Overview

On Tuesday, December 16, 2003, President Bush signed S. 877, the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, or the "CAN-SPAM Act of 2003" ("Act"). The Act creates a single national standard designed to control the growing problem of deceptive or fraudulent commercial e-mail.

This legislation was largely sought by retailers, marketers and Internet account providers seeking a single set of rules that would apply nationwide and preempt 35 state spam laws.

The Act does not ban commercial e-mails but rather outlines a series of practices that must be followed when sending commercial e-mails. The Act does ban certain fraudulent or deceptive practices and criminalizes techniques used by spammers to avoid detection. The Act also calls upon the Federal Trade Commission ("FTC") to prepare a report to Congress within 6 months containing a plan and timetable for creating a Do-Not-E-mail ("DNE") Registry and addressing the feasibility, problems and issues involved in the creation of such a Registry. The Act does not require the FTC to create a DNE Registry.

State laws exclusively regulating use of electronic mail to send commercial messages are preempted by the Act. However, the Act does not preempt state laws or portions of state laws that prohibit falsity or deception in any electronic mail message or attachment to such an e-mail.

I. Scope of and Required Email Practices

What emails are covered by the Act?

The Act applies to all "commercial e-mails", whether solicited or unsolicited. The Act defines commercial emails as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service."

While the Act does not define "primary purpose" or "commercial product or service," the Act does require the Federal Trade Commission ("FTC") to issue regulations by January 1, 2005 on how to determine the primary purpose of a message.

What information does the Act require senders of commercial emails to include in their emails?

The Act requires all commercial emails to include:

- a legitimate return e-mail and physical postal address,
- a clear and conspicuous notice of the recipient's opportunity to "opt-out," that is, to decline to receive any future messages,
- a mechanism that may be used or an e-mail address (active for at least 30 days after message transmission) to which a recipient may send a message requesting not to receive any future e-mail messages from the sender,

- a clear and conspicuous notice that the message is an advertisement or solicitation, and
- clear notice in subject heading if messages include pornographic or sexual content.

Does the Act contain an exemption from the above requirements for e-mails sent to those individuals or firms with whom the sender has an existing business relationship?

No, the Act *does not* exempt e-mails to recipients with whom the sender has a prior or existing business relationship, as many of the State laws do. Instead, the Act exempts only "transactional or relationship messages" from complying with these practices.

What is a "transactional or relationship message"?

A "transactional or relationship message" is an electronic mail message the primary purpose of which is:

> (1) to facilitate, complete, or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender;
>
> (2) to provide warranty information, product recall information, or safety or security information with respect to a commercial product or service used or purchased by the recipient;
>
> (3) to provide information with respect to a subscription, membership, account, loan, or comparable ongoing commercial relationship involving the ongoing purchase or use of products or services offered by the sender to the recipient;
>
> (4) to provide information directly related to an employment relationship or related benefit plan in which the recipient is currently involved, participating, or enrolled, or;
>
> (5) to deliver goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender.

The Act provides that the FTC may, by regulation, modify the definition of "transactional or relationship message" to expand or contract the categories of messages that are treated as commercial e-mails under the Act.

Are there any circumstances where a commercial e-mail does not have to include the notice that the message is an advertisement or solicitation?

Yes. If the recipient has given their prior consent to receive commercial e-mails from the sender, the sender does not have to include the clear and conspicuous notice that the e-mail is an advertisement or solicitation. Such messages must, however, include notice of the recipient's opportunity to decline to receive other messages from the sender and the sender's physical postal address.

Must the sender honor an opt-out request made by a recipient?

Yes, the Act requires that senders honor all opt-out requests. If a recipient makes a request to not receive commercial mail messages from the sender, it is unlawful for the sender to send another commercial electronic mail message at any time after *ten days* from the receipt of the original message *unless* the recipient has consented to receive e-mails subsequent to the first request to not receive commercial e-mails.

Senders are also prohibited from selling, leasing exchanging or otherwise transferring for any purpose, disclosing the e-mail address of any recipient who has opted-out once the opt-out request has been received.

Can the sender offer a menu of opt-out options?

