JIST 2(1) 2005

The Information Institute

Journal of Information Science and Technology

www.jist.info

New Federal Anti-Spam Law is Not Enough

Jordan M. Blanke

Stetson School of Business and Economics
Mercer University, 3001 Mercer University Drive
Atlanta, GA 30341
(678) 547-6313, (678) 547-6160 (FAX)
blanke_j@mercer.edu

Abstract

A new federal anti-spam law took effect in the United States on January 1, 2004. It will do very little to decrease the volume of spam, especially in the near future. Many states now have less protection against spammers than they had before the new law took effect. This article reviews the existing problems with spam, examines the new federal law, discusses why state laws have become less important, and explores some options for the future.

Keywords: spam, anti-spam, CAN-SPAM Act, federal legislation, preemption

Introduction

The costs associated with bulk unsolicited commercial email, or spam, have increased dramatically. Recent studies estimate that in 2003 spam cost U.S. businesses anywhere from $10 to $87 billion (Hansell, 2003a). One study puts the cost of spam worldwide at $20.5 billion for 2003 and predicts that the amount will increase to $198 billion by 2007 (Swartz, 2003). While it

is difficult to determine an exact amount, one study found that an average employee receives 13.3 spam messages and spends about 6 ½ minutes managing the spam each day. This means that companies lose about 1.4 percent of each employee's productivity, or the productivity of one out of every 72 employees. This costs about $874 per employee each year (Hansell, 2003a; Swartz, 2003).

The volume of spam has reached epidemic proportions and continues to grow. America Online ("AOL") discards about 80 percent of the 2.5 billion messages sent daily to its subscribers (Hansell, 2003a). In a statement prepared by the Federal Trade Commission ("FTC") for a Senate subcommittee studying spam, it was reported that AOL "recently blocked an astonishing 2.37 billion pieces of spam in a single day" (Prepared Statement, 2003). Spam now accounts for 40 to 60 percent of total email traffic ("President Bush," 2004). One spam-filtering company estimates that the percentage of spam in email rose from 42 percent in February 2003 to 58 percent in December 2003 and to 60 percent in January 2004 despite the enactment of the new federal Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM Act," 2003), which became effective on January 1, 2004 (Olsen, 2004c; Ward, 2004).

The FTC Report

In its Prepared Statement (2003), the FTC concluded that the two main problems associated with spam were the deception and fraud characterizing the vast majority of spam, and the Internet infrastructure problems flowing from the sheer volume of the spam. As the federal government's main consumer protection agency, the FTC's mission is to protect against unfair or deceptive acts affecting commerce. Accordingly, most of the Prepared Statement addressed fraudulent and deceptive practices related to spam.

The FTC described three research projects it conducted. In the first, the "Remove Me" surf, the agency set up dummy email accounts and identified over 200 messages that purported to allow recipients to remove themselves from spam lists. It found that 63 percent of the supposed links failed to work.

In the "Spam Harvest" project, the agency posted email addresses in various locations on the Internet and studied how often those addresses ended up on spam lists. It found that 100 percent of addresses posted in chat rooms received spam, with one address receiving spam only eight minutes after posting. It also found that 86 percent of addresses posted in newsgroups or on Web sites received spam, as did 50 percent of addresses given to free personal Web page services.

In the "False Claims in Spam" study, the FTC examined 1000 pieces of spam received by consumers and forwarded to the agency, received pursuant to the "Spam Harvest" project, and received on FTC computers. It found that over 40 percent of the spam contained some sort of false claim in its content. About 55 percent of the spam contained offers for business or investment opportunities, adult-oriented products or services, or credit card, mortgage,

insurance or other financial services. Of these messages, 90 contained false claims. The study found that a third of the spam contained falsities in the "from" line and 22 percent contained falsities in the "subject" line. Overall, 66 percent of the spam contained at least one fraudulent or deceptive claim.

The FTC discussed its "Spam Forum," a public hearing held in April and May of 2003. It noted that participants included consumers, Internet Service Providers ("ISPs"), law enforcement authorities, marketing services, bulk email marketers, anti-spammers, and retailers and manufacturers. The agency reported that three themes dominated the discussions: 1) that the volume of spam is increasing sharply; 2) that spam imposes real costs; and 3) that spam is an international problem. It concluded that solving the spam problem would not be easy or quick, and would require an integrated effort involving technological, legal and consumer action. It asked for legislation expanding the agency's authority to act to combat spam.

