SUMMARY OF PUBLIC LAW 108-187
THE CAN-SPAM ACT OF 2003

On December 16, 2003, President Bush signed into law the CAN-SPAM Act of 2003. CAN-SPAM stands for "Controlling the Assault of Non-Solicited Pornography and Marketing."

The Act is codified as Title 15, Sections 7701 through 7713 and Title 18, Section 1037 of the *United States Code*.

What the Law Covers

The CAN-SPAM Act applies to "commercial electronic mail messages,"which Title 15, §7702(2)(A) defines as electronic mail messages whose primary purpose is to advertise or promote a commercial product or service. The definition excludes "transactional or relationship messages," which Title 15, §7702(17) generally defines as emails relating to an earlier transaction, or an ongoing business relationship, between the sender and the recipient. The Federal Trade Commission is authorized to modify the definition of "transactional or relationship messages" to reflect future technological changes.

Criminal Offenses

Title 18, §1037 defines the following acts relating to commercial email as crimes:

(1) Gaining unauthorized access to a computer and sending spam[1] from it;
(2) Re-transmitting spam with the intent to mislead others about its origin;
(3) Sending spam containing materially falsified header information[2];
(4) Registering for five or more email accounts or two or more domain names under a false identity, and sending spam from any combination of those accounts or domain names; and

---

[1] The Act does not use the term "spam." Instead, it uses the term "multiple commercial electronic mail messages." Title 18, §1037(d)(3) defines "multiple" as more than 100 emails a day, more than 1,000 a month, or more than 10,000 a year.

[2] The Act generally defines "material" in terms of impairing a recipient's or service provider's ability to identify the sender. Title 15, §7702(8) defines "header information" as an email's source, destination, and routing information, including the originating email address and domain name.

Copyright © 2003-04 PAUL RUSCHMANN, J.D. All Rights Reserved.

(5) Sending spam from five or more Internet protocol addresses that the sender falsely claims to own.

It is also a crime to conspire to commit any of these offenses.

Title 18, §1037 also provides for the following penalties:

(1) A fine, up to five years in prison, or both, if the crime was committed:

(A) In furtherance of another felony; or

(B) By a person previously convicted of sending spam or of one of the computer crimes defined by 18 U.S.C. §1030.

(2) A fine, up to three years in prison, or both, for a crime involving any of the following circumstances:

(A) Gaining unauthorized access to a computer and sending spam from it;

(B) Registering 20 or more email accounts or 10 or more domain names under a false identity, and sending spam from any combination of those accounts or domain names;

(C) Sending more than 2,500 emails a day, more than 25,000 a month, or more than 250,000 a year;

(D) Causing $5,000 or more in losses to others, during a one-year period, as a result of the crime;

(E) Obtaining $5,000 or more in value, during a one-year period, as a result of the crime; or

(F) Acting as the leader or organizer of three or more other offenders.

(3) In all other cases, a fine, up to a year in prison, or both.

The sentence must also include forfeiture of the proceeds of the crime as well as the computer equipment used to commit it.

The CAN-SPAM Act also directs the U.S. Sentencing Commission to consider enhanced sentences for offenders who:

- Obtained email addresses by "harvesting" them (automatically collecting them from an online source in violation of the owner's privacy policy) or by "dictionary attacks" (randomly generating them by computer);
- Knew that the emails involved in the offense contained a falsely registered domain name; or
- Sent large quantities of emails in connection with another crime, such as fraud, identity theft, obscenity, child pornography, or sexual exploitation of children.

Copyright © 2003-04 PAUL RUSCHMANN, J.D. All Rights Reserved.

Additionally, Title 15, §7704(d)(5) provides that a sender of sexually-oriented email who fails to label it as such or to conceal the sexually-oriented material is subject to a fine, up to five years in prison, or both.

Prohibited Acts

Title 15, §7704(a) forbids a sender of commercial email to do any of the following:

(1) Place materially false or misleading information, relating to the sender's identity, in the header. Header information will be considered false or misleading if:

- It contains a domain name or email address obtained through false representations, even if the information is technically accurate; or
- It disguises the originating computer's identity because the message was re-transmitted through another computer.

(2) Place false or misleading information, relating to the email's subject matter or contents, in the subject line.

(3) Fail to provide a return email address or other online mechanism by which the recipient can ask not to be contacted any more.

(4) Continue sending email to a person who has asked not to be contacted, or distributing that person's email address to others for the purpose of sending spam.

