

Spam Canned Throughout the Land? Summary of the CAN-SPAM Act With Commentary

By Dan Fingerman

Published in the *Journal of Internet Law*
Volume 7, issue 8, February 2004, page 1

Dan Fingerman is an associate at **Mount & Stoelker, P.C.** in San Jose, California. Dan practices in the areas of intellectual property and business litigation, with experience in many technology areas such as computer hardware and software, semiconductor manufacturing, electronic design automation (EDA), memory devices, information systems, communication systems and protocols, digital imaging, electrical engineering, and optics. Dan earned his J.D. from the **Boston University School of Law** in 2003 and bachelors degrees in economics and political science from **Yale University** in 2000. Dan also writes a blog called **DTM :<|**, at www.danfingerman.com/dtm.

Introduction

The rise of the Internet brought the scourge of unsolicited commercial email (spam). The volume of spam has grown exponentially since the early 1990s, when non-academics and non-scientists first logged on in large numbers. Frustrated users drown in the flood of messages. Businesses and institutions are embarrassed when marketers hijack their servers and use them to send spam. Parents try in vain to shield their children from ubiquitous pornography advertisements.

Meanwhile, the economic burdens of spam rival the social ones. In paper-based "direct mail" campaigns, a response rate of one buyer per 100 mailings is often sufficient to break even. The cost of sending email is so much lower than the cost of sending paper mail that a rate of one buyer per 100,000 emails is likely to yield a profit. In other words, if 0.001% of spam recipients make a purchase, the advertising channel is funded for everyone. The cost of email only seems lower to the sender, however, because most of it is borne by the receiver and the receiver's Internet Service Provider (ISP).¹ Email users spend their valuable time dealing with spam, while ISPs pour resources into their networks to handle the ever-growing load.

Congress debated anti-spam legislation for five years without results, but we now have our first national anti-spam law. In October 2003 the Senate passed the CAN-SPAM Act, short for the "Controlling the Assault of Non-Solicited Pornography and Marketing Act." Some Congressional ping pong ensued, and the House and Senate adopted identical language in late November.² President George W. Bush signed the bill in mid-December.³ The new law took effect on 1 January 2004.

At its most basic level, the CAN-SPAM Act makes it *legal* to send unsolicited commercial email so long as its source and nature are not disguised, resources were not misappropriated to send it, and consumers have a meaningful way to avoid receiving future mailings. The Act is a reasonable first step toward reducing spam, although it arguably comes five years too late. Congress has made a genuine effort not to be heavy handed with the rights of marketers while giving the rest of us some sharp teeth to fight spam. In this article I summarize and comment on the eleven major substantive provisions of the Act. These provisions deal with: false or misleading headers, subject and pornography labeling, resource misappropriation, dictionary attacks and harvesting, meaningful opt-out mechanisms, vicarious liability, private mail policies, preemption of state laws, rulemaking authority, studies required of the Federal Trade Commission (FTC), and enforcement and penalties.

False or Misleading Headers

Spammers have strong incentives to conceal their identities and the origin of their mail. The CAN-SPAM Act makes several common methods for this concealment illegal. The Act's "false or misleading header" provision addresses a problem that is easy for non-technologists to grasp, despite the complexity of the technology, and the solution it codifies is simple.

Consider an analogy between spam and paper "junk mail," delivered to your home by the post office. When your mail arrives, you can throw away the obvious junk mail before settling down to read the rest. Imagine, however, that an advertisement slips through your initial scan because the return address on the envelope seems to be from your bank. Instead of finding your bank statement inside, you find a flier for hard core pornography, complete with glossy color photographs. This wolf-in-sheep's-clothing scheme annoys most people, and many others find the content of the ad offensive, especially when such ads are sent to their children.

An email "header" is the electronic analog of the paper envelope. A header has three parts: (1) addressing information, which controls where the email is delivered; (2) origin information, which documents where the message originated; and (3) routing data, which documents the intermediary mail servers that handled the message as it traversed the Internet. Most email applications display the addressing and origin information by default — these are the familiar "to" "from," and "date" lines. Routing information is less familiar because most email applications hide it unless the user takes an extra step to have it displayed.

