

**SUMMARY OF CAN-SPAM ACT OF 2003  
S. 877 (BURNS-WYDEN)  
AS PASSED BY THE SENATE OCTOBER 22, 2003**

	<b>DESCRIPTION</b>
<b>TITLE</b>	Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act of 2003)
<b>CONGRESSIONAL FINDINGS</b>	Makes 12 findings relating to the need for the legislation.
<b>PUBLIC POLICY DETERMINATIONS</b>	Senders of unsolicited commercial e-mail should not mislead recipients as to the source and content of e-mail, and recipients should have a right to opt-out from the receipt of unsolicited commercial e-mail.
<b>DEFINITION OF COMMERCIAL ELECTRONIC MAIL MESSAGE</b>	A commercial electronic mail message is an electronic mail message, the primary purpose of which is to advertise or promote a commercial product or service, including content on an Internet website operated for a commercial purpose.

	<b>DESCRIPTION</b>
<b>DEFINITION OF IMPLIED CONSENT</b>	<ol style="list-style-type: none"> <li>1) Implied consent exists when there has been a business transaction between the sender and the recipient within the previous three year period, the recipient was given an opportunity to opt-out from the receipt of unsolicited e-mail at the time of the transaction or in the first e-mail received from the sender after the Act's effective date, and the recipient has not opted-out.</li> <li>2) A visit to a website where the recipient did not knowingly submit an e-mail address does not constitute implied consent.</li> <li>3) If a company's division or line of business holds itself out as a particular line of business or division, rather than as the entity of which it is a part, the line of business or division is treated as the sender of an e-mail.</li> </ol>
<b>DEFINITION OF TRANSACTIONAL OR RELATIONSHIP MESSAGES</b>	<p>Transactional or relationship messages are e-mails, the primary purpose of which are:</p> <ol style="list-style-type: none"> <li>1) To facilitate, complete or confirm a commercial transaction;</li> <li>2) To provide warranty, product recall or safety or security information with respect to a commercial product or service used or purchased by recipient;</li> <li>3) To provide notification concerning a change in terms or features, standing or status, or account balance or statement information regarding a subscription, membership, account, loan or other ongoing commercial relationship;</li> <li>4) To provide information directly related to an employment relationship or related benefit plan involving recipient; or</li> <li>5) To deliver goods or services including updates and upgrades that recipient is entitled to receive under a previous transaction.</li> </ol>

	<b>DESCRIPTION</b>
<p><b>DEFINITION OF UNSOLICITED COMMERCIAL E-MAIL MESSAGE</b></p>	<p>An unsolicited commercial e-mail message is a commercial electronic mail message sent without the recipient’s prior affirmative or implied consent, and which is not a “transactional or relationship message.”</p>
<p><b>CRIMINAL PROHIBITIONS REGARDING MULTIPLE COMMERCIAL E-MAILS</b></p>	<p>It is a criminal offense to knowingly:</p> <ol style="list-style-type: none"> <li>1) Access a computer without authorization and intentionally send multiple commercial e-mails from or through such computer;</li> <li>2) Use a computer to relay or retransmit multiple commercial e-mails with the intent to deceive or mislead recipients, or any Internet access service, as to their origin;</li> <li>3) Falsify header information in multiple commercial e-mails and intentionally send such messages;</li> <li>4) Register, using information that falsifies the identity of the registrant, for five or more e-mail accounts or online user accounts or two or more domain names and intentionally send multiple commercial e-mails from such accounts or domain names; or</li> <li>5) Falsely represent the right to use five or more Internet protocol addresses and intentionally send multiple commercial e-mails from such addresses.</li> </ol> <p>The term “multiple commercial e-mails” means more than 100 e-mails sent during a 24 hour period, more than 1,000 e-mails sent during a 30 day period, or more than 10,000 e-mails sent during a one year period.</p>
<p><b>CRIMINAL PENALTIES REGARDING MULTIPLE COMMERCIAL E-MAILS</b></p>	<p>Punishment for a violation of the above prohibitions is:</p> <ol style="list-style-type: none"> <li>1) A fine of up to \$250,000 for an individual or \$500,000 for an organization, and/or imprisonment for up to five years: <ul style="list-style-type: none"> <li>• If the violation is a repeat violation;</li> <li>• If the violation is committed in furtherance of any felony under state or federal law; or</li> <li>• If the defendant has previously been convicted under federal law prohibiting computer fraud, or state or federal law regarding the sending of multiple commercial e-mails or unauthorized</li> </ul> </li> </ol>