The Organisation for Economic Co-operation and Development ("OECD") held a "Workshop on Spam" in February of 2004 in Belgium. One of the conclusions of the Workshop was that "[t]here is no single solution to the problem of spam. A multi-disciplinary approach focusing on technical, regulatory and self-regulatory measures as well as consumer and business education is necessary in order to develop sustainable solutions to spam." (Report of the Workshop, 2004).

Legislative Efforts

State Law

In 1997 Nevada became the first state to enact legislation specifically targeted at spam (Magee, 2003). California, Washington and Virginia followed shortly thereafter. Today, at least 36 states have statutes that regulate spam. The approaches taken by the states vary greatly (Blanke, 2004). About half of the states with anti-spam laws require the inclusion of an "ADV:" label in the subject line. About half require an "ADV:ADLT" label for sexually explicit or adult-oriented material. Two thirds of the states require an "opt-out" mechanism for those wishing to be removed from future mailing lists. Slightly fewer require inclusion of a valid and functioning reply email address.

Almost all of the states with anti-spam legislation prohibit the falsification of transmission or routing information in spam. Most of them ban the use of third-party addresses or domain names without the consent of the third party. This is particularly important since much spam employs "spoofing" or other techniques that make it appear that the message is sent from a legitimate source. Two of the states that have attempted to aggressively fight spam, California and Virginia, prohibit the transmission of spam that violates the policies of an ISP.

Most states permit civil suits to be brought against spammers by either individual recipients of spam or by ISPs. Most of these states allow the plaintiff to pursue actual damages or specified statutory amounts, varying from $10 to $1000 per message, plus attorney fees and costs. Most states

also permit actions to be brought by the state attorney general on behalf of its citizens.

About half of the states with anti-spam laws provide for misdemeanor criminal sanctions, with about seven of those also including felony criminal sanctions. Virginia law makes it a felony to send certain spam if the volume exceeds 10,000 recipients in a 24-hour period, 100,00 recipients in a 30-day period or 1,000,000 recipients in a 1-year period (Virginia Code Annotated, 2003).

Within the last year, different types of plaintiffs filed lawsuits in several states using a variety of these laws. In Washington, an individual recipient of spam sued a telemarketer for sending him hundreds of unsolicited emails ("Man Sues Firm," 2004). AOL filed five separate actions in Virginia against alleged spammers ("AOL Files Suit," 2003), and Microsoft filed suit in New York (Hansell, 2003c). Attorneys general in California, New York and Missouri also brought actions against spammers (Grady, 2003; Hansell, 2003c; "Missouri AG Files Lawsuit," 2003).

Probably the most significant development involving state law, however, occurred in September of 2003 when California passed the toughest anti-spam law to date (California Business & Professional Code, 2004). It was the first law to take an "opt-in" approach to spam, prohibiting any unsolicited commercial email. Unlike most state laws that require a recipient to "opt-out" by requesting that no more email be sent, this law prohibited email from being sent to anyone who had not previously requested it. The law also authorized civil suits by private individuals receiving such unsolicited email, and provided for statutory damages of up to $1,000 per message. The law was to take effect on January 1, 2004 (Hansell, 2003b).

Federal Law

Legislation seeking to restrict email was proposed to Congress as early as 1991, although it was not until the last several years that efforts to pass such a bill became intensified (Magee, 2003). The 108th Congress had no fewer than nine separate bills introduced to the House and Senate, before finally passing the CAN-SPAM Act of 2003. The final impetus to pass the CAN-SPAM Act came, ironically, from marketing groups that had long opposed federal legislation (Olsen, 2003). Because of the newer, stricter laws being enacted in states like California and Virginia, marketing groups, who had previously opposed any federal legislation, began supporting bills like the CAN-SPAM Act. The main reason for this support was the likelihood that a federal law would preempt the tougher state laws (Archie, 2003; Freeman, 2004).

The transparency of this support had not gone unnoticed. Back on the first day of the FTC's Spam Forum in April 2003, a group representing the attorneys general of 44 states and the District of Columbia announced that it would not support either the CAN-SPAM Act or one of the other proposed bills before Congress (McGuire, 2003). The group feared that passage of such a law would weaken consumer protections in many of the states that

already had passed anti-spam laws. It opposed the federal bills not only because they would preempt tougher state laws already on the books, but also because the bills did not provide for private actions by individuals.