(5) Fail to do all the following:

- Identify the email as an advertisement, unless the recipient has given prior affirmative consent to receiving the email;
- Advise the recipient of the right to ask not to be contacted; and
- Include the sender's mailing address.

Title 15, §7704(b) defines the following as "aggravated violations":

(1) Obtaining email addresses by "harvesting" or "dictionary attacks";

(2) Automatically registering for multiple email accounts for the purpose of sending spam; and

(3) Knowingly re-transmitting spam through another computer without the computer owner's authorization.

Title 15, §7704(c) authorizes the Federal Trade Commission to define additional practices as aggravated violations.

Title 15, §7704(d) imposes the following additional requirements on the sender of sexually-oriented email:

Copyright © 2003-04 PAUL RUSCHMANN, J.D. All Rights Reserved.

- Identify it with a subject label, to be prescribed by the Federal Trade Commission; and
- Ensure that the initially viewable portion of the email not include the sexually-oriented material itself.

These additional requirements do not apply if the recipient has given prior affirmative consent to receiving the sexually-oriented email.

Title 15, §7705 generally forbids the owner of a business to promote it, or to allow the promotion of it, by means of spam.

Enforcement

Title 15, §7706(a) generally authorizes the Federal Trade Commission to treat violations of the CAN-SPAM Act as unfair or deceptive trade practices. Title 15, §7706(d) authorizes the Commission to exercise the same enforcement powers it exercises under the Federal Trade Commission Act, and subjects violators to the same penalties as those for violating the Federal Trade Commission Act.

Title 15, §7706(f) authorizes a state attorney general or other state agency to sue a person who allegedly committed a prohibited act defined by Title 15, §7704(a) or an aggravated violation defined by Title 15, §7704(b). Remedies include all of the following:

- An injunction against further violations.
- The larger of the following:
  Actual damages; or
  Statutory damages of $250 per email, up to a maximum of $2 million (the maximum does not apply in cases where the sender misrepresented his or her identity).

  A court may triple the damage award if the violator "wilfully and knowingly" committed a prohibited act defined by Title 15, §7704(a) or an aggravated violation defined by Title 15, §7704(b). On the other hand, a court may reduce the award if the violator took reasonable steps to avoid violating the law.
- Attorney's fees and costs.

The Federal Trade Commission may intervene in a lawsuit brought by a state agency, and may have it removed to federal court. A state agency may not sue if the Commission or some other federal agency has already begun legal proceedings against that person.

Title 15, §7706(g) authorizes an Internet service provider to sue an alleged

Copyright © 2003-04 PAUL RUSCHMANN, J.D. All Rights Reserved.

violator. A service provider is entitled to the same remedies as a state agency, except that statutory damages are $100 per email if the sender misrepresented his or her identity; and $25 per email, up to a maximum of $1 million, if the sender committed any other violation.

Effect on State Anti-Spam Laws

Title 15, §7707(b) provides that the CAN-SPAM Act pre-empts state laws except:

> (1) To the extent that those laws prohibit falsity or deception in commercial electronic mail messages; or
> (2) Those laws are either not specific to electronic mail (e.g., they deal with trespass, contract, or tort law) or govern "acts of fraud or computer crime."

Miscellaneous Provisions

Title 15, §7707(c) provides that the CAN-SPAM Act does not affect the lawfulness of an Internet service provider's policy of refusing to handle certain types of email messages.

Title 15, §§7708, 7709, 7710, and 7712(a) direct the Federal Trade Commission to do the following:

- Within six months, submit to Congress a plan and timetable for establishing a national "Do-Not-Email" registry. The Commission may establish the registry nine months after the Act is signed into law.
- Within nine months, submit to Congress a report that includes:
  - (A) A system for paying a reward, of at least 20 percent of the civil penalty collected from a violator, to the first person who identified that violator and supplied information leading to the collection of the civil penalty. The Commission may establish the reward program one year after the Act is signed into law.
  - (B) A mechanism for electronically submitting complaints about spam to the Federal Trade Commission.
- Within 18 months, develop a plan for the mandatory labeling of the subject line of commercial email messages.
- Within two years, report to Congress on the effectiveness of the Act and on the need to amend it.

Copyright © 2003-04 PAUL RUSCHMANN, J.D. All Rights Reserved.

Title 15, §7712(b) directs the Federal Communications Commission, within nine months, to adopt rules designed to protect mobile service customers from unwanted commercial messages.

Effective Date

Except for the provisions governing the "Do-Not-Email" registry, the CAN-SPAM Act's effective date is January 1, 2004.

Copyright © 2003-04 PAUL RUSCHMANN, J.D. All Rights Reserved.