ESPC

Email Sender & Provider Coalition

17 May 2007

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, NW
Washington, DC 20580

_Re:_ ESPC Written Comments for the FTC's 2007 Spam Summit

Dear Secretary,

On behalf of the ESPC, I thank you for this opportunity to continue our participation in the anti-spam policy dialogue that has been a shared central concern of both the FTC and our organization for several years. Our membership has met to review the topics suggested in the FTC's Press Release, and as an initial matter we would like to express our strong support for both the timing and thematic focus of the anticipated Spam Summit. Our written comments are organized in response to certain topics you have identified for treatment at the event.

- **Defining the Problem**

We agree that in the years since the FTC's last Spam Forum in 2003, two major trends have characterized the email marketplace. The first--a shift on the part of the email marketing industry to a federal compliance regime under the CAN-SPAM Act, ever-wider adoption of email authentication by legitimate senders, and the expanded recognition of pro-consumer industry best practices, such as those required for membership in our organization. Second--in stark contrast to these positive developments, we have witnessed a proliferation of fraudulent botnets that increase the volume of illegitimate email, as well as malicious phishing attacks orchestrated by spammer networks.

We have also noted that consumers are not without tools to manage some of the negative effects of the spam problem. As highlighted in the Executive Summary of our recent study into consumer inbox management,[1] consumer sophistication in the use of available tools to separate desired emails from unwanted email in their inbox has grown considerably. Such inbox management techniques not only suggest that consumers are to an extent able and willing to take matters into their own hands – to separate the wheat from the chaff – but

[1] *See* 27 March 2007 Press Release, "Consumers Savvy About Managing Email According to ESPC Survey Results; Embrace Numerous Tools and Methods to Manage Spam Reporting and Unsubscribing," and link to Executive Summary *available at* http://espcoalition.org/032707consumer.php

also remind us of the crucial role that ISPs play in ensuring that wanted emails do in fact reach consumers.

ISPs are critical to protecting inboxes from the effects of botnet attacks not only because they can use authentication as an indicator to filter, but also because they provide user interface tools in web browsers to help consumers sort their own incoming messages once they pass through the filters. This central ISP role underlines the overriding importance of communication and coordination amongst ISPs. Currently, ISPs use a mixture of filter and feedback algorithms – and not all are using authentication as a measure of a sending domain's consistency. We urge the FTC to explore the extent to which greater inter-ISP harmonization of practices would help contribute to better coordinated anti-spam efforts.

This need for ISP harmonization is also important to retain focus on the preservation of the email ecosystem as a whole. Given the substantial value and increased convenience to consumers that characterizes wanted email communications, it is critical to maintain a balanced objectivity when exploring helpful techniques for reducing the volume of harmful email. A baseline challenge for any group seeking to identify the scope of the problem is that it must contend with the reality that reporting *on raw email volume*--such as that reported in the "Postini" study cited in the 30 January 2007 letter[2] sent to Chairman Majoras by the leadership of the House Subcommittee of Commerce, Trade, and Consumer Protection--can directly influence calls for spam regulation that mischaracterizes the scope and nature of the threat to this email ecosystem.

For example, by reporting that "Postini blocked more than 25 billion spam messages in December, representing a 144 percent increase from December 2005 to December 2006," accounting for "nearly 94 percent of all electronic mail on the Internet,"[3] a logical but erroneous inference can be drawn that all such blocked email was fraudulent, non CAN-SPAM compliant messaging. This characterization by anti-spam vendor services such as Postini provides an easily digestible, highly simplified sound bite that tells only a fragmented and incomplete story, which can only be of limited utility as the basis for sound public policy judgments. Reporting such a statistic misses the point that from a consumer protection standpoint, our critical focus must be directed towards what email makes it into a consumer's inbox, and what harms can flow from such messaging.

[2] *Available at* http://energycommerce.house.gov/Press_110/110-ltr.013107.FTC.CAN-SPAM.pdf

[3] *See* Press Release, *available at* http://www.postini.com/news_events/pr/pr011007.php

Further, ISPs and legitimate senders have a shared interest in reducing both harmful email and the instances of "false positives,"[4] which are somewhat more insidious in their negative effect on consumers. While criminal email practice is a natural focus in the debate on spam, the effect of false positives on legitimate marketers is the under-discussed flip-side of the anti-spam phenomenon, itself contributing to consumer economic harm. In addition to the hassle experienced by consumers that do not receive expected messages, according to one Ferris Research study the cost to businesses of false positives may have been as much as 3.5 billion in a single year.[5] The nature of both harms again counsels us to focus on the ISP gatekeeper role. Efforts to bring the ISPs closer to one another and legitimate sender practices will help mitigate this second type of harm that can result from irregular email management practices by ISPs.