Furthermore, criticism of the proposed CAN-SPAM Act came from the Chairman of the FTC, Timothy J. Muris. In a speech in August of 2003, while Congress was considering passage of the bill, Muris warned that the Act might do more harm than good and might actually make it more difficult for the agency to pursue spammers (McCullagh, 2003). Muris reportedly told one anti-spam group that if the bill were passed, the FTC would probably continue to pursue spammers under pre-existing laws (McCullagh, 2003).

Despite protests that the CAN-SPAM Act might weaken the laws with which the FTC, state attorneys general, and private citizens could battle spammers, Congress passed the law, the President signed it, and it became effective on January 1, 2004.

International Law

As in the United States, legislation is being proposed and passed around the world. The European Union adopted the Directive on Privacy and Electronic Communications (Directive, 2002). Article 13(1) of the Directive takes an "opt-in" approach and prohibits e-mail to anyone who has not given prior consent. European countries are beginning to enact anti-spam legislation. Other countries, including Australia, Israel, South Korea and Taiwan, have proposed or adopted new laws.

Countries are also beginning to cooperate more with each other in order to address the problem at more global levels. For example, the FTC recently reached an agreement with Great Britain and Australia, permitting agencies in the three countries to share information in order to more effectively fight spammers.

The CAN-SPAM Act of 2003

Generally the CAN-SPAM Act regulates the transmission of "commercial electronic mail messages." These are defined as electronic mail messages whose "primary purpose" is "the advertisement or promotion of a commercial product or service" (CAN-SPAM Act, 2003). The definition excludes "transactional or relationship" messages. These messages include correspondence involving prior transactions between the parties, such as sales of goods or services, warranty information, product recalls, and employee benefit plan information.

The Act prohibits false or misleading transmission information and deceptive subject headings. These prohibitions regulate the "from" and "subject" lines of commercial email. The Act requires that every commercial email contain a valid physical postal address of the sender, and a functioning return email address, to which the recipient may communicate his desire to opt-out of receiving any further emails from the sender. The Act requires the

sender to honor such an opt-out request within 10 days. The Act also prohibits the use of "address harvesting," "dictionary attacks," and any other automated means to compile or generate a list of email addresses.

The Act provides for criminal sanctions for those who knowingly

1. initiate the transmission of multiple commercial emails from a computer without authorization,
2. relay or retransmit multiple commercial emails with intent to deceive or mislead recipients or ISPs as to the origin of such emails,
3. initiate the transfer of multiple commercial emails containing materially falsified header information, or
4. register 5 or more email accounts or 2 or more domain names that materially falsify the identity of the actual registrants (CAN-SPAM Act, 2003).

"Multiple" is defined as more than 100 emails during a 24-hour period, more than 1,000 emails during a 30-day period, or more than 10,000 during a 1-year period. These limits are more restrictive than those in the Virginia statute. Penalties include fines and imprisonment of up to 1, 3 or 5 years, depending upon the severity of the violation. Factors that may influence the severity include registration for 20 or more falsified email accounts or 20 or more falsified domain name registrations, or the transmission of more than 2,500 emails within a 24-hour period, 25,000 within a 30-day period, or 250,000 within a 1-year period.

Enforcement of the Act

Violations of the Act are deemed to be unfair or deceptive acts or practices, and therefore, enforceable by the FTC. Other federal agencies, such as the Federal Deposit Insurance Corporation, the Securities and Exchange Commission, and the Federal Communications Commission, are also authorized to enforce violations within the scope of their respective responsibilities.

The Attorney General of a state may bring a civil action on behalf of the citizens of that state in federal district court for violations of certain sections of the Act. The suit may seek actual damages or statutory damages in the amount of $250 for each unlawful email received, up to $2,000,000, plus attorney fees. In addition, treble damages may be awarded for willful violations

Internet service providers are also authorized to bring suit for violations of certain provisions of the Act. The suit may seek actual damages, or statutory damages of up to $100 per email that contains false or misleading transmission information, or up to $25 per email for other violations, up to $1,000,000, plus attorney fees. Treble damages may also be awarded for willful violations.

The Act does not authorize actions to be brought by private individuals, however. This is of particular significance because the Act specifically preempts most state laws that would authorize such suits.

Preemption

The CAN-SPAM Act preempts any state law that "expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message." It does not preempt state laws that "are not specific to electronic mail, including State trespass, contract, or tort law," or other state laws "to the extent that those laws relate to acts of fraud or computer crime." (CAN-SPAM Act, 2003).

