



THE BUSINESS SOFTWARE ALLIANCE POSITION ON SPAM

The Business Software Alliance (“BSA”) is the foremost organization dedicated to promoting a safe and legal digital world. BSA is the voice of the world’s commercial software industry and its hardware partners before governments and in the international marketplace.

BSA believes that spam, i.e. unsolicited bulk emails and other unsolicited electronic messages with a primary commercial purpose, is a serious and growing threat to the efficiency and safety of the online experience at work and home. Spam does not, however, include transactional or relationship messages such as those sent to customers with respect to products or services (or such similar products or services) they have purchased from the sender.

The volume of spam is rising. Today’s spam does more than clog inboxes with unwanted email. Botnets – networks of hijacked personal computers that spammers use to conceal their identities – have become the preferred method for sending spam. Even more seriously, spam has become a major source of:

- Fraud – “phishing” where a computer user is lured to a website that is intended to trick the user into divulging personal information.
- Malware – opening an email or going to a website may infect a user’s computer with spyware or viruses (or hijack the personal computer for use in a botnet).
- Pirated and counterfeited software – software is offered at “bargain prices” too good to be true because in fact it is not; users who order from these sites do not receive legitimate software, and may also be divulging sensitive payment information to unknown entities.

BSA’s members have been at the forefront of efforts to combat spam through technological means such as spam filters, have collaborated with the national and state governments on lawsuits against spamming operations across the globe, and have continually been educating consumers about the dangers of spam and how they can protect themselves.

At the same time, BSA believes that governments should not impose technology mandates that require the use of particular software or hardware to try to stop spam, because such laws and regulations will impede innovation and result in less protection.

While legislation enables enforcement authorities to have the right tools, legislation in itself is not sufficient to address the problem. It is important to ensure that there is adequate and appropriate enforcement of the laws with sufficient funding and resources, as well as cooperation between the public and private sector. International cooperation is a key component of an effective anti-spam policy as the Internet is borderless and spammers operate across national laws and boundaries.

To the extent that countries are considering enacting spam legislation, BSA believes it should include characteristics such as the following:

- Require that header information (an electronic message's source, destination and routing information) must be accurate, complete and identify the person who initiated the message.
- Prohibit deceptive subject lines (cannot mislead the recipient about the contents or subject matter of the message).
- Prohibit "spoofing" or misuse of a third party's domain name (e.g. in source, destination, reply address fields, etc.).
- Require that the electronic message give recipients a method to choose not to receive future messages by including a functional unsubscribe capability (i.e. "opt-out") and permit this to be done for some but not all of a company's electronic messages (e.g. by product line).
- Provide for government enforcement, as well as permitting Internet Service Providers (ISPs) and other online service providers to sue for violations of the spam laws, rather than creating a general private right of action to sue for damages.
- Prohibit dictionary attacks and the use of scripts or other automated means for address harvesting to collect a large number of email accounts to target with spam.

Countries should impose tough sanctions for violations of these requirements. These include civil liability for the recovery of damages, including statutory damages, as well as injunctions. For the intentional and truly egregious cases, criminal penalties should be provided.

Countries should also facilitate commercial and legal enforcement actions by ISPs and other online services by:

- Developing appropriate guidelines and best practices for ISPs to ensure an adequate level of security and privacy of the networks and users in a competitive market.
- Ensuring that they are not liable for good faith efforts to block spam (while not requiring them to attempt to do so).
- Enabling them to obtain pre-action discovery orders identifying customers of ISPs who are involved in spamming.
- Establishing appropriate volume requirements for unsolicited messages that need to be exceeded before enforcement actions are taken.
- Preserving the usual balance of the burden of proof on the parties in enforcement actions.