

CAN-SPAM Act of 2003: Will Act Can or Uncan SPAM?

The John Marshall Law School

By **Henry N. Meier, Jr., Esq.**
Of Counsel, CorpLaw Associates LLC



Henry is Of Counsel to CorpLaw Associates LLC. He has over 20 years of experience in IP, corporate transactional, and e-commerce law. He can be reached at henry@corplaw.com or at 847.784.1300. The firm's web site is www.corplaw.com.

- 1.0 Background
- 1.1 Onslaught of Unsolicited Commercial Electronic Mail (“UCE”)S
- 1.2 UCEs often not benign. See FTC report of scams run by bulk Email; Exhibit A.
- 1.3 Litany of Abuses. See Section 2 of CAN-SPAM Act - Congressional Findings and Policy.
- 1.4 Patchwork of State Anti-Spam laws.
- 1.5 Congress’ Response - Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, or the “CAN-SPAM Act of 2003”, or the “Act”. The CAN-SPAM Act of 2003 includes criminal provisions.

- 2.0 Key Terms Defined. See Section 3 of Act.
- 2.1 “Commercial Electronic Mail Message” as defined, a “CEM”, looks at “Primary Purpose” of the message, which must be advertisement or promotion of product or service. Before 16 December 2004, the Act requires the FTC to further define “Primary Purpose” by rule-making. Act §3 (2)(A) - (D).
- 2.2 “Internet Access Service” is broader than an ISP concept, and is defined as: (4) The term “Internet access service” means a service that enables users to access content, information, electronic mail, or other services offered over the Internet, and may also include access to proprietary content, information, and other services ... 47 U.S.C. 231(e)(4).
- 2.3 A “Protected Computer” is broadly defined as a computer:
 - (B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States ... 18 U.S.C. §1030(e)(2)(B),
- 2.4 Other Significant Terms: “Affirmative Consent” - see § 3(1); “Header Information” - see §3(8); “Routine Conveyance” - §3(15); and “Sender” - §3(16).
- 2.5 FTC may modify some definitions as needed to accommodate technology changes. §3(17)(B).
- 3.0 Prohibited Activities.
- 3.1 In General. The CAN-SPAM Act prohibits any falsification of information or any action intended to mislead in relation to sending of a CEM to a Recipient. § 4 describes criminal activities which require the knowledge of the Sender to be a violation of the Act.
 - 3.1.1 A Sender cannot send a CEM without authorization. §4(a) [§1037(a)(1) - access].
 - 3.1.2 A Sender cannot use another “Protected Computer” to relay a message with the intent to mislead as to the origin of the message. [§1037(a)(2)].