The routing portion of the header is created in stages while the email is in transit. After the sender transmits the message, his mail server hands it off to another mail server, which sends it to another, then another — each one being one step "closer" to the recipient. Eventually (usually after five or six hops), the message will reach the recipient's ISP, which delivers it to his inbox. Every computer on the Internet is assigned an Internet Protocol (IP) address consisting of four numbers separated by periods ("dots"). Every IP address uniquely identifies one computer and translates ("resolves") to a short series of character strings for more convenient identification. This translation is what allows web surfers to type *www.yahoo.com* instead of *66.218.71.80* to view Yahoo!'s home page.

Each intermediate mail server adds a new line to the top of each email's header. This line typically includes the server's IP address, the date and time, the action it performed, and other data. One can trace the entire chain of mail servers by starting at the top of the header and working down. For example, an email I received recently has these two consecutive lines in its header:

- Received: (from uucp@localhost) by andros.alumniconnections.com [198.212.10.70] (8.11.6+Sun/8.11.6) id hAPEpit20254; Tue, 25 Nov 2003 09:51:44 -0500 (EST)
- Received: from voyager.bna.com(149.79.136.49) by andros via smap (V2.1) id xma010225; Mon, 24 Nov 03 15:04:27 -0500

The first line was written by my mail forwarding service, which later sent the message to my ISP, and my ISP later delivered the message to me. This computer is named *andros.alumniconnections.com*, which resolves to the IP address *198.212.10.70*. Before that, the message was handled by a server named *voyager.bna.com* (*149.79.136.49*). This makes sense because the email in question was an Internet law newsletter from a publishing company named BNA. Also note that each line has a date and time stamp — which indicate that the BNA server held the email from 3pm until 10am the next day before sending it. The other data in these header lines need not concern us here.

The identities of the most active spammers are well known, and the IP addresses of their servers are easy to discover. In theory, this should make it easy for an automated anti-spam filter to scan incoming mail for the IP addresses of known spam sources. If it finds one, it can delete the message, separate it from other mail, or take any other action specified by the user. Spammers know this, however, so they program their servers to forge their stamps — that is, they simply record false IP addresses.

The CAN-SPAM Act makes this practice illegal by prohibiting the transmission of spam with false or misleading header information.⁴ It defines header information as "materially misleading if it is altered or concealed in a manner that would impair the ability of a recipient...to identify, locate, or respond to a person who initiated the...message."⁵ The Act also forbids the use of headers that are technically accurate but which contain an email address, IP address, or domain name obtained by "false or fraudulent pretenses or representations" for the purpose of sending spam.⁶ The point is to force spammers to identify themselves in their mailings. This provision is important in its own right, and it complements the opt-out provision discussed below. However, the language has problems.

The Act defines origin data as "the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message."⁷ This definition practically begs spammers to form shell corporations, hire short-term employees, or otherwise procure many "names" under which to send spam. It also fails to cover the widespread use of throwaway email accounts at sites like Hotmail. The Act later states that the "from" line is not considered misleading if it "accurately identifies any person who initiated the message."⁸ This paragraph is silent on the inclusion of an email address in the "from" line, so it could be interpreted to permit a spammer to identify himself there by name alone — which is not very useful for a recipient trying to contact him. This would certainly impair the ability of the recipient to respond to the message, which seems to be illegal under the section quoted above, but this more specific provision would take precedence over the general definition as a matter of statutory construction.

Subject and Pornography Labeling

The "subject labeling" provisions of CAN-SPAM are really a subset of the "false or misleading header" provisions. I discuss them separately here because, although the subject line is part of the header, the Act has several specific requirements for the subject line.

First, the Act makes it unlawful to send spam whose "subject heading...would be likely to mislead a recipient...regarding the contents or subject matter of the message."⁹ This standard is rather vague — it is hard to say, for example, whether a coy or humorous subject line would trigger liability as misleading. Congress chose not to require such specific information as the name of the product being advertised or the name of the person selling it. Therefore, we will have to wait for caselaw before we really know what misleading means.

Second, the Act requires any spam "that includes sexually oriented material" to carry in its subject line a mark or notice to be prescribed by the FTC.¹⁰ However, spam may advertise such material without a subject line label if the material is not displayed automatically upon

opening the email, absent additional some affirmative act by the recipient.¹¹ To take advantage of this exception, the spam may contain only the instructions for viewing the indecent material and not the material itself.¹²

The "sexually oriented material" provision may be difficult to defend if challenged under the First Amendment. It is a content-based regulation of speech, which triggers strict scrutiny.¹³ This will require the government to show a compelling interest in the regulation and that it is narrowly tailored to accomplish that interest.¹⁴ The courts have repeatedly recognized a compelling government interest in protecting minors from indecent material,¹⁵ but this law reaches far beyond this goal. It limits the delivery of spam containing indecent material to *everyone*, not just children. It may be very difficult to justify this extra regulation of indecent material when all other spam is regulated to a lesser degree.

