

Summer 2004

A Dollar Short: The Impact of the Can-Spam Act of 2003 on Illinois Businesses, 37 J. Marshall L. Rev. 1289 (2004)

Timothy S. O'Brien

Follow this and additional works at: <https://repository.law.uic.edu/lawreview>



Part of the [Computer Law Commons](#), [Internet Law Commons](#), and the [State and Local Government Law Commons](#)

Recommended Citation

Timothy S. O'Brien, A Dollar Short: The Impact of Can-Spam Act of 2003 on Illinois Businesses, 37 J. Marshall L. Rev. 1289 (2004)

<https://repository.law.uic.edu/lawreview/vol37/iss4/6>

This Comments is brought to you for free and open access by UIC Law Open Access Repository. It has been accepted for inclusion in UIC Law Review by an authorized administrator of UIC Law Open Access Repository. For more information, please contact repository@jmls.edu.

A DOLLAR SHORT: THE IMPACT OF THE CAN-SPAM ACT OF 2003 ON ILLINOIS BUSINESSES

TIMOTHY S. O'BRIEN*

INTRODUCTION: THE HIGH PRICE OF LIFE IN THE FUTURE

The popular 1960s cartoon series, *The Jetsons*, portrays a future existence wherein the blundering protagonist, George, complains about the length of his three-hour workday.¹ While only a fantastical cartoon, the series depicts the pinnacle of workplace efficiency: George's job is to supervise a computer's actions, and a three-hour workday is standard.² Today's American workplace has yet to reach the heights of efficiency illustrated in *The Jetsons*, though it has evolved dramatically over the last decade.³ Due to advancements in technology, American workers today are reaching unprecedented levels of efficiency and accessibility.⁴ Of

* J.D. Candidate, January 2005. The author would like to thank both the previous and current boards of *The John Marshall Law Review* for their dedication and commitment to this publication. The author would especially like to thank his family and closest friends for their enduring support, without which he never would have made it through law school. This comment is dedicated to his father, a remarkable attorney and an even more remarkable mentor and friend.

1. *The Jetsons*, <http://www.tvtome.com/tvtome/servlet/ShowMainServlet/showid-3723/> (last visited Aug. 2, 2004). The series, still running in syndication today, first ran on ABC during the 1962 and 1963 seasons and was revived in 1984. *Id.* The writers of the series accurately predicted several future conveniences, such as the information from an entire set of encyclopedias fitting into a cartridge no larger than a cigarette lighter and tele-video communication. *Id.* In the episode titled "Uniblab," George is charged with programming a new computer and is forced to work the entire three-hour workday. *The Jetsons - Uniblab*, <http://www.tvtome.com/tvtome/servlet/GuidePageServlet/showid-3723/epid-61681/> (last visited Aug. 2, 2004). His primary complaint at the end of the day is that his finger is sore from pushing too many buttons. *Id.*

2. *The Jetsons - Uniblab*, <http://www.tvtome.com/tvtome/servlet/GuidePageServlet/showid-3723/epid-61681/> (last visited Aug. 2, 2004).

3. See Scot M. Graydon, *Much Ado About Spam: Unsolicited Advertising, the Internet, and You*, 32 ST. MARY'S L.J. 77, 82 (2000) (describing the new economic opportunities in the last decade resulting from the development of e-commerce).

4. See Jeffrey L. Kosiba, Comment, *Legal Relief from Spam-Induced*

these advancements, nothing has had greater force in American workers' ability to communicate globally than the e-mail system.⁵

In the 1990s, e-mail exploded in popularity, becoming the most oft-used computer application.⁶ Exponentially growing, it is estimated that the number of electronic mailboxes in existence by the year 2005 may surpass 1.2 billion.⁷ Ironically, the ubiquitous accessibility responsible for the meteoric rise in e-mail use also generated one of the e-mailer's greatest enemies: unsolicited commercial e-mail ("UCE").⁸ The anonymous nature of e-mail, coupled with the global popularity of the Internet, has spawned an onslaught of UCE in recent years.⁹ More generally referred to as "spam," UCE is popular with mass marketers for three primary reasons: ease of distribution, a high potential of reaching its audience, and extraordinarily low cost.¹⁰

Average private home e-mail users employ e-mail systems for personal use and the typical effect of spam on this user is

Internet Indigestion, 25 DAYTON L. REV. 187, 190-92 (1999) (providing a brief history of the development of the Internet, accessing the Internet and the tremendous growth in popularity that made the Internet accessible to most of the world).

5. See *id.* at 192 (describing the advantages of electronic mail over regular postal mail, especially the ability of millions of users to communicate globally on an instantaneous basis).

6. Cindy M. Rice, Comment, *The TCPA: A Justification for the Prohibition of Spam in 2002? Unsolicited Commercial E-Mail: Why Is It Such a Problem?*, 3 N.C. J.L. & TECH. 375, 376-77 (2002). A survey of Internet users revealed that e-mail is the primary Internet activity, with the average user spending seven to eight hours per week online. *Id.* See also Sabra-Anne Kelin, *Business Law, Electronic Commerce: Commercial E-mail: State Regulation of Unsolicited Commercial E-Mail*, 16 BERKELEY TECH. L.J. 435, 436 (2001) (stating that among the wide variety of applications available to Internet users, the most widely used application is electronic mail).

7. Rice, *supra* note 6, at 376. Additionally, it is estimated that, by 2005, the number of individual e-mails sent daily worldwide will exceed 36 billion. *Id.*

8. *Id.* at 378. "[G]iven the number of people online and using e-mail . . . advertisers are attempting to capitalize on this seemingly endless pool of potential customers." *Id.*

9. *Id.*

10. Graydon, *supra* note 3, at 82. See also Cathryn Le, Comment, *How Have Internet Service Providers Beat Spammers?*, 5 RICH. J.L. & TECH. 9, ¶3 (1998) (describing the advantages of sending UCE instead of conventional postal junk mail), at <http://law.richmond.edu/jolt/v5i2/le.html>.

Businesses incur minimal cost through mass e-mail advertisements because Internet users are not charged for how much information they send. Bulk e-mailing takes only minutes to complete, and the advertisements are transmitted to the recipients' electronic mailboxes almost instantaneously, regardless of geographical location. This method of advertising is faster and cheaper than any other means of cold advertising, including door-to-door, phone and postal mail solicitations.

