

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 Nominum, Inc.

Sandy Wilbourn, Sr. V.P. Of Engineering
Bruce Van Nice, Dir. Of Product Marketing
Nominum, Inc.
800 Bridge Parkway, Suite 100
Redwood City, CA 94065
(650)381-6000

July 6, 2016

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

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

Reply Comments of Nominum, Inc.

A. Introduction

Nominum™ submits these reply comments in the Federal Communications Commission’s (“Commission”) Notice of Proposed Rulemaking entitled Protecting the Privacy of Customers of Broadband and Other Telecommunications Services (“*BIAS Privacy Notice*”).¹

Nominum, which develops Domain Name System (“DNS”) software and value-added subscriber-facing applications used by more than 500 million subscribers to conduct more than 1.6 trillion transactions every day, submits these reply comments to highlight the record support for its positions advocating for the Commission to (i) permit the continued use and sharing by broadband Internet access service (“BIAS”) providers of network data, particularly domain name system (DNS) information, to promote network operations and security, without requiring the consent of customers; (ii) modify or clarify the proposed standard for such use and sharing to avoid creating uncertainties that might reduce the sharing of DNS data and reduce innovation

¹ Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, Notice of Proposed Rulemaking, 31 FCC Rcd. 2500 (rel. Apr. 1, 2016) (*BIAS Privacy Notice*).

that would improve security, e.g., change the “reasonably necessary” standard in paragraph 117 to “reasonable” if the Commission may apply that standard to the sharing of DNS data, or clarify that such use and sharing is deemed “reasonably necessary” and falls outside the requirement of customer consent; (iii) ensure that BIAS providers can continue to share information with one another, software vendors and researchers to address cyber threats and promote operational efficiency; (iv) adopt a privacy and consent framework that is consistent with consumer expectations and does not inhibit operations and innovations that could benefit consumers, such as parental controls and data usage notifications; and (v) support innovation and BIAS flexibility to develop alternative means of providing meaningful notice to consumers, such as through in-browser messaging, as discussed in our initial comments.

B. The Commission Should Explicitly Support Collection, Use and Sharing of Customer PI for Network Operations and Security.

The *BIAS Privacy Notice* proposed to not require customer approval for collection, use and disclosure of customer PI for “the efficient delivery of BIAS.”² The Notice further proposes to permit BIAS providers to use or disclose CPNI “whenever reasonably necessary to protect themselves or others from cyber security threats or vulnerabilities.”³ As Nominum noted in its initial comments, to the extent that the Commission treats DNS data as falling within the scope of CPNI, Nominum does not challenge the Commission’s understanding that section 222(d) protects the collection, use and disclosure of customer PI, including DNS, for operational and security purposes.⁴ We remain concerned, however, about the Commission creating uncertainty, including through the Commission’s “reasonably necessary” standard proposed in paragraph 117

² *BIAS Privacy Notice*, 31 FCC Rcd. at 2539, para. 111.

³ *Id.* at 2541, para. 117.

⁴ Nominum comments at 4, n. 9.

of the NPRM which is too restrictive – points raised by other commenters in the record.⁵

Nominum, therefore, urges the Commission to provide the clarity that is necessary to ensure that the sharing of DNS data that has been vital to security improvements and innovation continues unabated. It could modify the standard governing BIAS conduct in paragraph 117 to “reasonable” and explain that sharing DNS data for operational and security purposes normally meets this standard. Alternatively, the Commission could make explicit in an order that the collection, use and disclosure of customer PI, including DNS, for purposes of promoting network operations and security is deemed “reasonable necessary” and falls outside the scope of the customer consent requirement.