Resource Misappropriation

CAN-SPAM's prohibition on resource misappropriation fills a large gap in the "false or misleading header" provision and extends it in a manner that extends standing to file lawsuits to many new potential plaintiffs. As explained above, spammers go to great lengths to conceal the origin of their mail. In addition to forging header stamps, they often relay mail through other people's open or insecure mail servers without permission. This allows them to further obfuscate their spam's origin and routing. CAN-SPAM addresses this by deeming the header to be misleading if the sender "uses another...computer to relay or retransmit the message for purposes of disguising its origin."¹⁶

The concept of resource misappropriation is difficult for many non-technologists to understand at first. Congress borrowed it from a line of judicial opinions based on a tort called trespass to chattel. A "chattel" is simply an item of personal property — a toaster or a chair, for example. Two people cannot simultaneously make toast or sit down using the same chattel, so the common law allows the owner to sue for damages and injunctive relief when a trespasser uses his chattels without permission. Money damages are assessed according to the delay the owner experienced before he could satisfy his hunger or relax his legs, plus the cost of any necessary repairs following the trespasser's use. The crux of the resource misappropriation policy in the Internet context is that computing and data transmission capacity are chattels just like toasters and chairs.

Everyday experience gives us the intuition that only one person can use a computer at a time: most personal computers have only one keyboard and one display. In the spam context, we must look at the technology on a deeper level. The Internet relies on powerful computers called servers, which respond to queries from many people at the same time. When I read Yahoo!'s home page, odds are good that many others are reading it at the same time. This is not normally a problem because web servers are designed to deliver ("serve") thousands or millions of pages simultaneously. Eventually, however, the number of readers exceeds the capacity of even the most powerful server. In that event, users will experience delays — or worse, the server will "crash" under the burden.

A similar phenomenon occurs with mail servers, the computers that process email. Suppose the average email user sends and receives 20 legitimate messages per day and receives 80 pieces of spam per day. This forces the average ISP's mail server to spend 80% of its time processing spam, leaving only 20% for the mail that paying customers want. Instead of buying a server adequate for its customers' needs, the ISP must buy a more expensive one, equipped with five times the processing capacity, to accommodate the extra load. Additionally, the rate of increase in spam far exceeds that of legitimate email, forcing the ISP to upgrade more often. Similarly, the ISP has to pay for substantially more transmission capacity ("bandwidth") than its customers would need, absent spam. Even if the ISP filters out and deletes spam as a service to its customers, it still requires the extra capacity because it must still receive every piece of mail and scan it for spam-like features. These costs, of course, are passed on to consumers.

The first case to examine spam from this perspective was *CompuServe v. Cyber Promotions*.¹⁷ CompuServe (an ISP) sought an injunction to prevent Cyber Promotions from sending spam to its customers. Citing *Thrifty-Tel, Inc. v. Bezenek*,¹⁸ the court wrote, "Electronic signals generated and sent by computer have been held to be sufficiently physically tangible to support a trespass cause of action."¹⁹ In other words, electrical impulses constitute a physical invasion of property when they are sent into a privately-owned system without permission. The *Thrifty-Tel* court reached this conclusion in the context of phone "phreaking" (attempting to crack authorization codes to make long distance calls without paying). The *CompuServe* court merely extended it to apply to mail servers. The most famous decision in this line of cases, *eBay v. Bidder's Edge*,²⁰ extended the same reasoning to include web servers.

CAN-SPAM creates a right of action for any ISP "adversely affected" by a violation of the Act.²¹ This obviously covers ISPs whose customers receive illegal spam. However, under the logic of *Thrifty-Tel*, *CompuServe*, and *eBay*, it also includes any ISP that owns a mail server used to relay spam without permission — even if none of its customers receive spam. By using the mail server, the spammer has diminished its capacity to process mail for its owner, which reduces its economic value for the duration of the spammer's unauthorized use. Impairment of the mail server's value does not require physical damage to the server.²² Although the actual damages from such an incursion are very small, the Act provides for substantial statutory damages. By creating such a large field of potential plaintiffs, Congress has created the possibility of enormous civil penalties for illegal spam.

