BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of	)
	)
Restoring Internet Freedom	) WC Docket No. 17-108)
	)

REPLY COMMENTS OF THE MESSAGING, MALWARE AND MOBILE
ANTI-ABUSE WORKING GROUP

The Messaging, Malware and Mobile Anti-Abuse Working Group ("M³AAWG") hereby

replies to the comments filed in response to the Notice of Proposed Rulemaking ("NPRM")

adopted by the Federal Communications Commission ("Commission") on May 18, 2017 in the

above-captioned proceeding.[1]

I.   Introduction and Summary

Advances in Internet communications technology have empowered billions of people

around the world to connect to each other and access and share information and content over the

open Internet. Unfortunately, these breakthroughs also have enabled and escalated the threat

posed by malfeasants seeking to leverage these abilities to carry out misdeeds. The various

forms of online abuse – such as spam, botnets, malware, phishing, and distributed denial of

service ("DDoS") attacks – remain a constant and growing threat to Internet users' online

experiences, and they impose a substantial cost on consumers and industry each year.

Facing the growing need to constantly protect Internet users from this cascade of

disruptive activity, M³AAWG was created by members of the messaging industry (e.g., ISPs,

network operators, email service providers, researchers, and technology vendors) to enhance

---

[1] *Restoring Internet Freedom,* Notice of Proposed Rulemaking, 32 FCC Rcd. 4434 (2017).

consumer trust by developing industry-wide policies and procedures to address messaging issues and other forms of online abuse.[2] In the twelve years since its inception, M³AAWG has long recognized the specific threat posed to broadband users and networks by botnets and other attacks, and it has been a strong supporter of the evolving security measures and network management techniques that ISPs must use to detect, thwart, and prevent those attacks.

Unfortunately, many ISPs' current and future technical efforts to rid networks and devices of online abuse, including those which M³AAWG helped develop, could still be undermined by the unintended consequences of a common carriage framework. For this reason, we support Commission action to ensure that ISPs have the flexibility to deliver new solutions and protections against rapidly-advancing threats to the Internet ecosystem.

II.   BIAS Providers Play a Critical Role in Protecting Internet Users

As the number of connected consumers and devices continues to grow, broadband Internet service providers must play an integral and expanding role to ensure the security of their customers and help protect Internet users around the world. This security facilitates the fundamental trust on which Internet users rely in order to conduct economic activity and social interaction online. Accordingly, the development, implementation, and operation of advanced online security measures by broadband service providers is essential to maintaining a vibrant and safe Internet, and recognizing the technical sophistication and societal importance of these measures should be at the forefront of the Commission's deliberations in this proceeding.

---

[2] M³AAWG's membership roster is available at https://www.m3aawg.org/about/roster.

Some commenters have thus far ignored or undervalued the critical role that ISPs play in securing and supporting the diverse ecosystem of Internet companies.[3] In doing so, these commenters discount the contributions that ISPs and other ecosystem players have made, individually and collectively, to adopt advanced methods and technologies designed to prevent online abuse and ensure a safe Internet for their users, as well as users of other networks. For example, as part of the Internet service they offer, ISPs use advanced detection methods to identify abusive email and other hostile data traffic that the industry works to prevent.[4]

Commenters who are skeptical of the classification of BIAS (Broadband Internet Access Service) as an information service fail to observe the breadth and technical complexity of the multifaceted strategies that ISPs use to mitigate online attacks and other abuses:

- ISPs are eminent providers of Domain Name System ("DNS") service and help prevent countless DNS-enabled attacks, such as DDoS attacks, through their implementation of DNS Security Extensions ("DNSSEC") technology;

- ISPs also provide competitive, over-the-top services, similar to Google DNS and OpenDNS products;

- Many ISPs vigilantly monitor their networks for suspicious traffic and attacks, and they proactively block or redirect traffic when suspicious traffic is found;

---

[3] *See, e.g.,* Joint Comments of Internet Engineers, Pioneers, and Technologists, WC Docket No. 17-108, at 12 (filed July 17, 2017).

