



United States Council for International Business

1212 Avenue of the Americas, New York, NY 10036-1689
tel: 212-354-4480 – fax: 212-575-0327
e-mail: info@uscib.org – Internet: www.uscib.org

Serving American Business as U.S. Affiliate of:

International Chamber of Commerce (ICC)
International Organisation of Employers (IOE)
Business and Industry Advisory Committee (BIAC) to the OECD
ATA Carnet System

USCIB COMMENT ON THE CAN-SPAM RULEMAKING

(April 16, 2004)

Introduction:

The United States Council for International Business welcomes the opportunity to submit comments to the Federal Trade Commission (FTC) on the CAN-SPAM Act Rulemaking, Project No. R411008. Our comments will focus on the international aspects of the rulemaking, namely analysis and recommendations concerning how to address commercial email that originates in or is transmitted through or to facilities or computers in other nations.

At the outset, we would like to highlight the importance our members place on USCIB's continued work program through our international affiliates to combat spam through cooperation with law enforcement and the promotion of technology and other self-regulatory solutions. Our members are committed to working to preserve the Internet as a viable means of legitimate commercial communication. Effective and appropriate law enforcement cooperation to combat fraudulent commercial communications will be an essential component in this endeavor. We look forward to continuing to work with governments and law enforcement to achieve our shared objective.

Our member companies take every measure to comply with U.S. law, including the CAN-SPAM Act (hereinafter referred to as the Act). It is critical to note that when countries attempt to apply their laws to companies in other countries, or to regulate activities of companies that relate solely to their activities abroad, companies may be subjected to different, competing and possibly conflicting legal obligations, making compliance extremely difficult, if not impossible. It is our belief that international initiatives of governments should focus on tackling those who send fraudulent commercial emails, not law-abiding companies. Such a focus will go a long way towards combating spam.

Accordingly, we urge the U.S. Government and all governments to develop a template for law enforcement cooperation and to take every precaution to prevent:

1. the imposition of different, competing or conflicting legal obligations; and
2. the scope of domestic laws and policies from including bulk commercial email that is not intended primarily for recipients in that country;

More detailed recommendations are set forth below.

Scope of CAN-SPAM:

The scope of the Act defines a "protected computer" by cross-referencing the Fraud and Related Activity in Connection with Computers Act, 18 U.S.C 1037(e)(2). The definition includes two prongs with the relevant prong for the purposes of this comment being:

"[a computer] which is used in interstate or foreign commerce or communications, including a computer located outside of the United States that is used in a manner that affects interstate or foreign commerce or communications of the United States."

Our members have identified two important concerns with the scope and international aspect of the Act. First is the potential unintended consequences of the cross-border effect of the Act and the potential implications it may have for businesses and consumers. Second is that the international application of the law does not comport with the technological realities of the Internet and packet-switching. We address each of these concerns in more detail below.

Cross-border Effect:

Laws around the world related to Spam vary as to their substantive provisions, including the definitions and mechanisms concerning customer consent. A good example is the comparison of the Act and the E.U. Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (hereinafter referred to as “the Directive”).

In summary, the Act has two primary objectives:

1. to make unlawful the transmission of commercial emails that:
 - are unauthorized and intentional – 1037(a)(1),
 - deceive and mislead as to the origins of the message – 1037(a)(2);
 - falsify header information 1037(a)(3); or
 - falsify the identify of the sender through the false registration of multiple email accounts or domain names or false representation of an actual registrant – 1037(a)(4) & (5).
2. to require the senders of commercial electronic mail to include an opt-out mechanism in such mail and to prohibit future communications after an opt-out request becomes effective.

In summary, the Directive has one objective:

to prohibit the sending of all commercial emails where there has not been explicit prior (opt-in) consent except where there is an existing commercial relationship with a customer and communications include a mechanism to opt-out.

This comparison illustrates how the possible cross-border application of the Act can create significant confusion and uncertainty for business as to the prevailing substantive law applicable in a given situation. In addition, where the substantive provisions of the laws of different countries vary (as is true in the case of the Act and the Directive) without clarity as to which law is applicable in a given situation, the uncertainty, difficulty, and risk associated with operating in a global market-place, which the Internet epitomizes, are magnified greatly. Indeed, they can make global operations via the Internet impracticable.

To provide the necessary certainty for business, the U.S. government should analyze, through consultation with the private sector, which country’s laws should prevail when a company sends unsolicited commercial email. USCIB asserts that the application of the laws of the country of the company sending the email provides the maximum certainty for business. A second, though less workable and therefore less preferable option, is to ensure that a country’s laws are not applied if bulk email is not intended primarily for recipients in that country (as determined by the totality of the circumstances). This would minimize the possibility of a company- that is in good faith complying with the law- being penalized simply because a small portion of the bulk emails are sent to a particular country. This is also important given that a sender of email, in many instances, may not know the actual geographic destination of an email and could therefore unknowingly subject itself to the laws of another country. Whichever test is chosen, a company should be subjected to the laws of only one country. To do otherwise would:

- divert governmental resources from the real source of the problem, fraudsters; and
- diminish significantly the use of email commercial communication by companies, which would likely result in increased prices and reduced product offerings and ultimately customer satisfaction.