Dictionary Attacks & Harvesting

Before spam can do any harm, it must be sent somewhere, which requires lists of email addresses. The CAN-SPAM Act addresses two common and harmful techniques for generating these lists. The first, called "dictionary attacks," entail systematically generating character strings in the hope that some will turn out to be valid email addresses.²³ The second, called "harvesting," involves scanning the text of web pages, chat rooms, message boards, and other electronic media for email addresses posted by users.²⁴ The Act does not make these practices illegal *per se* — rather, they are aggravating factors that may trigger treble damages.

Dictionary attacks can cause substantial harm to large ISPs, and the larger the ISP, the more susceptible it is. Computers are good at creating massive amounts of text in simple

patterns. By combining popular words and names, a spammer can "guess" many valid email addresses at a popular ISP like America Online (AOL). With over 35 million customers, AOL probably has several customers named John Smith, and one of them might have the address *johnsmith@aol.com*. A computer program can very quickly combine thousands of popular names and words in thousands of permutations apiece. Meanwhile, another program generates serial text strings, beginning with *a* and running through *z*, then starting again with *aa* and running through the alphabet repeatedly. This method picks up more valid addresses, albeit at a lower rate of success than the program combining common words. Large ISPs are the most enticing targets for dictionary attacks because they have the most users, giving spammers the best chance of scoring hits. They are, in a sense, victims of their own popularity; and their mail servers suffer the same harm described above, in the context of trespass to chattels.

Harvesting causes two main types of harm. First, automated scanning can overburden a server with queries. To highlight this harm, Congress limited this aggravating factor to situations where the addresses are harvested from proprietary areas, where the operator has posted a privacy policy that promises not to share email addresses with third parties.²⁵ Second, many Internet users are aware of harvesting techniques and try to avoid them, which causes a chilling effect on the use of the web and discussion fora. Many users refuse to post their addresses in such media, for fear that they will be inundated with spam. This reluctance to display contact information stifles communication and harms free speech interests. Harvesting causes the same chilling effect in non-proprietary fora such as Usenet, where free speech interests are arguably at their peak because no single host has meaningful control over content or distribution. Unfortunately, the Act ignores these fora altogether.

Meaningful Opt-Out Mechanisms

The most controversial part of the CAN-SPAM Act is its adoption of an opt-out regime, which permits spam to be sent without prior consent from the recipient. Instead, it requires spammers to stop sending it only after the recipient so requests.²⁶ Two separate provisions fall under the "meaningful opt-out" umbrella. The "working unsubscribe" provision requires all spam to include instructions for the recipient to opt out of receiving future mailings.²⁷ The "anti-resubscribe" provision forbids spammers from transferring addresses from the opt out list from one mailing to other mailing lists or to other spammers.²⁸ The opposite regime (*opt-in*) would require spammers to document that each recipient has affirmatively requested to be on the relevant mailing list.

An opt-in regime offers greater protection for consumers' privacy and economic interests, but opt-out better protects the freedom of speech. The First Amendment states that "Congress shall make no law...abridging the freedom of speech, or of the press." Despite this plain language, the Supreme Court has held that not all speech is equal. For example, indecent speech (e.g., ordinary pornography) is protected from most government interference, whereas obscene speech²⁹ and child pornography³⁰ enjoy no First-Amendment protection. Commercial speech receives an intermediate level of protection.³¹

A "prior restraint" — the great bugbear in First Amendment jurisprudence — occurs when the government prohibits a message before the speaker has a chance to communicate it.

The fundamental liberty of free expression demands that everyone have a chance to voice his thoughts — a proposition that applies even to speech that is socially harmful, like defamation or threats of violence. It is simply not possible to articulate a definition that captures all harmful speech without being overbroad. To avoid these problems, we only punish harmful speech *after* it has been uttered, when a detailed analysis of the speech and its context is possible. This allows some harms to occur that we might otherwise prevent, but a system of prior restraints would create more and greater harms by discouraging socially-necessary speech. The practical application of this idea is that everyone must have an opportunity to stand in a public square, tap passers-by on the shoulder, and ask, "Would you like to hear what I have to say?" However, the First Amendment does not guarantee a right to force others to listen. Everyone has a right to answer, "No." Spam is a modern, commercial-speech embodiment of the traditional tap on the shoulder, and the opt-out regime codifies the listener's opportunity to say no.

