advertising. EB's investigation found that, also unbeknownst to Verizon consumers, third parties were using Verizon's UIDH for their own purposes, which included restoring cookie IDs that customers had cleared from their browsers. This was allegedly done without Verizon customers' knowledge or consent, thereby circumventing consumer choice.

    In the wake of our investigation and the subsequent $1.35 million settlement agreement, Verizon Wireless must now notify consumers about its use of UIDH for its targeted advertising programs. Moreover, Verizon must obtain customers' opt-in consent before

sharing UIDH with third parties, and obtain either opt-in or opt-out consent before sharing it internally among Verizon corporate affiliates.

3. Has the FCC initiated any enforcement actions against BIAS providers regarding online privacy since March 2016? If so, please identify them for my staff.

Response: The Commission's ongoing enforcement investigations are confidential and law enforcement sensitive. To preserve the fairness of the adjudicatory process, we cannot disclose information about ongoing enforcement investigations. However, please see the above response to question number two, which discusses the FCC's March 2016 settlement with Verizon over its alleged failure to inform, or accurately inform, Verizon customers of its insertion of UIDH into consumers' mobile internet search traffic, as well as Verizon's alleged failure to obtain consumer consent to use UIDH.

4. How does FCC's current enforcement position under 222(a), as articulated in the May 20, 2015, Enforcement Bureau Guidance, differ from that proposed by the NPRM?

a. If it does not, why is the FCC undertaking a rulemaking?

Response: When the Commission reclassified BIAS as a telecommunications service in the *Open Internet Order*, we declined to forbear from applying Section 222 of the Communications Act of 1934, as amended ("Communications Act" or "Act') to BIAS providers. However, we did forbear from applying the existing rules implementing Section 222 to BIAS providers. The Enforcement Bureau Guidance you reference in your question provides guidance to BIAS providers about how EB intends to enforce Section 222's requirements during the time between the effective date of the *Open Internet Order* and any subsequent Commission action providing further guidance or adopting regulations that would apply Section 222 more specifically to BIAS. This Guidance also explained that, in the interim, EB will focus on whether broadband providers are taking reasonable, good-faith steps to comply with Section 222.

The NPRM proposes specific rules to implement the requirements of Section 222. These proposed rules focus on transparency, consumer choice, and data security. However, these rules are not final. We are currently in the middle of a rulemaking proceeding, and are seeking comment on multiple issues associated with applying Section 222(a) to BIAS providers. We have heard, and expect to continue to hear, from industry and consumers regarding these proposed rules. The final rules will be informed by this input.

Once the comment period has concluded, all comments have been reviewed, and the final rules have been developed and approved by the Commission, these final rules will give BIAS providers and their customers certainty about consumer privacy protections. These rules will provide consumers with: (1) clear expectations about how their information is used, stored, and shared; (2) how their privacy rights will be protected; and (3) what they can do to exercise those privacy rights.

5. **Did the FCC "identify and assess alternative forms of regulation and … to the extent feasible, specify performance objectives, rather than specifying the behavior or manner of compliance that regulated entities must adopt" as suggested by Executive Order 12,866 ("Regulatory Planning and Review")?**

   a. **If so, please provide my staff with that assessment.**
   b. **If not, why not?**

   Response: To the extent that this Executive Order applies requirements to independent agencies, we have taken steps to act consistently with the principles articulated within.

   In the NPRM, the FCC seeks comment both on specific proposals to protect the privacy of BIAS customers' data and a wide variety of approaches for doing so. The FCC's proposals are intended to be flexible and goal oriented. Therefore, the proposals aim not to be overly prescriptive. For example, the NPRM proposes rules that would require BIAS providers to adopt data security practices that are technically feasible, yet calibrated to the nature and scope of the provider's activities as well as the sensitivity of the data.

6. **Please explain with particularity if and how the FCC has complied with the President Clinton and President Obama Executive Orders on Regulation with respect to the NPRM. In particular:**

   a. **What specific steps did the FCC take to comply with Executive Order 13,619 ("Identifying and Reducing Regulatory Burdens")?**
   b. **What specific steps did the FCC take to comply with Executive Order 13,609 ("Promoting International Regulatory Cooperation")?**
   c. **What specific steps did the FCC take to comply with Executive Order 13,579 ("Regulation and Independent Regulatory Agencies")?**
   d. **What specific steps did the FCC take to comply with Executive Order 13,563 ("Improving Regulation and Regulatory Review")?**
   e. **What specific steps did the FCC take to comply with Executive Order 12,866 ("Regulatory Planning and Review, and Amendments")?**

   Response: To the extent that these Executive Orders apply requirements to independent agencies, we have taken steps to act consistently with the principles articulated within.

7. **In what ways is the proposed rule in the NPRM different from EU privacy law?**

   a. **In what ways are they similar?**

   Response: It is important to first note that the General Data Protection Regulation ("GDPR" or "Regulation") is an adopted and final regulation. The FCC's proposed rules are neither adopted nor final. The proposed rules are simply proposals upon which we seek comment. Additionally, we welcome commenters to propose alternative proposals.

As you may be aware, the European Union ("EU") recently released the GDPR, which will go into effect on May 25, 2018. Once it goes into effect, the GDPR will replace the existing EU Data Protection Directive of 1995 ("Directive"). Unlike the Directive, the GDPR will apply directly to EU member states.

One principal difference between the GDPR and the Commission's proposed rules is the regulations' scope. The GDPR applies broadly to all "processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system." In contrast, consistent with the more sector-specific approach taken in U.S. privacy law (as reflected the Communications Act, as well as the governing statutes for HIPAA, FERPA, and others), the Commission's proposed rules would only apply to the use and disclosure of personal information that BIAS providers obtain by virtue of providing an internet access service.

In terms of specific requirements, the Commission's proposed rules and the GDPR both focus on transparency, choice, and data security. This is not surprising, given that these principles are at the heart of the well-regarded Fair Information Practice Principles ("FIPPs"). But the GDPR's approach in regulating these foundational values varies significantly from our proposed approach. The GDPR sets out its requirements in much greater detail, which is evidenced by the document's significant length. Following 173 preambles, there are 57 pages of regulations. In contrast, the FCC's proposed regulations (found in Appendix A of the NPRM) are 10 pages long. Moreover, the GDPR's regulations address topics not included in our proposed rules, such as the concept of a "right to be forgotten." In short, the GDPR and NPRM differ in scope and specificity, despite sharing certain high-level goals.

8. How does the FCC cabin its discretion to impose penalties and forfeitures against BIAS providers in light of its conclusion that Terracom and YourTel America could have been liable for as much as $9 billion?

a. Will the FCC address its discretion to impose penalties in the final rule?