Id.

frustration and delay.¹¹ Business organizations, on the other hand, rely upon e-mail systems as a critical component of their internal and external communication networks.¹² For the corporate computer network, therefore, spam is not simply an annoyance, but rather an epidemic that requires constant attention from information technology (“IT”) departments and increased budgets from finance departments simply to contend with the daily UCE deluge that invades a company’s computer network.¹³ For the average corporation, skyrocketing investment in technology, lost man-hours within IT departments, and slipping productivity spell steady streams of lost revenue.¹⁴ Given the level of labor and investment that this battle requires, the efficient workplace environment risks extinction before ever having a chance to exist.

Federal efforts to curb spam are simply not enough.¹⁵ Illinois, as home to some of the world’s most influential global corporations,¹⁶ must provide a greater protection to its hometown

11. See Michael A. Fisher, *The Right to Spam? Regulating Electronic Junk Mail*, 23 COLUM.-VLA J.L. & ARTS 363, 364 (2000) (explaining that the marketing technique employed by the spammers results in wasted time and inconvenience to the consumer). The UCE demands some effort on the part of the e-mail user and accordingly, “excessive amounts of . . . solicitation can be a significant waste of time, and a great annoyance, to the consumer.” *Id.*

12. Rice, *supra* note 6, at 377. E-mail systems afford corporations the opportunity to rapidly address issues ranging from simple client correspondence to order placing, billing issues, and internal communication. *Id.* Furthermore, with the increasing trend toward flex-time and remote working arrangements for these employees, e-mail has become the primary means of communication. *Id.* The use of e-mail within the workplace has grown substantially in the last several years; roughly eighty percent of people use e-mail in the workplace today. *Id.* The volume of e-mail in the workplace has also dramatically risen, increasing fifty percent in 2001 with similar increases expected in coming years. *Id.*

13. David E. Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, 35 U.S.F. L. REV. 325, 336 (2001).

Spam represents a significant proportion of all e-mail traffic, consuming massive amounts of network bandwidth, memory, storage space, and other resources. Internet users and system administrators spend a great deal of time reading, deleting, filtering, and blocking spam Spam and anti-spam measures frequently interfere with other e-mail traffic and other legitimate Internet uses.

Id.

14. See Kelin, *supra* note 6, at 436-37 (explaining the loss in corporate revenue resulting from the battle against spam). “[S]pam can . . . cause networks to shut down completely” as well as impose “[c]osts . . . on the recipient [that] include money spent for Internet access time to download, read and delete the spam.” *Id.*

15. See Jennifer Jacobs, *New Law Likely Won’t Stop E-Mail Spam; Foreign Sources Aren’t Required to Obey Legislation that Goes into Effect Today*, THE POST-STANDARD (Syracuse), Jan. 1, 2004, at A1 (describing the doubt related to the effectiveness of the newly enacted CAN-SPAM Act of 2003).

16. The top five global public corporations headquartered within Illinois are

businesses. This Comment focuses primarily on efforts that Illinois must undertake in order to better protect its corporations. Part I provides a basic background to the problems associated with spam and the various steps that a company must take to fight back. This Part then focuses on the current federal regulations on spam and the potential constitutional difficulties that a state faces when proposing state regulations to deal with spam. Part II targets the shortcomings of the current federal regulations and provides a historical perspective on Illinois's attempts to regulate spam. The final Part proposes a resolution and the potential impact that it could have on Illinois corporations and the "spamming" industry itself.

II. BACKGROUND: IF THE SPAM ISN'T ON MY COMPUTER SCREEN, WHY DO I CARE?

A. *How Do I Get Rid of All of This Junk E-Mail?*

With the development of each new avenue of communication comes the inevitable mass-marketing schemes: the telephone begat the telemarketer; the fax machine begat junk faxes; and e-mail spawned the "spammer."¹⁷ As advertisements such as these become less of a nuisance and more of an outright invasion, courts become more willing to intervene and regulate commercial activity and speech.¹⁸

Both the content within individual UCEs and the text of their subject lines range from the innocuous and innocent to the graphic and obscene.¹⁹ Corporate networks and servers are typically

Boeing, Sears Roebuck & Co., Kraft Foods, Allstate Corp., and Walgreen Co. *Chicago's Largest Public Companies*, CRAIN'S CHI. BUS., May 5, 2003, at www.chicagobusiness.com/cgi-bin/article.pl?feature_id=7&page_id=1357&format=list (last visited July 29, 2004). The top five companies alone employ an estimated 750,000 people (though not all Illinois residents) and in 2002 had an aggregate revenue of over \$180 billion. *Id.*

17. See generally Fisher, *supra* note 11, at 373-74 (providing a history of the marketing methods that develop alongside new technologies). With every new mode of communication introduced, an entrepreneurial group springs forth to exploit that avenue for a commercial purpose, ultimately to a point of misuse. *Id.*

18. *Id.* Courts historically are more open to regulations of commercial speech when the "new technology has made solicitations very annoying, invasive, or susceptible to unprecedented levels of misuse." *Id.*

19. FED. TRADE COMM'N, FALSE CLAIMS IN SPAM: A REPORT BY THE FTC'S DIVISION OF MARKETING PRACTICES 2-3 (2003), available at <http://www.ftc.gov/reports/spam/030429spamreport.pdf> [hereinafter FTC]. An extensive report of spam e-mail compiled by the FTC concluded that the types of offers presented in spam e-mails falls into one of eight categories: Investment/Business Opportunity; Adult; Finance; Products and Services; Health; Computers/Internet; Leisure/Travel; Education; and Other. *Id.* Of these categories, Adult, Finance, and Investment/Business Opportunity

programmed to “weed out” e-mails containing certain triggers, such as obscene language or subject lines indicating that the message is spam.²⁰ Despite a company’s best efforts, these filtering efforts often generate two problems: (a) the filtering mechanism may be over-inclusive, weeding out legitimate e-mails;²¹ and (b) spammers frequently utilize false return addresses or place misleading information in the subject line to create the illusion of a legitimate message.²² The steady barrage of spam into a company’s computer network places strenuous burdens on servers, and devours precious data capacity, memory, and other network capabilities.²³ Fighting back requires dedicated IT resources, increased labor costs, increased costs from Internet service providers (“ISPs”), and continued investment in spam

account for fifty-five percent of all spam sent. *Id.* The Investment/Business Opportunity category comprises offers such as work-at-home opportunities and chain letters. *Id.* The Adult category consists primarily of offers for pornography or dating services. *Id.* Finally, the Finance category involves offers for credit cards, refinance opportunities, insurance services, mortgage services, and similar other personal financial services. *Id.*

20. See Caroline E. Mayer & Ariana Eunjung Cha, *Making Spam Go Splat: Sick of Unsolicited E-Mail, Businesses are Fighting Back*, WASH. POST, June 9, 2002 (describing the almost draconian steps that corporations and Internet Service Providers are taking to filter spam before it gets through to the network), <http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&contentId=A15849-2002Jun8¬Found=true.html>. See generally Sorkin, *supra* note 13, at 336-43 (listing several of the threats that spam presents to the network and the steps taken by corporations to head them off).