We believe that it is critical for the FTC to address these concerns as it continues its review of the international application of the Act. In doing so, we hope that the United States will serve as a model for other countries. This is particularly important in light of the fact that these concerns apply to the foreign subsidiaries of U.S. parented companies.

Rather than pursuing cross-border application of the Act, we encourage the U.S. Government to engage in active cooperation with law enforcement agencies to actually combat the problem -- the commercial communications of fraudsters, not entities trying in good faith to comply with the law. Such cooperation has already been enshrined in the Council of Europe Convention on Cybercrime (hereinafter referred to as "the Convention") and the OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders (hereinafter referred to as the Guidelines).

Technological Realities:

Unlike voice analog telephony, emails are not transmitted over a dedicated line. Rather, they are transmitted through packet-switching based on the Internet Protocol, a system that dissects any given communication into many packets that travel across the Internet's network of networks through different paths, recreating the message at the end of the transmission at the recipient's computer. It is almost inevitable that a packet from an email message sent from someone in Argentina to someone in Canada or France will, given the architecture of the Internet, be "transmitted through" many countries including the United States, in most cases, without the knowledge of the sender.

Our members are concerned that a broad reading of the Act could encompass e-mail messages "transmitted through" the U.S. and therefore likely encompass a large percentage of their *international* communications. Such a broad reading would inappropriately cover e-mail messages that are routed through but not destined for the U.S. and, more importantly, could create a precedent for other countries to claim similar jurisdiction. This further complicates the uncertainties noted above, possibly subjecting a company to the laws of every country through which a single packet of one of its communications is routed. This again decreases the incentive to use e-mail as a medium of communication. It also has direct implications for our member companies given their global presence.

USCIB Recommendations:

As the FTC contemplates the international implications of the Act, USCIB respectfully submits below criteria upon which any international strategy should be based. Given the concerns noted above, USCIB and the International Chamber of Commerce (ICC) have long advocated the application of the country-of-origin principle in the context of consumer protection measures and business-to-consumer transactions in the context of e-commerce. In the context of business-to-business transactions, USCIB and ICC support freedom of contract, otherwise known as party autonomy. The country-of-origin principle and party autonomy provide certainty for business, minimizing the application of different, competing, and possibly conflicting laws.

Nevertheless, we have tailored our recommendations based on the current text of the Act. Our recommendations follow:

1. domestic laws or policies related to spam should not seek to enforce against a communication on the basis of a portion (e.g. a packet or series of packets) from that communication that is *routed through*, but not *destined for* a recipient in, that country;
2. the laws and policies related to spam of the country from which a company is sending bulk commercial email should apply; alternatively, but less preferable, the application and enforcement of domestic laws or policies related to spam should not include bulk commercial email that is not intended primarily for recipients in that country, as determined by the totality of the circumstances;

3. governments should take every precaution to resist subjecting companies to different, competing and possibly conflicting, legal obligations;
4. governments should ensure that all countries have laws that make fraudulent commercial communication illegal, ensuring that such laws are narrowly tailored so as not to inadvertently encompass legitimate commercial communications; and
5. the U.S. Government's international strategy to combat spam should focus on promoting effective and appropriate law enforcement cooperation to combat fraudulent and deceptive commercial email.

A Template for Effective and Appropriate Law Enforcement Cooperation:

Effective and appropriate law enforcement cooperation should be pursued actively by the U.S. and other governments instead of unnecessary cross-border application of laws. As noted above, the Council of Europe Convention on Cybercrime and the OECD Guidelines provide models for pursuing such cooperation. USCIB offers the following views on a template for effective and appropriate law enforcement cooperation:

1. A request for cooperation from one law enforcement agency to a law enforcement agency in another country should only be honored 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. For example, provisions related to mutual assistance among law enforcement should not compel a U.S.-based company to respond to a request made directly by a non-U.S. law enforcement agency; rather, the non-U.S. law enforcement agency should seek the assistance of the appropriate U.S. law enforcement agency which would then, if appropriate, seek the cooperation of the U.S.-based company in accordance with applicable process and procedural controls.

Moreover, USCIB believes it is essential for the U.S. Government and all governments negotiating law enforcement cooperation mechanisms to consult actively and regularly with their respective private sectors. As noted above, business is a partner in the fight against spam and looks forward to working with law enforcement in this regard. However, business' ability to cooperate is constrained by business and technological realities. Therefore consultation in the development of cooperation mechanisms is essential.

Finally, it will be important for business to work with law enforcement agencies in countries that are not equipped currently to address fraudulent commercial communications, whether as a result of their legal framework or technical capacity.

Conclusion:

USCIB greatly appreciates the opportunity to share our views with you on the international application of the CAN-SPAM Act. We hope that these comments are helpful. Please do not hesitate to contact us if you would like to discuss these comments further.