From: Messaging Anti-Abuse Working Group (MAAWG)
Date: November 11, 2010
Subject: Comments on "Global Free Flow of Information on the Internet," RIN 0660-XA20, Docket Number 100921457-0457-01, Fed. Reg. Vol. 75, No. 188, Sept. 29th, 2010, pps. 60068 et. seq. http://www.ntia.doc.gov/InternetPolicyTaskForce/gffi/FR_gffinoi_09292010.pdf

Introduction

Thank you for the opportunity to submit comments on the Department of Commerce's ("DoC") request for comments relating to "Global Free Flow of Information on the Internet," (hereafter, "the DoC request").

The Messaging Anti-Abuse Working Group (MAAWG) is an international non-profit industry-led organization founded to fight online abuse such as phishing, botnets, fraud, spam, viruses and denial-of-service attacks. MAAWG draws technical experts, researchers and policy specialists from a broad base of Internet Service Providers and Network Operators representing over one billion mailboxes as well as from key technology providers, academia and volume sender organizations. The multi-disciplinary approach at MAAWG (www.MAAWG.org) includes education, advice on public policy and legislation, development of industry best practices, guidance in the development of industry standards, and the facilitation of global collaboration.

The DoC Request for Comments and Remarks on "Laws Prohibiting the Sending of Unsolicited Email"

On page 60070 of the DoC notice in the Federal Register, in section 1 ("Types of Restrictions on the Free Flow of Information on the Internet"), we noted the statement that:

> In the United States and numerous countries around the world, the Internet has flourished as an economic and social innovation motivated by the complementary goals of encouraging the free flow of goods and services and the commitment to freedom of expression. At the same time, governments may place restrictions on the types of information available over the Internet in their jurisdiction for a number of reasons, including protecting consumers or the property rights of users. *Numerous countries, for example, have laws prohibiting certain activities online, including […] the sending of unsolicited email.* [emphasis added]

That recitation, along with the DoC's request for input on:

> What role, if any, can the Department of Commerce play in helping to *reduce restrictions* on the free flow of information over the Internet? [emphasis added]

might lead some to believe that the DoC may be contemplating changes which could potentially result in a loosening of U.S. or global anti-spam restrictions.

As the Department ponders future cyber initiatives, **MAAWG hopes that it will carefully avoid any new cyber policies that might undercut existing or future global anti-spam regulatory regimes. MAAWG strongly supports efforts to limit messaging abuse in all its forms, including supporting appropriately drawn domestic and international regulations prohibiting the sending of unsolicited email.**

In the absence of suitable regulatory limitations, unwanted email has the potential to ultimately render email useless as a communication medium for personal communications, consensual commercial communications, and protected political and religious speech.

As such, we believe that well-crafted anti-spam measures are a prime example of a type of restriction that is readily accepted as legitimate by community consensus. We ask that you honor and support that community consensus when formulating future cyber policies.

Identifying Best Practices; Policy Enforcement

Section 2 of the DoC request ("Identifying Best Practices"), beginning on page 60071, asks

> Are there alternatives to government-mandated restrictions on the flow of information on the Internet that can realize legitimate policy objectives? Are there any best practices or baseline criteria for the development, articulation, and enforcement of policies restricting information flows that should be pursued by governments?

While appropriate national anti-spam legislation is the foundation for effective global anti-spam operations, national anti-spam policy is ultimately backstopped by block lists, filters and other technical anti-spam measures. Those technical approaches help ISPs to realize the legitimate policy objective of preventing illegal spamming, and provide technical enforcement of anti-spam policies when voluntary compliance with national anti-spam laws is imperfect.

In the area of best practices, MAAWG helps its members and the community as a whole think about preferred approaches for preventing messaging abuse through the ongoing publication of white papers and best current practices (BCPs). MAAWG BCPs are publicly available online at http://www.maawg.org/published-documents and we would urge you to review them as examples of how policies and technical measures can be successfully employed to address spamming and other messaging abuse, thereby protecting other online information flows.

With respect to your question "Are there any best practices or baseline criteria for […] enforcement of policies restricting information flows that should be pursued by governments?" we would note that policies without adequate funding and staffing for enforcement are ultimately doomed to failure. Unfunded mandates are a particular concern when federal authorities assert exclusive jurisdiction over a subject matter area, effectively saying, "I've got the ball," yet then proceeding to drop it rather than catch it. For example, FTC enforcement actions relating to messaging abuse under CAN-SPAM have been quite limited recently, presumably because hardworking FTC staffers simply have insufficient resources to bring additional enforcement actions, even though the FTC has exclusive authority in substantial aspects of the anti-spam enforcement area.

Procedural Due Process and Transparency

The DoC request also asked, "How should governments assure adequate levels of procedural due process and transparency to users, publishers and intermediaries when there is a determination that restricting the free flow of information is necessary?" We can find excellent examples and counter-examples in existing practice.

Consider the Office of Foreign Assets Control (see http://www.ustreas.gov/offices/enforcement/ofac/index.shtml). OFAC publishes its "Specially Designated Nationals" list in a variety of human and machine-readable formats. This public disclosure process is necessary for administration of the SDN program's objectives, but also ensures transparency and accountability, and procedures do exist for listed SDNs to apply to get unblocked. This is an excellent example of how a governmental restriction program can be run transparently and even-handedly, albeit in a financial rather than purely information-related context.