[4] M³AAWG published a series of 'best practices' documents outlining some of the methods that major ISPs and other messaging providers currently use to prevent phishing and other abusive email traffic. *See, e.g.,* M³AAWG, Anti-Phishing Best Practices for ISPs and Mailbox Providers (2015), *available at* https://www.m3aawg.org/sites/default/files/M3AAWG_AWPG_Anti_Phishing_Best_Practices-2015-06.pdf

- ISPs exchange information and data about attack traffic and related malware with security researchers, other ISPs, M³AAWG, and other organizations so that the Internet community is better able to collectively defend itself;

- ISPs develop and promote informational resources and best practices to prevent future attacks; and

- ISPs distribute anti-virus software, often as a component of the service they offer to customers.

These strategies mirror and often supplement the activities of other information services residing on the edge of the network. For example, leading Internet messaging provider WhatsApp applies many of the same anti-spam measures that ISPs include as part of their service and use to detect and prevent abusive messaging activity.[5] Accordingly, the Commission should recognize the proper classification of these diverse activities as part of a singular information service and take action to ensure that ISPs are afforded the same degree of flexibility as other information service providers to deliver new solutions and protections for their customers and other Internet users.

III.   ISPs Help Ensure the Security of the Domain Name System

The DNS resolution service that ISPs provide is an integral, non-management function that involves the computational generation, acquisition, storage, transformation, processing, retrieval, utilization, and delivery of information in milliseconds to enable worldwide communication over the Internet; these actions alone exhibit all of the characteristics of an information service. Moreover, while these operations may be performed for some consumers by

---

[5] Cathal McDaid, HeadsUp for WhatsApp, Adaptive Mobile (Jan. 15, 2015), *available at* https://www.adaptivemobile.com/blog/headsup-for-whatsapp.

third-party DNS service providers, ISPs occupy a meaningful position in the system because

their DNS servers are often distributed in a closer proximity to the end user, which results in

performance gains. For example, Comcast's DNS service is distributed across 28 different local

metropolitan areas in order to bring DNS servers as close in proximity to its Internet customers

as possible while maintaining capacious DNS cache performance.[6]

The secure provision of rich, widely-distributed DNS service by ISPs is important to the

Internet ecosystem because it helps prevent the proliferation of spam-related malware. Most

virulent malware exploit vulnerabilities in DNS architecture in order to carry out attacks; for

example, some malware might generate large volumes of trial-and-error DNS queries to

determine the website hosting servers to which it should connect and deposit its spam.

Additionally, malware can interfere with DNS connectivity in order to redirect users from

legitimate sites to rogue or "fake" websites that conduct phishing and social engineering schemes

or generate advertising revenues. Bad actors also employ DNS interference tactics to block

access to malware remediation resources, such as security updates and anti-virus tools, and direct

users to malicious websites that install additional malware on the user's device.

ISPs play a significant role in preventing these kinds of exploits by using and promoting

advanced security measures. For example, many ISPs use DNSSEC, which prevents DNS

interference through the use of cryptographic signatures that verify domain name data, thereby

protecting users from malicious or compromised websites. Major ISPs in the United States began

deploying DNSSEC in 2010, and other DNS service providers around the world quickly

followed. In this manner, the eminence and security-minded diligence demonstrated by ISPs

---

[6] Comments of Sandvine, WC Docket No. 17-108, at 3 (filed July 14, 2017).

helped shepherd other providers in the DNS system toward the adoption of stronger security

measures that prevent online attacks.

IV.   ISPs Implement and Invest in Secure Information Technologies to Prevent Attacks and Unwanted Traffic

Many of the protections enjoyed by Internet users are made possible by the constant

efforts of ISPs to deploy new information technologies and security enhancements in the services

they offer and drive adoption of those enhancements throughout the ecosystem.

In addition to the security benefits enjoyed by ISP customers, the security technologies

nurtured and pioneered by ISPs can also provide additional protection to the ecosystem at large.

For example, ISPs have made significant investments in DDoS monitoring and mitigation

technologies to ensure the availability and safety of their Internet access services during an

attack. Successful DDoS attacks have the ability to rapidly spread their impact across the

Internet; active DDoS attacks can quickly comprise over 10% of a country's entire Internet

traffic, and larger DDoS attacks are generating volumes of malicious traffic that are approaching

a terabit per second.[7] To meet this threat, ISPs have invested in the development of specialized

equipment and software that are designed to detect traffic anomalies and separate suspicious

traffic from normal traffic to prevent a potential attack from negatively impacting the Internet

experience of other users.

