Policy Statement

ICC policy statement on 'spam'[1] and unsolicited commercial electronic messages

Prepared by the Commission on E-Business, IT and Telecoms

Introduction

Businesses and consumers around the world have come to rely on the speed and convenience of e-mail and other types of electronic communications. In the space of a few short years e-mail has become an essential tool to do business, get information, and keep in touch. There has been much controversy about the problem of "spam" and how it may be curtailed. As different legal rules apply to electronic communications in different jurisdictions, there is no generally accepted definition of the term 'spam.' Consequently, our purpose in this paper is to identify illegitimate or unacceptable electronic communications, a topic on which we believe there is general agreement.

> By 'spam', ICC means harmful, fraudulent, malicious, misleading or illegal communications, generally sent in bulk. This is the definition of 'spam' as used in this paper.
>
> By 'spammers', we mean entities sending 'spam' as defined above.
>
> The section below focuses on describing unacceptable electronic messages and differentiating them from acceptable electronic commercial marketing messages that follow accepted codes of industry practice.

Distinguishing between what ICC and its members all agree should be categorized as 'spam' and legitimate commercial electronic communications brings two clear benefits:

- It recognizes the legitimate needs and benefits of commercial electronic communications, and
- It allows governments and others to focus on the real problem of harmful, fraudulent, malicious, misleading or illegal communications.

[1] The term 'spam' is used in this document because it is currently the commonly used term

38, Cours Albert 1er, 75008 Paris, France
Telephone +33 1 49 53 28 28 Fax +33 1 49 53 28 59
Web site www.iccwbo.org E-mail icc@iccwbo.org

1. Responsible and legitimate marketing practices are the basis of self-regulation

ICC supports a coherent self-regulatory framework in which all parties in marketing and advertising share their proportionate responsibility for marketing messages sent using electronic media. This means that companies should follow industry codes that set standards of ethical conduct, such as the ICC Guidelines on Marketing and Advertising Using Electronic Media, revised and updated in 2004.

Responsible and legitimate marketers who follow the ICC relevant[2] guidelines will take measures including the following:

- When collecting personal data, follow the provisions in the ICC International Code on Direct Marketing[3] on informing the data subject, collection, use and transfer of data, security of data and provision and use of privacy policy statements. In jurisdictions where no privacy legislation currently exists, companies should consider observing the privacy principles outlined in the ICC Privacy Toolkit.[4]

- Target messages so that their recipients are likely to have an interest in the subject matter or offer.

- Do not use misleading subject headers in commercial emails.

- Disclose the identity and contact details of the sender, allowing recipients to opt out of future marketing messages.

Companies that follow these guidelines are clearly different from entities sending spam. To focus government efforts where they are most needed and to ensure the communications networks continue to be a viable means of commercial communication for legitimate businesses, it is essential for public policy to recognize this difference. We strongly encourage governments to focus their efforts on measures that will target without penalizing legitimate marketers.

2. Legitimate marketing-focused electronic communications are not 'spam'

The fact that an electronic communication has a commercial nature in and of itself does not make that communication 'spam'. Spam - harmful, fraudulent, malicious, misleading or illegal communications, generally sent in bulk – often has the following characteristics:

- It may include false header information or an opt-out mechanism that does not work or is not honoured; i.e. it may be fraudulent and misleading.

- It may be used to advertise products and services with misleading claims, or sell products such as prescription drugs illegally; i.e. it may be misleading, illegitimate and potentially harmful.

- Spammers may acquire individuals' contact details in unethical, illegal, or misleading ways;

[2] The ICC International Code on Direct Marketing includes provisions on the collection of personal data.
[3] Available online at http://www.iccwbo.org/home/statements_rules/rules/2001/code_of_direct_marketing.asp
[4] Available online at http://www.iccwbo.org/home/e_business/word_documents/TOOLKIT-rev.pdf

i.e. it may be illegitimate/illegal.

- As described below, spam may be the vehicle for viruses or fraudulent schemes; i.e. it may be malicious and illegal.