As noted in our initial comments, DNS offers valuable operational insights that benefit consumers and is an efficient and effective way for BIAS providers, researchers and security vendors to identify cyber threats.⁶ A number of commenters to the *BIAS Privacy Notice* agreed that certain network information, including DNS data, is beneficial to promoting a safe and secure experience for consumers.⁷ For example, a group of researchers from the Georgia Institute of Technology, FarSight Security and ThreatStop (collectively “Georgia Tech Researchers”), which includes the inventor of DNS, provided examples of ways in which BIAS providers take steps to promote a more secure environment while maintaining an operational environment that meets consumer expectations.⁸ The Georgia Tech Researchers explained that BIAS providers “have a unique vantage point to identify abuse, restore network trust and remove

⁵ National Cable & Telecommunications Ass’n. (NCTA) comments at 76-77 (noting uncertainty with the standard); CTIA comments at 139-142 (noting the need for clarity); Information Technology Industry Council comments at 14 (noting the standard is too restrictive).

⁶ Nominum comments at 4.

⁷ With regards to DNS data specifically, NCTA notes that the Internet Engineering Task Force “considers DNS data and the results of a DNS query obtained by or initiated from an ISP’s end user to be public.” NCTA comments at 61.

⁸ Georgia Tech comments at 2, 6.

cyber threats.”⁹ As such, the group notes BIAS providers “can help an infected customer’s network traffic from attacking and harming another customer.”¹⁰

Similarly, Upturn notes a variety of tools BIAS providers have and should be allowed to continue to use, including DNS queries, for “valid network management purposes, including to detect infections of malicious software, and real user traffic to identify and block such domains.”¹¹ And as the Messaging Malware Mobile Anti-Abuse Working Group (“M³AAWG”) notes, collaboration amongst industry participants “working against bots, malware, spam, viruses, DoS attacks and other online exploitations,” is critical to creating an environment that both protects privacy and security.¹² M³AAWG notes various techniques, including DNS Blackhole Lists, that promote security and often as a common good with “no additional benefit” to the BIAS provider.¹³

These tools not only rely on network data, but they rely on being able to develop information over an extended period of time and a broad data set in order to provide analytics that help BIAS providers prepare for future, unknown risks. As Nominum stated in its comments, it was through its access to DNS research over more than seven years that it was able to develop innovations to DNS server software that have resulted in smarter servers that are capable of automatically protecting themselves and the ultimate target of distributed denial of service attacks.¹⁴ M³AAWG provides additional examples of services that rely on broad data sets

⁹ *Id.* at 3.

¹⁰ *Id.*

¹¹ Upturn comments at 6-7.

¹² M³AAWG at 1.

¹³ *Id.* at 3. *See also* Deepfield Networks comments at 2,3(filed under “Craig Labovitz”) (citing the beneficial uses of DNS information for network management).

¹⁴ Nominum comments at 2.

with historical data to be effective and predictive of potential future harms.¹⁵ These efforts can be jeopardized under any consent regime because the loss of data hinders the predictive ability of the information. Moreover, as a practical matter any consent regime, whether opt-in or opt-out, is unworkable. This is because it would require that network data be segregated based on whether permission for its use was provided. In an environment where most BIAS providers make widespread use of dynamic IP addresses, segregating data in real time, as IP addresses change and as customer consent changes, presents an exceptional, potentially insurmountable, challenge.

Further, Nominum, M³AAWG and others caution that positive uses of information could be jeopardized by an unclear, ambiguous or restrictive regime where uncertainty deters the sharing and participation of BIAS providers. Commenters identified harms to the delivery of both BIAS itself and content, and the ability to block SPAM, malware, and other network abuses, as potential adverse impacts of restrictive or ambiguous regulations given the high levels of collaboration involved in addressing these problems. A restrictive or ambiguous regulatory standard will have an adverse impact on consumers, making networks less stable and secure and more difficult and costly to operate. There are no substitutes for extensive hard data to support network security and operations. Less DNS data and less sharing means correspondingly less insight.