One of the most effective toolsets that ISPs and the rest of the Internet industry have at

their disposal to prevent large-scale attacks and toxic activities are blocking services or "block

lists." These lists, which are comprised of known IP addresses and URLs associated with

malfeasants and malicious traffic, are made available to and used by ISPs and other network

---

[7] Nicky Woolf, *DDoS attack that disrupted internet was largest of its kind in history, experts say*, The Guardian (Oct. 26, 2016), https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

operators to protect their users.[8] By reducing access to these dangerous destinations and

monitoring suspicious traffic on their networks, ISPs help prevent a significant quantity of spam,

attacks, and other online abuse.

V.   ISPs Collaborate with the Industry on Best Practices, Technical Standards, and Protective Software to Prevent Malware and Other Online Abuse

An important non-management function performed by ISPs is working hand-in-hand with

the online security community to develop and promulgate industry best practices and other

recommendations to prevent harmful messages and other abuses from being transmitted across

their networks. For example, ISPs regularly submit recommendations to the Internet Engineering

Task Force on ways for providers to remediate the effects of subscriber computers that have been

infected with malware. Similarly, most of the ISP members of M³AAWG have published a set of

best practices to help subscribers combat and prevent viruses, spyware, and malware.[9]

ISPs also contribute their perspectives and technical expertise to many standards-based

bodies aimed at driving security-by-design into technology and service development. The Wi-Fi

Alliance is one such organization that sets standards for Wi-Fi technology and services,

including mandatory security certification, to ensure the safety and reliability of personal

networks and public access points connected to the Internet. Another industry group, CableLabs,

is comprised of cable Internet access service providers that work together to develop industry-

specific technical specifications, including security protections that ensure the privacy, integrity,

---

[8] *See, e.g.,* The Spamhaus Project, SBL Advisory: The Spamhaus Block List (last visited August 1, 2017), *available at* https://www.spamhaus.org/sbl/.

[9] *See, e.g.,* AT&T, Fighting Malware: Protect Your Computer to Keep Your Data Safe (last visited August 1, 2017), *available at* http://www.att.net/smartcontrols-FightMalware; *see also* CenturyLink, Consumer Internet Protection Program (last visited August 1, 2017), *available at* http://www.centurylink.com/home/support/internetprotection/; Comcast, Ways to Protect Your Computer from Viruses and Malware (last visited August 1, 2017), *available at* https://www.xfinity.com/support/internet/computer-virus-protection/.

and availability of their Internet access service.[10] In addition to their contributions to standards-based security initiatives, as mentioned, most major ISPs also offer free protective software, such as anti-virus and firewall applications, to help customers protect their devices from malware and other intrusions.

VI.   Conclusion

These diverse functionalities – providing DNS service and security, adopting and investing in advanced traffic monitoring and other security-promoting information technologies, contributing to industry best practices and technical standards, and distributing anti-virus software, among many others performed by ISP – are all part of a single integrated information service that ISPs offer, and not a singular telecommunication service or an information service provided alongside a severable telecommunication service. A common carriage framework may undermine many of the current and future technical efforts that are necessary to protect the safety of Internet users. Ensuring a safe and open Internet requires that the productive energies of the Internet industry's technical experts remain focused on current efforts to combat malicious attacks and other online abuses, and not be diverted to deciphering regulations or defending their actions against spurious legal claims raised by perpetrators of online abuse.

For the forgoing reasons, the Commission should take action to ensure that the Internet industry retains its flexibility to deliver new solutions and protections against ever-evolving threats to the ecosystem. Accordingly, as a working group that has been effective in fostering cooperation among ISPs, network operators, researchers, and technology vendors to meet the

---

[10] *See* CableLabs, CableLabs Inform[ED] Insights, Securing Networks in the Broadband Age (Spring 2017), *available at* https://www.cablelabs.com/wp-content/uploads/2017/04/Securing-Networks-in-the-Broadband-Age-2017.pdf.

security needs of Internet users around the world, M³AAWG offers the Commission its

assistance as a source of technical information on any of the aforementioned topics and issues.

                                        Respectfully submitted,

                                        [SIGNATURE]
                                        /s/
                                        Jerry Upton
                                        Executive Director

                                        Messaging, Malware and Mobile
                                        Anti-Abuse Working Group
                                        781 Beach Street, Suite 302
                                        San Francisco, California 94109
                                        https://www.m3aawg.org

August 27, 2017