21. Mayer & Cha, *supra* note 20. A spammer sent a mass e-mail to hundreds of politicians bearing the return address of then Central Intelligence Agency Director R. James Woolsey. *Id.* Because of the return address used, the spam e-mail easily bypassed the filters designed to block such e-mail. *Id.* Ironically, when Mr. Woolsey himself sent a follow-up e-mail warning the recipients of the spam e-mail, the servers blocked Mr. Woolsey’s message because it contained the word “porn.” *Id.* See also Sorkin, *supra* note 13, at 345-46, 349 (describing some of the technical glitches which allow certain spam to bypass filters while legitimate e-mail can be blocked).

22. FTC, *supra* note 19, at 3-5. Of the spam messages analyzed by the FTC, one-third contained false information in the “from” line and twenty-two percent carried false information in the “subject” line. *Id.* at 3, 5. The “from” line was falsified in such a manner as to “obscure [] the true identity of the sender.” *Id.* at 3. The main types of disguising in the “from” line included: stripping the sender’s identity from the line; suggesting a business relationship in the line; suggesting a personal relationship in the “from” line; or replacing the sender’s information with the recipient’s information. *Id.* The false “subject” lines similarly suggested business or personal relationships, relayed information unrelated to the content of the e-mail or was designed to appear that the spammer was replying to a message sent from the recipient. *Id.* at 5. See *infra* note 27 (discussing the efforts of the Can Spam Act of 2003 to outlaw both falsified messages in subject lines and fraudulent return addresses).

23. Sorkin, *supra* note 13, at 336-37.

filtering software.²⁴ It is estimated that these efforts costs American businesses \$8.9 billion each year.²⁵

B. Won't the New Federal Law Stop All of These E-Mails?

President George W. Bush signed the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM") into law on December 16, 2003.²⁶ CAN-SPAM outlaws fraudulent subject lines in e-mails and requires a valid return address that allows the recipient to request removal from the mailing list.²⁷ Though well-intended, CAN-SPAM does not provide adequate protection for corporations.²⁸ In essence, the Act legalizes spam by providing a framework of compliance for the spammer.²⁹ Furthermore, the burden is placed on the recipient of

24. *Id.* at 337. The increased costs for the ISPs generally reflect the ISPs' own increased costs for dedicated labor and financial resources required to battle spam. *Id.* These costs are then typically passed on to the corporate customer. *Id.*

25. Dannielle Cisneros, *Do Not Advertise: The Current Fight Against Unsolicited Advertisements*, 2003 DUKE L. & TECH. REV. 10, 14 (2003).

26. The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003) [hereinafter CAN-SPAM].

27. The relevant portions of the Act are reproduced below:

Whoever, in or affecting interstate or foreign commerce, knowingly . . . materially falsifies header information in multiple commercial electronic mail messages and intentionally initiates the transmission of such messages, . . . or conspires to do so, shall be punished.

Id. §4(a).

It is unlawful for any person to initiate the transmission to a protected computer of a commercial electronic mail message if such person has actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that a subject heading of the message would be likely to mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message.

Id. §5(a)(2)

It is unlawful for any person to initiate the transmission to a protected computer of a commercial electronic mail message that does not contain a functioning return electronic mail address or other Internet-based mechanism, clearly and conspicuously displayed, that (i) a recipient may use to submit, in a manner specified in the message, a reply electronic mail message or other form of Internet-based communication requesting not to receive future commercial electronic mail messages from that sender at the electronic mail address where the message was received; and (ii) remains capable of receiving such messages or communications for no less than 30 days after the transmission of the original message.

Id. §5(a)(3)

28. See Alyson Ward, *Smothered by Spam*, FORT WORTH STAR-TELEGRAM, Jan. 13, 2004, § 5 (Business and Financial), at 1 (describing the surprising ineffectiveness of the CAN-SPAM Act). See also Jacobs, *supra* note 15 (stating that the Act has no jurisdiction over foreign spammers).

29. Dwight Silverman, *New Law Takes Effect, But it Seems to Can Little Spam*, HOUS. CHRON., Jan. 3, 2004, at B1. "Can-Spam has been referred to as

the e-mail to seek removal from the mailing list.³⁰ The full impact of CAN-SPAM is discussed in greater detail below.

C. Can the State Do That? Regulating Commercial E-Mail at the State Level

Given the newly enacted federal legislation, what ability to protect its businesses does a state retain? While CAN-SPAM preempts state anti-spam statutes,³¹ states still have an ability to pursue legal action against egregious spammers.³² Though under CAN-SPAM private citizens no longer retain a right to bring a direct cause of action,³³ a states retains the power to pursue the rights of its own citizens.³⁴ Despite this, several states still express grave concerns about the efficacy of CAN-SPAM.³⁵ Past history of attempted federal spam legislation reveals concerns about enforcement and the influence of lobbying groups.³⁶ Arguments against CAN-SPAM are not unlike those against its failed predecessors: by focusing on false claims, rather than calling for

the 'You Can Spam Act,' because what it really does is set out guidelines for legitimate companies to send unsolicited commercial e-mail." *Id.*

30. *Id.*

31. CAN-SPAM § 8(b). Tamara Loomis, *Will the Federal Spam Law Really Unclog E-mail Boxes?*, LEGAL TIMES, Jan. 12, 2004, at 22. Thirty-four states had passed anti-spam legislation, a number of which were stricter than CAN-SPAM. *Id.*

32. Loomis, *supra* note 31. In New York, days after the enactment of CAN-SPAM, the state's Attorney General announced a lawsuit against a New York-based spammer rooted in the state's anti-fraud statutes. *Id.*

33. *Id.*

34. CAN-SPAM § 7(f).

In any case in which the attorney general of a State, or an official or agency of a State, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by any person who violates [certain sections] of this Act, the . . . State, as *parens patriae*, may bring a civil action on behalf of the residents of the State . . . (A) to enjoin further violation of section 5 of this Act by the defendant; or (B) to obtain damages on behalf of residents of the State.