Response: In 2014, the Commission released a Notice of Apparent Liability for Forfeiture ("NAL") against the two carriers after EB's investigation revealed that more than 300,000 customers' personal information was stored on unprotected, internet-accessible servers. This personal information included names, Social Security numbers, driver's license numbers, and other sensitive information. Because the companies failed to provide reasonable protection for their customers' personal information, anyone with access to a search engine could gain unauthorized access to this sensitive customer proprietary information ("PI").

In the NAL, the Commission found that the carriers apparently, willfully, and repeatedly violated Sections 201(b) and 222(a) of the Communications Act of 1934 as amended. The carriers: (1) failed to reasonably protect the confidentiality of consumers' PI, which the carriers collected and stored; (2) failed to employ reasonable data security practices to protect consumers' PI; (3) engaged in deceptive and misleading practices by misrepresenting to

consumers in the companies' privacy policies that they employed appropriate technologies to protect consumers' PI when they had not; and (4) engaged in unjust and unreasonable practices by failing to inform consumers that their PI had been compromised.

Based on the Commission's review of the facts and circumstances surrounding the apparent violations, the Commission proposed a forfeiture of $10 million. As required in 47 U.S.C. § 503(b)(2)(E), to determine the forfeiture amount, the Commission considered "the nature, circumstances, extent, and gravity of the violation and, with respect to the violater, the degree of culpability, any history of prior offenses, ability to pay, and such other matters as justice may require." In July 2015, the Commission settled the case against TerraCom and YourTel America for $3.5 million.

The Commission would be required by 47 U.S.C § 503(b)(2)(E) to apply the same statutory factors in determining an appropriate forfeiture amount in any enforcement action against BIAS providers. Additionally, in 1997 the FCC adopted a "Forfeiture Policy Statement" that established guidelines for the Commission to consider when determining Section 503(b) forfeiture amounts. The purpose of these guidelines is to "provide the needed measure of predictability to the process and uniformity to our administrative sanctions." The guidelines provide a non-exhaustive list of violations and base forfeiture amounts for each violation. These base amounts are significantly lower than the Section 503(b) maximum forfeiture amounts.

While Section 503(b) of the Act authorizes the Commission to impose a maximum forfeiture, the Commission will continue to exercise its discretion, in light of the evidence and the statutory factors in 47 U.S.C. §503(b)(2)(E), to propose and impose an appropriate forfeiture.

Regarding whether the Commission will address its discretion to impose penalties in the final rule, it is premature to say. The Commission is still evaluating the hundreds of thousands of comments filed in this proceeding.

9. Does any other federal or state agency have the power and discretion to impose $9 billion penalties on non-BIAS providers for alleged online privacy violations?

Response: We are not in a position to comment on the legal authorities and jurisdictional reach of other federal or state agencies' penalty authority.

10. What evidence does the FCC have that consumers are less able or likely to switch their BIAS providers than their search engines or social networks?

Response: Consumers face high costs when changing BIAS providers. Among the costs that consumers may experience are: (1) early termination fees; (2) installation fees; (3) activation fees; and (4) the cost of new or replacement equipment (if owned equipment is not compatible with the new service). Further, a lack of alternative BIAS providers may mean that consumers have no choice in BIAS provider. In contrast, consumers can choose to use (or not use) a website or application ("app") on a minute-by-minute basis, as the process of

switching search engine, web browser, or social network typically involves the click of a button.

11. Has the FCC conducted any economic studies of technological innovation in the pre-broadband internet? If so, please provide them to my staff.

a. If not, why not?

Response: The Commission has long given careful thought to economic consideration of technological innovation over the network. Many of the Commission's policies over the years have sought to promote innovation both in common carrier networks and among activities occurring over the carrier's network.

For example, in 1966, three years before the birth of the ARPANET, the FCC began its consideration of the interdependence and confluence of computer and communications services with the Computer Inquiries. This examination recognized that the economic and innovative promise of the computer era would rely on the underlying communications carriers. The Computer Inquiries thus sought to directly address the ability of communications carriers to foster and support computer services. As one senior Commission staffer, Bernard Strassburg, explained around the time the first Computer Inquiry (*Computer I*) was initiated, "[f]ew products of modern technology have as much potential for social, economic, and cultural benefit as does the multiple access computer."

Multiple Commission documents from the pre-broadband era reflect economic consideration of technological innovation for computer services and what came to be known as the internet. They are listed below and attached as supplements to this response:

- The Computer Inquiries;
- The Stanford Research Institute reports, commissioned under *Computer I*, which directly addressed how to foster an open communications platform upon which innovation could transpire;
- OSP Working Paper 29 (March 1997), more commonly known as Kevin Werbach's "Digital Tornado: The Internet and Telecommunications Policy," which directly addresses how the internet fits within communications policy and discusses how the internet enables innovation; and
- The Stevens Report of 1998, in which the FCC considered the position of the internet within communications policy following the Telecommunications Act of 1996.

12. Has the FCC conducted any economic studies of technological innovation in the terrestrial telephone market over the last 30 years? If so, please provide them to my staff.

a. If not, why not?

Response: The sources referenced in my response to question 11 also reflect economic studies of technological innovation in the terrestrial telephone market over the last 30 years.

Moreover, since 1998, the Commission has consistently produced a report entitled "Trends in Telephone Service." This report contains summary information about the size, growth, and development of the telephone industry, including data on market shares, minutes of calling, number of lines, and telephone subscribership. The report also provides information about access charges, advanced telecommunications and broadband services, consumer expenditures for service, infrastructure, international telephone traffic, local telephone competition, telephone rates and price changes, toll service providers, and universal service support. All of these reports are available online: https://www.fcc.gov/general/trends-telephone-service.

13. **Has the FCC conducted any economic studies of technological innovation in the mobile telephone market over the last 30 years? If so, please provide them to my staff.**

    a. If not, why not?

    Response: Per congressional directive, the FCC releases annually the "Mobile Wireless Competition Report," which analyzes competitive conditions in the mobile wireless industry and contains data and information related to, among other areas, the number of subscribers and connected devices; price metrics; usage levels; percentage of the population covered by a certain number of providers; investment and profitability measures; and market concentration figures. More recent reports have included an examination of spectrum holdings; backhaul; infrastructure; devices; and mobile operating systems and applications. The first report was released in 1995, with the most recent version, the Eighteenth Report, issued earlier this year. Copies of the annual reports are available at: https://www.fcc.gov/reports-research/reports/commercial-mobile-radio-services-competition-reports.