This is not to say that all responsibility for legitimate practices must shift exclusively to the ISPs. To the extent that there are really two classes of spam – malicious email that does not conform to CAN-SPAM (phishing, botnet, etc.) and other email that may not be malicious, but nevertheless does not conform to CAN-SPAM or industry best practices. Responsibilities and tactics for combating these different classes of spam need to be differentiated. It should be the strong focus of an ISP to protect consumers from the former, most dangerous form of spam. But responsibilities and tactics can shift when it comes to the second class of spam. This is where industry self-regulation and the voice of the consumer through the provision of appropriate tools can be most effectively applied.

As important as email security may be, the legitimate email sending industry needs to do its part to help strike an appropriate balance between security concerns and the legitimate uses of email for communication and commerce. Email is increasingly displacing postal mail as the channel consumers prefer to use for communication to and from the companies with which they do business. Therefore, it is vital to the preservation of the email ecosystem to amplify the concept of "consumer protection" as one that embraces both protecting consumers from email that is harmful and unwanted as well as protecting the receipt of email that is in fact desired and wanted. The marketplace and regulators need to be as sensitive to the viability of the email medium for communication and commerce as it has become about its security. Securing a medium by constraining communication and commerce would be a false victory.

[4] By "false positive" we refer not only to legitimate messages that are delivered to bulk/junk mail folders erroneously, but also to legitimate email blocked completely by an ISP and never delivered at all.

[5] *See* Sharon Gaudin, *False Positives, Spam's Casualty of War Costing Billions,* August 8, 2003, *available at* http://www.enterpriseitplanet.com/security/news/article.php/2246371.

From a legislative perspective, the botnet problem falls largely outside the purview of regulating legitimate senders, and thus is a matter apart from the framework of the CAN-SPAM Act. Clearly senders utilizing botnets have not and will not respond to compliance mandates of the sort suggested by the CAN-SPAM Act that help to govern the legitimate email industry. This reality also holds for fraudulent phishing type emailers.

A key characteristic of the spam problem has in fact shifted. Because past challenges were often characterized by huge bulk mail "blasts" from single IP addresses, one responsive tool had been to look at the volume of email being sent from a few IP addresses. Now, the botnet phenomenon demonstrates an opposite trend – broad distribution of a few messages across many IP addresses. With the growth of CAN-SPAM compliance in the legitimate marketing industry, one is more likely to see high volume emailers that send from dedicated IP networks to be legally compliant, whereas the fraudulent, malicious and deceptive mail is sent via highly distributed dynamic ISP-designated addresses. This realignment of threat to distributed networks is an important attribute of the post CAN-SPAM landscape. It also confirms that CAN-SPAM as a public policy tool is doing exactly what it could reasonably have been expected to achieve: It is driving better practices within the law-abiding email sending community. The inability to enforce CAN-SPAM against actors that will not respect any law, including the FTC Act, is not itself a basis for pressing new legislation. Nothing suggests that these bad actors will abide by any additional law. Investigation and inter-ISP coordination would be a far more promising focus of future efforts.

- **<u>Putting Consumers Back in Control</u>**

In our view, the focus on consumer "inbox experience" is critical, as opposed to focusing on raw email volumes generally. In short, public debate should center on which email should and should not be presented to consumers for further consideration.

In December 2006, the ESPC conducted a survey in conjunction with marketing research firm Ipsos to provide insight into the email behaviors of today's consumers. The ESPC surveyed a random sample of 2,252 Internet users from top U.S. ISPs (AOL, MSN/Hotmail, Yahoo!, Lycos, Excite, Gmail, Netscape, and Compuserve) in order to gauge consumers' behaviors and views toward spam, unsubscribe features and emerging anti-spam technologies. The results showed that the average American is extremely email-savvy, and most have very specific opinions on email and spam and how to manage both. 73 percent of respondents have used email for six or more years and over 80 percent check their email at least once per day.

Those surveyed also showed a familiarity and affinity for using "Report Spam" and "Unsubscribe" features, with over 80 percent of respondents using each of them to manage their inboxes. Additionally, the results indicate a clear desire by consumers for greater support from ISPs, email providers, and marketers so that they can more easily control their mail experience. Most would like to see tools like "Unsubscribe" and "Report Fraud" buttons (90 percent and 80 percent respectively) added to their email programs. 53 percent of respondents claimed they would be more likely to open and read email if the sending company was certified with an icon displayed in the email inbox.

Among the conclusions we draw from this research is that today's consumers are educated about email and, according to the results, very willing to use the functionality available to them to manage their email, and to provide specific feedback about their wants and needs for doing so. These email-savvy consumers have a strong voice and they want to make sure it gets heard when large ISPs are developing email programs and anti-spam technologies.

The Spam Summit will be an important opportunity to engage the reality that consumers are in many ways the forgotten constituent in the email world. Can industry and government be effective in engaging consumers by focusing on the development of consumer tools in the email clients themselves, or will pure paternalism instead emerge as the regulatory norm?