Thus most of the provisions of the 37 anti-spam laws passed by states will probably be preempted (Olsen, 2004a). It will be interesting to see how much leeway states will be given to enforce state laws that prohibit "falsity or deception." While the Act appears to exempt such state law from preemption, the federal law itself certainly does pertain to these same false and deceptive acts. A spammer prosecuted under a state law would certainly claim that the federal law preempts such a provision. This issue will likely be tested in the near future.

State laws that are not specifically directed at spam will have a much better chance of surviving a preemption challenge. The Act excludes laws based in trespass, contract and tort law, as well as those relating to acts of fraud or computer crime. New York is one of the few states that has not passed an anti-spam law, but has aggressively pursued spammers under its general fraud provisions (Hansell, 2003c). The new federal law should not preempt these efforts.

Compliance So Far

Early reports about compliance with the new law are not promising. One email filtering company reported that, for the first week in January, spam accounted for 84 percent of all emails, up from 80 percent in mid-December (Hansell, 2004). Another email filtering company reported that for a 30-day period ending in February, only 3 percent of 10,000 random pieces of commercial email examined contained a valid postal address and an opt-out link, as required by the new law (Olsen, 2004c).

Even more disturbing are the efforts to evade the law by using perceived loopholes in the definitions of the Act. For example, one spammer has claimed that the "primary purpose" of his email was not commercial, but rather was "to deliver a 'crazy USA state law of the week' (in this case, a dubious notice that it is illegal in Massachusetts to put tomatoes in clam chowder)" (Ulbrich, 2004). Also, some spammers are including the required postal address and other notices in graphic images that are invisible to spam filters, but technically "included" in the email (Ulbrich, 2004).

The Future

Technology

As the FTC predicted in its Prepared Statement, the solution to the spam problem will be neither quick nor easy. It will involve changes both technological and legal in nature. Bill Gates recently predicted that, "Two years form now, spam will be solved" ("Gates: Spam to be Canned," 2004). Whether by incorporating new filtering mechanics into operating systems (Rubell, 2003) or by developing new "computational puzzles" to thwart automated spam transmissions ("Gates: Spam to be Canned," 2004), technology certainly will be involved in the eradication of spam.

The Law

During the next couple of years, we will undoubtedly see a number of cases brought under both state and federal laws. One recurrent issue certainly will be the extent of the preemption of state law by the CAN-SPAM Act. Other challenges will involve the scope and definition of the terms within the federal law. We will also see more international agreements as more countries resort to new legislation.

The most important legal developments, however, may be those initiated by the FTC. Under the CAN-SPAM Act, the FTC is required to make certain findings and recommendations within specified time periods. Within 120 days of enactment (January 1, 2004), the FTC is required to prescribe a plan to clearly identify commercial emails containing sexually oriented material. The agency has already begun the process of requiring such marks or tags (Olsen, 2004b). This labeling requirement will supercede those state laws that (were largely ignored and) mandated "ADV:ADLT" in the subject line of a sexually explicit or adult-oriented email.

Within 6 months the FTC is charged with developing a plan and timetable for the establishment of a nationwide Do-Not-E-Mail registry. Such a plan would presumably be similar to the Do-Not-Call list and would probably inspire some challenges under the First Amendment.

Within 9 months the FTC is required to submit to Congress a plan for rewarding private individuals who supply information to the FTC leading to the successful collection of civil penalties for violations of the Act. The reward would be not less than 20 percent of the civil penalty collected, and would presumably provide an incentive for reporting violations and a disincentive for violating the Act.

Within 12 months the FTC is required to issue regulations defining the relevant criteria for determining the "primary purpose" of an email. This will, hopefully, eliminate one of the perceived definitional loopholes in the Act.

Within 18 months the FTC must set forth a plan requiring commercial email to be identifiable by its "subject" line. This may or may not include the use of the "ADV:" label previously required by many states, but preempted by the Act.

Finally, within 24 months the FTC must report back to Congress on the

effectiveness and enforcement of the provisions of the Act. The report must specifically

1. analyze the "extent to which technological and marketplace developments" may have affected the "practicality and effectiveness" of the Act,
2. analyze and make recommendations about the international aspect of the transmission of commercial email, and
3. analyze and make recommendations about obscene and pornographic email (CAN-SPAM Act, 2003).

