

SUMMARY OF SENATOR WILSON’S ANTI-SPAM ACT OF 2003 (H.R. 2515)

PROVISION	H.R. 2515 AS INTRODUCED JUNE 18, 2003
TITLE	“Anti-Spam Act of 2003” [Section 1]
CONGRESSIONAL FINDINGS	Makes 10 findings relating to the need for the legislation. [Section 2(a)]
PUBLIC POLICY DETERMINATIONS	Government has a substantial interest in regulating commercial e-mail, consumers and ISPs should not have to bear the costs of unwanted commercial e-mail, and recipients of commercial e-mail have a right to decline to receive unwanted commercial e-mail. [Section 2(b)]
INCLUSION OF IDENTIFIER, OPT-OUT, E-MAIL ADDRESS, AND PHYSICAL ADDRESS	<p>Sender of commercial e-mail must include:</p> <ol style="list-style-type: none"> 1) Clear and conspicuous identification that the message is a commercial e-mail; 2) Clear and conspicuous notice of opportunity to opt-out of future commercial e-mails from sender or affiliates; 3) A functioning return e-mail address or other Internet-based mechanism, clearly and conspicuously displayed, that: <ol style="list-style-type: none"> a) Recipient may use to send a reply e-mail opting-out from future commercial e-mails from sender at the e-mail address where the message was received; b) For other Internet-based mechanisms, directly submits such opt-out request or clearly and conspicuously provides a manner for submitting such request. Return e-mail address does not fail to satisfy these requirements if it is temporarily and unexpectedly unable to receive messages due to a problem

	<p>out of sender's control, if the problem is corrected within a reasonable time; and</p> <p>c) Is capable of receiving such messages for at least 30 days after original message is sent.</p> <p>4) Sender's valid physical street address. [Section 101(a)(1)]</p>
<p>PROHIBITION OF SENDING E-MAIL AFTER OPT-OUT</p>	<p>1) Sender or affiliate, or any person acting on behalf of sender or affiliate, may not send commercial e-mail to recipient who has opted-out for 5 years after opt-out takes effect.</p> <p>2) Opt-out shall take effect 10 days after receipt of request unless the Federal Trade Commission ("FTC") determines another reasonable time period to allow such request to take effect.</p> <p>3) No person acting on behalf of sender or affiliate may assist in providing or selecting e-mail addresses to which commercial e-mail is sent in violation of opt-out request.</p> <p>4) Sender or affiliate may not sell, lease, exchange or otherwise transfer or release recipient's e-mail address for any purpose other than compliance with the Act or other provision of law. [Section 101(b)(1)]</p> <p>5) Opt-out shall not be considered to have been made with respect to a commercial e-mail if the message falls within the scope of an express and unambiguous invitation, or consent was granted by recipient after opt-out request was made <i>and</i> recipient had clear and conspicuous notice (at the time invitation or consent was granted) that:</p> <p>a) Recipient was granting the invitation or consent;</p> <p>b) The scope of the invitation or consent would be covered by the invitation or consent; and</p>

	<p>c) The commercial e-mail includes a functioning return e-mail address or other Internet-based mechanism for the purposes of making opt-out requests. [Section 101(b)(2)] [See this section—does not specify if the functioning return e-mail address mechanism that sender must inform recipient of is on the original e-mail or the e-mail sent after consent]</p>
<p>FALSE OR MISLEADING HEADER INFORMATION OR SUBJECT HEADINGS</p>	<p>No person may send commercial e-mail or commercial transactional e-mail that contains or is accompanied by false or misleading header information or that contains a subject heading likely to mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message. [Section 101(c)]</p>
<p>ILLEGALLY HARVESTED E-MAIL ADDRESSES</p>	<p>1) No person may send a commercial e-mail prohibited by the Act’s identification, opt-out, or false or misleading header information provisions if:</p> <ul style="list-style-type: none"> a) Recipient’s e-mail address was obtained by automated means from an Internet website or proprietary online service operated by another person, and b) The website or online service contained a notice at the time the address was obtained stating that the operator of such website or online service will not give, sell or otherwise transfer addresses maintained by such site or service to any other party for the purpose of sending commercial e-mail. <p>2) No person may send a commercial e-mail or commercial transactional e-mail if recipient’s e-mail address was obtained by automated generation of addresses. [Sections 101(d) and 101(e)]</p>
<p>WARNING LABELS FOR SEXUALLY ORIENTED MATERIAL</p>	<p>1) No person may send a commercial e-mail that includes sexually oriented material that:</p> <ul style="list-style-type: none"> a) Does not include in its subject heading the marks or notices prescribed by FTC, or