Id.

35. David McGuire, *States Object to Spam Legislation*, WASH. POST, Apr. 23, 2003. Forty-four states and the District of Columbia did not formally support the lobbying efforts of the bill that became CAN-SPAM. *Id.*

36. Kosiba, *supra* note 4, at 208-09. Past attempts at passing federal spam regulation met with strong opposition from both sides of the table: consumer advocacy groups as well as marketing associations. *Id.* In most instances, neither side felt that their respective needs were adequately addressed by the proposed legislation. *Id.* Jonathan Krim, *Draft of Bill on Mass E-Mail is Called Weak*, WASH. POST, May 13, 2003, <http://www.washingtonpost.com/ac2/wp-dyn/A47350-2003May12?language=printer>. Because of the strong marketing and Internet industry lobbyists, the current federal spam legislation does "more to protect mass e-mail advertising than to combat spam." *Id.*

strict regulation, the Act does not go far enough.³⁷

The pre-emption of state statutes that provided greater protection than CAN-SPAM forces state agencies to consider alternative means of regulation in order to serve its citizens.³⁸ Aside from the potentiality of contravening a federal statute, such action is also scrutinized at a constitutional level. First, any regulation of commercial speech is in danger of violating the First Amendment.³⁹ Second, an individual state attempting to regulate interstate commerce may violate the dormant Commerce Clause.⁴⁰

1. Does the Action Violate the First Amendment?

To determine whether an action related to commercial speech violates the First Amendment, courts apply the *Central Hudson* test.⁴¹ The four-part *Central Hudson* test asks “as a threshold matter whether the commercial speech concerns unlawful activity or is misleading.”⁴² If the speech is misleading or unlawful, there is no right to First Amendment protection.⁴³ However, if the speech is not misleading or unlawful, the court asks three follow-up questions: (i) “whether the asserted governmental interest is substantial”;⁴⁴ (ii) whether the regulation “directly advances the

37. *Le*, *supra* note 10, ¶¶ 40-41.

38. *See Loomis*, *supra* note 31, at 22 (noting that a group of state Attorneys General stated the loopholes and standards of proof in the Act make it difficult to enforce).

39. “Congress shall make no law . . . abridging the freedom of speech.” U.S. CONST. amend. I. *See Graydon*, *supra* note 3, at 91-92 (explaining the Supreme Court’s *Central Hudson* test to determine if and when commercial speech warrants protection by the First Amendment).

40. “The Congress shall have power . . . to regulate commerce . . . among the several states.” U.S. CONST. art. I, § 8, cl. 3. *See Michelle Armond, III, Cyberlaw: B. Regulating Conduct on the Internet: State Internet Regulation and the Dormant Commerce Clause*, 17 BERKELEY TECH. L.J. 379, 380-85 (2002) (introducing a number of constitutional issues that state legislators face when attempting to regulate commercial messages that are involved in interstate commerce).

41. *Missouri v. Am. Blast Fax, Inc.*, 323 F.3d 649, 653 (8th Cir. 2003). The Supreme Court reversed a district court decision holding that a portion of the Telephone Consumer Protection Act of 1991 (TCPA) violated the First Amendment guarantee of freedom of speech. *Id.* at 652. The relevance of *American Blast Fax* to spam is the restriction imposed on commercial speech. *American Blast Fax, Inc.* was in the business of sending unsolicited commercial advertising to fax machines. *Id.* The TCPA made it illegal “to send an unsolicited advertisement to a telephone facsimile machine.” *Id.* (citing Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227(b)(1)(C) (2000)).

42. *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm’n*, 447 U.S. 557, 566 (1980).

43. *Id.*

44. *Id.* The court concluded that the Government has a “substantial interest” in regulating commercial advertisements via facsimile “in order to prevent the cost shifting and interference such unwanted advertising places

governmental interest asserted”;⁴⁵ and (iii) whether the regulation is “more extensive than is necessary to serve that interest?”⁴⁶ Actions relating to commercial speech are constitutional if and only if all of these questions are successively found in the affirmative.⁴⁷

2. *Does the Action Violate the Dormant Commerce Clause?*

The second constitutional hurdle facing state regulations is the dormant Commerce Clause. A violation of the dormant Commerce Clause occurs when “the states impermissibly intrude on this federal power [to regulate commerce among the several states] when they enact laws that unduly burden interstate commerce.”⁴⁸ Determining whether the dormant Commerce Clause is violated requires a two-part test, commonly referred to as the *Pike* balancing test.⁴⁹ The first step of the test requires determining whether the law is “facially discriminatory” and favors in-state interests at the expense of interstate commerce.⁵⁰ If the state action is held to be facially neutral, the second part of the test is applied, wherein the local benefits are balanced against the burdens that the regulations place on interstate commerce.⁵¹ A

on the recipient.” *Am. Blast Fax*, 323 F.3d at 655. A determination of whether there is a substantial government interest involves a thorough consideration of the construction of the statute and its legislative history. *Id.*

45. *Cent. Hudson*, 447 U.S. at 566. The Government bears the burden of proving the “challenged regulation advances the Government’s interest in a direct and material way.” *Am. Blast Fax*, 323 F.3d at 655 (citing *Cent. Hudson*, 447 U.S. at 566). This inquiry “helps ensure that there is ‘a reasonable fit between the legislature’s ends and the means chosen to accomplish [them].’” *Id.* (quoting *Lorillard Tobacco Co. v. Reilly*, 533 U.S. 525, 556 (2001)). The Court found that the TCPA’s regulation of commercial advertisements via fax “directly and materially advance[d] the asserted governmental interest.” *Id.* at 658.

46. *Cent. Hudson*, 447 U.S. at 566. In respect to the regulation of commercial speech, the court must determine whether the means employed are “narrowly tailored” to achieve the legislator’s intended objective. *Am. Blast Fax*, 323 F.3d at 659. The court concluded that restricting the commercial advertisements via facsimile in the manner in which the TCPA did presented means that were narrowly tailored to its objectives. *Id.* at 660.

47. *Cent. Hudson*, 447 U.S. at 566. Failure to answer one of the final three tests in the affirmative demonstrates that the speech is protected by the First Amendment. *Id.*

48. *State v. Heckel*, 24 P.3d 404, 409 (Wash. 2001). See discussion at *infra* note 56.