- **Technological Tools for Keeping it Out of the Inbox**

Many technological developments are responsive to the issues identified by our consumer research. In this vein, we feel that it is critical to focus on ISP engagement. We note the positive trend consistent with our own ESPC membership guidelines: 85% of the marketing domains used by Fortune 500 companies appear to be using authentication, as reported by Microsoft in its 2007 study conducted earlier this year. The next step for authentication practice will be for cross-ISP recognition of authentication as a key criterion of sender identity.

Another tool we recommend is broad based implementation of the "unsubscribe" button feature in web browsers, consistent with RFC 2369, which establishes a standard way for users to subscribe and unsubscribe from email lists within a web browser. Our research has suggested that senders would consider a "report fraud" button similarly helpful for inbox management. Such a tool might also help the FTC streamline certain of its investigatory and enforcement efforts, in collaboration with ISPs.

- **Stakeholder Best Practices**

Responsive to the evolving and differentiated threat to inbox management, we believe that the future for best practices in the email space is one that focuses on how *differentiation* should occur at the ISP level. We have identified the reorientation of the spam problem from what was once the single or selected IP address "blast" of volume spam to the highly distributed cross-IP address approach of the botnet phenomenon. We have identified authentication as a practice that can help ISPs differentiate a legitimate sender's characteristics from that of the virtual botnet sender. Where an ISP has established an abuse complaint feedback mechanism for consumers, for example via a 'spam' button in the web browser, a distinction may be observable as between the feedback given a legitimate IP address or domain versus the many complaints per million likely received by a spammer. These are but three types of differentiation already observable in the marketplace.

Further, various provisions of the CAN-SPAM Act itself point to other attributes that ISPs and law enforcement can use to differentiate legitimate senders and spammers. For example, §7704(a)(1) of the Act speaks to prohibitions on fraud in the use of headers, including IP addresses, domain names, routing information, from domains, subject lines, etc. Demonstrable differentiation exists with respect to each of these sub-elements. To cite but one example, a legitimate large-volume email sender generally has a stable number of designated IP addresses provided through a registry or an IP host, which will be used relatively consistently by that legitimate sender.[6] In contrast, a spammer will typically use compromised computers or foreign IP addresses, often sending *inconsistent* volumes of messages. The IP range and number of IP addresses used by such spammers tends to also be rather dynamic.

With respect to § 7704(a)(4) of the Act, clearly the requirement of unsubscribe automation is a basis for differentiation. Legitimate senders have an unsubscribe mechanism in their email that works in a statistically provable manner. Such senders typically automate their reply-to messages to make sure that recipient feedback is processed within the 10-day period required by the Act. A spammer, in contrast, neither offers nor honors unsubscribe messages. Attempts to reply to a message directly often will fail, because the spammer sent the message from a forged or fraudulent domain.

Further, the Act's §7704(b) focus on harvesting properly recognizes a basis for differentiation insofar as the FTC's study show that the majority of spam flows as a byproduct of harvesting. ISPs' use of spamtraps for anti-spam purposes can help easily distinguish among the types of senders that are mailing to them. Legitimate mailers will send very few messages per million to such a spamtrap, whereas a spammer will find the vast majority of sent email will find its way into such harvesting traps.

[6] This reinforces the importance of the Internet Corporation for Assigned Names and Numbers' (ICANN's) role in verifying legitimate domain registrations. Given that legitimate senders register accurate WHOIS records, it is important for ICANN to require authentication and transparency with domain name registrations to ensure that domain names are not fraudulently purchased and used for spamming.

Each of these aforementioned ways of differentiating legitimate email communications from fraudulent spam messages must contribute to the focus at the ISP on how filtering mechanisms can and should work. The role of the legitimate email sending community is to elaborate on the ever-expanding list of attributes that helps positive differentiation to occur. We note that none of the aforementioned mechanisms are keyed to the concepts of either notice or consent, but instead are objective characteristics that tend to help differentiate legal email from spam.

To the extent that the legitimate sending community can continue its work to demonstrate uniformity in positive and consistent sending characteristics—best practices—the ISP community should focus more closely on collaborating with anti-spam advocates to (a) close down access points to malware-downloading botnets through which consumer computers are accessed; (b) collaborate by sharing abuse feedback data across ISPs in a manner that speeds up identification of compromised consumer machines to shut down their access to email; (c) create systems that can track the point of spam inception and enable law enforcement to take swifter action; and (d) as stated earlier in our comments, enforce email authentication to help improve the ability to distinguish legitimate messages from true spam.

*   *   *   *

We thank you once again for this opportunity to share ideas that we believe should animate the FTC's upcoming Spam Summit. As always, we are at your disposal for further discussions, and would be most happy to speak with you about any of the aforementioned topics of primary concern to our broad membership.

Respectfully submitted,

TREVOR HUGHES

J. Trevor Hughes
Executive Director, ESPC
266 York Street
York, Maine 03909

Ph. 207-351-1500
Fax. 207-351-1501
thughes@espcoalition.org