- 3.1.3 A Sender cannot materially falsify “Header Information” on any CEM. [§1037(a)(3).
- 3.1.4 A Sender cannot falsify the identity of the registrant of 5+ Email accounts or 2+ Domain Names, to transmit CMEs from them. [§1037(a)(4)].
- 3.2 Penalties. §4 [§1037(b)].
 - 3.2.1 The penalties for any violation under 3.1, above, are severe. Penalties may run from fines and a minimum of one (1) year in prison.
 - 3.2.2 Aggravated Penalties. Certain conditions may serve to increase the fines and imprisonment up to 3 to 5 years, such as the volume of CEMs sent, if any one person suffers a loss of at least \$5,000 in one year, or if offense is committed in furtherance of a felony.
 - 3.2.3 Forfeiture of gains from such activities may also be applied by the court.
 - 3.2.4 In determining penalties, each CEM to each recipient can be a separate offense.
- 4.0 Other Protections for CEM Recipients
- 4.1 False or Misleading Transmission Information Is Prohibited. §5(a)(1). The “From” line must accurately identify the Sender of the CEM. Header Information must accurately identify the computer that sent the CEM.
- 4.2 Deceptive Subject Headings are Prohibited. §5(a)(2).
- 4.3 Inclusion of a Functioning Return Address is Required. §5(a)(3). This is the mechanism by which a Recipient may reply to request that no further CEM be sent from that Sender. It must remain functional for 30 days after each CEM is sent.
- 4.4 Ten days after receiving an objection, CEMs cannot be sent to a Recipient. §5(a)(4).
- 4.5 Identifier, Opt-Out and Physical Address. §5(a)(5). Each CEM must contain clear and conspicuous identification that it is a solicitation, a notice to opt-out of receiving more CEMs from the Sender, and a valid physical address of the Sender.
- 4.6 The Act has provisions for Aggravated Violations if Address Harvesting or Dictionary Attacks are used in relation to CEMs. §5(b).
- 4.7 Warning Labels Must Be Placed On CEMs Containing Sexually Oriented Material. §5(d).
- 4.8 Exceptions. Applies to many offenses described above.
 - 4.8.1 Prior Affirmative Consent.
 - 4.8.2 Transactional or Relationship Messages. §3(2)(B) and §3(17). This is not a CEM.
- 4.9 Third Party may be responsible for False Transmission Information if Third Party owns 50% or more of violator, or if it knew of violation, or derived economic benefit from CEM promotion. §6(b).
- 5.0 Enforcement §7
- 5.1 Federal Trade Commission. In general, FTC will enforce CAN-SPAM Act of 2003. Other regulatory agencies may be involved jointly with FTC.
- 5.2 States. Sections of Act may be enforced by State Attorneys General. The Act allows States to obtain statutory damages, up to a \$2,000,000 limit, along with attorneys fees.
- 5.3 Internet Access Providers. §7(g). This term is broader than “ISP”, and may include corporate employers. There are also provisions for statutory damages, up to \$1,000,000, and attorneys fees.
- 5.4 No Private Right of Action.
- 5.5 Rewards. §11. The Act requires the FTC to develop recommendations to permit rewards to anyone who provides information regarding violations of the Act.

- 5.5 Do-Not-Email-Registry. §9. The Act also requires the FTC to report to Congress Committees on the feasibility of creating a nationwide “Do Not Email” Registry.
- 6.0 Reaction to the Act
The CAN-SPAM Act of 2003 has received less than a favorable review. This Act is not viewed as signaling the end of UCEs - SPAM.
- 6.1 Business Week Online, 1/7/04. See Exhibit B, attached.
http://www.businessweek.com/technology/content/jan2004/tc2004017_2996_tc078.htm .
- 6.2 Spamhaus.org. <http://www.spamhaus.org/news.lasso?article=150> .
- 6.3 New business opens in response to Act. See Exhibit C, attached.
<http://www.internetnews.com/IAR/article.php/3297891> .
- 7.0 Resources - Web Sites and More.
- 7.1 Spam Laws - Federal and State. <http://www.spamlaws.com/federal/108s877.html> .
- 7.2 Gardner, Carton & Douglas Web site. www.gcd.com . See Exhibit D, attached.
- 7.3 Federal Trade Commission: www.ftc.gov .
 - 7.3.1 Send Spam to FTC’s Spam collector: uce@ftc.gov .
- 7.4 Electronic Privacy Information Center. www.epic.org . Has a searchable database.
- 7.5 Wired News - CAN-SPAM.
http://www.wired.com/news/business/0,1367,62020,00.html?tw=wn_tophead_3 .
- 7.6 PC World - CAN-SPAM. <http://www.pcworld.com/news/article/0,aid,114363,00.asp> .

CorpLaw Associates LLC is a law firm of experienced business attorneys who deeply understand their clients’ businesses and who use best practices to achieve their clients’ business goals. The firm provides full support for businesses. For clients who need on-site legal help, CorpLaw is one of only a few firms that specializes in this model. Our mailing address is CorpLaw Associates LLC, 400 Central Avenue, Suite 150, Northfield, Illinois 60093. We can be contacted at 847.784.1300 or at firm@corplaw.com. Our web address is www.corplaw.com.