49. *Pike v. Bruce Church, Inc.*, 397 U.S. 137, 142 (1970).

50. *Id.*

51. *Id.*

If a legitimate local purpose is found, then the question becomes one of degree. And the extent of the burden that will be tolerated will of course depend on the nature of the local interest involved, and on whether it could be promoted as well with a lesser impact on interstate activities.

Id.

law that is facially neutral and does not unduly burden interstate commerce in favor of local interests does not violate the dormant Commerce Clause.⁵²

Though seemingly daunting when applied to regulation of the Internet, it is possible for such state action to overcome dormant Commerce Clause issues. Prior to the enactment of CAN-SPAM, two examples of state e-mail legislation represented the outer boundaries of state regulation of e-mail.⁵³ Though now preempted, the New York and Washington Acts serve as models for formulating valid potential state action regarding e-mail.

Washington's Commercial Electronic Mail Act ("Washington Act") prohibited deceptive e-mail or any e-mail with mislabeled subject lines.⁵⁴ The Washington Act allowed criminal sanctions as well as civil penalties.⁵⁵ The Supreme Court of Washington held in *State v. Heckel* that because the Washington Act sought to regulate only those e-mails sent from within the state or to a known resident of the state, it was not regulating interstate commerce.⁵⁶ Secondly, the benefits to the state's residents outweighed any burdens placed upon the senders of the commercial e-mail.⁵⁷ Finally, the Washington Act did not create an inconsistency among the several states as it "merely create[d] additional, but not irreconcilable, obligations" on the sender.⁵⁸

New York's former e-mail regulation, however, violated the

52. *Id.*

53. Both the State of Washington and the State of New York enacted e-mail statutes that were challenged on constitutional grounds. The Washington Act survived the challenge. See *infra* note 56 and accompanying text (discussing the Act and the proceedings that held it to be constitutional). Conversely, the New York Act violated the dormant Commerce Clause. See *infra* note 59 and accompanying text (discussing the Act and what deemed it unconstitutional).

54. Commercial Electronic Mail Act, WASH. REV. CODE §§ 19.190.005-19.190.070 (2003).

55. *Id.*

56. *Heckel*, 24 P.3d at 409. The Supreme Court of Washington, in upholding the constitutionality of the Act, applied the *Pike* balancing test and reversed a trial court decision that held the Act unduly burdened interstate commerce. *Id.* at 406. "[T]he Act does not burden interstate commerce by regulating when or where recipients may open the proscribed UCE messages. Rather, the Act addresses the conduct of spammers in targeting Washington consumers." *Id.* at 412. See Wash. Rev. Code § 19.190.020 (limiting violations of the Act to those unsolicited messages that are sent "from a computer located in Washington or to an electronic mail address that the sender knows, or has reason to know, is held by a Washington resident . . .").

57. *Heckel*, 24 P.3d at 411-12.

58. *Id.* at 412 (quoting *Instructional Sys., Inc. v. Computer Curriculum Corp.*, 35 F.3d 813, 826 (3d Cir. 1994). "The inquiry under the dormant Commerce Clause is not whether the states have enacted different anti-spam statutes but whether those differences create compliance costs that are 'clearly excessive in relation to the putative local benefits.'" *Id.* (quoting *Pike*, 397 U.S. at 142).

dormant Commerce Clause, as held in *American Libraries Ass'n v. Pataki*.⁵⁹ The court in *American Libraries* held that regulation of activity within the Internet is “wholly insensitive to geographic distinctions.”⁶⁰ Spam proponents argue the direct interpretation of this holding is that no state action regarding UCE or the Internet will be held constitutional.⁶¹ A distinction must be made, however, between generally regulating activity on the Internet and regulating the sending of e-mail from within the state or to a resident of that state. The court in *American Libraries* reviewed the constitutionality of the New York Act as applied to “all Internet activity,”⁶² a stark contrast from action that seeks only to apply to intrastate activity.

III. ANALYSIS: WHY NAYSAYERS CALL IT THE “YOU-CAN-SPAM ACT.”

This Part analyzes the recently enacted CAN-SPAM Act, including the international effect of this legislation. This discussion also includes a comparison of American “opt-out” legislation and European “opt-in” legislation. Following this is an exploration of measures Illinois took in the past to combat spam.

A. *The CAN-SPAM Act is Not Enough to Battle Spam*

To date, no single administrative body regulates the Internet.⁶³ Some areas of the Internet can be akin to the Wild West; individual corporations maintain complete control over their own computer networks, but none whatsoever over the Internet or another person’s network.⁶⁴ Though federal agencies are beginning to recognize the serious nature of spam,⁶⁵ the onus is

59. *American Libraries Ass'n v. Pataki*, 969 F. Supp. 160, 170 (S.D.N.Y. 1997).

60. *Id.*

61. *See, e.g., Ferguson v. Friendfinders, Inc.*, 94 Cal. App. 4th 1255, 1260, 1264 (Cal. Ct. App. 1st Dist. 2002) (describing the respondent’s argument that a California statute regulating commercial e-mail violated the doctrine established in *American Libraries*). The court found the argument to be invalid as the California statute is not regulating the entire Internet, but rather a narrower subsection of the Internet which would not interfere with or burden interstate commerce. *Id.* at 1264.

62. *Am. Libraries*, 969 F. Supp. at 170. *Cf. Ferguson*, 94 Cal. App. 4th at 1261-62 (holding that the jurisdictional limitations in the California statute create a distinction from the New York statute at issue in *American Libraries*).

63. *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1018 (S.D. Ohio 1997). *CompuServe* is the first major case to deal with the broad implications of mass e-mailing. *Id.* The case provides a general overview of the history and technology behind the Internet and discusses failed attempts to regulate the Internet. *Id.*

64. *See id.* (discussing the infancy of the Internet as well as the attempts by different branches of government or various corporations to regulate the Internet).

65. *See, e.g., DISGRUNTLED PHILLIES FAN ARRESTED FOR E-MAIL SPAMS*,

still upon the corporation to protect its own interests.