Put simply, the entities that send spam differ from legitimate marketers because spammers do not respect applicable laws and regulations and do not honour users' preferences regarding commercial communications. This is the essence of spam.

3. Not all 'spam' messages have a commercial intent.

An increasing proportion of spam messages – particularly emails – have no marketing or solicitation purpose at all, and are sent primarily to spread computer viruses (e.g. the ILOVEYOU virus) or as a means to fraudulently acquire personal information. The latter type of message, known as 'phishing', may purport to be from a legitimate business or bank, and ask for individuals' credit card numbers, bank account details or other personal information. These messages may even include links to bogus or 'spoofed' websites that lure users into providing their personal information. Once acquired, the personal information can be used to commit identity theft and de-fraud individuals and organizations. This is becoming a serious information security issue giving a new aspect to the problem of spam.

In their frustration over harmful or fraudulent electronic messages, some countries have banned all unsolicited commercial communications. However, these measures have not shown any appreciable decrease in the volume of spam because senders of spam operate outside the law, respecting neither 'opt-in' nor 'opt-out' rules. Not only has the real problem worsened, but marketing by email has been made much more cumbersome and costly to legitimate businesses. 'Opt in' measures have lessened the ability of legitimate businesses, particularly small and medium businesses, to maintain and expand their customer bases using the responsible, targeted use of innovative marketing techniques made possible by the Internet.

The toolkit approach to fighting spam

Spam – harmful, fraudulent, misleading or illegal messages generally sent in bulk, and not simply "unsolicited" or unauthorized electronic messages - is a serious, international, cross-sectoral problem that must urgently be tackled by the coordinated efforts of all interested parties in the information society. It harms consumers and business, as both are users of information and communication technologies. Dialogue and exchange of expertise between the public and private sectors are vital to successfully address this challenge, and to ensure that the networked economy continues to benefit users worldwide.

The private sector brings unique and valuable insights to this dialogue. As business owns and manages many of the networks and systems that are most burdened with spam, the business community has significant and up to date expertise in fighting spam. Most importantly, business plays a fundamental role in developing the innovative technological solutions that address spam. We look forward to continued and constructive dialogue, at all levels and with all affected stakeholders, to foster workable and effective solutions to spam.

Business endorses a multi-faceted approach to fighting spam:

- Education and cooperation: Business and government must work together in public-private partnership to educate users and businesses in the fight against spam.
- Technology: Industry should continue to develop technological solutions to spam, working with governments and consumers to promote awareness of technological approaches.
- Industry's role in fighting spam: Business can best manage legitimate unsolicited commercial e-mail with industry codes of conduct and other self-regulatory tools.
- Government enforcement: Governments should ensure that relevant existing legislation covers harmful, fraudulent, misleading or illegal messages and is effectively enforced.

A coordinated effort in each of these areas is the best way to effectively deal with, while ensuring that businesses and consumers can enjoy the convenience and ease of electronic communications.

1. Education and co-operation: Business and government must work together in public-private partnership to educate users and businesses in the fight against spam.

Effective awareness and education is the primary tool in combating spam as it provides users with important tools they need to manage their e-mail and personal information. As users learn to reduce and deal effectively with spam, it will become a less attractive activity for spammers. Users need to be discerning when releasing their e-mail addresses and how to use software and other tools to deal with spam addressed to them.

Awareness and education are the joint responsibility of all stakeholders. Industry continues to inform users about how to protect the privacy of their information when registering with a website or purchasing a product. Industry also exchanges information on best practices for effective spam-handling procedures, and develops tools that empower users to choose which e-mail they will receive. As industry is at the cutting edge of dealing with spammers' latest techniques, it is best positioned to understand the problem and to introduce solutions. Industry will work with relevant stakeholders to promote awareness among users and to disseminate new and more effective methods to avoid or reduce spam.

