

## Understanding the "CAN-SPAM" Act

### Summary

The CAN-SPAM Act takes effect on January 1, 2004. Although the Act is quite detailed, in general the Act has the following immediate effects:

- Prohibits falsification of identity in commercial e-mails.
- Requires an opt-out choice in all commercial e-mails.
- Opt-out choices must be honored in 10 business days.
- Commercial e-mail must disclose that it is a solicitation.
- Sexually oriented material must be clearly marked as such.
- Commercial e-mail must contain a postal address.
- Pre-empts most state laws that expressly regulate commercial e-mail.
- Prohibits harvesting e-mail addresses from certain web-sites.
- Prohibits "dictionary attack" methods of creating e-mail addresses.
- Prohibits hijacking IP blocks.
- Is enforced by the Department of Justice and Federal Trade Commission.
- Creates a private right of action for "Internet Access Services" for certain violations of the Act.

The Act applies to:

- the originators of e-mails sent in violation of the Act;
- those whose products are promoted in the e-mails; *and*
- those who knowingly provide services to violators of the Act.

The Act carries civil penalties of up to \$2 million. Internet Service Providers may sue in federal district court for up to \$3 million. Criminal penalties include forfeiture of property and up to 5 years in jail.

### Analysis

The CAN-SPAM Act reflects Congress' increasing concern about two issues related to SPAM. First, in hearings about the Act, industry representatives presented evidence that in 2001 SPAM represented 8% of all email traffic. By 2003, SPAM represented 50% of all e-mail traffic. Congressional investigators determined that two-thirds of all SPAM had some fraud associated with it – from falsification of header information to scams designed to steal financial information. Fully 20% of SPAM contained some sort of sexually oriented material.

Second, almost thirty states had passed some type of law regulating SPAM. The most sweeping of these, in California, was set to take effect January 1<sup>st</sup>. Congress determined that difficulty complying with each state's laws would interfere with interstate commerce, since businesses would be forced to develop compliance strategies for thirty different laws, even if they were not engaged in e-mail marketing.

As a result, Congress took the unusual step of conferring on the Act prior to its introduction in either the House or Senate. Aside from some minor technical clarifications, the Act received an expedited review. The express goal of this quick review was to ensure that the Act pre-empted the California state SPAM statute.

### What is SPAM?

The Act covers any e-mail message "the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)." The Act specifically exempts transactional and/or relationship messages. These messages are e-mails with individuals with whom you have a business relationship, and with whom you need to communicate about that relationship. For example, a travel site sending an e-mail regarding a late flight would

be a transactional e-mail. However, it is unlikely that a travel site sending an e-mail about a promotional matter would be transactional even if the recipient had previously purchased a ticket.

#### Definitional Issues

For most companies not actually engaged in e-mail solicitations commonly thought of as SPAM, the most frustrating aspect of the Act is the lack of clarity used to define key words and phrases used in the Act. These words and phrases are sure to be the subject of litigation. Consequently, a prudent strategy will be for companies whose businesses do not depend on e-mail to take a narrow view of all defined words. Examples are:

- “clear and conspicuous”
- “primary purpose”
- “Internet Access Service”
- “routine conveyance”
- “knowledge fairly implied on the basis of objective circumstances,” “actual knowledge,” “knows or should have known”
- “materially false/misleading”
- “sexually oriented material”

Further adding to possible litigation risks, some of these definitions, such as “Internet Access Service” and “sexually oriented material” are defined by reference to other statutes. Interpretations given to these terms in unrelated statutes may have limited relevance to a SPAM statute. For example, the term “Internet Access Provider” is defined by reference to the section of the Communications Act of 1934 that regulates distribution of sexually oriented materials to minors. This particular definition may exclude web hosting providers, since it relies on the distinction between access to content, and providing, or facilitating provision of, that content.

The Act makes significant use of the terms “actual knowledge” or “knowledge fairly implied on the basis of objective circumstances.” It seems likely that these terms will initially be

used to target SPAM-haus’ (companies whose business is to engage in unsolicited e-mail campaigns). However, as third party service providers become aware of the use of their facilities to transmit commercial e-mail in violation of the Act, absent further definitional clarity, this awareness may rise to at least the “knowledge fairly implied...” standard.

#### Transmission of e-mail and opt out provisions

Section 5 of the Act prohibits the use of false or misleading transmission information, requires accurate subject headings and a return e-mail address. This section specifically applies to header information, from line and subject lines. Generally speaking, this section prohibits acts that would cause the information in any of those to contain “materially misleading” information.

Each e-mail must also contain a functioning return email address and instructions that will allow a recipient to opt out of future e-mail communications. The e-mail address must function for at least thirty days following transmission of the e-mail. In addition, each e-mail must contain a physical address to which postal mail may be sent.