1. *Why Spam is Such a Popular Marketing Tool*

One of the most appealing attributes of sending spam is the low cost to the sender.⁶⁶ As with most rules of economics, costs in a transaction must be borne by one of the parties; with spam, the recipient bears that cost.⁶⁷ The costs involved in using spam as a marketing tool are remarkably one-sided: the average spammer is capable of e-mailing 10,000 electronic mailboxes for under \$100,⁶⁸ while the corporate recipients spent almost \$9 billion in 2002 attempting to avoid receiving spam.⁶⁹ The net result of this cost-shift is that the spammer, with little regard for conserving resources, has no interest in self-regulation.⁷⁰ Based partly on this inequity, the federal government decided that legislative action was necessary in order to reign in the spammers.⁷¹

2. *The Limitations of CAN-SPAM*

After years of failed attempts to regulate unsolicited commercial e-mail,⁷² Congress finally passed CAN-SPAM late in 2003.⁷³ CAN-SPAM marks the first legislation designed to regulate commercial activity on the Internet.⁷⁴ It must be made

Reuters, Oct. 8, 2003 (describing the FBI's arrest of a hacker in Glendale, CA who sent thousands of forged and fraudulent e-mails to a Philadelphia newspaper, crippling the newspaper's network).

66. Graydon, *supra* note 3, at 82.

67. Sorkin, *supra* note 13, at 335.

68. *You've Got Spam*, at <http://public.findlaw.com/internet/nolo/ency/A6F26AE8-C831-469E-81157FC4252D98CB.html> (last visited Aug. 3, 2003).

69. Brian Morrissey, *Report: Spam Cost Corporate America \$9B Last Year*, at <http://www.internetnews.com/IAR/article.php/1564761> (Jan. 6, 2003). The report, compiled by Ferris Research, calculated the cost of spam to corporations by focusing on three primary categories: "loss of worker productivity; consumption of bandwidth and other tech resources; and use of technical support time." *Id.*

70. Sorkin, *supra* note 13, at 335.

71. CAN-SPAM § 2(a). One of the congressional findings leading to the passage of CAN-SPAM is related to this cost-shifting. *Id.* "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, or for the time spent accessing, reviewing, and discarding such mail, or for both." *Id.* § 2(a)(3).

72. See Gary S. Moorefield, Note, *SPAM - It's Not Just for Breakfast Anymore: Federal Legislation and the Fight to Free the Internet From Unsolicited Commercial E-Mail*, 5 B.U. J. SCI. & TECH. L. 10, ¶¶ 25-33 (1999) (reciting a brief history of six proposed federal spam regulations and the inability of Congress to pass them), available at <http://www.bu.edu/law/scitech/volume5/5bujst/10.pdf>.

73. President Bush signed CAN-SPAM into law on December 16, 2003.

74. See *Senate Approves Antispam Bill*, REUTERS, http://news.com.com/2100-1028_3-5095408.html (last modified Oct. 22, 2003) [hereinafter "Senate"] (describing the passage of Senate Bill 877, the pre-cursor to CAN-SPAM).

clear, however, exactly what CAN-SPAM regulates. The Act outlaws only *fraudulent* or *deceptive* commercial e-mails⁷⁵ and enables the Federal Trade Commission (“FTC”) to research the *feasibility* of establishing a “do not e-mail (spam)” registry similar to the “do not call” registry enacted on October 1, 2003 to regulate telemarketers.⁷⁶

Though well intended, CAN-SPAM falls short of providing strong enough relief for corporations. The proposed e-mail registry alone presents several difficulties. First, if the registry were created, there would still remain an essentially unlimited ability to send commercial e-mails to any person not on the registry.⁷⁷ A second major failing of this registry falls on corporate IT departments where not every individual recipient within the corporation is on the registry, or where the registry does not allow entire domain names to be registered.⁷⁸ Furthermore, the mere creation of such a registry could take years, as evidenced by the fact that almost twelve years elapsed between authorization and activation of the federal “do not call” registry.⁷⁹ Finally, private rights of action are abolished under CAN-SPAM.⁸⁰ Therefore, all causes of action are brought by the State Attorney General’s office or through the FTC.⁸¹ Such action could prove to be too costly and of too low a priority for a government with severe budget constraints.⁸²

75. Estimates conflict as to the percentage of commercial e-mails that are actually fraudulent or deceptive. Congressional findings declare that “[m]ost of [unsolicited commercial e-mail] messages are fraudulent or deceptive in one or more respects.” CAN-SPAM § 2(a)(2). However, FTC research indicates that less than one-third of the commercial e-mails sent are fraudulent. FTC, *supra* note 19, at 3-5.

76. *Senate, supra* note 74.

77. Coalition Against Unsolicited Commercial E-Mail, *CAUCE Comments on FTC Decision Not to Create a Do Not Spam Registry*, at <http://www.cauce.org/news/index.shtml> (June 16, 2004) [hereinafter CAUCE].

78. *Id.*

79. CAN-SPAM § 9. There is a key distinction between a bill that *empowers* the FTC to create a “do not e-mail” registry and a bill that *requires* the agency to create the registry. CAUCE, *supra* note 77. The Federal Communications Commission received the power to create the “do not call” registry in 1991, but the list was not created until 2003. *Id.* The argument follows that had the agency been required to create such a list, as well as given appropriate timetables for implementation, the “do not call” registry would have been active by the mid-1990s. *Id.*

80. CAN-SPAM § 7.

81. *Id.* In May 2003, representatives from the FTC and the National Association of Attorneys General made it clear that the agencies do not have the resources necessary to pursue enough anti-spam suits in order to even make a dent in the spam problem. CAUCE, *supra* note 77.

82. CAUCE, *supra* note 77. In order to have a deterrent effect, the spam regulations will have to be enforced and prosecuted in a vigorous and consistent manner. *Id.* Neither state budgets nor the federal budget have the flexibility to provide for extra law enforcement officials and prosecutors

B. International Implications

1. The Effect of CAN-SPAM on Other Countries

In the most simple of terms, there are two forms of anti-spam legislation: "opt-in" legislation and "opt-out" legislation.⁸³ The distinction between the two revolves around recipient choice: a recipient who "opts in" is requesting that the spammer send him e-mail; the recipient who "opts out" is telling the spammer not to send him any e-mail.⁸⁴ CAN-SPAM is "opt-out" legislation that requires the recipient to take affirmative steps to stop receiving e-mails.⁸⁵ "Opt-in" legislation, popular in Europe, effectively outlaws all *unsolicited* commercial e-mails, making it unlawful to forward commercial e-mails to any person not requesting e-mails from the sender.⁸⁶

In America, the Direct Marketing Association and other pro-spam groups heavily lobbied for the passage of CAN-SPAM.⁸⁷ Marketing groups favor this "opt-out" legislation as it requires the recipient to take active measures to remove himself from mailing lists and it does not place the burden on the spammer to seek and compile active recipient lists.⁸⁸ Several European countries, where "opt-in" legislation is currently enacted, fear that European spammers will move their operations to the United States where there is only "opt-out" legislation, effectively undercutting European efforts to block spam.⁸⁹

dedicated solely to spam. *Id.*

83. The Spamhaus Project, *Mailing Lists vs. Spam Lists*, at <http://www.spamhaus.org/maillinglists.html> (last visited October 26, 2003) [hereinafter The Spamhaus Project, *Mailing Lists*].