A similar definitional problem counsels against regulating one channel of speech uniquely, especially one so affected with technology as email. New communication technologies frequently blur the lines between older channels of communication, and all evidence points to this trend accelerating. Consider, for example, the difficulty of regulating voice transmissions over IP networks (VoIP) as telephone communications.³² However we define email, we run the risk of snaring within that definition other speech channels such as instant messaging, mobile text messaging, and an unknowable number of channels not yet invented. Mitigating such an obvious danger by adopting a conservative rule, at least at first, is only prudent — further justifying the opt-out regime in lieu of the more popular opt-in regime.

Vicarious Liability

The Internet's transcendence of international borders makes it difficult to enforce many laws that would be used to regulate it. The ability of any person to relocate his business and assets abroad with little or no disruption in operations can render any government impotent to prosecute criminals and enforce civil judgments. Furthermore, spam outfits tend to be tiny, judgment-proof corporations. The CAN-SPAM Act anticipates these problems and contains two provisions designed to alleviate them. Both provisions render third parties liable for spam sent by other people, under certain conditions.

First, the Act extends liability to anyone whose business is promoted via spam with false or misleading headers.³³ The conditions for this liability are fairly expansive. Liability attaches if the person "knows, or should have known,"³⁴ that his business was promoted in an illegal email and if he "received or expected to receive an economic benefit from such promotion."³⁵ However, such a person can avoid liability by making a reasonable effort "to prevent the transmission" of the emails or to "detect the transmission and report it to the" Federal Trade Commission (FTC).³⁶

Second, the Act extends liability to some vendors who sell goods and services to spammers.³⁷ The general rule is one of no liability for such vendors, subject to two exceptions.³⁸ The first exception creates liability for vendors with "a greater than 50 percent ownership or economic interest in" the spamming operation.³⁹ The second exception creates liability for any vendor who has actual knowledge that spam is being sent with false or misleading headers and

"receives, or expects to receive, an economic benefit from" it.⁴⁰ This provision is easily interpreted to capture vendors who benefit from the sale of basic office equipment to businesses they know to belong to spammers.

Private Mail Policies

By making certain kinds of email illegal, CAN-SPAM renders other kinds of email legal, by implication. Unfortunately, some spam that Congress intended to ban will inevitably slip through cracks in the law's definitions. (This is a fundamental shortcoming of the English language, not necessarily a fault of Congress.) Therefore, the Act expressly permits ISPs to devise and implement their own, private email-handling policies that extend beyond the law.⁴¹

Without this provision, ISPs would be vulnerable to lawsuits for blocking more slippery forms of spam. Blocking mail that is technically legal arguably renders ISPs liable for such torts as interference with business relations (for blocking legal business communications) and defamation (for falsely labeling messages as "spam" and, by implication, the senders as "spammers"). Much like § 230 of the Telecommunications Act of 1996,⁴² this provision is designed to protect ISPs from an onslaught of litigation that could drive them out of business.

Preemption of State Laws

Like many federal statutes, the CAN-SPAM Act expressly preempts some state laws. In general, it supercedes any state law "that expressly regulates the use of electronic mail to send commercial messages, except to the extent that [it] prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto."⁴³ Second, the Act permits states to adopt laws that are "not specific to electronic mail,"⁴⁴ such as those that regulate "trespass, contract, or tort"⁴⁵ or prohibit "acts of fraud or computer crime."⁴⁶

Rulemaking Authority

The CAN-SPAM Act vests primary rulemaking authority in the Federal Trade Commission (FTC).⁴⁷ However, the Act empowers ten other government agencies and officials to enforce its provisions with respect to entities and channels of commerce within their jurisdictions,⁴⁸ and it encourages them to invoke "any other authority conferred on [them] by law" toward that end.⁴⁹ This implies that they may promulgate rules to aid in the enforcement of CAN-SPAM if they possess rulemaking authority under some other law. These rules, however, would apply only within the agencies' and officers' limited jurisdictions, whereas rules promulgated by the FTC would apply generally.