Conclusion

The passage of the CAN-SPAM Act is an important milestone in the fight against spam. However, it is not the end of the war. It is merely the beginning of a new battle that will be fought largely with rules to be determined by the FTC over the next couple of years and with new weapons designed by the prevailing technology of the time.

References

"AOL Files Suit Intending to Halt Spam Attacks," National Law Journal (25:79), April 28, 2003, p. B5.

Archie, J. C., "Spam Gets Canned," The Internet Newsletter, December 23, 2003.

Blanke, J., "Canned Spam: New State and Federal Legislation Attempt to Put a Lid On It," Computer Law Review and Technology Journal (8:2), Winter 2004, pp. 305-321.

CALIFORNIA BUSINESS & PROFESSIONAL CODE §§ 17529, 17538.45 (West Supp. 2004).

Controlling the Assault of Non-Solicited Pornography and Marketing Act (or CAN-SPAM Act) of 2003, 15 U.S.C.A. §§ 7701 - 7713 (2004).

Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37.

Freeman, D. R., "CAN SPAM Act: A Compliance Challenge," E-Commerce Law & Strategy, January 14, 2004.

"Gates: Spam to be Canned by 2006," CBS News.com, January 24, 2004.

Grady, B., "California Wins Its First Anti-Spam Judgment," USA TODAY, October 24, 2003.

Hansell, S., "Totaling Up the Bill for Spam," The New York Times, July 28, 2003a, p. C1.

Hansell, S., "California is Set to Ban Spam," The New York Times, September 24, 2003b, p. C1.

Hansell, S., "New York and Microsoft Expected to File Civil Suits in Spam Case," The New York Times, December 18, 2003c, p. C1.

Hansell, S., "Spam Keeps Coming, But Its Senders Are Wary," The New York Times, January 7, 2004, p. C1.

Magee, J., "The Law Regulating Unsolicited Commercial E-Mail: An International Perspective," Santa Clara Computer & High Technology Law Journal, (19:2), May 2003, pp. 333-382.

"Man Sues Firm Over Deluge of Unsolicited E-Mails," USA TODAY, January 6, 2004.

McCullagh, D., "Bush OKs Spam Bill - But Critics Not Convinced," CNET news.com, December 16, 2003.

McGuire, D., "States Object to Spam Legislation," The Washington Post, April 30, 2003.

"Missouri AG Files Lawsuits Under New Anti-Spam Law," USA TODAY, October 9, 2003.

Olsen, S., "Ad Groups Lobby for Antispam Law," CNET news.com, November 13, 2003.

Olsen, S., "California 'Disempowered' by Federal Spam Law," CNET news.com, January 22, 2004a.

Olsen, S., "FTC Proposes Adult Spam Labels," CNET news.com, January 28 2004b.

Olsen, S., "Study: Spammers Turning a Blind Eye to the Law," CNET news.com, February 10, 2004c.

Prepared Statement of the Federal Trade Commission on "Unsolicited Commercial Email" Before the Senate Committee on Commerce, Science & Transportation, 108th Cong. 13 (May 21, 2003).

"President Bush Signs Law to Can Spam," The Information Management Journal, January/February 2004, p. 17.

Rubell, P., "Technology Law and Practice: New Federal Law to Take Effect, But Will Spam Be Conquered?," New York Law Journal, December 23, 2003.

Report of the Workshop, Organisation for Economic Co-operation and Development Workshop on Spam, February 2-3, 2004.

Swartz, N., "The International War on Spam," The Information Management Journal, September/October 2003, pp. 18-24.

Ulbich, C., "Spam Travels Into Gray Area," Wired News, January 29, 2004.

VIRGINIA CODE ANNOTATED § 18.2-152.3:1 (MICHIE Supp. 2003).

Ward, M., "How to Make Spam Unstoppable," BBC News, February 4, 2004.

Author

Jordan "Jody" Blanke is a Professor of Computer Information Systems and Law at the Stetson School of Business and Economics at Mercer University in Atlanta. He earned undergraduate and graduate degrees in computer science from the State University of New York at Stony Brook and a law degree from Emory University School of Law. He has taught a wide

variety of courses in computer science, computer information systems, and law during his twenty years of college teaching. His areas of interests include privacy, copyright and trademark law, and human factors in design. He has recently published articles in the American Business Law Journal, the Fordham Intellectual Property, Media & Entertainment Law Journal and the Rutgers Computer & Technology Law Journal, and authored a chapter in the Social, Ethical and Policy Implications of Information Technology.