    In addition to the formal annual report focusing on the mobile wireless industry, the Commission has undertaken analysis of technological innovation in the mobile telephone market in other proceedings where the mobile industry is not the sole focus, as well as in rulemakings that concern the mobile wireless industry. Some recent examples of focused mobile analysis in broader items include the most recent Broadband Progress Report, available at https://www.fcc.gov/reports-research/reports/broadband-progress-reports/2016-broadband-progress-report, and the National Broadband Plan, available at https://www.fcc.gov/general/national-broadband-plan.

14. **In your Net Neutrality NPRM you stated, "We interpret sections 706(a) and (b) as independent and overlapping grants of authority that give the Commission the flexibility to encourage deployment of broadband internet access service through a variety of regulatory methods, including removal of barriers to infrastructure investment and promoting competition in the telecommunications market, and, in the case of section 706(b), giving the Commission the authority to act swiftly when it makes a negative finding of adequate deployment. The rules we propose today would be authorized by sections 706(a) and (b) because they would 'encourage the deployment' of advanced telecommunications capability by promoting competition in the telecommunications market and removing barriers to infrastructure investment." Under this reasoning, were the FCC to conclude that the privacy rules—against BIAS**

providers or the edge—would "encourage the deployment" of "advanced telecommunications capability", the rules would arguably be authorized by Section 706.

a. You testified before the Subcommittee that "Sec. 706 is something we've asked about in the proceeding and has a bearing on this but we're doing it under Sec. 222 of Title II."
   i. What does "a bearing" mean?
   ii. Do you have the *legal authority* to regulate BIAS provider privacy practices under Section 706?
   iii. If not, why not?

Response: Our proposed broadband privacy rules seek comment on whether our Section 706 authority supports these rules. The scope of the Commission authority's under this Section has been the subject of significant debate in the comments, and the time for input is not yet over. Neither the FCC nor a court has opined on this question, and we welcome the views of commenters in this proceeding. Since the record has not yet closed—and my fellow Commissioners have not had a chance to have their say on this—it would be premature to definitively answer this important question.

b. You testified before the Subcommittee that you "do not *intend* to impose these rules on edge providers."
   i. Do you have the *legal authority* to impose these rules on edge providers under Section 706?
   ii. If not, why not?

Response: As I have repeatedly said, edge providers are outside of the scope of this rulemaking. This rulemaking proposes rules that would apply to broadband internet access service providers. Whether or not the Commission has legal authority under Section 706 to impose rules on edge providers is not at issue in the broadband privacy NPRM.

15. Why did the FCC choose to begin this proceeding while the Title II Order is still under review?

a. If the Court of Appeals strikes down the Title II Order as it relates to broadband, would it moot this proceeding?
b. If the Court of Appeals strikes down the Title II Order as it relates to wireless broadband, how will that affect this proceeding?
c. Does the FCC intend to issue a new NPRM responding the the Court of Appeals decision when it comes down?
   i. If not, why not?

Response: As a result of classifying broadband internet access service as a telecommunications service, section 222 of the Act necessarily applied. In the *Open Internet Order*, the Commission stated that it intended to commence a rulemaking to clarify obligations under that provision. Indeed, providers have complained that without further guidance, they do not know how to comply with the Act—and have argued as much in a

request to stay the *Open Internet Order*. It is therefore incumbent on the Commission, and on me as Chairman, to bring greater clarity to what broadband providers are expected to do in order to comply with section 222 of the Act—and to do so in a timely manner.

In response to questions (a)-(c), since the U.S. Court of Appeals for the D.C. Circuit ("D.C. Circuit") upheld the *Open Internet Order* in its entirety: (a) this proceeding is not mooted; (b) there was no effect on this proceeding; and (c) no further NPRM is necessary.

16. The NPRM, relying on the 2012 FTC privacy report, states: "Today, as the FTC has explained, BIAS providers are '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.'" But, as a report by Peter Swire of Georgia Tech explains, a substantial and increasing amount of online traffic is encrypted — including both DNS queries and substantive data — which substantially limits the data available to BIAS providers. And technologies such as VPNs, some of which are designed specifically to address these sorts of privacy concerns, are increasingly being designed and made available for ordinary internet users. For instance, just last month one of the major web browsers added a built in, easy-to-use, VPN service to its web browser.

a. Is that 2012 FTC report is still accurate, or has it been overtaken by changes in technology over the last 4 years?

Response: Regardless of technological advances, the fact remains that BIAS providers maintain a unique position with customers. Unlike edge providers or websites, a BIAS provider carries all of a customer's internet traffic and has some visibility into all—and detailed visibility into a lot—of a customer's online behavior, including a tremendous amount of personal information, even if encrypted. This is a different relationship than the one customers have with a website or app that they can choose to use (or not use) on a minute-by-minute basis.

b. What happens to this rule if technological change does overtake them?

i. Will the FCC go through a rulemaking in the future to address any technological concerns relating to privacy?

ii. What factors will inform any such decision by the FCC?

Response: We have proposed rules that are intended to be flexible enough to adapt to technological change. I expect any final rules we adopt to be similarly flexible. I cannot say what a future Commission might choose to do, as rules can be amended and updated, and I cannot speak to the factors that a future Commission may choose to rely upon when deciding whether to pursue a future rulemaking. I can tell you that I think the hallmarks of any rules the Commission adopts on broadband privacy should be ensuring consumers have the benefit of transparency, choice, and data security.

17. Peter Swire recently published a comprehensive report on BIAS providers and privacy.

a. In this report Swire observes, "[U]sers today often connect to the internet with multiple devices and from multiple locations, and at far higher speeds. This means that any single BIAS provider views a diminishing portion of a user's internet activity, and that the portion they do not carry represents an enormous and growing volume of data and transactions."

i. Do you disagree?

ii. How will the FCC intend to address this argument in its final rule?

Response: Technical evidence in the record suggests that use of multiple devices increases the granularity of customer data that a BIAS provider can collect. Further evidence in the record shows that in a mobile context, connecting to the internet from multiple locations might yield more data for a mobile BIAS provider due to the location information derived.

Regarding the FCC's intended response to this argument, it is premature to say. We are currently still evaluating public comments from a diverse set of stakeholders.

b. Swire also observes, "With encrypted content, BIAS providers cannot see detailed URLs and content even if they try."

i. Do you disagree?

ii. How will the FCC intend to address this argument in its final rule?

Response: Technical evidence in the record indicates that a BIAS provider can still derive significant data about customer internet use even with encrypted content. For example, a BIAS providers can still see the websites customers visit, how often they visit them, and the amount of time they spend on each website. Using this information, the BIAS provider can piece together enormous amounts of information about an individual—including private information such as whether a customer has a medical condition or financial concerns.