By proposing a “reasonably necessary” standard, for example, the Commission may inadvertently inject uncertainty into many of the sharing efforts related to security that are outlined above and in the record if the Commission means for this standard to apply to the

¹⁵ M³AAWG at 2-4.

sharing critical network information such as DNS data.¹⁶ For example, will a BIAS provider's denial of access to certain IP addresses based on inaccurate reporting that the address has a demonstrated history of abusive practices lead to a circumstance where consent should have been required since the action was not "necessary" to protect the consumer?¹⁷ This uncertainty could deter BIAS providers from sharing information that could enhance security or network performance.¹⁸ To remove such uncertainty, Nominum suggests that the Commission should adopt a standard that looks at whether the collection, use and disclosure of customer PI for network operation and security purposes was "reasonable" as opposed to whether the action was "reasonably necessary to protect themselves or others from cyber security threats or vulnerabilities." This modification to the standard should help provide BIAS providers with the higher level of certainty needed to continue to share information with each other and researchers to promote a safer and more secure experience for their customers. The Commission could also include statements that provide helpful clarifications along with this change in the language of the standard.

Alternatively, to the extent that the Commission means to apply this standard to DNS information, the Commission should clarify that where the collection, use and disclosure of customer PI is intended to advance operation or security measures, it is presumed or "deemed"

¹⁶ *BIAS Privacy Notice*, 31 FCC Rcd. at 2541, para. 117.

¹⁷ M³AAWG at 2.

¹⁸ Comcast notes uses that are even broader including protection of copyrighted information and preventing the distribution of child pornography and other illegal activities. Comcast comments at 59-60. These are worthy efforts that the Commission should ensure are not unnecessarily limited by a poorly crafted standard that deters collaboration.

“reasonably necessary.” The Commission would need to make such a clarification either in the text of an order or by adding qualifying language to its proposed rule § 64.7002(a)(3).¹⁹

The record in this proceeding is replete with examples of beneficial uses that come from sharing of information between BIAS providers and researchers as it relates to promoting a safe and secure Internet experience. Nominum urges the Commission to adopt requirements that recognize these opportunities and continues to promote them.

C. The Commission Should Ensure BIAS Providers Can Continue to Share Information with One Another, Software Vendors and Researchers

As alluded to above, the effort necessary to address cyber threats effectively and promote operational efficiency rely heavily not only on a BIAS provider’s own network engineers, but also on a collaboration with other BIAS providers, software vendors and researchers. Some “disclosure” of information is contemplated in the Commission’s proposal, but Nominum wishes to underscore that a number of commenters emphasized the importance of continued collaboration.²⁰ Nominum joined a joint letter filed with the Commission that calls for an explicit exemption for data shared with researchers, protocol developers, security technology specialists and related organizations.²¹ In this regard we also note that leading BIAS provider Comcast notes in its comments the importance of relying on researchers and academics to assist in improving the integrity and reliability of its service.²² In adopting rules, we would ask that the Commission make clear that sharing of customer PI with researchers is permitted so that this critical link to developing better responses to cyber threats remains available and effective. A

¹⁹ *BIAS Privacy Notice*, 31 FCC Rcd. at 2601, App. A, “Proposed Rules.”

²⁰ Deepfiled comments at 3, Georgia Tech Researchers comments at 3, 6, M³AAWG comments at 1-2 “ISPs continue to provide the critical collaboration that we all need to fight the good fight”).

²¹ Letter from Nick Feamster, Princeton University, to Chairman Tom Wheeler, WC Docket No. 16-106, Research Exemption Letter (filed July 6, 2016).

²² Comcast comments at 60.

reduction in visibility brought about by an opt-in regime or a reduction in data sharing as a consequence of greater uncertainty will have an adverse impact on service delivery and security.

D. The Commission Should Avoid Adopting an Overly-Broad Framework That Could Hinder Innovations That May Provide Beneficial Tools to Consumers.

There is a nascent trend toward using network data, including DNS data, to enable consumers to better determine what content they can view in their homes, allow parents to regulate usage within the home, and deter various forms of malware and phishing. Malware detection, parental controls and real-time notifications are innovations that provide consumers with more information, and enhance their experience, by using information gathered as part of the consumer's interaction with the network.²³ These opportunities will allow BIAS providers and others to continue to develop services to provide consumers greater choice and control over their Internet experience.