- Governments should support and complement industry efforts to educate users (including SMEs) on avoiding and reducing spam, and managing their personal information online.
- Governments should work with industry to increase awareness and use of workable solutions and mechanisms to report and deal with e-mail, instant messaging or SMS abuse. Governments and business should input reporting and opt-out web addresses to the ICC

Global Online Resource on Spam,[5] an online resource for users to report spam and make privacy complaints, with links to reporting and opt-out resources in over thirty countries around the world.

- Business should continue and expand efforts to make more businesses aware of acceptable marketing practices by educating them about encouraging them to become compliant with self-regulatory codes.

2. Technology: Industry should continue to develop technological solutions to spam, working with governments and consumers to promote awareness of technological approaches.

Business will continue to develop and improve filtering and other technologies that reduce spam. As spammers can change their tactics as quickly as industry develops new defensive techniques, technological responses to spam must continuously and rapidly adapt. Business is constantly improving the ability of these technologies to distinguish between spam and other communications, and developing products that are easier to use.

Business recognizes the significant challenge to information security presented by spam and has responded with innovations such as enterprise level network monitoring, traffic analysis and virus checking in order to protect information systems and networks. A new approach to spam is the use of "smart" systems that not only can adjust automatically to spammers' changing tactics, but can be customized to suit the preferences of individual users.

Governments should avoid mandating specific anti-spam technologies, and focus on creating and sustaining a climate in which business continues to innovate, develop and improve technological solutions to the ever-changing problem of spam.

- Governments should ensure that anti-spam measures are technology-neutral and, where relevant, based on standards agreed to by business. Governments should not mandate specific technological anti-spam measures, or try to force companies to adopt measures that cannot be supported in the marketplace.

- Governments should continue to allow Internet service providers (ISPs) and other companies to block spam on their respective networks and systems, keeping in mind the benefits of legitimate commercial e-mail.

[5] http://www.iccwbo.org/home/menu_electronic_business.asp

3. Industry's role: Business can best manage legitimate unsolicited commercial e-mail with industry codes of conduct and other self- regulatory tools

Businesses want to ensure the trust of their customers by sending them targeted and potentially interesting messages intended to begin or enhance a customer relationship. It is also in business' interest to maintain the usefulness of the Internet and associated communication technologies as a medium for responsible and acceptable commercial messages. Business can help free government resources to address spam by developing oversight and compliance mechanisms to manage legitimate unsolicited commercial e-mail using industry codes of conduct and other tools.

Industry codes, guidelines, and private sector best practice initiatives, such as the ICC Guidelines on Marketing and Advertising Using Electronic Media [6], the FEDMA European Code of Practice for the Use of Personal Data in Directing Marketing,[7] Antispam – A Guideline from The Confederation of Danish Industries and ITEK[8], the GBDe voluntary practices in its Recommendation on Unsolicited Electronic Communications[9], and Truste.org[10] are an effective way to spread best practices.

- Governments should respect and encourage industry codes of conduct and best practices that establish guidelines for the responsible business use of unsolicited commercial e-mails.

- Business should continue to use codes and best practices to educate more companies about acceptable direct marketing practices.

4. Government enforcement: Governments should ensure that relevant existing legislation covers all electronic messages and is effectively enforced

Business urges governments to adopt balanced legislative approaches as part of a toolkit of possible ways to combat spam. Governments should review existing laws and regulations to see if they sufficiently address spam.

New legislation or amendments, where needed, should focus on preventing illegitimate, fraudulent, or harmful messages. Measures should be drafted with care to reduce the volume of while preserving legitimate business use of the Internet as a communications and marketing medium. Laws should distinguish between harmful, fraudulent, misleading or illegitimate electronic communications sent by unknown parties from communications sent by responsible companies to individuals to create or sustain a customer relationship.

