



---

**From:** Messaging Anti-Abuse Working Group (MAAWG)  
**Date:** December 3, 2010  
**Subject:** Comments on UK Department for Business Innovation & Skills Consultation on Implementing the Revised EU Electronic Communications Framework

Thank you for the opportunity to submit comments on the UK Department for Business Innovation & Skills consultation on implementing the Revised EU Electronic Communications Framework [http://www.bis.gov.uk/consultations/revised-eu-electronic-communications-framework]

The Messaging Anti-Abuse Working Group (MAAWG) is an international non-profit industry-led organization founded to fight all forms of 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](http://www.MAAWG.org)) includes education, advice on public policy and legislation, development of industry best practices, guidance in the development of industry standards, and facilitation of collaboration among stakeholders.

Recognizing that the Revised EU Electronic Communications Framework ("the Framework") touches on a broad range of issues, the comments from MAAWG on the implementation of the Framework are restricted to the Security and Integrity of Networks. In response to question 7 in the document entitled "Overall approach and consultation on specific issues" ("the Consultation Document"), we offer the following comments:

## **I. Prevention of messaging abuse**

MAAWG supports the EU initiative to improve the security and resiliency of electronic communications networks.

We believe the single most vital cybersecurity issue facing communication networks and users has been and continues to be messaging abuse, including spam and phishing. Spam and phishing are mainstays of the underground economy, facilitating and motivating much of the malicious behavior that takes place there. For example, spam is the customary "bearer service" for the delivery of phishing messages and consumers' PCs are routinely targeted by malware to create new "bots" (hidden automated email robots) that can be used to send spam.

As such, an important component of improving security on networks is for network providers to take appropriate steps to ensure that their networks are not used to send spam or to propagate botnets. Many service providers - either knowingly or unwittingly - become vehicles for messaging abuse that undermines the security of the Internet. Service providers must be able to detect and prevent spam, malware and other abuse from originating within their networks. Service providers must also be able to educate end-user customers on safe computing practices, help protect end-user devices from unauthorized access, and provide assistance to end-users whose devices become compromised through messaging abuse.

## **II. Information sharing**

Spammers and other criminals should not be able to hide behind privacy legislation. The detection, prevention and investigation of messaging abuse requires that service providers are able to quickly and effectively share information between service providers and with enforcement agencies. Therefore, it is essential that information sharing be encouraged and not inadvertently hampered by legislation and practices aimed at the protection of privacy.

---

**MAAWG**

Messaging Anti-Abuse Working Group

P.O. Box 29920 ■ San Francisco, CA 94129-0920 ■ [www.MAAWG.org](http://www.MAAWG.org) ■ [info@MAAWG.org](mailto:info@MAAWG.org)

Regulators and enforcement agencies must also continue to build on their relationships to share information and cooperate in the enforcement of legislation aimed at reducing messaging abuse. We note that the Canadian Parliament is currently considering anti-spam legislation (Bill C-28) that would provide the relevant enforcement agencies with significant powers to share information and cooperate with foreign enforcement agencies.

In conclusion, MAAWG would like to thank you for the opportunity to submit these comments for your consideration, and we would welcome the opportunity to provide further assistance to the UK Department for Business Innovation & Skills on its work in this important area. Please feel free to contact us if you have any questions, or if we can be of any further assistance.

Sincerely

/s/ Jerry Upton

Executive Director

[Jerry.Upton@maawg.org](mailto:Jerry.Upton@maawg.org)