Spam is Not Delicious – An Update on the CAN-SPAM Act of 2003

Charles R. B. Stowe*

Abstract

The unsolicited commercial communication via email is perhaps the most effective and cheapest of all marketing strategies. The result is that millions of emails are cluttering up inboxes. Other than unsolicited telephone calls, there is no single political issue that has garnered such bi-partisan support as attempts to legislatively curtail the use of spam. The result is a plethora of state legislation and, more recently, the Can-Spam Act of 2003 that that pre-empts state law. When this topic was first researched for presentation at the September 2003 ACET conference, the federal law was not included because there were several competing versions working their way through the legislative process. This paper is not based on the September 2003 ACET presentation titled "SPAM is not Delicious" but is an expansion and updating to provide insight on a new federal law, the CAN-SPAM Act of 2003. This paper briefly outlines the recent federal legislation and provides a timetable of when federal agencies will have to submit proposed regulations to enforce the intent of Congress. Readers should beware that the entire anti-spam effort is truly a work-in-progress that may require years before the legal landscape is fully defined. Ultimately, because the internet is truly a global institution, the United States will have to negotiate international agreements with other jurisdictions because unscrupulous spammers will simply transfer their operations to other countries beyond the jurisdictional reach of the United States. Meanwhile, legitimate U.S. companies need to develop an understanding of Can-Spam Act of 2003 and related legal issues.

Introduction

The huge growth of the use of email and the corresponding growth of unsolicited commercial email traffic is literally filling email inboxes to a point where employees and email users are wasting hours deleting messages. With approximately 140 million Americans using email regularly, the political pressure has resulted in state laws being enacted to deal with the barrage of emails (Senate Report).

A brief overview of the provisions of the Can-Spam Act of 2003 and a brief presentation of the timetable for agencies to submit proposed regulations consistent with the intent of the act provides a helpful guide to the future issues that courts may have to contend with. Included in this brief overview is an outline of some of the criticisms of the act and how some commentators view the consequences of this legislation on the use of email for marketing purposes. With the passage of the federal law, web-based organizations that market products or services through email will have to devote resources to monitoring federal agencies and cases over the enforceability of the new law.

* Charles R. B. Stowe MBA, JD, Ph.D, Professor, Sam Houston State University, email fin_crs@shsu.edu

The Scope of the Problem

Estimates show that as much as 48% of all email transmitted on the internet is now spam, up from twenty two percent in 2003 (Taylor). According to a U.S. Senate report, "more than 2 trillion spam messages are expected to be sent over the Internet this year, or 100 times the amount of direct mail advertising pieces delivered by the U.S. mail last year." (Senate). Given the cost of using even bulk mail, there is no question as to why marketers prefer using email which is practically free. An FTC study presented in May 2003, found that two-thirds of spam contains fraudulent, misleading, or objectionable content (Garcia). Almost everyone using email has been solicited by merchants of various organ enlargement products (for both sexes), drugs (particularly Viagra), so-called business opportunities, solicitations for fake charitable causes and lures to websites that may contain viruses, spy ware, or other intrusive computer codes. Even more alarming is the invasion of worms or computer viruses that may enter when a message is opened. A study from the European Union reported that "spam cost Internet subscribers worldwide $9.4 billion each year," and "research organizations estimate that fighting spam adds an average of $2 per month to an individual's internet bill (Senate Rep.)." There are estimates that the cost to U.S. businesses resulting from the spam invasion exceeded $10 billion in 2003 with $4 billion being attributed to productivity losses from time wasted screening unwanted email. The remaining $6 billion of expenditures has been traced to network system upgrades, unrecoverable data, and increased personnel costs (Senate).

The popularity of spam may be attributed to its negligible cost as compared with other media. A full color, graphically exciting email containing video and sound clips and links to elaborate websites may be sent for far less than by mail. The estimated cost to the spammer has been estimated at $320 per million messages or $.00032 per email (Vaknin). Web mailing services offer millions of addresses for pennies each and there are no postage fees, printing costs, or handling costs. Low cost is one attraction but the real lure is that spam works! A 2003 survey by the Direct Marketing Association (DMA, showed that email solicitations drew about 46 million Americans to buy products and services last your ($7.1 billion in sales) of which 11 million of them in response to advertisers previously unknown to the purchaser (Direct Marketing Association).

