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 AT GEORGETOWN UNIVERSITY

In our original comment filing[1] we raised concerns that if the FCC were to implement the privacy rules proposed in the current NPRM, the resultant privacy regime would be needlessly ambiguous and burdensome. In particular, we noted that the proposed rules run the risk of further segmenting an already complex regulatory environment and many of its protections are either redundant with or better implemented through FTC regulation. One alternative we suggested was the protection of sensitive information through the use of encryption by edge providers. A number of commenters[2] have argued that encryption is an inadequate requirement to ensure privacy and that, in practice, even encrypted data can reveal sensitive information such as browsing preferences to BIAS providers.

We agree that unencrypted metadata, such as routing information, can be used to make assumptions about the contents of encrypted data. However, there are a number of important caveats the Commission should consider as it incorporates these comments into the development of new rules, if any:

[1] ID# 60002080298
[2] *E.g.*, Reply of Paul Ohm, WC Docket No. 16-106, ID #ID10622254783425

i) Although arguably insufficient, encryption is nonetheless necessary to the provision of privacy in the Internet space. A regime which fails to ensure end-to-end (i.e. edge-provider to edge-provider) encryption is unlikely to ensure meaningful consumer privacy protections.

ii) By the time that rules regarding the collection of sensitive information are relevant, a privacy regime has already failed. The failure to encrypt sensitive data in transit represents grave and negligent oversight and rules which directly address such behaviors are the best protections for consumer privacy.

iii) The class of information which encryption cannot conceal often overlaps with that information most critical to provision of BIAS. Overly broad regulations targeting this genre of data may thus impose significant new costs and constraints on BIAS providers.

Regarding the first point, encryption represents a critical component of any information security strategy. Unencrypted information should be handled with the assumption that any sufficiently interested party (be it a BIAS, criminal, researcher, or other entity) can gain access to the full contents of that information – oftentimes undetected. Provably strong and vigorously tested encryption tools are freely available for the vast majority of common programming languages and computing infrastructures.[3] Today, encryption can be both robust and rapid enough to protect information at negligible costs. Numerous standards organizations, major industry players and even the federal government have begun the push towards end-to-end TLS encryption. A privacy regime that fails to impose edge-to-edge encryption standards of this

[3] In the commercial space, see for example https://www.symantec.com/website-security/ and in the free and open source space see, for example, https://letsencrypt.org .

nature will, at best, descend into rapid irrelevance and, at worst, complicate and delay promising improvements.

Additionally, commenters seeking regulatory alternatives to edge-level encryption standards tend to focus on behavioral standards, such as those embodied in the NPRM, that restrict a BIAS from collecting and using certain types of sensitive information. Although we are not opposed to reasonable baseline limitations on the usage of sensitive information, it is important to recognize that, by the time a BIAS provider has the ability to collect sensitive information that could "*threaten a person's financial security, reveal embarrassing or even harmful details of medical history, or disclose to prying eyes the intimate details of interests, physical presence, or fears*",[4] something has gone horribly wrong. Asymmetric key exchange protocols such as TLS offer the relative benefit of consumer certainty in the security of their information. If both parties to a conversation use TLS properly, the data in transit is impossible for any eavesdropper to interpret. Behavioral norms on the other hand require consumer faith in the benevolent intentions of BIAS providers, belief that BIAS providers themselves are invulnerable to malicious infiltration by cybercriminals, and confidence in the FCCs ability to maintain a nearly omniscient compliance verification capacity. End-to-end encryption at the edge provider level will always provide more robust and verifiable consumer privacy protections than behavioral regulations and rules imposed on BIAS providers alone. Even if encryption is not a perfect solution to all privacy concerns, a strong encryption regime is preferable by far to a bureaucratically and resource constrained regulatory one.

Finally, commenters who have argued that encryption does not provide complete protection against the analysis of flow data and other unencrypted metadata are correct in their recognition

[4] NPRM Paragraph 2

the collection of such data may raise privacy concerns. In this context, baseline behavioral rules regarding the collection, use and sharing of this information may represent the best available mechanism towards ensuring consumer privacy. However, such rules must be implemented with nuanced awareness of the unique obligations of BIAS providers. Much of this unencrypted metadata is critical to the provision of effective BIAS routing services. Information like the "domain names of websites visited by users" is an essential component of how the Internet functions. Adding steep regulatory burdens on BIAS providers to limit their ability to collect, analyze and share this data for operational or security purposes can impose significant costs and decrease quality of service. Flow information based on geographic region, time of day, demographic, or even individual browsing patterns is necessary to optimize network resource allocation, anticipate consumer demand and identify irregular behaviors indicative of malicious activity (e.g. DDoS attacks). The ability to affordably collect, responsibly share, and analyze this data is essential to the continued function of the Internet infrastructure that BIAS providers maintain. As such, regulations in this area should be imposed with great caution and consideration of their wider impacts on the provision of BIAS.

We agree that encryption may not be the perfect solution to all privacy challenges. Nevertheless, encryption represents an essential component of any modern privacy regime. Encryption is most effective when implemented by edge-providers in an end-to-end manner using affordable and demonstrably secure cryptographic protocols. By requiring edge providers to use encryption, it is possible to bolster consumer confidence while simultaneously limiting the compliance verification burden and the risk of malicious or unintentional breaches. In those few cases where edge encryption is inadequate to protect privacy, the Commission would do well to

consider carefully the impact of any proposed rules on the ability of BIAS providers to offer high-quality and optimized access to their customers.