84. *Id.*

85. CAN-SPAM § 5(a)(3)(A)(i).

86. The Spamhaus Project, *Mailing Lists*, *supra* note 83.

87. See Carol Krol, *Federal Anti-Spam Law Passage is Imminent*, at <http://www.btonline.com/cgi-bin/article.pl?id=12001> (Dec. 8, 2003) (stating that company stakeholders were pleased with the impending passage of Can-Spam and that a "national standard on e-mail marketing" is a "wonderful early Christmas present").

88. The Spamhaus Project, *United States Heads Toward Legalization of Spam*, at <http://www.spamhaus.org/news.lasso?article=10> (Oct. 22, 2003) (arguing that CAN-SPAM will effectively legalize the practice of spamming, and explaining the negating effect that this could have on European laws) [hereinafter The Spamhaus Project, *Legalization of Spam*].

89. Dugie Standeford, *Opt-out and Weak Enforcement Said to Foster International Spam*, WARREN'S WASHINGTON INTERNET DAILY, Jan. 13, 2004, available at 2004 WL 60517143. Standeford quotes British Member of Parliament as stating: "With so much unsolicited commercial e-mail and pornography flooding the U.K., the U.S.'s reputation as a commercial partner is suffering because Britons believe no one's prepared to do anything." *Id.* See also The Spamhaus Project, *Legalization of Spam*, *supra* note 88 (arguing that CAN SPAM actually removes legal barriers to spamming and makes it difficult for Europe to maintain and enforce its laws).

2. *The Effect of International Spammers on the United States*

Much like the European countries that fear spam originating from the United States, the United States accordingly must fear spam originating from unregulated countries.⁹⁰ Many of the most egregious spam messages originate offshore, and therefore are outside the jurisdictional reach of CAN-SPAM.⁹¹ With no immediate ability to identify the e-mail's country of origin, a recipient may unwittingly request removal from an off-shore spammer.⁹² This request for removal will likely generate the opposite effect; the spammer now knows there is a live e-mail address and the volume of spam sent to that address will increase.⁹³

C. *The Impact of Spam on Illinois Businesses*

Aside from being home to some of the world's most influential businesses,⁹⁴ Illinois is also home to thousands of smaller, close corporations.⁹⁵ Spam's impact on Illinois businesses is far-reaching and includes lost man-hours, wasted financial resources, steadily increasing investment in equipment upgrades, and exposure to security breaches.⁹⁶ The exposure to the Internet is one of the most difficult for IT departments to grapple with as twenty-two percent of spam messages contain false text in the

90. Jacobs, *supra* note 15.

91. *See id.* (stating that many spammers are overseas and outside of the reach of CAN-SPAM); Silverman, *supra* note 29.

92. Jacobs, *supra* note 15.

93. Silverman, *supra* note 29.

94. *See Chicago's Largest Public Companies*, *supra* note 16. (listing a number of the world's most influential corporations that have headquarters in Illinois).

95. *See* 2002 ILL. SEC. OF STATE CORPORATION STATISTICS (providing figures relating to incorporated entities registered with the State of Illinois and designating those incorporated as LLCs, Subchapter S Corporations and C-Corporations).

96. Credence E. Fogo, *The Postman Always Rings 4,000 Times: New Approaches to Curb Spam*, 18 J. MARSHALL J. COMPUTER & INFO. L. 915, 919 (2000). Aside from dedicated human resources, the most expensive costs to IT departments are upgrades to servers and other network equipment required to increase the network bandwidth simply to carry the load of UCEs flowing steadily in and out of the system. *Id.* One of the greatest problems facing IT staff comes not from spam that gets through the server and winds up on the recipient's desktop, but rather from the UCE that is recognized by the server and bounced back to the sender, which is generally an invalid return e-mail address. *Id.* This return e-mail is then sent back to the server, along with a notification that there is an invalid e-mail address. *Id.* By the end of the process, no fewer than four messages are logged into the company's server. *Id.* Therefore, a company with 100 employees who each receive ten pieces of recognized spam per day would result in an additional 4,000 messages logged into the server daily.

subject line.⁹⁷ The goal of these false messages is to connote some sort of pre-existing relationship between the sender and the recipient, making it more likely that the recipient will open the e-mail.⁹⁸ The threat to network security is greatest at this point, as viruses can be launched unknowingly by the recipient opening the e-mail, sending an entire network grinding to a halt or exposing a delicate corporate infrastructure to hackers.⁹⁹ Though CAN-SPAM addresses fraudulent e-mail, there is no means of protection from the foreign-sourced fraudulent e-mails.¹⁰⁰

D. A Brief History of Illinois Action in Response to Spam

Illinois enacted a series of statutes in its attempt to manage the havoc that spammers wreak on corporations.¹⁰¹ Similar to CAN-SPAM, Illinois's statute targeted fraudulent e-mail and required recipients to "opt out" of receiving further e-mails.¹⁰² But Illinois also went further than CAN-SPAM by imposing affirmative regulations such as requiring advertisement labels in the e-mail's subject line.¹⁰³ Any recipient "opting out" or otherwise qualifying under the Acts was entitled to either statutory or actual damages.¹⁰⁴ Though the Acts sought regulation of fraudulent spam, the impact to the spammer was minimal, if present at all.¹⁰⁵ Despite the state regulation, due to increasing volumes of spam,¹⁰⁶

97. FTC, *supra* note 19, at 5.

98. *Id.* at 5-6.

99. See Sorkin, *supra* note 13, at 336 (describing how simply opening an e-mail may launch a virus and the obvious threat to network security that this presents).

100. CAN-SPAM § 5.

101. Electronic Mail Act, 815 ILL. COMP. STAT. 511/1-511/905, (2002); Computer Crime Criminal Act, 720 ILL. COMP. STAT. 5/16D-1-5/16D-7 (2000) [hereinafter Computer Crime Act]; Consumer Fraud and Deceptive Business Practices Act, 815 ILL. COMP. STAT. 505/1-505/12 (2002) [hereinafter Consumer Fraud Act].