The Pre-emption of State Laws

The federal law pre-empts state legislation against spam. By the time Congress decided to take action to regulate spam, some 34 states including Texas had passed their own statutes. From a practical perspective, many of the state laws could not be effectively enforced for a number of reasons. The problem of asserting jurisdiction poses both a legal and practical challenge. Much of the offensive spam does not contain traceable addresses. Determining the address of the real sender is a technical problem. If the address is valid, the issue is whether the alleged offender has a legally meaningful contact with the state so as to permit the state courts to assert their jurisdiction.

Another practical barrier to the enforcement of state laws against spammers is that many states lack the organizations and technical capabilities to track down spammers. With technical resources being absorbed by the war against terrorists and state-budgets

being cut, it is not likely that states would create and properly fund prosecutors to go after spammers (unless the issue concerns the protection of children).

A good example of state action against an alleged spammer promoting pornography was the announcement of the arrest of Jeremy Jaynes. Jaynes operates under the pseudonym "Gaven Stubberfield." According to the anti-spam organization Spamhaus, Stubberfield was ranked number 8 on the group's top 10 spammers list for November 2003 for offers of pornography and "get rich quick" offers. The Virginia Attorney General Jerry Kilgore made the announcement of the charges at AOL headquarters citing that "falsification (of e-mail headers or routing information) prevents the receiver from knowing who sent the spam or contacting them through the 'from address' of the email … which makes this e-mail a crime in Virginia (Borland).

Some states laws were written to provide ordinary citizens with the right to launch a private lawsuit against violators. However, during the legislative process, this right was often diluted by the realities that individuals seeking legal redress would end up spending far more than they would ever have the hopes of recovering. In Texas, for example, the anti-spam law permitted aggravated private citizens to sue spammers, but their recovery was limited to the lesser of "$10 per email received or $25,000 for each day an unlawful message is received."(Saba). While the individual would be able to also recover their attorney's fees, the law specifically exempted violators from being sued as a class action. The result is that few attorneys would have much incentive to represent a complainant. In passing the federal law, Congress was obviously persuaded that the issue of spam required a national solution due to some of the factors mentioned above.

Survey of the Act

The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, hereinafter referred to as the CAN-SPAM Act of 2003, was passed without dissent by the House on December 8, 2003 and President Bush signed the Act into law on December 16, 2003. Section 2 of the Act contains Congressional findings and policy. The findings reflect the following:

> (1) that electronic mail has become an extremely important and popular means of communication…
> (2) that the convenience and efficiency of electronic mail are threatened by the extremely rapid growth in the volume of unsolicited electronic mail …
> (3) the receipt of unsolicited commercial electronic mail may result in costs to recipients who cannot refuse to accept such mail and who incur costs for the storage of such mail…
> (4) The receipt of a large number of unwanted messages also decreases the convenience of electronic mail…
> (5) Some commercial electronic mail contains material that many recipients may consider vulgar or pornographic in nature…
> (6) The growth in unsolicited commercial electronic mail imposes significant monetary costs on the providers of Internet access services, business, and educational and nonprofit institutions that carry and receive such mail…(15 USCA Section 7701).

The statute notes that many senders purposefully disguise the source of the mail, they purposefully use misleading titles to induce people to read the messages, and that many senders use computer programs to gather large numbers of electronic mail addresses on an automated basis from internet websites or on-line services where users must post their addresses. Congress acknowledged that many States have enacted legislation to reduce unsolicited email, but since electronic mail addresses do not specify a geographic location, it can be extremely difficult for law-abiding businesses to know with which of the disparate statutes they are required to comply. Furthermore, Congress acknowledged that "the development and adoption of technological approaches and the pursuit of cooperative efforts with other countries will be necessary as well."(15 USCA Section 7701).

The Can-Spam Act does not ban spam. However, it does specifically prohibit several annoying practices. For example, using a computer program to enter another's computer to intentionally transmit multiple commercial email messages from or though such computer is illegal under the new law. "Materially" falsifying header information in multiple commercial electronic mail messages or using information that 'materially falsifies the identity of the actual registrant for five or more mail accounts, or falsely representing oneself to be the registrant or the legitimate successor in interest to the registrant of 5 or more Internet Protocol addresses (spoofing) is now illegal. Congress provided for both civil and criminal penalties. Penalties include a fine and prison up to five years if the offense was committed in furtherance of any felony under either federal or state law. Congress defined multiple transmission as "more than 100 electronic mail messages during a 24 hour period, more than 1,000 electronic mail messages during a 30-day period, or more than 10,000 electronic mail messages during a 1 year period" (18 USCA Section 1037).