Regarding the FCC's intended response to this argument, it is premature to say. We are currently still evaluating public comments from a diverse set of stakeholders.

c. Swire also observes, "[W]idespread use of Virtual Private Networks ("VPNs") and third-party proxy services, are further limiting BIAS provider visibility."

i. Do you disagree?

ii. How will the FCC intend to address this argument in its final rule?

Response: Technical evidence in the record indicates that VPNs are not being widely adopted and, even when used, still provide incomplete protection for consumers.

Regarding the FCC's intended response to this argument, it is premature to say. We are currently still evaluating public comments from a diverse set of stakeholders.

18. During your testimony you said, "There has always been this relationship between networks and consumers that we respect that information because we're only getting it because we have to have it for the network to work. This is a retreat from privacy. This is a retreat from what Americans have always expected from their networks."

a. Since this relationship has "always" existed between networks and consumers, please provide my staff with each BIAS provider that this applied to prior to 2015 in their capacity as BIAS providers.

i. Please list all orders issued by the FCC between the enactment of Section 222 in 1996 and 2000 showing that a BIAS provider was required to comply with Section 222.

Response: In my testimony, I referred to consumers' expectations of privacy when using communications networks. This expectation of privacy derives from consumers' long-standing relationship with their telephone service provider. Consumers expect their communications providers to keep information about how consumers use communications networks private and secure. Consumers have the same expectations of privacy when using broadband internet networks, the communications network of the 21st Century. Additionally, a large percentage of consumers receive internet access service from companies that have traditionally provided them telephone service (such as AT&T and Verizon). Consumers have relied upon these communications providers to keep their communications information private and secure for decades. That reliance should not change just because they are using BIAS.

b. What enforcement or regulatory actions did the FCC take between 1985 and 1995 to protect user privacy in the NSFnet?

i. Did the FCC require opt-in consent for any data use on the NSFnet?

Response: The FCC did not take any enforcement action to protect user privacy when using the NSFnet. The FCC did not set a specific consent standard for data use on NSFnet. NSFnet's appropriations act authorized NSF to support the use and development of this network "primarily for research and education in the sciences and engineering." Users took this to mean that use of NSFnet for commercial purposes was not allowed.

19. The proposed rule creates a strong disincentive for BIAS providers to develop innovative products that may benefit consumers in exchange for access to their personal information. For instance, some BIAS providers have considered offering discounted prices for internet service in exchange for receiving personalized advertisements from the BIAS provider. This NPRM sends a clear signal that the FCC disapproves of such programs and would expose BIAS providers that do try to develop such programs to potential government investigation and liability, making it less likely that they will be offered.

a. What steps, if any, has the FCC taken to study the potential impact this rule will have on the cost of internet access?

Response: Adopting rules to ensure transparency, choice, and security for customer data will inspire customer confidence in BIAS providers' services. The FCC's proposal is built on well-established principles and best practices—fundamentally, the notion that consumers deserve transparency, choice, and security with respect to their personal information. Requiring BIAS providers to follow these principles is entirely consistent with a competitive marketplace. For instance, nothing in the proposed rules would prevent a BIAS provider from using and sharing a customer's personal information so long as they obtain the customer's approval.

The NPRM recognizes that it is not unusual for consumers to receive perks in exchange for use of their personal information, and that "free" services in exchange for information are common in the broadband ecosystem, while at the same time acknowledging the concerns stemming from these practices. The NPRM invites comment on these concerns as well as the benefits to consumers of business practices that offer customers financial inducements for their consent to use and share their confidential information, and whether the Commission should adopt rules concerning the use of such practices.

20. As proposed, the rule has the potential to pose undue burdens on the ability of small carriers to comply with and meet the financial obligations that will come with this proposal.

a. What steps are being taken to ensure that the rule proposed in the NPRM do not place additional burdens on smaller, rural, and regional carriers?

Response: The NPRM seeks specific comment on the impact of the proposed rules on small BIAS providers and businesses. For example, the NPRM seeks comment on the effects of each proposals on small providers, compliance costs for small providers, as well as alternatives to the proposals that could reduce burdens for small providers. In addition, as required by the Regulatory Flexibility Act of 1980, as amended, the Commission prepared an Initial Regulatory Flexibility Analysis of the possible significant economic impact on small entities by the proposed rules, and sought comment on its analysis.

b. Will there be any separate treatment for small, rural, and regional carriers regarding delayed implementation or small business exemptions to new requirements?

Response: In formulating the proposed rules, the Commission sought to provide flexibility for small providers whenever possible. The Commission set standards and goals that providers may reach in whatever way is most efficient for them. The NPRM seeks specific comment on exemptions for small providers. For example, the NPRM seeks comment on whether there are any small provider-specific exemptions that the Commission might build into our proposed approval framework. The NPRM also proposes that any specific security measures employed by a BIAS provider take into consideration the nature and scope of the BIAS provider's activities. We proposed this sliding scale approach to afford sufficient flexibility for small providers while still protecting their customers. Ultimately, we will

frame our final rules, including how those rules affect small providers, based on the responses on the record.

c. What will the Commission do to make sure the views of smaller, rural, and regional BIAS providers are considered in the privacy rulemaking?

Response: As noted above, the NPRM seeks specific comment on the impact of the proposed rules on small providers and businesses. For example, the NPRM seeks comment on the effects of each of the proposals on small providers, compliance costs for small providers, as well as alternatives to the proposals that could reduce burdens for small providers. In addition, as required by the Regulatory Flexibility Act of 1980, as amended, the Commission prepared an Initial Regulatory Flexibility Analysis of the possible significant economic impact on small entities by the proposed rules, and sought comment on its analysis. Ultimately, we will frame our final rules, including how those rules affect small providers, on the record in response to the NPRM and accompanying Initial Regulatory Flexibility Analysis.

21. Currently, under the FTC model, the level of privacy protection consumers can expect tracks the sensitivity of the information being transmitted. That is, the level of privacy consumers can expect is based on *what* is being transmitted (e.g. sensitive v. non-sensitive information). Under the proposed FCC rule, however, this would change and the level of privacy protection consumers can expect would depend on how the information is transmitted. That is, the level of privacy consumers can expect will be based on *where* it is being shared (e.g. over a BIAS provider or an edge provider).

a. What steps is the FCC taking to educate the public on this change?

Response: The FCC's proposal marks the start of the rulemaking process. The interest of consumers animates the entire proceeding, and we believe that providing consumers with notice, transparency, and choice over how their personal information is used by BIAS providers will advance that goal. In any event, all members of the public have an opportunity to offer their views of how best to protect broadband customer privacy and the impact on consumers of different approaches. The FTC has filed very constructive comments in the proceeding, and the public has the opportunity to review the FTC's comments and file replies.

b. What steps is the FCC taking to remedy any consumer confusion that results from this change?

