Chairman Tom Wheeler

Commissioner Mignon Clyburn
Commissioner Jessica Rosenworcel
Commissioner Ajit Pai
Commissioner Michael O'Rielly
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

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

August 6, 2016

Dear Chairman and Commissioners:

This is a joint statement of Internet researchers and technologists.

As noted in our original comments and as the Federal Communication Commission's ("FCC") NPRM notes, section 222 of the Communications Act allows an broadband internet access service ("BIAS") provider to collect, use and disclose CPNI "to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of,or subscription to, such services."[1] The NPRM, however, raised significant concerns around the collection, use, and disclosure of customer personal information as it relates to other beneficial uses.[2] In a letter filed in the above proceeding and dated June 27, 2016, we met with FCC staff to express concern that the privacy rules that the FCC is considering, if implemented as proposed in the NPRM, would negatively affect research and development work that is important for the operation and security of the Internet.[3]

On July 9, 2016, Professor Feamster presented some of these concerns in an *ex parte* presentation; at this presentation, members of the FCC's wireline bureau requested specific proposed language for a researcher exemption to the rule[4]. This letter includes proposed language for such an exemption.

The attached proposed language aims to exempt researchers and technologists who are engaged in Internet research that is vital to the security and functioning of the Internet and continued innovation, balancing consumer privacy with the benefits of technical research that fundamentally depends on data-sharing agreements between BIAS providers and Internet researchers. The language includes qualifying criteria for exemptions, as well as concrete examples of research (and researchers) who might commonly fall under this exemption.

We do not believe that the FCC should act as a clearinghouse or arbiter for such data-sharing agreements. Instead, we suggest possible mechanisms for abiding by best practice that researchers and BIAS providers should follow, such as obtaining approval from the appropriate research oversight or ethics board, whenever possible and applicable.

Thank you for considering this exemption and the attached proposed wording.

Respectfully submitted,

/s/

---

[1] 47 U.S.C. § 222(d)(2).
[2] https://ecfsapi.fcc.gov/file/60002079367.pdf
[3] https://www.fcc.gov/ecfs/filing/1070642992845
[4] https://www.fcc.gov/ecfs/filing/1071384086685

Manos Antonakakis
Georgia Tech

Michael Bailey
University of Illinois at Urbana-Champaign

Steve Bauer
MIT

Eric Burger
Georgetown University

Amogh Dhamdhere
Center for Applied Internet Data Analysis (CAIDA)

Nick Feamster
Princeton University

John Heidemann
University of Southern California
Information Sciences Institute

Erin Kenneally
UC San Diego and International Computer Sciences Institute (ICSI)

William Lehr
MIT

Paul Mockapetris
Inventor of DNS
ThreatSTOP

Vern Paxson
UC Berkeley and International Computer Science Institute (ICSI)

Jennifer Rexford
Princeton University

Jerry Upton
Messaging, Malware, and Mobile Anti-Abuse Working Group

Sandy Wilbourn
Nominum

NOTE: Unless otherwise indicated, all signatories to this letter have signed in their personal capacity, and not as representatives of their employers or any affiliated organizations.

Attachments:

Proposed language for researcher exception

Proposed Language for Researcher Exception

Amend proposed rule 64.7002(a) to add before subsection (4):

"To support research intended to enhance security, promote network operation, improve network performance, and other activities intended to advance subsection (1) and (3)."

Justification for Rule

The FCC recognizes the historically important role that collaboration and data sharing between BIAS providers and members of the research community has had. The impact of this collaboration has been far-reaching, and has included advancements in the development and deployment of new protocols that improve both the performance and security of the Internet. Examples of these developments include: IPv6 and DNSSEC deployment; malware detection and mitigation; spam filtering; and traffic engineering algorithms.

Continued collaboration and data sharing between BIAS providers and Internet researchers is critical to the future growth and vibrancy of the Internet, both in the U.S. and abroad.

Recognizing the importance of continued collaboration between BIAS providers and researchers, the FCC should exempt data exchange between researchers and BIAS providers. The above rule is intended to exempt research that meets the following criteria:

1. **Purpose of research.** The data satisfies research that aims to promote security, stability, and reliability of networks. The research should have clear benefits for Internet innovation, operations, or security.
2. **Research goals do not violate privacy.** The goals of the research does not include compromising consumer privacy;
3. **Privacy risks of data exchange are offset by benefits of the research.** The risks of the data exchange are offset by the benefits of the research;
4. **Privacy risks of the data exchange are mitigated.** Researchers should strive to use de-identified data wherever possible. Where individually identifiable data is used, researchers and BIAS providers should take measures to mitigate the risks associated with any private customer data. Data exchange should be secure, and risks of unintended data leaks should be minimized to every extent possible.
5. **The data adds value to the research.** The research is enhanced by access to the data.

The first criterion above is intended to limit the type of research that is within the scope of the exemption so the exemption remains narrowly tailored. To further ensure the exemption is narrowly tailored, the Commission could make clear that the types of researchers eligible for the exemption is also limited.

Below, we provide examples of categories of researchers who, while not solely academic, commonly use data from BIAS providers to advance the Internet's resiliency, reliability, security, and operational capabilities. These categories represent groups that already exchange data with BIAS providers. The following categories of researchers would be within the scope of the rule to the extent they are performing research in accordance with the above criteria:

1. **Researchers at universities.** Researchers associated with a degree-granting academic institution who are performing research under or as an affiliate of that institution. This group specifically includes university professors, postdoctoral research associates, research scientists, and students.
2. **Researchers at academic research laboratories.** Research scientists associated with an academic research lab, defined as a lab that is affiliated with a university. An example of such an organization is the International Computer Science Institute (ICSI).
3. **Industrial researchers.** Researchers who are affiliated with an organization, such as an industrial research lab or industry consortium, that is investigating historical, current, and future threats to the security and stability of the Internet. Examples of industry consortia include the Messaging, Malware, and Mobile Anti-Abuse Working Group (M^3AAWG), the Anti-Phishing Working Group (APWG), and the Internet Systems Consortium

(ISC). Researchers at industry labs such as Verisign Labs and Nominum are also examples of researchers who fall into this category.

4. **Protocol developers and related deployment organizations.** Protocol developers who are actively developing protocols—either as part of an organization or as an individual contributor—within a non-profit protocol standardization body, such as the Internet Engineering Task Force (IETF), the Internet Research Task Force (IRTF), or the World Wide Web Consortium (W3C); or, a protocol deployment organization, such as the Internet Society's (ISOC) Deploy360 program or the DNSSEC Deployment Initiative.

Many of these organizations already abide by the above criteria and also have internal review bodies or other mechanisms to safeguard the handling of data. For example, university research in the U.S. involving personal data is subject to Institutional Review Board (IRB) review. These narrowly defined categories of researchers, coupled with the narrowly tailored research criteria, will help ensure that an exemption for researchers is limited in scope and that these entities that have traditionally worked with BIAS providers to promote a safer, more resilient, reliable, and innovative Internet for consumers can continue to do so.

To ensure that the data is not used for purposes beyond the scope of the research criteria outlined above, we would urge the FCC to make clear that researchers operating under the exemption are not permitted to re-sell or further distribute the data they receive from BIAS providers.