Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
Preserving the Open Internet	)	GN Docket No. 09-191
Broadband Industry Practices	)	WC Docket No. 07-52

COMMENTS OF THE MESSAGING ANTI-ABUSE WORKING GROUP

The Messaging Anti-Abuse Working Group ("MAAWG") hereby responds to the Commission's Notice of Proposed Rulemaking (the "NPRM") in the above-captioned proceeding.[1]

I. Introduction and Summary

Hundreds of millions of people throughout the world can readily and seamlessly communicate and interact with each other over the open Internet. Unfortunately, spam and other forms of online abuse such as botnets, malware, phishing and denial of service attacks persistently threaten to diminish these users' online experiences, and impose substantial costs on consumers and industry each year.

In order to protect consumers and businesses against these threats, MAAWG was created by members of the messaging industry to enhance consumer trust and confidence by developing universal policies and procedures to address messaging abuse. MAAWG's open and diverse membership roster is comprised of Internet Service Providers ("ISPs"), network operators, email service providers and technology vendors from around the world.[2] These members, who collectively represent over one billion mailboxes, work voluntarily and collaboratively to combat

[1] *In the Matter of Preserving the Open Internet*, GN Docket No. 09-191, WC Docket No. 07-52, Notice of Proposed Rulemaking, FCC 09-93 (Rel. Oct. 22, 2009) (hereinafter "NPRM").
[2] MAAWG's membership roster can be viewed at http://www.maawg.org/about/roster.

all forms of current and emerging modes of online abuse across fixed and mobile broadband access platforms. A major focus of MAAWG is on the threats posed to users of broadband networks by bots and botnets. In the five years since its inception, MAAWG has evolved to become the leading global organization for comprehensively addressing the challenges of online messaging abuse.

MAAWG commends the Commission for its commitment to preserving a safe and secure Internet, as discussed in the NPRM.[3] Effective online security measures are essential to maintaining a vibrant Internet, and the importance of preserving these measures should be at the forefront of the Commission's deliberations in this proceeding. As such, the Commission's inclusion of methods to combat "unwanted" and "harmful" Internet traffic in its proposed definition of "reasonable network management" would be an appropriate starting point in helping to ensure that MAAWG's members can continue in their collective efforts to combat forms of online abuse, should the Commission ultimately choose to adopt new rules.[4] As explained below, however, industry efforts to rid networks and devices of spam and other forms of online abuse could still fall victim to the unintended consequences of "open Internet" regulation unless the Commission takes steps to ensure that industry retains the flexibility to address current and future security threats.

[3] *See*, *e.g.*, NPRM ¶ 9 (recognizing the importance of allowing broadband providers to manage their networks in a way that will further the safety, security, and accessibility of the Internet); *id.* ¶ 15 (stating that the Commission's proposed rules would "enable broadband providers to reasonably manage their networks and will help ensure a safe and secure Internet where unwanted traffic such as computer viruses and spam is limited.").

[4] *See id.* ¶ 135 ("Reasonable network management consists of: (a) reasonable practices employed by a provider of broadband Internet access service to (i) reduce or mitigate the effects of congestion on its network or to address quality-of-service concerns; (ii) *address traffic that is unwanted by users or harmful*; (iii) prevent the transfer of unlawful content; or (iv) prevent the unlawful transfer of content; and (b) other reasonable network management practices." (Emphasis added)).

II. The Scale of the Abuse Problem and Industry's Response

The Internet ecosystem continues to thrive because there is a large community of stakeholders who collaborate to enhance the user experience in the face of a relentless parade of intrusions and attacks. With respect to messaging abuse, MAAWG has developed a series of quarterly reports on "Email Metrics" to track the amount of abusive email that is being sent to more than 500 million mailboxes worldwide.[5] These reports also provide policymakers with a guide to understanding the effectiveness of industry's efforts in obstructing abusive emails before they reach users. As recent MAAWG Email Metrics illustrate, the sheer volume of messaging abuse that occurs on the Internet today is staggering. During calendar year 2008, the percentage of email identified by participating MAAWG members as "abusive" ranged between 89% and 92%.[6] This percentage is based on service providers' detection methods in identifying abusive email and reflects the continuing high level of abusive email that the industry works to prevent from clogging users' inboxes, as well as the need for continued industry cooperation and diligence.