Response: As noted above, the FCC's proposal marks the start of the rulemaking process. The interest of consumers animates the entire proceeding, and we believe that providing consumers with notice, transparency, and choice over how their personal information is used by BIAS providers will advance that goal. In any event, all members of the public have an opportunity to offer their views of how best to protect broadband customer privacy and the impact on consumers of different approaches.

22. The FTC has a long history of dealing with consumer privacy issues. But before it issued its 2012 Privacy Report, it went through a thorough process of holding a series of workshops with privacy experts, advocates and industry stakeholders, issued a draft staff report and took comments before adopting a final report. The FCC held one workshop a year ago and a year later issued a complex NPRM with 500 questions, tentative conclusions and proposed rules.

a. Do you believe this process is adequate for such sweeping rules?

Response: Yes, I do. The NPRM follows the requirements for notice-and-comment rulemakings set forth in the Administrative Procedure Act ("APA"). The Commission put interested parties on notice more than a year ago that it would address broadband privacy issues through a separate rulemaking proceeding. There has been a great deal of public discussion about how the Commission should approach a broadband privacy rulemaking, many of which the NPRM seeks comment on. Further, I do not believe that the scope of the NPRM was unanticipated, given the existing statutory and regulatory privacy requirements that apply to voice telecommunications carriers and cable and satellite operators.

23. Congress adopted a privacy regime for cable television in 1984 in Section 631 of the Cable Act. Congress adopted a privacy regime for telephone service in 1996 for voice telephony service in the 1996 Act. And Congress adopted a privacy regime for direct broadcast satellite service in 2004. What legislation has Congress passed that *explicitly* establishes a privacy regime for broadband internet access services?

Response: Section 222 of the Communications Act expressly applies to telecommunications carriers—it does not go on to expressly include or exclude particular types of telecommunications services (e.g., circuit-switched telephone service). In finding that broadband internet access service is a telecommunications service, the Commission subjected broadband internet access service to the obligations found in Title II of the Communications Act. While the Commission forbore from many of these requirements and their implementing rules, the Commission declined to forbear from Section 222, in recognition of the need to ensure broadband customer have privacy protections. Section 222 of the Communications Act sets forth the obligations of all telecommunications carriers, including BIAS providers, to protect the privacy of customer information; it is not limited to voice services.

24. Section 222 of the Communications Act, the statutory provision under which you propose to adopt a broadband privacy rule, was adopted in 1996. Where in the text of Section 222 does the FCC find the authority to justify that it should be applied to broadband internet access services?

Response: Section 222 of the Communications Act reflects the obligations of "every telecommunications carrier" to protect the privacy of customer information. The Commission's reclassification of broadband internet access service as a telecommunications service brought such services under the purview of Section 222.

25. The Communications Act of 1996 also adopted specific provisions relating to the internet and interactive computer services, such as Section 230 and Section 706. In other words Congress specifically enacted legislative provisions pertaining to broadband service in the 1996 Act.

a. Does Section 230 explicitly reference broadband privacy?

Response: Section 230 of the Communications Act sets forth certain policy objectives and findings, and also sets forth requirements regarding parental control protections. Among the policies it espouses is to "encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the internet and other interactive computer services." It also states that the provision is not intended to limit the applicability of the Electronic Communications Privacy Act of 1986.

b. Does Section 706 explicitly reference broadband privacy?

Response: Section 706 addresses the deployment on a reasonable and timely basis of advanced telecommunications capability. It specifically tasks the Commission with using measures that promote competition in the local telecommunications market or other regulating methods that remove barriers to infrastructure investment. The D.C. Circuit has upheld the Commission's judgment that Section 706 grants the Commission independent rulemaking authority to regulate BIAS providers. The NPRM seeks comment on whether Section 706 would independently support the proposed rules governing the privacy and security practices of BIAS providers.

c. What other provisions of the 1996 Act explicitly reference broadband privacy?

Response: Section 222 addresses the privacy of customer information for customers of telecommunications carriers. Because of the reclassification of broadband internet access service as a telecommunications service in the *Open Internet Order*, recently upheld by the D.C. Circuit, Section 222 applies to broadband internet access services.

26. For over a decade the FTC privacy framework has done an effective job of balancing the privacy interests of consumers with the interest in fostering new and innovative uses of data that promote customized offerings, new services and new capabilities. This framework has applied uniformly to all entities in the broadband ecosystem. Privacy groups and industry interests have agreed that the framework has worked well for American consumers and American companies. Chairwoman Ramirez testified, "I think the FTC has done a very effective job in addressing consumer privacy and ensuring consumer information is appropriately safeguarded."

Your proposal differs from the FTC framework in significant respects. For example, under the FTC approach opt-out for use of customer data is the default approach for all but the most sensitive data. Under your approach opt-in is the default approach for almost all uses. Under the FTC's approach, data that was de-identified or aggregated

was carved out from the notice and choice framework. Under your approach, only data that is de-identified and aggregated will be carved-out. These are very important differences.

a. Why did the FCC not adopt the FTC's privacy framework for its proposed rule?
   i. For each of the differences mentioned above (i.e. opt-out vs. opt-in, de-identified or aggregated vs. de-identified and aggregated), please explain why the FCC chose the approach that it did.

Response: The FTC's and FCC's work to protect consumers' privacy stems from different grants of statutory authority. Both agencies have structured their privacy frameworks around the same principles of transparency, choice, and security.

As the expert agency on communications policy issues, the FCC is well positioned to ensure consumers have the right level of control over their own information while also continuing to work closely with the FTC.

For decades, U.S. privacy law has entrusted expert agencies with oversight of privacy practices of the entities they regulate. The FTC itself enforces many sector-specific financial privacy laws along with other financial regulators. Additionally, the Department of Education oversees the privacy practices of schools and other educational institutions, and the Department of Health and Human Services oversees privacy practices of health plans, doctors, and hospitals.

It is also important to emphasize that the NPRM is the start of a rulemaking process, and thus the FCC has not at this time adopted any particular framework. We continue to solicit views on the record.

b. Because the FCC did not adopt the FTC's privacy framework, please identify with particularity the aspects of the FTC's approach the FCC finds ineffective or insufficient to protect consumer privacy.

Response: The FCC has not yet adopted specific broadband privacy rules. The FTC has offered constructive comments on our proposal and we look forward to reviewing the whole record and moving towards final rules based on the record.

27. The EU-US Privacy Shield was negotiated in large part on the premise that the FTC has a "history of strong privacy enforcement generally." Indeed, according to Chairwoman Ramirez in her statement to EU Commissioner Jourová, "The FTC's enforcement actions—in both the physical and digital worlds—send an important message to companies about the need to protect consumer privacy."

a. Does the FCC disagree with the position that the FTC has a "history of strong privacy enforcement generally"?

