

# ;login:

**THE MAGAZINE OF USENIX & SAGE**

April 2004 • volume 29 • number 2

## inside:

### THE LAW

Appelman: CAN-SPAM: New Federal Anti-Spam Law Sets  
Nationwide Standards for Commercial Email Messages

**USENIX**

The Advanced Computing Systems Association

# CAN-SPAM

## New Federal Anti-Spam Law Sets Nationwide Standards for Commercial Email Messages

The new federal law regulating spam went into effect on January 1, 2004. It creates a single nationwide set of rules governing commercial email that overrides the inconsistent standards in state anti-spam law. It also criminalizes certain conduct and creates new civil penalties with substantial monetary fines.

Unfortunately, CAN-SPAM is a toothless tiger that nullifies most aspects of every state's anti-spam laws and leaves spam victims without meaningful legal recourse. The single exception is that it doesn't preempt state laws which prohibit false or deceptive content in any portion of a commercial email message or its attachments. Thus, the suits that Serge Egelman is so joyfully bringing against spammers under state law as described in the accompanying article may soon be a thing of the past.

This article outlines CAN-SPAM's most salient features and presents recommendations for compliance.

### The Need for Federal Legislation

Unsolicited commercial email ("spam") has dramatically increased during the past three years.<sup>1</sup>

In the absence of federal legislation, many states passed their own laws to regulate spam. Those laws imposed standards and requirements that differed significantly from state to state. Since email addresses don't specify geographic locations, it is almost impossible for commercial email senders to know with which of the disparate state statutes they were required to comply.

California passed a law in October that would have flatly prohibited sending unsolicited commercial email messages to recipients unless they opted in to receiving them. Other states passed different anti-spam laws with different compliance standards. Also, many of these state laws were opposed by the direct marketing sector. As a result, the pressure on Congress to establish nationwide (and more forgiving) rules became intense. CAN-SPAM is the result.

### Summary of the New Law

The new law:

- Prohibits senders from using false "header" information, false return addresses, and deceptive subject lines
- Requires senders to include valid physical postal addresses in their messages
- Requires senders to provide an opt-out mechanism and to comply with all opt-out requests
- Mandates labeling in the subject line of messages containing adult-related content
- Makes advertisers legally responsible for compliance by their email service vendors

by Dan Appelman

Dan Appelman is a partner in the international law firm of Heller Ehrman, White & McAuliffe, LLP. He practices intellectual property and commercial law, primarily with technology clients, and is president-elect of the California Bar Association's Standing Committee on Cyberspace Law.



[dan@hewm.com](mailto:dan@hewm.com)

1. In 2001, spam accounted for approximately seven percent of all email traffic, whereas it now accounts for over 50 percent. Some estimates are as high as 70 percent.

- Authorizes the Justice Department, the Federal Trade Commission, and other federal agencies to enforce the new law and establishes fines and jail terms for violators
- Permits state attorneys general and Internet service providers to bring civil suits and to be granted injunctive relief, money damages, and attorney fees
- Authorizes (but does not require) the Federal Trade Commission to create a national “do not email” registry
- Pre-empts all state laws that regulate commercial email, except to the extent that state law prohibits falsity or deception in messages or their attachments.

### **PRINCIPAL PROVISIONS OF THE NEW LAW**

#### **NO FALSE OR MISLEADING TRANSMISSION INFORMATION**

It is now illegal to send email messages that contain materially false or misleading “header” information (i.e., information that identifies the source, destination, or routing of an email message). Header information that does not identify the true email address of the sender because of false source information, because the sender has registered for multiple email accounts, or because the message has been routed through other computers for the purpose of disguising its origin is considered materially misleading.

CAN-SPAM makes it a crime to promote a trade or business, or the products or services of a trade or business, using commercial email messages that contain false or misleading transmission information. Businesses that hire advertising companies or email service vendors to help them promote their goods or services by email may themselves be deemed to have violated the Act if the email contains false or misleading transmission information, such as disguising the true identity of the sender.

#### **NO DECEPTIVE SUBJECT HEADINGS**

It is now illegal to send commercial email that includes subject headings that are likely to mislead the recipient about the content or subject matter of the message.

#### **COMMERCIAL EMAIL MUST INCLUDE AN IDENTIFIER, AN OPT-OUT MECHANISM, AND A PHYSICAL ADDRESS**

All commercial email messages must include (i) a clear and conspicuous identification that the message is an advertisement or solicitation; (ii) a clear and conspicuous notice of the opportunity to opt out of receiving further commercial email messages; and (iii) the sender’s postal address.

#### **COMMERCIAL EMAIL MUST INCLUDE A FUNCTIONING, ACCURATE, CONSPICUOUS RETURN EMAIL ADDRESS**

The new law requires that all commercial email messages contain return email addresses that recipients can use to opt out of receiving future solicitations. These return addresses must appear conspicuously in the email message, they must be accurate, and they must function for at least thirty days after the transmission of any outgoing message.

#### **NO CONTINUED SENDING AFTER OPT-OUT**

The new law gives senders a ten-day grace period after receiving any opt-out request in which to cease sending further email messages to that recipient. Continuing to send emails after that date will be deemed a violation of CAN-SPAM. It will also be illegal for the sender or any other person who knows of the recipient’s opt-out request to give

the recipient's email address to anyone else. This provision is Congress's attempt to restrict the common practice of selling or exchanging recipient email mailing lists.

### **ACTIVITIES THAT WILL MAKE THE VIOLATIONS DESCRIBED ABOVE MORE SERIOUS**

#### ADDRESS HARVESTING AND "DICTIONARY" ATTACKS

Under CAN-SPAM, it is illegal to transmit commercial email messages to email addresses that are obtained using automated means from certain Internet Web sites or online services. This prohibition includes collecting email addresses from those Web sites and online services that have privacy policies stating that their email addresses will not be shared with those who would use them for commercial purposes. The new law also prohibits sending commercial email messages to email addresses that are generated by combining names, letters, or numbers into random permutations.