	<p>b) Does not provide that the matter in the message that is initially viewable to recipient when the message is opened includes only marks and notices prescribed by FTC, required notice and opportunity to opt-out, and instructions or mechanism to access the sexually oriented material.</p> <p>2) FTC shall prescribe, within 120 days after enactment of the Act, marks or notices to be included in or associated with commercial e-mail that contains sexually oriented material.</p> <p>3) “Sexually oriented material” means any material that depicts sexually explicit conduct, unless the depiction constitutes a small and insignificant part of the whole, the remainder of which is not primarily devoted to sexual matters. [Section 101(f)]</p>
ACTION BY ISPS	<p>Establishes a private right of action in U.S. district court for ISPs if ISP is adversely affected by a violation. Remedies include injunctive relief and/or recovery of the greater of actual losses or statutory damages as follows:</p> <p>1) For violations of identification and notice and opportunity for opt-out provisions of the Act, \$10 for each separate e-mail address to which message is sent. Total damages per message sent may not exceed \$500,000 unless violation was knowing or willful in which case this limit is raised to \$1.5 million. [Section 102(a)(1)] [Also mentions that court may reduce the \$10 per-violation amount if due care and reasonable practices were involved and violation occurred in spite of good faith efforts to comply with such practices—however, if the amount otherwise determined exceeds \$75,000, the court may not reduce the \$10 amount “such that the amount determined...is less than \$75,000”]</p> <p>2) For violations of header, subject heading, harvesting and sexual orientation provisions of the Act, \$100 for each separate e-mail address to which message is sent. [Section 102(a)(2)]</p>
ACTION BY STATES	<p>1) State attorneys general may bring enforcement action in federal court for violations</p>

	<p>of the Act.</p> <p>2) Remedies include injunctive relief and/or recovery of the greater of:</p> <p>a) Actual losses, or</p> <p>b) \$500 for each e-mail address to which message is sent. This amount is increased to up to \$1,500 for willful or knowing violations of the Act.</p> <p>3) State attorney general must inform FTC before initiating action; FTC may intervene in the litigation.</p> <p>4) State attorney general may not bring an action against a party while FTC action is pending. [Also includes provision stating that this Act doesn't prevent attorney generals from exercising investigation powers under state law or to prevent other state officials from exercising their authorities]</p> <p>5) States may also recover attorneys' fees. [Sections 103 and 104]</p>
FTC ENFORCEMENT	FTC may enforce the Act with the same powers and authorities as FTC may enforce the FTC Act. [Section 105]
CRIMINAL PENALTIES GENERALLY	Adds new chapter to United States Code for e-mail crimes. Defines "commercial electronic mail message" as any e-mail message containing a commercial advertisement or promotion of a product or service. The new chapter takes effect 120 days after enactment.
CRIMINAL PENALTIES FOR FALSE IDENTITY	<p>1) Provides criminal penalties for a sender who during a 30-day period sends 10 or more commercial e-mails that the sender knows falsifies the sender's identity.</p> <p>2) Penalties include a fine up to \$200,000 or imprisonment for up to one year or both.</p> <p>3) Where the violation occurs after conviction for a prior violation of this provision, or the violation involves 10,000 or more e-mails sent within a 30-day period, the sender</p>

	<p>shall be fined up to \$500,000 or imprisoned for up to two years or both.</p> <p>4) Identity may be falsified by any means. The following conduct is considered a falsification of identity:</p> <ul style="list-style-type: none"> a) Accompanying the message with header information that is false as to sender's identity or as to the routing of the message. b) Accessing a computer or computer network without authorization or exceeding authorized access and, through such conduct, sending from or through that computer or network the message that falsifies the sender's identity. c) Using information that falsifies the sender's identity to register for multiple e-mail accounts or domain names and sending the message from such accounts or domain names, or advertising such domain names without conspicuously including the identity and current contact information of the sender in the message. <p>5) [include factors considered by U.S. sentencing commission in determining sentence?]</p>
<p>CRIMINAL PENALTIES FOR FAILURE TO PLACE WARNING LABELS ON COMMERCIAL E- MAIL CONTAINING SEXUALLY ORIENTED MATERIALS</p>	<p>1) Provides criminal penalties for a person who knowingly sends a commercial e-mail that includes sexually oriented material and knowingly:</p> <ul style="list-style-type: none"> a) Fails to include in the subject heading the marks or notices prescribed by FTC, or b) Fails to provide that the matter in the message that is initially viewable to recipient when the message is opened includes only marks and notices prescribed by FTC, required notice and opportunity to opt-out, and instructions or mechanism to access the sexually oriented material.