	<b>DESCRIPTION</b>
	<p style="text-align: center;">access to computers.</p> <p>2) A fine of up to \$250,000 for an individual or \$500,000 for an organization, and/or imprisonment for up to three years, for:</p> <ul style="list-style-type: none"> <li>• Accessing a computer without authorization and intentionally sending multiple commercial e-mails from or through such computer;</li> <li>• Registering, using information that falsifies the identity of the registrant, for five or more e-mail accounts or online user accounts or two or more domain names and intentionally sending multiple commercial e-mails from such accounts or domain names, where the offense involves 20 or more falsified e-mail or online user account registrations or ten or more falsified domain name registrations;</li> <li>• A violation where more than 2,500 e-mails were sent in a 24 hour period, or more than 25,000 e-mails were sent during a 30 day period, or more than 250,000 were sent during a one year period;</li> <li>• A violation causing loss to any person aggregating \$5,000 or more during a one year period;</li> <li>• A violation causing gain to the violator aggregating \$5,000 or more during a one year period; or</li> <li>• A violation committed by the defendant in concert with three or more persons and the defendant was an organizer or leader.</li> </ul> <p>3) A fine of up to \$100,000 for an individual or \$200,000 for an organization, and/or imprisonment for up to one year, in all other cases.</p> <p>In imposing a sentence, the court shall order the defendant to forfeit to the United States any property traceable to proceeds obtained from such violations and equipment or technology used or intended to be used to commit or facilitate the violation.</p>
<b>U.S. SENTENCING GUIDELINES</b>	<p>The U.S. Sentencing Commission is to review and amend the sentencing guidelines to provide appropriate penalties for violations of the Act. The Commission shall consider sentencing enhancements for:</p>

	<b>DESCRIPTION</b>
	<ol style="list-style-type: none"> <li>1) Violators who harvested e-mail addresses from a website, proprietary service or other online public forum operated by another person without that person’s authorization;</li> <li>2) Violators who randomly generated e-mail addresses by computer;</li> <li>3) Violators who knew that the commercial e-mails involved in the violation contained an Internet domain with false registration information; and</li> <li>4) Violators convicted of other offenses, including offenses involving fraud, identity theft, obscenity, child pornography, and the sexual exploitation of children if such offenses involved the sending of large quantities of unsolicited e-mail.</li> </ol>
<b>PROTECTIONS FOR USERS OF COMMERCIAL E-MAIL</b>	<ol style="list-style-type: none"> <li>1) It is unlawful to initiate a commercial e-mail that contains header information that is materially false or misleading. Header information that includes an originating address, the access to which was obtained by false pretenses or false representations, is considered materially misleading.</li> <li>2) It is unlawful to initiate a commercial e-mail with a subject heading that the sender knows is likely to mislead a recipient about a material fact regarding the contents or subject matter of the message.</li> <li>3) It is unlawful to initiate a commercial e-mail that does not contain a functioning return address or other Internet based mechanism which a recipient can use to send a reply or use to opt-out from future commercial e-mail messages from the sender. This does not apply to a transactional or relationship message.</li> <li>4) It is unlawful to send an unsolicited commercial e-mail to someone who has opted-out. The sender has ten days to process the recipient’s opt-out request. The Federal Trade Commission (“FTC”) may modify this ten-day period.</li> <li>5) It is unlawful for a sender to sell, lease, exchange or transfer the e-mail address of a recipient who has opted-out for any purpose other than compliance with law.</li> <li>6) It is unlawful to send unsolicited commercial e-mail unless the message: <ul style="list-style-type: none"> <li>• Clearly and conspicuously indicates it is an advertisement or solicitation;</li> <li>• Provides clear and conspicuous notice of an opportunity to opt-out from receiving further</li> </ul> </li> </ol>

