Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of	)	WC Docket No. 16-106
Broadband and Other	)	
Telecommunications Services	)	

REPLY COMMENTS OF THE SECURITY AND SOFTWARE ENGINEERNIG RESEARCH CENTER (S^{2}ERC) AT GEORGETOWN UNIVERSITY ON PETITIONS FOR RECONSIDERATION

Dr. Eric Burger
Director, Security and Software Engineering Research Center at Georgetown
Georgetown University
37th & O St., NW
Washington, DC 20057

We provided comments prior to the issuance of the FCC's *Broadband Privacy Order*.[1] We will not rehash our original comment filing[2] or reply comments.[3] Rather, we will focus on just two issues raised by commenters in the proceeding on the petition for reconsideration.

Cyber Threat Sharing

There is a program of research at the S^{2}ERC working on the Cyber Threat Intelligence Information Exchange Ecosystem (CyberISE).[4] The goal of this program is to improve the security and stability of the nation's networks through the sharing of cyber threat intelligence.

[1] Protecting the Privacy of Customers of Broadband & Other Telecommunications Services, Report & Order, FCC No. 16-148, WC Docket No. 16-106 (November 2, 2016), herein referred to as the *Privacy Order*.
[2] WC Docket No. 16-106, Document ID # 60002080298
[3] WC Docket No. 16-106, Document ID # 10705641704886
[4] *See* https://s2erc.georgetown.edu/projects/cyberISE

With respect to iconectiv's comments,[5] we wholly endorse the request that if there will be further consideration of the *Privacy Order*, any changes do not impede the ability of Basic Internet Access Service (BIAS) providers to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services."[6] This exception to §222 is an important component in the cybersecurity arsenal of BIAS providers **and their customers**.

The iconectiv comments focus on fraud. Beyond the fraud use case, connectivity information and session metadata, both of which may contain Customer Proprietary Network Information (CPNI) such as source and destination IP address, domain names, etc. can also be critically important for BIAS providers to use to determine systemic attacks on the nation's networks as well as to tease out trends and common patterns of attack across different BIAS carrier networks. As such, we ask that any further rulemaking also ensure that the rules do not curtail limited, legitimate sharing of cyber threat indicators and intelligence.

There is global consensus that service providers should be allowed to exchange cyber threat intelligence with each other, including what the FCC may categorize as CPNI. For example, one project in the S^{2}ERC CyberISE program focuses on international business-to-business cyber threat intelligence sharing.[7] This research has found that even countries in Europe, which have some of the strictest data privacy regimes (including the new General Data Protection Regulation), some of which explicitly label IP addresses as protected data by law and statute, can still share such data within the community when it is "in the public interest." The concept of "in

[5] WC Docket No. 16-106, Document ID # 1030603821374
[6] *See* 47 U.S. Code §222(d)(2).
[7] See Sullivan, C. and Burger, E., *"In the public interest": The privacy implications of international business-to-business sharing of cyber-threat intelligence*, **Computer Law & Security Review: The International Journal of Technology Law and Practice**, (33) 1, 2017, pp. 14-29.

the public interest" is very similar to the U.S. Code §222(d)(2) exemption we currently have in the U.S.

Confusing Privacy Protections

Let us examine two anecdotes from people very well immersed in the technology and policy of the present technology that allegedly support the position that BIAS providers need regulation while edge providers do not.

The CDT comments in the present proceeding highlight a case of "one internet user reported searching for help with a potential alcoholism problem only to see targeted ads for the nearest liquor stores." [8] When the FCC published the original *Privacy Order*, then FCC Chairman Tom Wheeler opened his comments with, "Who would have ever imagined that what you have in your refrigerator would be information available to AT&T, Comcast, or whoever your network provider is?"[9]

Looking at the CDT's comments, the story referenced in the comments[10] is about an individual who did a search at Google (an edge provider) who then logged into Facebook (an edge provider) where the ads showed up. Limitations on BIAS providers have zero impact on this unfortunately common situation. If CDT can be confused over who is watching Internet users' browsing habits, it would be disingenuous to say the average Internet user would not.

Looking at the former Chairman's comments, it is unquestionable that it could be an abuse of the BIAS provider's position in the network to be looking inside packets emanating from the

[8] WC Docket No. 16-106, Document ID # 103072072904622 at 19-20.
[9] Wheeler, Tom, *Statement of Chairman Tom Wheeler*, FCC, October 27, 2016, https://apps.fcc.gov/edocs_public/attachmatch/DOC-341937A2.pdf
[10] *See* WNYC, *Note to Self: Day 2: The Search For Your Identity*, http://www.wnyc.org/story/privacy-paradox-day-2-challenge/

customer's refrigerator to figure out what is in the refrigerator. However, the fact the BIAS provider, or any random person on the network for that matter, can look inside the packets emanating from the customer's refrigerator is a major failure of the edge provider to secure their communications for the consumer. As the oft-referenced Upturn report notes, with 85% of edge providers failing to give their customers any security,[11] does it make sense to single out BIAS providers? To reiterate, this is not an excuse to allow BIAS providers to do deep packet inspection for anything other than security services. However, if the motivation of the FCC to promulgate regulations is to protect the consumer, it would be much more effective to require edge providers to provide a minimum amount of security to their customers.

Imagine the response of the average Internet user when they hear the government is intervening to protect their privacy. However, in both of the cases highlighted above, nothing in the *Privacy Order* helps the situation encountered. In other words, the average American will be very disappointed when they were told the FCC was imposing privacy preserving rules upon BIAS providers, only to find out their privacy was not preserved at all.

Worse, the current set of rules, marketed as privacy preserving, would give average Internet users a false sense of security. This is not an argument in favor of eliminating restrictions on BIAS providers. Rather, if the goal is to inform the American public they are being protected from tracking on the Internet, then the FCC (and FTC) should be protecting the American public from being tracked on the Internet, rather than leaving the American public vulnerable to tracking yet claiming to protect the public.

[11] Reike, A., Robinson, D., and Yu, H. *What ISPs Can See*, **Upturn**, "more than 85% of the top 50 sites still fail to encrypt browsing by default" (Introduction observation 1)

Consumers need a consistent set of privacy standards for their interaction with the Internet. The typical consumer has no idea the difference between a BIAS provider, an edge provider, a cloud provider, an over-the-top communications provider, and so on. To the user, it is all the Internet. As such, we urge the FCC, if it is to have any rules in this space, have uniform rules that apply to all relevant players.