The Act represents a compromise between those who would ban all unsolicited email and those who prefer no regulation at all. The Act permits businesses and marketers to send unsolicited email to anyone with an email address so long as they have identified themselves clearly, do not use fraudulent headers and honor consumer requests to cease sending them unsolicited commercial e-mail. The act makes it illegal to use false return addresses, to use 'dictionary attacks' or electronic harvests of e-mail addresses from unsuspecting email users. And marketers are now prohibited from using false or misleading subject lines to trick recipients into reading their messages.

All commercial emails will have to provide for an "opt out" provision permitting recipients to click back a message that would remove them from future mailings. The law provides that there should be no transmissions after 10 days after objection. Marketers will have to make sure that their messages all have an identifier that the message is an advertisement or solicitation, a "clear and conspicuous opportunity to decline to receive further messages" from the sender, and a valid physical postal address of the sender. Congress granted the Federal Trade Commission the right to modify the 10 day rule after considering the purposes of the opt out provision, the interests of recipients of email, and the burdens imposed on senders of lawful commercial email (15 USCA 7704).

Congress provided that the Federal Trade Commission will have the lead in the enforcement of the CAN-SPAM Act, but it granted enforcement powers to other federal agencies. For example, the Office of the Comptroller of the Currency will enforce the

law against national banks that they normally regulate. Similarly, the Federal Reserve System will oversee their member banks, and the Federal Deposit Insurance Corporation will oversee their banks that are not members of the Federal Reserve System or covered by the Office of the Comptroller of the Currency. The Securities and Exchange Commission will regulate brokers, dealers, investment companies and investment advisers. The normal regulators of insurance companies, either federal agencies or state boards of insurance will have enforcement powers concerning electronic marketing activities of the companies they normally regulate as will the Federal Communications Commission (broadcast industry), Secretary of Transportation (air or foreign air carriers), and Farm Credit Administration with respect to any Federal land bank, Federal land bank association, Federal intermediate credit bank or production credit association. The Act also gives civil enforcement powers to the states including injunctions to stop further marketing activities, to sue for damages on behalf of residents of the State for the actual monetary loss suffered by such residents.

Obtaining a court order to stop marketing efforts will not require a showing that the defendant knowingly violated the law. This means that the state in a civil action requesting either or both an injunction and monetary damages does not have to prove a particular state of mind on the part of the defendant. The statutory limitations for damages without a showing of state of mind is limited to the number of violations times $250 with a cap of $2,000,000. However, the court may increase a damage award to an amount equal to not more than three times if the court finds that the defendant committed the violation willfully and knowingly. In addition, courts are authorized to award attorneys fees to the State for the costs of their prosecution.

In the event a state prosecutor files an action against an alleged offender, the Federal Trade Commission has the right to intervene in the action and move the trial to a Federal District Court. However, this provision does not limit a state from initiating and conducting investigations, administering oaths and taking 'sworn testimony', or compelling the attendance of a witness or the production of documentary and other evidence. But if a federal agency has already begun a civil suit or and administrative action for violation of the Act, no official or agency of a State may bring an action. It is clear that Congress welcomed State involvement in the enforcement of the act, but wanted federal agencies to have the right to intervene on individual cases. Other than ISPs, there is no private right of action under the federal statute.

Directed Reports from the FTC

Within six months of the CAN-SPAM Act's passage, the Federal Trade Commission must inform Congress of a plan and timetable for the creation of a 'do-not-email me" list along with an explanation of how the list will be implemented. Within 9 months of passage of the act, the Federal Trade Commission must issue a report to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Energy and Commerce that proposes a system to reward those who supply information about violations of the act. Congress asked the FTC to design procedures whereby the FTC could grant a reward of not less than 20 percent of the total civil penalty collected for a violation of the act to the first person that identified the person in violation of the Act and supplies information leading to the successful

collection of a civil penalty by the Commission. By January 2005, the FTC must issue regulations defining the relevant criteria for determining whether a communication constitutes a "commercial electronic mail message." Unlike many state statutes, the federal law does not exempt e-mails to recipients with whom a sender has a prior or existing business relationship (Freeman). Eighteen months after the passage the FTC must set forth a plan for requiring commercial email to be identifiable from its subject line by means of compliance with Internet Engineering Task Force Standards, the use of characters “ADV” in the subject line or some other identifier or objection to that proposal if the FTC is against it.