To protect consumers and businesses against this avalanche of disruptive activity, industry players are required to utilize network management techniques as part of a multi-faceted strategy to provide end users with a more secure and stable messaging environment. For example, one of the most cost-effective tools that ISPs and other industry players have at their disposal are blocking services known as "block lists." These lists, which are composed of known IP addresses and URLs that are used by malfeasants to send unwanted messages, are

[5] *See*, *e.g.*, MAAWG Email Metrics Program: The Network Operators' Perspective, Report #10 – Third and Fourth Quarter 2008 (Mar. 2009), *available at* http://www.maawg.org/about/MAAWG_2008-Q3Q4_Metrics_Report.pdf.

[6] "Abusive" emails are communications that are generally understood as seeking to exploit end users, and should not be conflated with the term "spam" per se, as the precise definition of spam varies from country to country. Nevertheless, most observers would agree that the term "spam" can be understood as electronic communications that are not wanted or expected by a recipient.

made available to ISPs and other network operators by third party providers such as Spamhaus.[7] By controlling access to these addresses and URLs, the parties that collaborate to provide messaging services have been able to prevent a significant portion of inbound spam, thereby helping to protect end users from being inundated with unwanted messages and otherwise preserving the safe and reliable functioning of messaging across the Internet.

Another noteworthy aspect of the fight against messaging abuse is industry's ongoing effort to promulgate best practices and other recommendations[8] to prevent or diminish unwanted messages from being transmitted across networks. Participating members of MAAWG have, among other activities, published a set of best practices on how to combat viruses and spyware or malware that can take control of large numbers of computers,[9] submitted recommendations to the Internet Engineering Task Force on ways for providers to remediate and manage the effects of subscriber computers that have been infected with malicious bots,[10] and issued a set of voluntary principles aimed at enhancing the security of network infrastructure in the fight against spam.[11] As the community of entities endorsing and applying these recommended practices continues to grow, the more effective these practices have become.

III. Drafting Rules to Minimize Unintended Consequences while Providing for Flexibility to Adapt to New Threats

Given the ongoing threat of messaging and other forms of abuse, as well as the voluntary and collaborative response to such threats, MAAWG urges the Commission to draft any rules

---

[7] Additional information about the Spamhaus Project is available at http://www.spamhaus.org/.
[8] *See* MAAWG, *MAAWG Published Documents, available at* http://www.maawg.org/about/publishedDocuments/
[9] *See* MAAWG, *Managing Port 25 for Residential or Dynamic IP Space Benefits of Adoption and Risks of Inaction* (2005), *available at* http://www.maawg.org/port25/MAAWG_Port25rec0511.pdf.
[10] *See* J. Livingood, N. Mody and M. O'Reirdan, *Recommendations for the Remediation of Bots in ISP Networks*, Informational Draft Submitted to the Internet Engineering Task Force (Sept. 15, 2009), *available at* http://tools.ietf.org/html/draft-oreirdan-mody-bot-remediation-03.
[11] *See* MAAWG, *Expansion and Clarification of the BIAC and MAAWG Best Practices for Internet Service Providers and Network Operators* (2006), *available at* http://www.maawg.org/about/publishedDocuments/MAAWG-BIAC_Expansion0707.pdf.

intended to preserve the open Internet in a manner that anticipates and minimizes unintended consequences. Specifically, MAAWG asks the Commission to take note of block lists and other effective online security measures to ensure that its rules do not discourage such measures. MAAWG asks the Commission to state clearly that these network management techniques generally are "reasonable" and otherwise allowable. Although MAAWG understands the Commission's desire to articulate broad policies in this proceeding,[12] any ambiguities or subjectivity surrounding the permissibility of these security measures will deal a double blow to efforts that have effectively managed spam and other threats -- both by emboldening bad actors who seek to exploit the regulatory process and by chastening those who seek to preserve safe and reliable messaging services. Preserving a safe and open Internet requires that technical experts' energies are not diverted from their efforts to combat spam and other messaging abuses to parsing regulations or defending their actions against spurious legal claims by spammers and perpetrators of other forms of abuse on the Internet.