#### CREATING MULTIPLE ELECTRONIC ACCOUNTS

It is illegal under the Act to use automated means to register for multiple email accounts with an Internet registrar or online service provider.

#### RELAYING MESSAGES THROUGH UNAUTHORIZED ACCESS TO OTHER COMPUTERS OR NETWORKS

It is illegal under CAN-SPAM for senders to disguise the origin of their commercial email messages by sending them through computers or networks to which they do not have authorized access.

#### SPECIAL REQUIREMENTS PERTAINING TO SEXUALLY ORIENTED MATERIAL

CAN-SPAM requires commercial email messages that contain sexually oriented material to include marks or notices in their subject headings to inform recipients of their content and to facilitate filtering. It also limits the content that can be initially viewable by the recipient of such messages to (i) the aforementioned marks and notices; (ii) an opt-out mechanism; and (iii) instructions on how the recipient may access the sexually oriented material. The Act orders the Federal Trade Commission to prescribe the content of the marks and notices.

#### THE "DO-NOT-EMAIL" REGISTRY

CAN-SPAM requires the Federal Trade Commission to send Congress a plan and timetable for establishing a nationwide marketing "do not email" registry similar to the new "do not call" registry. But implementation of the plan is discretionary, not mandatory, and comments by several FTC commissioners indicate that the Commission is unlikely to establish the registry.

### **How Will CAN-SPAM Be Enforced?**

Most violations of CAN-SPAM will be enforced by the Federal Trade Commission under its authority to prosecute unfair or deceptive trade practices. The Commission will investigate consumer complaints, and those found to be engaging in unlawful practices will be subject to fines and possible prison sentences in actions brought in federal courts. Other agencies have authority to enforce the Act against certain defendants, such as banks and savings and loan associations, credit unions, broker-dealers, regulated investment companies, investment advisers, insurance providers, air carriers, and telecommunications service providers. In addition, the prohibitions against predatory and abusive email practices can be enforced by the federal Department of Justice.

CAN-SPAM can also be enforced by state attorneys general in civil actions in federal court. State officials can seek injunctive relief to prevent senders from continued viola-

tions as well as monetary damages and attorney fees. In addition, Internet access service providers who have been adversely affected by a violation of the Act can bring a civil action to enjoin further violations and to recover monetary damages and attorney fees.

Unlike many state laws that will now be preempted, the new federal law does not give private individuals the right to sue.

### **Against Whom Can CAN-SPAM Be Enforced?**

In general, the new law will be enforced against those who “initiate” the transmission of unlawful email messages. The Act defines “initiate” very broadly. It not only includes those who actually send the messages, but also those who create or pay for them. Many companies hire email service vendors to help them with their solicitations; and the new law applies to both. In addition, the Act makes it unlawful for any person to promote goods or services by means of commercial email messages they know or should know contain false or misleading transmission information. Customers of commercial email service vendors must therefore have a reasonable level of confidence that the service they use is in compliance with CAN-SPAM’s requirements or risk being held in violation of the Act themselves.

### **What is the Status of State Anti-Spam Laws After CAN-SPAM?**

CAN-SPAM explicitly supersedes all state laws that regulate the use of email to send commercial messages except to the extent that a state law prohibits falsity or deception in any portion of a commercial email message or its attachments. Therefore, most state anti-spam statutes will be preempted, including most of the provisions of the new California law that would have prohibited sending commercial email messages absent some preexisting relationship between the sender and the recipient. The new federal law imposes a nationwide “opt-out” standard that nullifies the much tougher “opt-in” approach adopted by California and several other states.

### **Issues Created by CAN-SPAM**

#### **PROBLEMS FOR ADVERTISERS**

Many commercial email solicitations involve three or more parties: the advertiser, the service provider that actually sends the email messages under contract with the advertiser, and the recipient. The new law makes the advertiser equally guilty or liable for the transgressions of the service provider. Advertisers will be required to closely supervise the practices of their service providers, and will be well advised to renegotiate their contracts to provide for indemnification and other protection in the event they are prosecuted or sued for the actions of their service providers.

#### **OPT-OUT LOGISTICS**

The new law gives senders ten days to comply with opt-out requests. In order to comply, the advertiser must purge the recipient’s email address from all of its service providers’ lists, which may be difficult within that short time frame. Advertisers may be compelled to require service providers to share opt-out information with one another, and service providers may resist those requests. If the opt-out requests are sent to the advertiser rather than directly to its service providers, the service providers may not find out about them in time to comply with the ten-day deadline.

#### LABELING REQUIREMENTS

The new law requires all commercial email messages to be clearly and conspicuously labeled as advertisements or solicitations. But the law includes no guidelines for satisfying this requirement.

### **Recommendations**

Everyone who sends commercial email messages must comply with CAN-SPAM. Here are a few suggestions for complying with the new law:

- Know the requirements of the new law and adopt a compliance plan.
- Designate someone within your organization to be in charge of implementing the plan.
- Keep records of opt-out and opt-in requests. Document how your company complies with those requests.
- Include a clearly explained opt-out mechanism in every commercial email message.
- Label all commercial email messages as advertisements or solicitations.
- Understand the compliance procedures of your service providers and make sure those procedures satisfy CAN-SPAM's requirements.
- Renegotiate your contracts with service providers to provide that they will indemnify you from any liability resulting from their failure to fully comply with CAN-SPAM.
- Review your insurance coverage to determine whether and to what extent it protects you in the event of suit.