And not later than 24 months, the FTC and the Department of Justice and “other appropriate agencies” shall submit a report to Congress that provides a detailed analysis of the effectiveness and enforcement of the provisions of this Act and the need (if any) for the Congress to modify such provisions (15 USCA Section 7709). This report will have to provide an analysis on the extent to which technological and marketplace developments have affected the practicality and effectiveness of the Act. The report will have to provide an analysis and recommendations concerning how to address commercial email that originates or is transmitted through to facilities or computers in other nations, and an analysis with recommendations concerning options for protecting consumers, including children, from the receipt and viewing of email that is obscene or pornographic (15 USCA 7709).

The Federal Communications Commission has 270 days from the date of enactment to promulgate rules to protect consumers from unwarranted mobile service commercial messages. The rules must allow consumers at the time they subscribe to wireless services the option to decline receiving mobile service commercial messages from the provider and in all future billing statements.

Criticism of the Act

Those who were looking for a law to make all spam illegal will be disappointed by the CAN-SPAM Act. Whether it is even constitutionally possible to enact a complete ban against spam is questionable. What Congress did was draw a legal analogy between the internet and the U.S. Post Office and between spam and "junk" mail. To have written a law banning all unsolicited mail would have resulted in a constitutional challenge based on the first amendment. There are Supreme Court opinions that recognize that free speech does include business communications though such protected commercial free speech is subject to regulation to prevent fraud. For example, in overturning a state bar rule banning all attorney advertising, the U.S. Supreme Court has ruled that commercial speech which services individual and societal interests in assuring informed and reliable decision making is entitled to some First Amendment protection (Virginia Pharmacy Board v. Virginia Consumer Council). The U.S. Supreme Court has also ruled that government restrictions on commercial free speech are enforceable if the regulation “(1) asserts a substantial interest in support of its regulation; (2) establishes that the restriction directly and materially advances that interest; and (3) demonstrates that the regulation is " 'narrowly drawn’” (Central Hudson Gas & Electric Corp. v. Public Service Commission of N.Y.).

In passing Can-Spam Act of 2003, Congress avoided certain protests by political, religious and non-profit groups by exempting their email communications. This exemption avoids a certain constitutional challenge to free speech by those groups.

Other critics cite the lack of a mandated 'do not send' directory much like the "do not call directory." However, the Act does require that the FTC come up with firm proposals on creating such a system. Congress may well have been concerned that the constitutionality of the "do not call" program has not been thoroughly tested along with a recognition of the technical difficulties for the implementation of such a program. The language of the statute asks the FTC to tackle the questions related to setting up a national 'don't send me' directory. Whether the U.S. Supreme Court will uphold the enforceability of government created 'do not call' or 'do not send' directories is uncertain at this writing. However, the Act is on stronger footing in banning false return addresses, the piracy of email addresses, and misleading subject lines. These restrictions have been upheld in constitutional challenges to government regulations of junk mail. Government policy is not to end junk mail but to prevent fraud. The CAN-SPAM Act initially protects legitimate use of email for solicitation, but in requiring traceable email addresses and physical addresses of spammers and in banning computer programs that harvest names from unsuspecting computers to increase the mailing, the Act may well serve as a deterrent to illegitimate spammers.

Some complain that the Act does not allow individuals to sue spammers. However, the law directs the FTC to propose a set of procedures that would provide a bounty or reward for those who turn in violators. While it is hard to predict, it may well be that the bounty or reward may be a more powerful incentive than the right to private action. Certainly, the complainants would not be required to hire attorneys and give up part of their reward under a bounty system. The Center for Democracy and Technology is critical that the law did not include a private right of action according to Ari Schwartz, associate director (Porter).

