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

June 27, 2016

Dear Chairman and Commissioners:

This is a joint statement of Internet researchers and technologists.

We are concerned that the privacy rules the FCC is now considering, if implemented as proposed in the NPRM, will negatively affect research and development work that is important for the smooth operation of the Internet and the future development and vibrancy of the Internet.

For more than 15 years[1], networking and security researchers have relied on measurements and data from BIAS providers to understand everything from security to network provisioning to the impact of new network technologies (*e.g.*, middleboxes) on deployed network protocols. A wide variety of ongoing networking research may be negatively affected by this rule, including research on topics such as Quality of Experience (QoE) measurement and other Internet performance measurement, network interconnection, malware, spam, broadband adoption, and more.

In addition, without access to traffic traces from real ISP networks, development and deployment of new Internet protocols—and the feedback loop necessary between developers and early deployers—may suffer.

We are particularly concerned with comments such as Paragraph 67 on Page 24 in the NPRM, which 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." Below, we summarize and reiterate comments from the research community which explain why this approach would gravely harm the research community.

Paragraphs 111–121 of the NPRM discuss possible exceptions and invite comment. **We urge the FCC to further include an exemption for researchers and technologists who are engaged in Internet measurement and security research, including (but not limited to) the topics we mention above.**

The Commission should take special note of the following recent comments on the Notice:

1. Manos Antonakakis, David Dagon, and Michael Farrell from the Georgia Institute of Technology; Paul Vixie from Farsight Security; and Paul Mockapetris and Tom Byrnes from ThreatSTOP, who wrote[2]:

[1] http://www.sigcomm.org/events/imc-conference
[2] http://apps.fcc.gov/ecfs/comment/view?id=60001973444

> *"The Notice does not make it sufficiently clear that network security monitoring is exempted from opt-in consent requirements. The Commission should state that consent is never required for security-focused monitoring and research. While portions of the Notice's language support this view, the Commission should remove all doubt, an explicitly distinguish security-focused research from marketing-focused research.*
>
> *For this reason, we strongly urge the Notice to be updated to reflect the import role cyber security has in ISP operations."*
>
> *"Depriving researchers of this data, in favor of a "consent to protect" interpretation of the Notice, will destroy the science of cyber public health in its early days. And since new IoT devices are introduced without ISP notice or coordination, a consent-to-protect system will mean ISPs learn of threats only when they've grown to significant scale."*
>
> *"Based on our shared failures in rapidly addressing spam, imposing limits on scientific research into new security problems may influence the protocol evolution of the Internet itself."*
>
> *"Requiring a consent-to-protect system will result in fewer sensors, less data, and less visibility, meaning that some threats will become visible only when they reach crisis proportions. Since no user has consented to the introduction of viruses in the first place, consent should not be required to help track, identify, and notify them about infections. The Notice should be amended to state that security-focused research does not require consent."*

2. Nick Feamster from Princeton University, who wrote[3]:

> *"Preventing ISPs from collecting this data and sharing it with vendors of security services or researchers will harm the security and performance of the Internet and threatens to inhibit research innovation."*
>
> *"Preventing ISPs from sharing network data with researchers will prove to be a tremendous setback for innovation."*
>
> *"The rulemaking should provide an explicit exception for researchers. As described above, network research fundamentally depends on cooperative data sharing agreements with ISPs."*
>
> *"The rulemaking should also provide an explicit exception for protocol developers and vendors. Protocol developers and vendors often need real packet traces from ISPs to test for correct functioning and interoperability. The inability to receive traffic traces from ISPs will severely limit vendors' and developers' ability to build and deploy network technology that functions correctly, safely, and securely. Some examples where limitations on such data sharing would have impacted development and deployment include protocols such as IPv6 and DNSSEC."*
>
> *"The rulemaking should provide an explicit exception for vendors who provide third-party security and network management services. Many vendors provide third-party services to help network operators operate or secure their networks. ISPs should be permitted to route network traffic to and through these third-party services to the extent that doing so can make the network operate better*

[3] http://apps.fcc.gov/ecfs/comment/view?id=60001973502

or more securely."

3. William Lehr and Steve Bauer from the Massachusetts Institute of Technology & Erin Kenneally from the University of California, San Diego, who wrote[4]:

   "In addition, we recommend that the FCC consider instituting an exception process for data sharing with third-party network researchers. We believe in most cases that such sharing is likely to fit within the category of data that needs to be shared to sustain the safe operation of the end-to-end Internet. For example, data about the configuration of services, technical performance and traffic statistical data – appropriately de-identified in most cases, is needed to inform research directed at designing better Internet technologies and evaluating market performance.

   Classifying the data shared with legitimate researchers in this way would allow researchers access without requiring costly explicit "opt-in" approval from each subscriber. Requiring such opt-in approval for the sorts of large data sets typically engaged by network researchers would be impractical and likely to pose an insurmountable cost burden, rendering the data inaccessible. Moreover, any additional costs- whether operational or viz legal risk- imposed on BIAS providers associated with their efforts to share data with network researchers would weaken their already weak incentives to share."

4. Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), who wrote[5]:

   "As with any area of cutting edge innovation, much of the new thinking and research that leads to technological advances for anti-abuse starts with security researchers."

   "All of this would be at considerable risk, given the significantly higher barriers to data sharing and data access the new NPRM would create. There is a threshold question of whether this work could even take place outside the context of a specific threat to the network or malicious attack."

   "So the data flows from ISPs that we depend upon for anti- abuse research could be adversely affected."

   "As such, ISPs would be dramatically less inclined to support such research and researchers due to the inherit [sic] risk this would now entail."

5. Sandy Wilbourn and Bruce Van Nice from Nominum, who wrote[6]:

   "As an essential part of every IP network, DNS data offers valuable operational insights that benefit consumers and is an efficient and effective way for security researchers to identify cyber threats."

   "Collecting DNS data for security purposes, and sharing anonymized data with researchers and other BIAS providers, should be explicitly permitted if consumers are to be fully protected from the effects of these threats. Section 222(d) permits disclosure and we believe the Commission should make clear that disclosure of this kind is permissible."

[4] http://apps.fcc.gov/ecfs/comment/view?id=60001975212

[5] http://apps.fcc.gov/ecfs/comment/view?id=60001973184

[6] http://apps.fcc.gov/ecfs/comment/view?id=60001975188

As a result of our concerns, we urge you to ensure that any privacy rules issued by the FCC include an explicit exemption for data shared with researchers, protocol developers, security technology specialists, and related organizations.

Thank you in advance for your consideration.

Respectfully submitted,

/s/

Manos Antonakakis
Georgia Tech

Michael Bailey
University of Illinois at Urbana-Champaign

Steve Bauer
MIT

Eric Burger
Georgetown University

kc Claffy
Center for Applied Internet Data Analysis (CAIDA)

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.