The opt out provisions, while relatively simple for e-mail marketers to administer, may create liability for third parties who provide services to them. Third parties may violate the Act if they are acting on behalf of an e-mail marketer and fail to honor an opt-out request - or – if they had, or should have had, knowledge that an e-mail they received was in fact an opt-out request and do not take action on that request. Third party service providers who regularly receive emails from recipients of e-mail from their customers requesting to be removed from a customer’s mailing list should develop processes to track and address these requests.

#### Address Harvesting and Dictionary Attacks

SPAMMERS often harvest e-mail addresses by spidering websites for contact information. Section 5 of the Act allows website owners to post a notice that they do not “give, sell,

or...transfer” the e-mail addresses set out on the site. As a result, these addresses may not be used to transmit commercial e-mail.

The Act also prohibits dictionary attacks (use of computer programs to generate addresses) or the use of other automated methods to send SPAM, create multiple mail boxes, or relay mail through service providers without their consent.

#### Labeling

The Act requires that commercial email state that it contains advertising. There is no requirement to use particular language – such as “ADV” – however, any notice must be “clear and conspicuous.”

Commercial e-mail of a sexual nature, must be particularly labeled. The definition of “sexually oriented material” uses definitions contained in the statute regulating Child Pornography. This statute, while providing clear guidance, contains very broad definitions. As a result, the labeling provision may cover a large category of email. The Act attempts to accommodate free speech concerns by exempting e-mails containing a small and insignificant amount of sexually oriented material. The term “small and insignificant” is not defined, creating a potential issue for certain e-mail marketers.

#### Using SPAM to promote your business

Section 6 of the Act regulates the use of commercial e-mail to promote your business. It also governs the use of third parties to do so on your behalf. This section provides for third party liability if you knew or should have known that your business was promoted in violation of the Act. You will have violated the Act if you “received or expected to receive” an economic benefit from the promotion, and took no “reasonable” action to prevent the e-mail promotion or report it to the FTC.

The Act provides a safe harbor for businesses providing services to companies who are marketed in violation of the Act, unless: they have a greater than 50% ownership interest in

the business; have actual knowledge that the business is being marketed in violation of the Act; or receive or expect to receive an economic benefit from the promotion. This final carve out from the safe harbor statute is troublesome. U.S. law is unsettled on what constitutes enough economic benefit to trigger third party liability. In particular, courts are divided on this issue as it relates to third party Trademark infringement. The legal analysis underlying this “economic benefit” theory in a Trademark infringement matter has been used extensively by courts in other matters involving litigation of issues presented by the internet. As a result, this analysis may be attractive to courts reviewing the Act.

#### Enforcement

The FTC and Department of Justice are charged with enforcing the Act. There has been significant skepticism regarding the availability of additional resources to Justice in order for it to carry out its enforcement obligations. The FTC, which previously expressed an interest in regulating SPAM, will likely take the lead in enforcement actions.

Internet Access Providers retain the right to bring an action in U.S. district court if they have been affected by certain violations of the Act, or a pattern or practice of violations. In addition to procuring injunctive relief, they may also recover their actual damages or up to \$3 million. This provision is troubling for third party service providers since large Internet Access Providers often accuse them of turning a blind eye towards SPAMMERS in their quest for customers. Should the FTC or Justice fail to enforce the Act as aggressively as these providers deem necessary, it is foreseeable that they would avail themselves of this remedy.

The Act does not pre-empt state laws that do not expressly regulate e-mail. Many third-party service providers are subjects of SPAM suits under state laws governing trespass and other property torts. Because of this exception, it is unlikely that the Act will be effective in circumscribing nuisance suits directed at third

party service providers, or lessen the compliance load placed on them when they are required to respond to subpoenas and other discovery requests in similar litigation against SPAMMERS.

#### Quick Compliance Steps

- Develop a documented compliance plan to investigate and address all SPAM complaints.
- Review all contracts, including click-wrap, and other internet based contracts, to ensure that you have notified customers, in a clear and conspicuous manner, that you will be contacting them by e-mail about their accounts.
- If you market by e-mail, anticipate several detailed reviews of the Act to create marketing campaigns that comply with the labeling and content requirements set out in it.
- Do not rely on subcontractors who run e-mail campaigns to insulate you from liability.
- Place a notice on websites stating that you do not allow e-mail marketers to use e-mail addresses for marketing purposes.

This article is intended merely as a general summary of the relevant law for background purposes. I can assist in advising what labeling, screening, reporting, and methods of maintaining records and general company information are necessary to minimize potential liability.

This article is based on my analysis of the Act *prior* to January 1, 2004. Laws change, administrative agencies issue guidelines, and courts make rulings – please consult with your attorney before making decisions based on this article.

David Snead is an attorney in private practice in Washington D.C. His practice focuses primarily on representing web hosting providers, ISPs, and other entities involved in the dissemination

of content and provision of services over the internet. In his 10 years in this area, Mr. Snead has represented ISPs, web hosts, and telecommunications providers both in-house and as outside counsel. Mr. Snead received his J.D. in 1991 from Georgetown University Law Center and is a member of the bars of the District of Columbia and State of New Mexico.