FTC Chairman Timothy Muris has stated his concern that the FTC does not have the funding nor the staff or technical expertise to create and monitor the "do not send" directory program (Trussell). Chairman Muris has also expressed concern that since email addresses are not public knowledge, a national directory of 'do not send' requests could be broken into by aggressive hackers resulting in more spam (Trussell). When the FTC provides their report on creating a national directory, this issue will again be debated before committees of Congress.

A First Step

The passage of the Can-Spam Act of 2003 is not a resolution of how government will tackle the problem of spam, but rather, a declaration that the issue will receive attention from the Federal Trade Commission in what will be a series of new regulations and initiatives. There are major issues to be resolved such as what actually constitutes spam, how spam will be identified to readers in the subject line, and exactly how legitimate marketers can safely use spam. With some fairly serious penalties for abuse, some illegitimate spammers will have to go overseas to operate their scams, but their exodus may be short lived as the federal government is instructed to pursue international solutions to the spam issue. The problem for legitimate marketers is to consider the

implications of the new law on current operations. The first consideration is to be sure that the communications contain a physical address which is a new requirement. A second issue is to examine who will actually send the emails and to whom. The use of a third party to send out spam will not isolate or protect the principle from liability if the email service uses illegal techniques to develop mailing lists (such as computer programs that harvest names out of unsuspecting PC owners). Therefore, marketers should review their contracts and further restrict the types of email strategies that had been unregulated. The 'opt out' provision of the law means that 'good faith' efforts must be made to honor those requests and not to misuse the return reply as merely a confirmation of receipt of an email. Keeping abreast of FTC rules and regulations should be a formal part of any marketing group's responsibilities. And finally, commercial entities should continuously review their email marketing strategies for compliance with the major provisions of the law. The Can-Spam Act legitimizes the use of email for distributing advertising messages while at the same time imposes some fairly serious penalties for those who might abuse this manner of communication.

References

Borland, John "Virginia Files Felony Spam Charges" *CNET News*, December 11, 2003, 3:11 PM PST at http://news.com.com/2100-1028_3-5120673.

Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n of N.Y., 447 U.S. 557, 100 S.Ct. 2343, 65 L.Ed.2d 341

Direct Marketing Association, Press Release, "DMA Statement Re: Operation Slam Spam (August 22, 2003) www.the-dma.org/cgi/disppressrelease?article=484++++++ as cited in Porter, Rebecca "Smothered by Spam," Trial, February, 2004, Association of Trial Lawyers of America.

E-Commerce Law and Strategy, "Anti-Spam Legislation is Signed into Law", Vol. 20, No. 9, January 14, 2004, ALM Properties, p. 5

Freeman Jr., D. Reed "Can Spam Act: A Compliance Challenge" *E-Commerce Law and Strategy*, Vol. 20, No. 9, p. 1.

Garcia, Beatrice E. "Spam Haters; More is Coming to Your Computer, A Research Firm Says…" *Miami Herald*, Sept. 30, 2003, at 1 available at 2003 WL 62533689 cited in Trussell, Jacuelyn "Is the CAN-SPAM Act the Answer to the Growing Problem of Spam?" *Loyola Consumer Law Review* 2004.

Porter, Rebecca "Smothered By Spam," Trial, February, 2004, Association of Trial Lawyers of America

S. Rep. No. 108-102, 2003 WL 21680759 at *2 (July 16, 2003).

Saba Jr., John D. “eProclamation: No More Spam in Texas” Texas Bar Journal, September, 2003.

Taylor, Humphrey “Large Majority of Those Online Wants Spamming Banned” Harris Interactive, Jan. 3, 2003 at http://www.harrisinteractive.com/harris_poll/index.asp?PID=348

Trussell, Jacquelyn "Is the Can-Spam Act the Answer to the Growing Problem of Spam?" *Loyola Consumer Law Review, Vol. 16, 2004, p 175.*

Vaknin, Sam “The Economics of Spam” *United Press International* July 23, 2002 at http://www.upi.com/view.cfm?StoryID=20020723-121152-3651r) cited in Edwards, Michael B. “A Call to Arms: Marching Orders for the North Carolina Anti-Spam Statute” *North Carolina Journal of Law and Technology*, Fall 2002.

Virginia Pharmacy Board v. Virginia Consumer Council, 425 U.S. 748, 96 S.Ct. 1817, 48 L.Ed.2d 346.