The Act confers more detailed rulemaking authority upon the Federal Communications Commission (FCC). In addition to being one of the enumerated agencies mentioned above, the FCC will be required to promulgate rules to "protect consumers from unwanted mobile service commercial messages."⁵⁰ Interestingly, the Act specifies that those rules must create an *opt-in* regime for mobile messaging⁵¹ — in contrast to the *opt-out* regime for commercial email. This probably indicates more about the relative lobbying clout of the telecommunications behemoths,

vis-à-vis Internet service providers, than the relative harm caused by commercial messages in these two media.

FTC Studies & Do-Not-E-Mail Registry

Much of the territory covered by the CAN-SPAM Act is uncharted, so it requires the Federal Trade Commission (FTC) to study several issues in the years following its enactment. For example, the FTC must report to Congress (1) within nine months to recommend a system for rewarding informants who report violations,⁵² (2) within 18 months with a plan to require commercial email to include a marker in the "subject" line (such as "ADV"),⁵³ and (3) within two years to document the effectiveness and enforcement of the Act.⁵⁴

In the most important report, due within six months,⁵⁵ the FTC must devise "a plan and timetable for establishing a nationwide marketing Do-Not-E-Mail registry."⁵⁶ However, the Act does not require the FTC to implement the registry. In fact, it prohibits implementation until at least nine months have passed since the Act's enactment.⁵⁷ Additionally, the Act makes no provision for funding the registry. The mandatory three-month delay, however, will give Congress time to consider the FTC's proposal and, perhaps, allocate funding.

Enforcement & Penalties

Generally, the CAN-SPAM Act treats offenses as if they were unfair or deceptive acts or practices proscribed by the Federal Trade Commission (FTC) Act and grants general enforcement powers to the FTC.⁵⁸ It also gives enforcement powers to ten other agencies and officers where an offense involves an entity or a channel of commerce already within their jurisdictions.⁵⁹ Finally, it grants private rights of action to Internet Service Providers (ISPs)⁶⁰ and to States to bring suits on behalf of their citizens.⁶¹ These provisions represent a compromise between factions that lobbied for a private right of action for individuals and those that lobbied for enforcement to be restricted to the U.S. Attorney General.

The Federal Communications Commission (FCC) has the second-broadest enforcement powers under the Act, after the FTC. Congress charges the FCC with enforcement "with respect to any person subject to the" Communications Act of 1934.⁶² This provision is surprisingly broad — covering individuals, businesses, and channels of commerce that one does not normally associate with the FCC. For example, any device that uses the broadcast spectrum must comply with the Communications Act. By conferring authority over all "persons" subject to that Act, CAN-SPAM may permit the FCC to enforce the spam law against most manufacturers and users of modern electronic devices. The Act does not limit the FCC's authority to spam related to such devices.

The CAN-SPAM Act establishes criminal penalties for some offenses.⁶³ Generally, it provides for fines, imprisonment for up to five years, and forfeiture of property used in the commission of the offense.⁶⁴ Liability attaches only upon sending "multiple" emails that violate the Act, and "multiple" is defined as 100 messages in any 24-hour period, 1,000 messages in any 30-day period, or 10,000 messages in any one-year period.⁶⁵ Aggravating factors that may affect sentencing include: the sending of many more emails than the minimum number to trigger

liability, prior convictions under CAN-SPAM, commission of the offense in furtherance of a felony, causing damages totaling more than \$5,000, obtaining a benefit worth more than \$5,000, and organizing a conspiracy of three or more people to violate the Act.⁶⁶

Civil remedies provided for under the CAN-SPAM Act include injunctive relief, actual damages, and statutory damages. Many forms of injunctive relief and cease & desist orders do not require any showing of knowledge on the part of the defendant.⁶⁷ States may seek actual monetary losses suffered by their residents,⁶⁸ and ISPs may seek their own actual damages but not those of their customers.⁶⁹ States may seek statutory damages of \$250 per offending email,⁷⁰ up to a total of \$2 million.⁷¹ ISPs may seek statutory damages of only \$100 per offending email that includes a false or misleading header⁷² or \$25 per other offending email,⁷³ up to a total of \$1 million.⁷⁴