Yes. A sender of commercial e-mails may give recipients a menu of options from which to choose the types of commercial e-mail they no longer wish to receive, as long as the menu includes an option to receive no further commercial email communications of any kind from the sender.

Would e-mails sent by the listing agent or broker to a seller who has listed their home for sale, or by an agent or brokerage to a prospective buyer, be considered transactional or relationship messages?

In either case, as long as the broker or agent has established a service relationship with the client, such as listing the property for sale or entering into a buyer's broker agreement with an interested buyer, such communications between broker/agent and customer/client are probably covered. Other messages, such as those that solicit sellers or buyers who are not presently firm clients, are probably not covered.

Would e-mails sent by a REALTOR® association or a MLS to its memberships be considered a transactional or relationship message and thus exempt from the Act's requirements?

Yes, provided the message relates to association/MLS services offered or available to members as a membership benefit. It should be noted, however, that there is no exemption for non-profits and, consequently, some e-mails advertising products or services available for purchase may be interpreted by the FTC as subject to the same requirements as commercial e-mails.

II. Deceptive And Other Egregious Practices Are Expressly Prohibited

What does the law prohibit?

The Act also prohibits the most egregious spam practices including: e-mail harvesting (email addresses gathered by computer programs that search public areas on the Internet to compile, capture, or otherwise "harvest" lists of e-mail addresses from web pages, newsgroups, chat rooms, and other online destinations); dictionary attacks (a technique to create as many possible letter combinations for e-mail addresses at large ISPs or e-mail services, hoping to find a valid address); sending bulk spam from a computer accessed without authorization; sending bulk spam through open relays (open mail servers are configured to accept and transfer email on behalf of any user anywhere, including unrelated third parties and so an "open relay" in your e-mail server allows any e-mail sender anywhere to pass messages through your server and onto the ultimate recipients); falsifying header information; using deceptive subject lines; registering for 5 or more e-mail accounts using false registration information; and using these accounts to send bulk spam.

III. Do-Not-Email Registry

Does the Act require the FTC to create a Do-Not-Spam Registry?

No. The Act requires the FTC submit by July 1, 2004 a report that includes a plan and timetable for establishing a Do-Not-E-mail Registry and an explanation of practical, technical, security, privacy, enforceability, or other concerns that the FTC has with such a registry.

It is important to note that the Act *does not require* the FTC to establish a Do-Not-E-mail Registry. Indeed, FTC Chairman Timothy Muris has already expressed concern that such a registry would be impossible to enforce because of the difficulty of tracking down the most egregious spammers. Thus the purpose of the report is not to create a Do-Not-E-mail Registry, but to study the issue and potential problems, and, ultimately, advise Congress on a course of action.

IV. Enforcement

Who will enforce the new rules?

The Act grants the FTC and other federal and State regulators enforcement authority over most organizations. Internet Service providers (ISPs) may also sue for injunctive relief and damages.

There is no private right of action for consumers.

What penalties exist for failing to comply with the new rules?

The Act includes criminal and civil penalties for violations. Damages of up to $250 per violation (or treble damages for willful violations), with a maximum award of $2 million

are possible. However, in actions taken by state AGs and ISPs, courts assessing damages are permitted to consider whether defendants have implemented and followed commercially reasonable compliance procedures in setting the level of damages.

The Act also criminalizes deception and other egregious tactics, such as falsifying header information, hacking, sending large numbers of commercial email, or falsifying registration. These practices are punishable by a maximum of five years imprisonment if committed in furtherance of any felony. Otherwise, offenders may receive up to three years imprisonment if the violation meets certain volume and damage thresholds.

Is there a safe harbor?

There is no safe harbor. However, in actions taken by state AGs and ISPs, courts are permitted to consider whether defendants have implemented and followed commercially reasonable compliance procedures in setting the level of damages.

How do these new rules affect existing state spam rules?

The Act preempts all state laws that expressly regulate commercial e-mail messages, except to the extent that the state laws regulate falsity or deception. State laws are preempted even if they are more stringent than the Act; thus, California's new anti-spam law is largely preempted.

When are the new rules in effective?

The Act will become effective on January 1, 2004.