	<p>2) Punishment shall be a fine of up to \$200,000 or imprisonment for up to one year or both.</p> <p>3) Where the violation occurs after conviction for a prior violation of this provision, or the violation involves 10,000 or more e-mails sent within a 30-day period, the sender shall be fined up to \$500,000 or imprisoned for up to two years or both.</p> <p>[include factors considered by U.S. sentencing commission in determining sentence?]</p> <p>4) “Sexually oriented material” means any material that depicts sexually explicit conduct, unless the depiction constitutes a small and insignificant part of the whole, the remainder of which is not primarily devoted to sexual matters. [This is identical to the definition in the earlier provision dealing with sexually oriented material; can we take this out?]</p>
<p>CRIMINAL PENALTIES FOR HARVESTING E- MAIL ADDRESSES</p>	<p>1) Provides criminal penalties for a person who knowingly obtains e-mail addresses from an Internet website or proprietary online service operated by another person without that person’s authorization and using automated means, and uses such addresses to violate the provisions relating to falsifying identity and sending sexually oriented material.</p> <p>2) Punishment shall be a fine of up to \$200,000 or imprisonment for up to one year or both.</p>
<p>CIVIL ENFORCEMENT BY ISPs</p>	<p>Establishes a private right of action in federal court for ISPs if ISP is adversely affected by a violation of the provisions relating to falsifying identity and sending sexually oriented material. Remedies include recovery of actual losses or, at ISP’s option, damages of \$500 for each e-mail message involved in the violation. The U.S. Justice Department may intervene in the litigation.</p>
<p>FTC AND JUSTICE DEPARTMENT</p>	<p>1) FTC and the U.S. Justice Department may enforce the provisions relating to falsifying identity and sending sexually oriented material with the same powers and</p>

ENFORCEMENT	<p>authorities by which FTC and the U.S. Justice Department enforce the FTC Act.</p> <p>2) U.S. Attorney General may also in a civil action recover a penalty of up to \$500 for each e-mail message involved in such violation.</p>
ENFORCEMENT BY STATES	<p>1) Unless the U.S. Attorney General or FTC has commenced action regarding the same conduct, state attorneys general may bring action in federal court for a violation of the provisions relating to falsifying identity and sending sexually oriented material.</p> <p>2) Remedies include damages of \$500 for each e-mail message involved in such violation.</p> <p>3) The U.S. Justice Department may intervene in the litigation.</p>
REGULATIONS	<p>FTC, after consulting with the Federal Communications Commission (the "FCC"), shall issue regulations to implement the Act within 12 months after enactment. This does not authorize FTC to require specific words, characters, marks or labels in a commercial e-mail to satisfy identification and notification and opportunity for opt-out requirements of the Act. [Section 301(a)]</p>
REPORT	<p>FTC, after consulting with FCC, shall submit a report to Congress regarding the need to protect the rights of users of e-mail to avoid receiving unsolicited commercial e-mail within 240 days after enactment. The report shall:</p> <p>1) Analyze the effectiveness and efficiency for preventing unsolicited commercial e-mail of requiring each such message to include specific words, characters, marks or labels identifying such message as an unsolicited commercial e-mail;</p> <p>2) Compare and evaluate alternative methods of protecting such rights including the extent to which such methods can facilitate screening and removal of unsolicited commercial e-mail;</p> <p>3) Compare and evaluate alternative methods for persons aggrieved by receipt of unsolicited commercial e-mail to report and submit such messages to FTC and</p>

	<p>alternative means of notifying the public of the availability of such methods; and</p> <p>4) Evaluate whether there is a need for additional FTC authority to expand or restrict the e-mail messages that are commercial for purposes of the Act or to further expand or restrict the prohibitions, limitations, definitions or exceptions of the Act and propose legislation to effectuate any such expansions or restrictions deemed necessary. [Section 301(b)]</p>
EFFECT ON OTHER LAWS	Supersedes any state or local law regulating commercial e-mail except those regulating falsification of sender's identity, sender's authentication information, header or routing information, or subject line information in commercial e-mail. [Section 302(b)]
EFFECT ON ISP'S POLICIES	The Act has no effect on an ISP's policy of declining to transmit, route, relay, handle, receive, or store certain types of e-mail messages. [Section 302(c)]
STUDY	FTC, after consultation with FCC, shall conduct a study within 24 months after enactment analyzing the effectiveness and enforcement of the Act and the need to modify it. This report shall include an analysis of the extent to which technological and marketplace developments may affect the practicality and effectiveness of the Act. [Section 303]
DEFINITIONS	Defines various terms, including "commercial electronic mail message," "commercial transactional electronic mail message," "electronic mail address," "electronic mail message," and "header information." [Section 304]
DEFINITION OF COMMERCIAL ELECTRONIC MAIL MESSAGE	Defined as any e-mail message containing a commercial advertisement or promotion of a product or service except for any commercial transactional e-mail message. [Section 304(3)] [Note: this definition is slightly different from the definition in the criminal penalties section]
DEFINITION OF COMMERCIAL TRANSACTIONAL ELECTRONIC MAIL MESSAGE	<p>Defined as any e-mail message the primary purpose of which is:</p> <p>1) To facilitate, complete, or confirm a specific commercial transaction, with or without consideration, between sender and recipient that recipient has previously agreed to enter into with sender; or</p> <p>2) To provide, relating to a specific commercial transaction or the product or service</p>

	<p>involved in the transaction,</p> <ul style="list-style-type: none"> a) A billing statement or information, b) Debt collection information, c) Product recall information, d) Warranty information, e) Safety or security information, f) An actual update or modification to a product or service, or g) Information requested by the recipient. [Section 304(3)]
EFFECTIVE DATE	120 days after enactment [Section 305]

070/03/H.R. 2515 (6-25-03)