Contrast this with federal agency firewall management practices. The federal government relies on firewalls to block hacking/cracking attacks on its information technology infrastructure, but it does not publish information about what is being blocked at any given time, why that block was imposed, or how a blocked site might be able to appeal that determination or get itself de-listed. This has resulted in material problems, as was the case in 2004 when Department of Defense employees working abroad found themselves unable to access the Federal Voting Assistance Program (FVAP) website (see "Pentagon Restricts Overseas Access to Voter Registration Site," USA Today, 9/21/2004, http://www.usatoday.com/news/politicselections/2004-09-21-voterreg-block_x.htm)

The best model for transparency and procedural due process in a filtering or block listing-related context is probably The Spamhaus Project (http://www.spamhaus.org/). Spamhaus carefully documents each SBL listing on its website, and is well known for promptly processing delisting requests once issues gets resolved.

Are Local Restrictions Effective?

Part 2 at page 60071 also asked, "How effective are local restrictions given the global nature of the Internet and the possibility of individual users circumventing government regulations?"

Local restrictions (such as U.S. statutes) form the basis for criminal and civil enforcement activity. While not every violation will result in investigation, prosecution and conviction, at least some of the worst offenders will typically end up being sanctioned, including prison time or financial penalties or having assets seized.

Spammers attempt to evade law enforcement attention by operating transnationally. However law enforcement is increasingly well positioned to work collaboratively with their counterparts abroad via the Legat ("Legal Attaché") program and other initiatives, although much work remains to be done.

One example of an initiative that deserves broader participation is the Council of Europe's Convention on Cybercrime (see http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm). While forty-three nations have signed that treaty, including the U.S., obviously over a hundred other nations still have not done so. The COE Convention on Cybercrime is admittedly not perfect, but it is an important first step and an initiative that deserves promotion to other nations as part of our ongoing diplomatic efforts, thereby giving local restrictions global reach.

Third Party Intermediaries

The DoC request, in part 4 at page 60073, asked among other things: "Are there specific principles or factors that governments should take into account when dealing with content restrictions and the intermediaries who might be in a good position to monitor postings and remove illegal or objectionable content?"

All organizations worry about being sued while trying in good faith to do the right thing. For example, many American ISPs were historically worried about being sued over their spam filtering efforts. Fortunately, the CAN-SPAM Act provided safe harbor provisions for good faith blocking efforts, thereby empowering ISPs to protect their customers while avoiding any potential increase in liability.

Other critical participants in the messaging ecosystem remain at risk of potentially costly and time-consuming litigation. One of the most noteworthy examples of this was the 2006 lawsuit brought by e360Insight against the Spamhaus Project. (Ssee http://en.wikipedia.org/wiki/The_Spamhaus_Project#e360_Lawsuit.) Given the critical role that third party intermediaries such as Spamhaus play, we need to better shield them from potentially crippling litigation if we want to be able to continue to rely on the critical services they provide.

We must also recognize that there are some third party entities which *could* help the Internet better deal with abuse and illegality but have explicitly renounced such a role. ICANN, the Internet Corporation for Assigned Names and Numbers is one example of a potentially highly influential third party entity that has chosen to explicitly disclaim any role when it comes to dealing with messaging abuse. As stated at http://www.icann.org/en/faq/#spam:

> *Is ICANN the proper authority to report spam?*
>
> No. ICANN is a private, non-profit technical coordination body for the Internet's name and numbering systems. The content of an e-mail message, ftp file, or web page bear no inherent relation to the assigned domain name, and therefore fall outside of ICANN's policy-making scope. If you have a problem with the way somebody is using the Internet, you should take it up directly with that person or with the applicable Internet Service Provider or governmental agency depending on the circumstances. . . [continues]

Because ICANN, a third party federal contractor, washes its hands of any responsibility when it comes to messaging abuse, the spam problem faced by the Internet is far worse than it needs to be. Consideration should be given to including explicit language prohibiting ICANN from ignoring messaging abuse and other illegal Internet activity the next time its contract is next reviewed and renewed.

International Cooperation

Finally, in section 6 on page 60073, the DoC request delves into aspects of international cooperation, asking:

> Are there some multi-jurisdictional, governmental forums or multi-stakeholder, private-sector organizations that are better suited than others to develop proposals or principles to guide governments as they develop policies concerning the free flow of information on the Internet?

We believe MAAWG should be considered as a leading example of what can be accomplished in this respect.

MAAWG brings together leading ISPs who are united in the fight against spam, but MAAWG also includes responsible senders, vendors, anti-spam activists, academics, registrars, representatives from the DNS community, law enforcement entities, those who are involved with mobile device messaging, and many others.

We welcome participation from virtually any stakeholder group worldwide that is actively working to prevent messaging abuse. We operate both within the United States and abroad, with a third of MAAWG meetings routinely conducted in Europe, and we maintain ongoing discussions aimed at broadening our engagement with other regions of the world.

Conclusion

Our membership stands ready to help the Department of Commerce with specific proposals or general advice related to messaging abuse and global collaboration in fighting Cybercrime while preserving the usability of the Internet. If we can help in any way, please do not hesitate to get in touch.

Sincerely,
/s/
Jerry Upton, Executive Director
Messaging Anti-Abuse Working Group
Jerry.Upton@maawg.org