	<b>DESCRIPTION</b>
	<p style="text-align: center;">unsolicited commercial e-mails; and</p> <ul style="list-style-type: none"> <li>• Provides the sender’s physical postal address.</li> </ul> <p>Except for a violation of 1) above, it is a defense if the sender has established and implemented reasonable practices and procedures to prevent violations, and a violation occurred despite good faith efforts to comply.</p>
<b>AGGRAVATED VIOLATIONS RELATING TO UNSOLICITED COMMERCIAL E-MAIL</b>	<ol style="list-style-type: none"> <li>1) It is unlawful to initiate, or assist in the initiation of, an unsolicited commercial e-mail that is unlawful as indicated in the previous section if sender knows, should have known or consciously avoids knowing that the address of the recipient was obtained using an automated means from a website or online service, or obtained by automated generation of e-mail addresses.</li> <li>2) It is unlawful to use scripts or automated means to establish multiple e-mail accounts from which the person sends unlawful unsolicited commercial e-mail.</li> <li>3) It is unlawful to knowingly relay or retransmit unlawful unsolicited commercial e-mail from a computer or computer network that the person has accessed without authorization.</li> <li>4) The FTC may identify additional activities and practices that are to be prohibited if they contribute substantially to the proliferation of unlawful commercial e-mail.</li> </ol>
<b>WARNING LABELS FOR E-MAIL WITH SEXUALLY ORIENTED MATERIAL</b>	<ol style="list-style-type: none"> <li>1) It is unlawful to send unsolicited commercial e-mail that contains sexually oriented material that: <ul style="list-style-type: none"> <li>• Fails to include in the subject heading the marks or notices prescribed by FTC.</li> <li>• Fails to provide that the part of the message that is initially viewable to the recipient when the message is opened includes only the marks or notices prescribed by FTC, clear and conspicuous notice that the e-mail is a solicitation or advertisement, notice of opportunity to opt-out, physical postal address of the sender, and instructions for accessing the sexually oriented material.</li> </ul> </li> <li>2) Within 120 days after enactment, the FTC, in consultation with the U.S. Attorney General, shall prescribe marks or notices to be included or associated with unsolicited commercial e-mail that contains sexually oriented material.</li> <li>3) “Sexually oriented material” means any material that depicts sexually explicit conduct as defined in 18 U.S.C. § 2256, unless the depiction constitutes a small and insignificant part of the whole, the</li> </ol>

	<b>DESCRIPTION</b>
	<p>remainder of which is not devoted to sexual matters.</p> <p>4) A violation is punishable as if it were a violation of the above criminal prohibitions on multiple commercial e-mails.</p>
<p><b>BUSINESSES KNOWINGLY PROMOTED BY E-MAIL WITH FALSE OR MISLEADING TRANSMISSION INFORMATION</b></p>	<p>1) It is unlawful for a person to promote a business or goods or services in a commercial e-mail which contains materially false or misleading header information if the person:</p> <ul style="list-style-type: none"> <li>• Knows or should have known in the ordinary course of business that the goods or services were being promoted in the message;</li> <li>• Received or expected to receive economic benefit from such promotion; and</li> <li>• Took no reasonable action to prevent the transmission, or detect the transmission, and report it to the FTC.</li> </ul> <p>2) A person providing goods and services who violates the above restriction is not liable for the violation unless the person:</p> <ul style="list-style-type: none"> <li>• Owns, or has a greater than 50 percent ownership or economic interest in, the business of the person violating the provision; or</li> <li>• Has actual knowledge that goods or services are promoted in a commercial e-mail that violates this provision, and receives or expects to receive an economic benefit from such promotion.</li> </ul> <p>3) Only the FTC and the specified federal and state insurance authorities may enforce this provision. State attorneys general and ISPs may not enforce this provision.</p>
<p><b>FTC ENFORCEMENT</b></p>	<p>The FTC is authorized to enforce violations as unfair or deceptive acts or practices under the Federal Trade Commission Act. Violations involving depository institutions, securities firms and insurers are enforced by the federal banking agencies, the SEC and state insurance authorities, respectively.</p>
<p><b>PRIVATE RIGHT OF ACTION BY INTERNET SERVICE PROVIDERS ("ISPs")</b></p>	<p>An ISP that is adversely affected by a violation of the above protections for users of commercial e-mail, the aggravated violations relating to unsolicited e-mail, and the provisions regarding warning labels for e-mail with sexually oriented material may bring an action in federal court against a violator. Remedies include injunctive relief, costs and attorneys fees, and the greater of actual damages or damages calculated as follows:</p>