Response: As an agency of general jurisdiction, the FTC does a terrific job working cooperatively with numerous state and federal agencies, including the FCC. The FTC has demonstrated great leadership in the area of protecting the privacy of consumers. Where it has sufficient rulemaking authority, it has adopted rules to ensure that consumers and business have clear guidance about the rules of the road. Where it does not have sufficient rulemaking authority, or where companies have violated its rules, the FTC has brought enforcement actions. While the FTC has an important role in protecting consumer privacy, Congress has enacted sector-specific privacy protections in a variety of areas.

The FCC and the FTC have worked together on privacy and other consumer protection issues for a very long time. The FTC has an important enforcement mandate under its Section 5 authority to address unfair or deceptive acts or practices and has demonstrated great leadership in the area of protecting the privacy of consumers. We look to the good work that the FTC has done in crafting our proposed rules.

b. If not, why did the FCC not adopt the FTC's approach to protecting consumer privacy?

Response: The FCC has not yet adopted broadband privacy rules. Our proposed approach draws on much of the FTC's privacy work. For example, both agencies have structured their privacy frameworks around the same principles of transparency, choice, and security. We recently received constructive comments from the FTC in response to our NPRM. We greatly appreciate and respect the FTC's commitment to consumer privacy as reflected in their decision to file comments and in the substance of their filing. The FTC's recent comments are an important part of the record upon which the Commission will rely in adopting final rules.

Since the Commission's legal authority is over broadband internet access service providers, the Commission is only proposing requirements that should be applied to those services. A consumer's relationship with its broadband service provider is different than the relationship a consumer has with a website or app. For example, consumers can move instantaneously to a different website, search engine, or app, but once they sign up for broadband service, consumers can scarcely avoid the network for which they are paying a monthly fee.

As the expert agency on communications policy issues, the Commission is well positioned to ensure consumers have the right level of control over the information they share with their broadband provider. But, we also recognize that we have complementary authority to the FTC in this space and the Commission is determined to continue its close working relationship with the FTC. In fact, the Commission and the FTC recently entered into an updated consumer protection Memorandum of Understanding ("MOU"). In the MOU, each agency recognized the others' expertise and agreed to coordinate and consult on areas of mutual interest.

28. Does the FCC believe that its decision to reclasify broadband internet service providers as common carriers decisively eliminates the jurisdiction of the FTC to police BIAS provider privacy under Section 5?

Response: The FTC Act contains an exemption for common carriers—as well as banks, savings and loan institutions, Federal credit unions, air carriers, and certain others—from the prohibition against unfair and/or deceptive acts or practices. I am on record stating that it is time for the common carrier exemption to be re-examined. However, under the current law the FTC lacks authority to regulate or bring enforcement actions concerning the provision of broadband internet access services. Unless and until the FTC Act is updated, authority to regulate the privacy practices of common carriers, including BIAS providers, lies with the FCC.

29. One theme of federal cyber initiatives is that the government provides resources and best practices (for example the NIST framework) which providers can then tailor to their unique cyber needs. This approach has been endorsed by the White House, Congress, industry, and even the FCC through its own "Cyber Policy Statement" — a collaboration with industry to establish a new public-private partnership to address cyber risks through voluntary, proactive industry measures.

a. The FCC's NPRM is an abrupt departure from the voluntary approach. Please explain the justification for this change.

Response: With respect to cybersecurity, the Commission has focused on a voluntary approach, as you note. With respect to Section 222 privacy requirements, the Commission has had rules in place for many years—it has not employed a voluntary approach.

b. Does the FCC envision any risk by incorporating cybersecurity guidelines developed under the guise of "voluntary industry standards?"

Response: Incorporating industry-developed, voluntary standards will not create unacceptable risk. Industry is best positioned to proactively plan for, and respond to, new developments in cybersecurity. As I stated in my June 2014 remarks at the American Enterprise Institute, I believe the private sector must step up to assume new responsibility and market accountability for managing cyber risks. In 2014 the Commission tasked its Communications Security, Reliability, and Interoperability Council ("CSRIC") with applying the voluntary NIST Cybersecurity Framework to the communications sector and determining how it might be utilized without constraining companies to its use. We also made clear that these voluntary pursuits must result in meaningful and measurable improvements to cybersecurity risk management. In 2015, the CSRIC delivered a Final Report on Cybersecurity Risk Management and Best Practices. The communications sector has begun to act on the recommendations from the Final Report and I believe the sector will continue to apply a disciplined, voluntary approach to their cybersecurity risk management.

c. Does the FCC predict that if such "voluntary" guidelines are made mandatory, future efforts to encourage voluntary industry best practices will be discouraged?

Response: I do not believe that enacting flexible standards, or high level principles (the "what") will discourage active participation in the development of voluntary best practices (the "how"). Let me reiterate though, our nation will be better positioned to address evolving cybersecurity threats if companies assess their risk landscape and proactively invest in defensive measures they deem appropriate.

30. The NPRM proposes that a person's physical address and telephone number be included among "protected information", even though that's not the case under the agency's CPNI rules for voice providers. Thus a phone company may share name and address in a phone book, but if a broadband provider were to share the same information, it would be in violation of the privacy rule. Given that you stated in your testimony that "there needs to be equivalency between those two [phone and broadband]" what justifies this discrepancy?

Response: As the NPRM explains, unlike fixed wireline voice providers in the 1990s, today's broadband providers do not publish directories of customer information. Even in the voice context, mobile providers have not published subscriber list information, and in the fixed context, customers have long had the option to request such customer information not be disclosed, inherently recognizing the personal nature of such information. Further, the NPRM explains, by signing up for broadband service, customers do not have a reason to believe that they are consenting to the public release of their name, postal address, and telephone number, none of which play the same role in the context of internet access as they do in the context of telephone service. In any event, we expect any final rules addressing this issue to be informed by public comment, including from consumers and the industry.

31. The NPRM includes a breach notification requirement. Currently 47 States have breach notification requirements.

a. Before proposing these requirements did the FCC undertake a federalism summary impact statement as encouraged by Section 9 of Executive Order 13,132, "Federalism"?
b. If not, does the FCC intend to undertake a federalism summary impact statement before issuing its final rule? If not, why not?

Response: Regarding the action the FCC intends to take to follow the principles suggested in Executive Order 13132, to the extent that this Executive Order applies requirements to independent agencies, we have taken steps to act consistently with the principles articulated within. We have carefully reviewed the states' data breach notification requirements and our proposal has been informed by those requirements. We have not undertaken a federalism summary impact statement. However, we welcome comments on the successes and shortcomings of those state statutes.