A court may award treble damages for aggravated offenses.⁷⁵ Aggravating factors include the collection of email addresses by automated harvesting,⁷⁶ automated generation of addresses in a dictionary attack,⁷⁷ automated creation of multiple email accounts from which spam is sent,⁷⁸ and unauthorized relaying of spam through mail servers.⁷⁹ States may recover attorney fees, in the court's discretion, but the Act does not provide for defendants to recover attorney fees from States.⁸⁰ In ISP suits, on the other hand, either party may recover attorney fees.⁸¹ In all suits brought by states and ISPs, damages are mitigated (but liability is not avoided) if "the defendant has established and implemented, with due care, commercially reasonable practices and procedures designed to effectively prevent...violations" of the Act or "the violation occurred despite [those] efforts."⁸²

Conclusion

Will the CAN-SPAM Act put a lid on spam? Or will its legacy be that marketers can legally spam us? Some anti-spam activists bitterly oppose it. The Coalition Against Unsolicited Commercial Email (CAUCE), for example, writes, "This legislation fails the most fundamental test of any anti-spam law, in that it neglects to actually tell any marketers not to spam. Instead, it gives each marketer in the United States one free shot at each consumer's e-mail inbox."⁸³ Furthermore, they lament its preemption of some state laws that are more protective of consumers.

Despite these problems, I am cautiously optimistic that CAN-SPAM will succeed. Yes, it legalizes some forms of spam, lending them undeserved legitimacy. Yes, it requires consumers to opt out of many individual spam lists, which most people will consider a chore. However, the statute's strengths balance out these shortcomings. The anti-harvesting provision will promote the free exchange of speech online. The anti-resubscribe provision will give consumers a reason to trust opt-out forms for the first time. The prospect of a comprehensive do-not-spam registry means that we may soon be able to swear off opt-out forms altogether. The ISP right of action, coupled with the resource misappropriation and vicarious liability provisions, will keep spammers and advertisers honest in civil court. Even if spam does not decline measurably soon after the Act takes effect, it will decline precipitously after the first spammer or advertiser loses a \$2 million judgment or goes to prison.

The specter of criminal penalties will make most businesses think twice about promoting their products via email. As the demand for advertising space falls, so will the supply of spam. Even if spammers relocate offshore, which critics argue is inevitable, their customers will not all relocate. Federal courts can reach these businesses or their assets. Most consumer e-commerce occurs via credit cards or other payment mechanisms that rely on assets in this country. A federal court can attach a company's receivable accounts as they are processed by Visa, MasterCard, or PayPal.

Spam will not disappear entirely under the CAN-SPAM Act, but it will decrease in terms of the number of emails sent, the costs it forces upon ISPs, and the annoyance it represents to consumers. This statute is a reasonable first step toward reducing spam — one that should be candidly evaluated in two years. By the time the FTC delivers its final report, we will have hard data on the Act's strengths and shortcomings and can discuss amendments from a position of knowledge. I look forward to that time, when we can take our second national step against spam.

¹ The Act uses the term "provider of Internet access service," but I will use Internet Service Provider (ISP) since that term is in more common usage.

² Sen. 877, 108th Cong. (25 Nov. 2003)

³ See e.g., Associated Press, *Bush signs legislation against spam*, SiliconValley.com (16 Dec. 2003) <<http://www.siliconvalley.com/mld/siliconvalley/news/editorial/7505263.htm>>

⁴ § 5(a)(1)

⁵ § 4(a) (amending 18 U.S.C. § 1037 to include this definition)

⁶ § 5(a)(1)(A)

⁷ § 3(8)

⁸ § 5(a)(1)(B)

⁹ § 5(a)(2)

¹⁰ § 5(d)(1)(A)

¹¹ § 5(d)(1)(B)

¹² § 5(d)(1)(B)(iii)

¹³ See *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

¹⁴ *Id.*

¹⁵ See e.g., *Ashcroft v. American Civil Liberties Union*, 535 U.S. 564 (2002); *American Civil Liberties Union v. Reno*, 217 F.3d 162 (2000).

¹⁶ § 5(a)(1)(C)

¹⁷ 962 F. Supp. 1015 (S.D. Ohio 1997)

¹⁸ 56 Cal. App. 4th 1559, 1567 (1996)

¹⁹ *CompuServe*, 962 F. Supp. at 1021

²⁰ 100 F. Supp. 2d 1058 (2000). Subsequently followed by *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238 (S.D.N.Y. 2000)).

²¹ § 7(g)(1)

²² *eBay*, 100 F. Supp. 2d at 1071; *CompuServe*, 962 F. Supp. at 1022.