- Relevant legislation (for example, laws and regulations on fraud, consumer protection, unfair competition) should include definitions that prohibit activities such as the use of false or

[6] http://www.iccwbo.org/home/statements_rules/rules/1998/internet_guidelines.asp.
The ICC Guidelines are currently under revision to be finalized in June 2004.
[7] http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp77-annex_en.pdf
[8] http://billed.di.dk/wimpfiles/lores/image.asp?objno=/298860.pdf
[9] http://www.gbde.org/spam03.pdf
[10] http://www.truste.org

misleading header information, false or misleading subject lines, fraudulent or claims or offers, the misuse of third-party domain names and IP addresses, and harvesting e-mail addresses through dictionary attacks or anonymous/automated collection procedures.

- The laws and policies on spam of the country from which a company is sending bulk commercial email should apply. Alternatively, but less preferably, the application and enforcement of laws or policies on spam should exclude bulk commercial email that is not primarily intended for recipients in that country. They should also not be enforced against a communication on the basis of a portion (e.g. a packet or series of packets) of that communication being *routed through* but not *destined for* a recipient in that country.

Effective enforcement by governments is essential. Private enforcement measures and private rights of action through the judicial system are also an important part of the fight against spam and should be upheld in law. Some countries have introduced rapid injunction procedures for both private and public enforcement actions.

- Governments should respect customer privacy and choice while allowing legitimate companies, including SMEs, to market their products and services.

- Governments should ensure they are able in law to impose effective fines or other penalties on spammers.

- Governments should focus on fraud and allocate sufficient resources to effectively enforce existing fraud laws with regard to electronic communications.

- Governments should have effective procedures for dealing with cross-border complaints.

- Governments should take every precaution to avoid subjecting companies to diverging, competing and possibly conflicting, legal obligations;

A template for effective and appropriate Law enforcement cooperation:

Effective and appropriate law enforcement cooperation should be pursued actively by governments instead of unnecessary cross-border application of laws. The Council of Europe Convention on Cybercrime and the OECD Guidelines provide models for pursuing such cooperation. A template for effective and appropriate law enforcement cooperation should ensure that:

1. A request for cooperation from one law enforcement agency to a law enforcement agency in another country should only be honoured if the alleged conduct is a violation of the laws of both the requesting and requested countries, i.e. dual criminality; and

2. A company should only be required to respond to and comply with requests from a law enforcement agency of the country where it is established and where the evidence is located. [11]

Business Actions

These action points were developed by ICC in conjunction with BIAC (Business and Industry Advisory Committee to the OECD) to complement the actions already proposed for governments.

- Business will work cooperatively with governments to increase awareness and use of workable opt-out solutions and mechanisms to report and deal with e-mail, instant messaging or SMS abuse.

- Business will continue to raise user awareness of how to reduce and deal with spam at the individual and enterprise level, particularly through initiatives such as the ICC Global Online Resource on Spam.

- Business will continue to develop technological solutions to spam.

- Business will use private enforcement actions against spammers where those actions are appropriate and likely to be effective.

- Business will continue to advocate effective and workable approaches to spam. To this end, we draw attention to the statements and marketing codes of the following business organizations International Chamber of Commerce (ICC), Federation of European Direct Marketing Association (FEDMA), Global Business Dialogue on Electronic Commerce (GBDe), and the Direct Marketing Association (DMA) and Antispam – A Guideline from The Confederation of Danish Industries and ITEK (spell it out).

- Business will continue to co-operate amongst industry associations to share and advocate policy and best practices globally.

- Business will continue to support and participate in international multi-stakeholder dialogue to develop practical approaches to combat spam.

Business looks forward to continued dialogue and coordinated action with governments to fight spam. This will reinforce the privacy and security of all users and ensure that the Internet remains a viable and attractive place to do business.

Document N° 373-22/114
2 December 2004 MvdL/MF/dfc

[11] For example, provisions on mutual assistance in the Council of Europe Convention on Cybercrime do not require companies to respond to a request made directly by an enforcement agency from a foreign country. Rather, the foreign law enforcement agency should seek the assistance of the law enforcement agency in the country of the company. The national agency could then seek the cooperation of the company in accordance with applicable process and procedural controls.