The Honorable Orrin G. Hatch

1. **Considering the magnitude of the FCC's proposed privacy rules, the fact that they were adopted by a bare majority of Commissioners with two strong dissents, and the fact that the legal challenges to the Open Internet Order and reclassification are currently pending in the courts, how would you respond to those who argue that the form, substance, and timing of the privacy rules all strongly suggest that the rules are being driven by the political calendar rather than by the kind of reasoned and deliberative process that is supposed to be the hallmark of independent agencies?**

   Response: In the *Open Internet Order*, which was recently upheld by the U.S. Court of Appeals for the D.C. Circuit, the Commission indicated that it intended to commence a rulemaking to clarify obligations under Section 222 of the Communications Act of 1934, as amended ("Act"), and staff of the Commission held a workshop on the issue last spring and began conversations with stakeholders. The NPRM was the next logical step in the process. Indeed, providers have complained that without further guidance, they do not know how to comply with the Act—and have argued as much in a request to stay the *Open Internet Order*. It is therefore incumbent on the Commission, and on me as Chairman, to bring greater clarity to what broadband providers are expected to do to comply with Section 222 of the Act—and to do so in a timely manner.

2. **Given that the FTC's current legal framework for enforcing consumer privacy and data security standards has been effective, what is the basis for the FCC's determination that a separate legal regime is necessary, would be effective, and would constitute an appropriate allocation of Commission resources? Why is the FCC not adopting the same longstanding privacy rules regime used by the FTC to enforce privacy and data security standards?**

   Response: The FTC has an important role in protecting consumer privacy under its Section 5 authority to address unfair or deceptive acts or practices. The FTC has successfully used this authority to take action against companies that do not keep their privacy promises to consumers or that fail to have reasonable data security practices for sensitive information, and these decisions have set important precedents for the internet ecosystem and beyond.

   While it is clear that the FTC has an important role in protecting consumer privacy, it is important to remember that Congress has enacted sector-specific privacy protections in a variety of areas. Some of these privacy protections extend to financial institutions, schools and other educational institutions, healthcare providers, and credit reporting agencies. And Congress has tasked various agencies with implementing and overseeing regulations in these areas. For example, the Department of Health and Human Services regulates the privacy practices of "covered entities" under HIPAA—such as doctors, hospitals, and health insurance plans.

   The FCC's proposed broadband privacy rules fit right alongside rules tailored to different industries and environments. Our goal is to protect consumers' privacy in our particular jurisdiction—the telecommunications market—which is why we are proposing rules

applicable to broadband internet access service ("BIAS") providers, not edge providers, which are subject to a regulatory framework with FTC oversight and enforcement and, often, state oversight as well.

As noted by the FTC in its 2012 Report, BIAS providers are not the same as edge providers. The idea behind our proposed broadband privacy rules is that BIAS providers shouldn't use their privileged position as the carriers of their customers' communications by taking the information they are entrusted with and using it for other purposes without first receiving the consent of their customers.

The Honorable Al Franken

1. **I've heard suggestions that holding BIAS providers to a different standard than edge providers is somehow inappropriate because consumers can't always distinguish between online entities and may not realize that they are regulated by different agencies and under different standards.**

   This argument seems to suggest that because consumers may not know that the website they visit isn't held to the same standard as their BIAS provider, that they would somehow prefer a *lower* standard of protection—just as long as it was uniform across entities. It also seems to suggest that if consumers were asked, they would allow companies to do whatever they want with their data because the consumers aren't experts on the U.S. regulatory scheme. I've also heard arguments that a majority of consumers might not actually favor the kind of control over their personal information that you're proposing to give them.

   But based on what I've seen and heard in recent years, the American consumers deserve a lot more credit than these arguments allow. We saw it with Net Neutrality and then again with the demise of Comcast-Time Warner Cable: consumers care about these issues and are increasingly tech-savvy.

   Chairman Wheeler, you have a unique perspective here. What do you know about consumers' role and interest in these issues?

   Response: Regardless of the platform, consumers want to know what information about them is being collected, how that information is shared, and how they can exercise choice over what is disclosed to third parties. Consumers expect more protection—and to be asked permission more explicitly—for a variety of reasons. Sometimes it is because the type of information itself is more sensitive. Other times, it has to do with who has the information, who gathered the information, or why the information was gathered.

   I believe that the NPRM is consistent with these expectations because it seeks to ensure privacy protections for more than just certain types of information—it also ensures privacy protections for certain uses of that information. For example, the NPRM seeks comment on protecting the privacy interests of consumers that share confidential information with

providers, and how to ensure that consumers do not lose these protections just because they are no longer a customer.

Consumers are actively participating in the public comment process of this ongoing rulemaking, so we are continuing to learn more about consumers' privacy expectations.

2. **As you know, in today's world, so many of our everyday objects are connected to the Internet. We have "smart watches", "smart TVs", and "smart thermostats".**

   Chairman Wheeler, can you talk about the kinds of information or insight that a BIAS provider can gain from devices that are connected to its network? As consumers become increasingly reliant on wearables and home appliances that connect to the Internet, why is it so necessary that companies are held to higher standards of privacy protection?

   Response: There are certain basic responsibilities that come with providing consumers with an on-ramp to the internet. BIAS providers occupy a unique position in the internet ecosystem as the gatekeeper through which all of a consumer's online activity (including a tremendous amount of personal information) must travel. A BIAS provider handles all network traffic, which means it has an unobstructed view of all of unencrypted online activity (such as webpages visited, applications used, and the times and dates of internet activity). On a mobile device, a BIAS provider has the capability to track the physical and online activities throughout the day in real time. Even when data is encrypted, a BIAS provider can still see the websites that a customer visits, how often they visit them, and the amount of time they spend on each website. Using this information, they can piece together enormous amounts of information about an individual—including private information such as a chronic medical condition or financial problems. As a result, the FCC's proposed approach is tailored to this unique position occupied by BIAS providers.

3. **A majority of Americans have smartphones now, and as a result—an increasing number of companies can track your location at any time. That means they have access to things like where you live, where you work, where you drop your kids off at school, and the doctors you visit. I have long fought to increase protections for Americans' sensitive location data. And I have a bill—the Location Privacy Protection Act—that would give consumers greater control of how their location information is collected, used, and shared.**

   Chairman Wheeler, you touched on this issue in your testimony, but can you expand on why protection of Americans' location data is so necessary? And how can widespread access to this information be abused?

   Response: For most of us location data is very sensitive. My mobile BIAS provider knows where I am at all times. It knows my regular commute patterns, and where I go during my leisure hours. If I have a family plan, it can track the comings and goings of my entire family and it can match that up to information about what websites we are visiting or what applications ("apps") we are using when and where. I believe that a consumer's right to

privacy should mean that consumers decide who can track their movements and for what purposes that information can be used.