²³ § 5(b)(1)(A)(ii)

²⁴ § 5(b)(1)(A)(i)

²⁵ *Id.*

²⁶ § 5(a)(4)

²⁷ § 5(a)(3)

²⁸ § 5(a)(4)(A)(iv)

²⁹ *Pope v. Illinois*, 481 U.S. 497, 500-01 (1987); *Smith v. U.S.*, 431 U.S. 291, 301-02, 309 (1977); *Miller v. California*, 413 U.S. 15, 24-25 (1973).

³⁰ See e.g., *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002).

³¹ *Central Hudson Gas & Electric Corp. v. Public Service Commission of N.Y.*, 477 U.S. 557 (1980). Many people believe that commercial speech should receive less protection because consumers are at risk from fraudulent and

deceptive commercial practices. Such arguments do have merit, and I do not mean to dismiss them, but a full treatment is beyond the scope of this article.

³² See e.g., Declan McCullagh, *FCC to form working group on VoIP regulation*, CNET News.com (1 Dec. 2003) <<http://news.com.com/2100-7352-5112424.html>>.

³³ § 6(a)

³⁴ § 6(a)(1)

³⁵ § 6(a)(2)

³⁶ § 6(a)(3)

³⁷ § 6(b)(1)

³⁸ *Id.*

³⁹ § 6(b)(2)(A)

⁴⁰ § 6(b)(2)(B)

⁴¹ § 8(c)

⁴² 47 U.S.C. § 230 (2000). See Robert Cannon, *Content Restrictions For Interactive Computer Services in the Telecommunications Act of 1996* § 1.2.2.2 (14 March 1996) <<http://www.cybertelexcom.org/cda/newslett.htm>> (summarizing the legislative intent and practical effects of § 230).

⁴³ § 8(b)(1)

⁴⁴ § 8(b)(2)

⁴⁵ § 8(b)(2)(A)

⁴⁶ § 8(b)(2)(B)

⁴⁷ § 13(a)

⁴⁸ § 7(b). See note 59 for the list of enumerated agencies and officers.

⁴⁹ § 7(c)

⁵⁰ § 14(b)

⁵¹ § 14(b)(1)

⁵² § 11(1)

⁵³ § 11(2)

⁵⁴ § 10

⁵⁵ § 9(a)

⁵⁶ § 9(a)(1)

⁵⁷ § 9(b)

⁵⁸ § 7(a) (referring to 15 U.S.C. § 57a(a)(1)(B) (2000))

⁵⁹ § 7(b). The enumerated agencies and officers are: the Office of the Comptroller of the Currency, the Board of Directors of the Federal Deposit Insurance Corporation, the Director of the Office of Thrift Supervision, the Board of the National Credit Union Administration, the Securities and Exchange Commission (SEC), the Secretary of Transportation, the Secretary of Agriculture, the Farm Credit Administration, the Federal Communications Commission (FCC), and state insurance authorities.

⁶⁰ § 7(g)

⁶¹ § 7(f)

⁶² 47 U.S.C. § 151 *et seq.* (2000)

⁶³ § 4(a) (amending 18 U.S.C. § 1037)

⁶⁴ *Id.*

⁶⁵ *Id.*

⁶⁶ *Id.*

⁶⁷ § 7(e)

⁶⁸ § 7(f)(1)(B)(i)

⁶⁹ § 7(g)(1)(B)(i)

⁷⁰ § 7(f)(3)(A)

⁷¹ § 7(f)(3)(B)

⁷² § 7(g)(3)(A)(i)

⁷³ § 7(g)(3)(A)(ii)

⁷⁴ § 7(g)(3)(B)

⁷⁵ § 7(f)(3)(C) (states), § 7(g)(3)(C) (ISPs)

⁷⁶ § 5(b)(1)(A)(i)

⁷⁷ § 5(b)(1)(A)(ii)

⁷⁸ § 5(b)(2)

⁷⁹ § 5(b)(3)

⁸⁰ § 7(f)(4)

⁸¹ § 7(g)(4)

⁸² § 7(f)(3)(D) (states), § 7(g)(3)(D) (ISPs)

⁸³ *CAUCE Statement on House Spam Bill Vote ¶ 1* (22 Nov. 2003) <<http://www.cauce.org/news/>>