In its comments, the Staff of the Consumer Protection Bureau of the Federal Trade Commission ("FTC Staff") noted that the Federal Trade Commission has "advocated that companies provide meaningful choices to consumers, with some level of choice being tied to consumer expectations." The FTC Staff recommended that opt-in consent should be limited to "sensitive information that could be collected by BIAS providers, including 1) content of communications and 2) Social Security number or health, financial, children's or precise geo-location data," noting that such an approach was more consistent with consumer expectation that differ between sensitive and non-sensitive information.²⁴ The FTC Staff noted that the proposal put forward by the Commission could "hamper beneficial uses of data that consumers may prefer, while failing to protect against practices that are more likely to be unwanted and

²³ NCTA lists other use cases for network traffic data that the Commission should consider as it develops its privacy framework. NCTA comments at 62.

²⁴ Comments of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission at 20.

potentially harmful.”²⁵ The FTC Staff is correct—the Commission’s proposal could hamper the use of DNS data to improve security.

This does not mean some form of a consent regime is not appropriate, be it opt in or opt out. The Commission should adopt a consent regime that will permit Nominum and others to continue to develop products that will allow BIAS providers to offer their customers more security and greater choice and control over their Internet experience. Allowing BIAS providers an opportunity to present their customers with these product offerings will help ensure that these “beneficial uses” of data are made available to consumers.

E. The Commission Should Allow BIAS Providers the Flexibility to Use New Technologies to Provide Timely Privacy and Other Notices to Consumers.

As Nominum demonstrated in its initial comments, in addition to the use of comparatively older tools like email, etc., increasingly there are innovative solutions to enable BIAS providers to alert consumers to information and choices, including tools that may be more likely to capture the attention of message recipients. Nominum noted that DNS-based, in-browser messaging can overcome limitations of legacy communications methods.²⁶ As CTIA notes in its comments, notification requirements should not be overly prescriptive, and instead should allow BIAS providers flexibility in determining both the time and context for obtaining consent.²⁷ Nominum agrees and believes that the Commission should afford BIAS providers flexibility in determining when and how to provide consumers meaningful notice. The Commission should make clear that tools, such as those offered by Nominum and others, are options as well. If the Commission does not do so, it will discourage innovation and continued efforts to empower consumers with notice and an opportunity to express their choices.

²⁵ *Id.* at 22-23.

²⁶ Nominum comments at 6.

²⁷ CTIA comments at 143-144.

F. Conclusion

As Nominum recommended in its initial comments, a clear policy on collection, use and disclosure of information for security and operational purposes is critical to ensuring a safe and more secure environment for consumers. Among the ways to avoid uncertainty and provide more clarity, Nominum recommends that the Commission revise the standard proposed in the *BIAS Privacy Notice* from “reasonably necessary” to “reasonable” and make clear that the sharing of network information, such as DNS data, for security and operational purposes is permitted by the rules without consent. Alternatively, the Commission could state that the collection, use and disclosure of network information such as DNS data is permitted and also that it qualifies as “reasonably necessary” for security purposes under the rules. In recognition of current practices and the benefits of collaboration, the Commission should also make clear that sharing network information with researchers and others is covered “disclosure” under the rules. Consistent with the recommendation from the FTC Staff, the Commission should reconsider its proposal to adopt a broad opt-in regime and instead consider adopting a consent regime that aligns with consumers’ expectations related to the sensitivity of the data being collected. Under such a regime, DNS data should not be considered among the most sensitive types of data. Providing flexibility will promote innovative ways of bringing consumers more information. Finally, the Commission should provide the flexibility for a BIAS provider to use tools like “in-browser” notification for notice and other purposes.

Sandy Wilbourn

/s/ Sandy Wilbourn