Broadband providers' protection of their consumers' location data requires, per Section 222(f) of the Communications Act, "express prior authorization of the customer." Because of this heightened statutory requirement, we proposed that use of location data requires BIAS providers to first get opt-in approval. As we noted in our proposal, consumer location data is one of the metrics that can be seen by BIAS providers even when the internet traffic is otherwise encrypted. Mobile BIAS providers can determine the customer's device location, and therefore the customer's location, anywhere that they use their mobile devices. Widespread access to this data could be abused by third parties.

The Honorable Chuck Grassley

1. **Rural Iowans rely on their phone connections to do business and stay connected to many vital services. Unfortunately, Iowans are still experiencing telephone calls not getting through, or they are receiving poor quality calls. I know that many of my constituents have repeatedly reported issues to the FCC, but this persistent problem has led to them being unable to file complaints each time. I am pleased that the FCC has looked at this issue and stepped up enforcement in some cases. However, more needs to be done. Consumers should be able to expect at least a minimum level of call quality and reliability. How is the FCC continuing to address this problem of least cost routers that attempt to minimize their costs by failing to deliver calls to rural areas where the cost to provide phone service is higher?**

   Response: The Commission continues to address specific call completion problems reported by rural carriers and consumers through dedicated channels established to ensure these problems are resolved promptly. As you noted, we have taken five enforcement actions that resulted in payments of more than six million dollars in civil penalties, fines, and voluntary contributions and commitments to improve service going forward. We're also engaged in an ongoing data collection effort, and our staff continues to examine this data to help inform its understanding of rural call completion problems and determine next steps. The Wireline Competition Bureau will issue a report regarding this data collection by August 30, 2017. Moreover, we continue to work with our partners at state utility commissions to provide, upon request, access to state call completion data.

2. **The Commission has traditionally deferred to Congress in copyright matters, recognizing that it has neither the authority nor expertise required to make copyright policy. When addressing the compulsory copyright for cable retransmission, the Commission acknowledged that "Congress is the body with the authority and the responsibility for making copyright policy" while the expertise of the Commission is "in the area of communications policy, not in the area of copyright."[1]**

[1] *In re Compulsory Copyright License for Cable Retransmission*, 4 FCC Rcd. 6711, 6711 (1989).

The proposed NPRM contemplates rules that could have significant impacts on the reproduction, distribution, display, and performance of copyrighted material. Has the Commission acquired new authority or expertise that would give it the confidence that it has fully addressed the concerns of copyright holders raised by the proposed rules?

Response: The FCC's authority to regulate communications has always existed alongside content owners' rights to control the duplication, distribution, or performance of their works. The co-existence of intellectual property and communications laws reflect Congress's effort to maintain a balance between the "interests of authors and inventors in the control and exploitation of their writings and discoveries" and "society's competing interest in the free flow of ideas, information and commerce."

Starting with broadcast, and continuing with cable, satellite, and the internet, the FCC has for more than 80 years regulated the networks that content owners use to transmit their works to the public. In these activities, the Commission has always recognized the statutory rights of content owners and has pursued policies that encourage respect for these rights. In addition, several FCC-related statutes explicitly prohibit the alteration of broadcasts or the theft of cable transmissions that contain copyrighted works.

The goal of this rulemaking is to promote competition, innovation, and consumer choice. It will not alter the rights that content owners have under the Copyright Act; nor will it encourage third parties to infringe on these rights. All of the current players in the content distribution stream, including cable and satellite companies, set-top box manufacturers, app developers, and subscribers, are required to respect the exclusive rights of copyright holders. The rulemaking will require any companies that enter this market subsequent to our action to follow the same requirements. Because the proceeding will not alter the rights that content owners currently have, and will extend the available protection to any new market entrants, the Commission is confident that this rulemaking will address the concerns of copyright holders.

3. **Has the Commission solicited input from other federal offices and agencies, with expertise in copyright issues, regarding this proceeding? In the past, the Commission has acknowledged that other federal entities have more expertise than the Commission with respect to copyright law. For instance, in its Report to Congress Pursuant to Section 208 of the Satellite Home Viewer Extension and Reauthorization Act of 2004, the Commission stated that it "will defer to the Copyright Office's expertise in these areas."[2] In the present instance, would the Commission defer to the expertise of the Copyright Office?**

Response: The Commission welcomes comments on its proposed rules from all interested stakeholders and has actively engaged with the United States Copyright Office. However, I will reiterate that this proceeding will not alter the rights that content owners have under the Copyright Act; nor will it encourage third parties to infringe on these rights. All of the

[2] FCC Report to Congress Pursuant to Section 208 of the Satellite Home Viewer Extension and Reauthorization Act of 2004, at 40 (2005).

current players in the content distribution stream, including cable and satellite companies, set-top box manufacturers, app developers, and subscribers, are required to respect the exclusive rights of copyright holders. The rulemaking will require any companies that enter this market subsequent to our action to follow the same requirements.

4. **Section 106 of the Copyright Act ensures that copyright holders have the exclusive right to, among other things, disseminate, reproduce, publicly perform, and publicly display their copyrighted content, protecting rights holders from unauthorized reproduction of their copyrighted content. In requiring the transmission of content to third-party computing devices, has the Commission considered whether its proposed rules facilitate the infringement of the exclusive rights of content creators by permitting unauthorized reproductions?**

   Response: The goal of this rulemaking is promote competition, innovation, and consumer choice. It will not alter the rights that content owners have under the Copyright Act; nor will it encourage third parties to infringe on these rights. All of the current players in the content distribution stream, including cable and satellite companies, set-top box manufacturers, app developers, and subscribers, are required to respect the exclusive rights of copyright holders. The rulemaking will require any companies that enter this market subsequent to our action to follow the same requirements.

   Specifically in our proposal we stated: "our regulations must ensure that Navigation Devices (1) have content protection that protects content from theft, piracy, and hacking, (2) cannot technically disrupt, impede or impair the delivery of services to an MVPD subscriber, both of which we consider to be under the umbrella of robustness (*i.e.*, that they will adhere to robustness rules), and (3) honors the limits on the rights (including copy control limits) the subscriber has to use Navigable Services communicated in the Entitlement Information Flow (*i.e.*, that they adhere to compliance rules.) Through robustness and compliance terms, we seek to ensure that negotiated licensing terms regarding subscriber use of content that are imposed by content providers on MVPDs and included in Entitlement Data are honored by Navigation Devices."

   Simply put, this means that the final rules will respect the exclusive rights of content creators and will not encourage or facilitate infringement.