MAAWG also urges the Commission to build flexibility into its rules so that entities that collaborate to provide messaging services can effectively combat spam and other online threats as those threats change in the future. Accordingly, MAAWG appreciates the Commission's endorsement of the need for network operators to have the flexibility to adapt their network management strategies in response to evolving user needs and the technical demands of preserving a high quality Internet experience.[13] Spammers, criminals and other bad actors in the Internet ecosystem do not simply sit idle in the face of collective industry efforts to protect

[12] *See* NPRM ¶ 12 (stating a preference for the case-by-case adjudication of open Internet principles over the crafting of detailed rules).

[13] *See*, *e.g., id.* ¶ 108 ("We intend reasonable network management to be meaningful and flexible"); *id.* ¶ 140 (including a "catch-all" provision to the proposed definition of reasonable network management to provide network operators with "additional flexibility" to experiment and innovate as user needs change."); *id.*, Statement of Chairman Julius Genachowski at 92 ("Broadband providers must be allowed meaningful latitude to solve the difficult challenges of managing their networks and providing their customers with a high-quality Internet experience.").

consumers and businesses from messaging abuse. As these malfeasants continuously adjust their schemes in a game of cat and mouse, the tools to fight abuse are necessarily in a constant state of flux. Thus, any regulation adopted by the Commission should acknowledge the relentlessly evolving nature of this ongoing challenge and allow the technical experts who manage networks on a day-to-day basis to respond to such threats as they arise, without first having to apply to regulators for permission. To the extent the Commission later finds that these immediate and necessary responses to spam and other forms of abuse raise regulatory or other concerns, MAAWG suggests that the Commission solicit input on these concerns and potential alternatives (*e.g.,* through the technical advisory process announced in the NPRM),[14] taking protective measures as necessary to ensure the confidentiality of information. The FCC should work closely with industry groups like MAAWG and the Anti-Phishing Working Group ("APWG") to act against many of these threats. Specifically, MAAWG offers its assistance as a source of technical information and would welcome the opportunity for members of the Commission or its staff to attend a MAAWG meeting. Working groups such as MAAWG and the APWG have proven to be very effective in cooperating to suppress spam and phishing and are now working to combat the botnet threat.

IV. Conclusion

As Chairman Genachowski has recognized, any regulation adopted in this proceeding should not be used as a "shield" for spam or other violations of the law.[15] Voluntary collaboration by industry has proven to be the most effective measure in addressing spam and other forms of abuse, and the magnitude of this problem often demands immediate attention. Thus, in adopting "open Internet" rules, MAAWG respectfully requests that the Commission

[14] *See id.* ¶ 177.
[15] *See id.*, Statement of Chairman Julius Genachowski at 93.

seek to preserve ongoing efforts to combat spam and other forms of abuse by drafting rules to sanction block lists and similar techniques so as to minimize the unintended consequences of new rules. Moreover, MAAWG requests that the Commission preserve the ability of technical experts to respond immediately to such abuse as it occurs. By doing so, MAAWG submits that the Commission will preserve safeguards against messaging and other forms of abuse and thereby, as this proceeding intends, protect the general health of the Internet ecosystem.

Respectfully submitted,

/s/ *Michael O'Reirdan*
Michael O'Reirdan, Chairman, MAAWG Board of Directors
Alex Bobotek, Vice Chairman, MAAWG Board of Directors
Jerry Upton, Executive Director, MAAWG

MAAWG Address
572 B Ruger Street
P.O. Box 29920 (mail)
San Francisco, California 94129-0920
Messaging Anti-Abuse Working Group

January 14, 2010