	<b>DESCRIPTION</b>
	<ul style="list-style-type: none"> <li>• \$100 times the number of violations (each e-mail is a separate violation) for every violation of prohibition on e-mails with a false or misleading header. There is no maximum amount of damages for violations involving false or misleading headers.</li> <li>• \$25 times the number of violations for all other violations, up to a maximum of \$1 million. This maximum increases to \$3 million where the violations were willful and knowing, or involved aggravated violations relating to unsolicited e-mail.</li> </ul>
<b>STATE ENFORCEMENT</b>	<p>1) State attorneys general may bring enforcement actions in federal court on behalf of state residents adversely affected by a violation of the above protections for users of commercial e-mail, the aggravated violations relating to unsolicited e-mail, and the provisions regarding warning labels for e-mail with sexually oriented material. Remedies include injunctive relief, costs and attorneys fees and the greater of actual damages or damages calculated as follows:</p> <ul style="list-style-type: none"> <li>• \$100 times the number of violations (each e-mail is a separate violation) for every violation of prohibition on e-mails with a false or misleading header. There is no maximum amount of damages for violations involving false or misleading headers.</li> <li>• \$25 times the number of violations for all other violations, up to a maximum of \$1 million. This maximum increases to \$3 million where the violations were willful and knowing or involved aggravated violations relating to unsolicited e-mail.</li> </ul> <p>2) The State attorney general must inform the FTC or appropriate federal regulator before initiating action. The FTC or appropriate federal regulator may intervene in the litigation. The State attorney general may not bring an action against a party while a federal action is pending.</p>

	<b>DESCRIPTION</b>
<b>EFFECT ON OTHER LAWS</b>	<p>The Act supersedes any state or local law or regulation that expressly regulates the sending of commercial e-mail, except those prohibiting false or deceptive commercial e-mail, or those laws that are not specific to e-mail including trespass, contract or tort law, and other state laws to the extent that such laws relate to acts of fraud or computer crime.</p> <p>The Act also does not affect the lawfulness or unlawfulness of an ISP's policy of declining to transmit or handle certain types of e-mail messages.</p>

	<b>DESCRIPTION</b>
<b>DO-NOT-E-MAIL REGISTRY</b>	<p>Within six months of enactment, the FTC is to provide to Congress a plan and timetable for establishing a nationwide Do-Not-E-Mail Registry, including any technical, practical, privacy enforceability or other concerns that FTC has regarding the registry and how the registry would be applied with respect to children with e-mail accounts. FTC may establish and implement the plan no earlier than nine months after enactment of the Act.</p>
<b>STUDY OF EFFECTIVENESS AND ENFORCEMENT OF THE ACT</b>	<p>The FTC, in consultation with the Justice Department and other appropriate agencies, is to submit a report to Congress within 24 months of enactment analyzing the effectiveness and enforcement of the Act and any need to modify it.</p> <p>The report is to include an analysis of the extent to which technological and marketplace developments may affect the practicality and effectiveness of the Act; an analysis and recommendations on addressing unsolicited commercial e-mail from other countries; an analysis and recommendations on options for protecting consumers, including children, from receiving and viewing unsolicited commercial e-mail that is obscene or pornographic.</p>
<b>REWARDS FOR INFORMATION ABOUT VIOLATIONS</b>	<p>The FTC is to submit a report to Congress within nine months of enactment that sets forth a system for rewarding those who supply information about violations of the Act. This system shall include:</p> <ul style="list-style-type: none"> <li>• Procedures for the FTC to grant a reward of at least 20 percent of the total civil penalty collected for a violation of the Act to the first person that identifies the violator and supplies information that leads to the successful collection of a civil penalty by the FTC; and</li> <li>• Procedures to minimize the burden of submitting a complaint to the FTC concerning violations of the Act, including procedures to allow electronic submission of complaints to the FTC.</li> </ul> <p>The FTC may implement the reward plan no earlier than 12 months after enactment of the Act.</p> <p>Within 18 months of enactment, the FTC is to report to Congress on a plan for requiring unsolicited commercial e-mail to be identifiable from its subject line, including the possibility of requiring the use of “ADV” in the subject line.</p>

<b>EFFECTIVE DATE</b>	The provisions of the Act are effective 120 days after date of enactment, except for the Do-Not-E-Mail Registry.
<b>TRAINING FOR REALTIME WRITERS ACT OF 2003</b>	Implements the Training for Realtime Writers Act of 2003, which directs the National Telecommunications and Information Administration to make competitive grants to eligible entities to promote training and placement of individuals as realtime writers in order to meet the requirements for closed caption video programming in the Communications Act of 1934 and rules prescribed thereunder.