102. Electronic Mail Act, § 10(a-5)-(a-15).

103. *Id.* § 10(a-15).

104. "The injured person may recover attorney's fees and costs, and may elect, in lieu of recovery of actual damages, to recover the lesser of \$10 for each and every unsolicited electronic mail advertisement transmitted in violation of this Section, or \$25,000 per day." Electronic Mail Act, § 10(c). In order to "qualify" or receive injury that the statute can remedy, you must be a recipient of an "unsolicited electronic mail advertisement." *Id.* §§ 511/5, 511/10.

105. See Sorkin, *supra* note 13, at 352-54 (arguing that opt-out activities are not effective in a corporate setting). Though "opt-out" can be highly effective in other areas of advertising, such as telemarketing, there is less likelihood of an anonymous spammer complying with a person's opt-out request. *Id.*

106. See The Spamhaus Project, *Legalization of Spam*, *supra* note 88 (arguing that CAN-SPAM encourages increased volumes of spam). "The United States Congress is . . . giving Unsolicited Bulk Email the green light and unleashing the spamming power of 23 Million American small businesses onto an Internet which already can not cope with the billions of unsolicited bulk mailings sent by just 200 current businesses." *Id.*

network security continued to be at an all-time low, exposed to viruses and clogged servers.

E. The Impact of CAN-SPAM on Illinois Businesses

The immediate and obvious effect of CAN-SPAM is pre-emption of the Illinois statute,¹⁰⁷ thereby removing the affirmative regulations that Illinois placed on spam. The protection that thus remains for Illinois businesses is the CAN-SPAM prohibition on fraudulent spam.¹⁰⁸ History demonstrates that a prohibition on fraudulent spam is at best a compromise.¹⁰⁹ Though some argue that only an outright ban on spam will suffice to assist Illinois businesses,¹¹⁰ such a measure is undoubtedly unconstitutional.¹¹¹ Tackling the fraudulent senders of spam is a formidable start, but with the technology battle that forces recipients to continually upgrade systems in order to battle spam, the spammers are likewise developing newer and better ways to get around the recipient's technology; employing fraudulent means is merely an amateur effort to beat this technology.¹¹²

One of the major issues that corporations face is the sheer volume of e-mail messages that filter through the servers on a daily basis.¹¹³ With a reduction in the numbers of e-mails sent comes a corollary freeing up of corporate resources dedicated to battling this mountainous volume of messages consisting largely of

107. CAN-SPAM § 8(b).

108. *Id.* § 5.

109. See CAUCE, *supra* note 77 (arguing that simply outlawing fraudulent practices in the sending of unsolicited electronic commercial advertisements grants spammers a "virtually unlimited license to send as much spam as they want, provided they don't tell lies while doing so").

110. See The Spamhaus Project, *Legalization of Spam*, *supra* note 88 (arguing that the only effective means to reduce the increasing volume of spam is to follow Europe's lead and outlaw the *unsolicited* commercial e-mails).

111. See Graydon, *supra* note 3, at 107-14 (applying the *Central Hudson* test to the regulation of spam). See also Fisher, *supra* note 11, at 410-11 (doubting the ability of a complete ban on spam to withstand a constitutional challenge because of the existence of less restrictive measures to combat spam).

112. See Michael O'Neil and David Senf, *Strategies to Manage the Spam Menace: Part 1*, at <http://www2.cio.com/analyst/report1746.html> (Sept. 17, 2003) (discussing new technologies that corporate IT departments may employ to combat the volume of spam received on a daily basis). See generally Paul Hoffman & Dave Crocker, *Unsolicited Bulk Email: Mechanisms for Control*, at <http://www.imc.org/ube-sol.html> (May 4, 1998) (debating the efficacy of various methods of battling spam and asserting that fraudulent e-mails are the easiest to contend with).

113. See Sorokin, *supra* note 13, at 336-39 (discussing the technological measures that corporations employ to deal with the volume of e-mail messages that a company receives as well as the exponential factor with which unsolicited commercial e-mails increase this volume).

spam.¹¹⁴ Yet, even if there is a reduction in the number of e-mails sent, under CAN-SPAM, the recipient is still burdened with taking the time to remove himself from the spammer's lists.¹¹⁵ In a regulated environment, a corporation should not be forced into a position where it is continuously expending its own resources to eliminate spam; this is no better than having no regulations at all.¹¹⁶

F. How Will Illinois Action Benefit Illinois Businesses?

Illinois corporations are a vital asset to the state's economy and revenue stream.¹¹⁷ During a time when the state faces one of its largest fiscal crises in history, with a soaring budget deficit and faltering economy,¹¹⁸ it is crucial to protect the hometown businesses. Revising and introducing programs outside of regulation will allow businesses to free up human, technological, and financial resources.¹¹⁹ Resources currently dedicated to battling spam can be refocused as new research and development, enhanced technology, and ultimately, greater investment in the community and creation of new jobs.¹²⁰ In the current environment, where costs are minimal to the spammer, the spammer operates almost free of consequences.¹²¹ These costs must be evened out if there is any hope to adequately assist

114. *Id.*

115. See Morrissey, *supra* note 69 (rebutting the argument that opting out of e-mail lists is not a time consuming activity). From an individual standpoint, opting out may take on average only 4.5 seconds of a recipient's time. However, when multiplied by ten unwanted e-mails per day, this consumes around one minute per day and five minutes per work week. See generally *id.* (calculating the human resource costs to a company when dealing with opt-out provisions). Given a company that has 100 employees, that is almost eight hours lost every week.

116. See Fisher, *supra* note 11, at 411-12 (denying the efficacy of opt-out provisions, citing concerns about abuse and the fact that it places the burden on the consumer to remove himself from the e-mail list). "[T]he public opt-out list is a singularly dangerous alternative. It might actually do more harm than good . . ." *Id.* at 411-12.

117. See generally 2001 ILL. DEP'T OF REVENUE ANN. REP. OF COLLECTIONS & DISTRIBUTIONS (summarizing the revenue that Illinois generated based on individual and corporate income and use taxes).

118. Christi Parsons & Adam Kovac, *State Pile of Unpaid Bills Reaches \$1.2 Billion*, CHI. TRIB., Apr. 4, 2002, at 1.

119. See Rutrell Yasin, *New Technologies Tackle Spam Problem*, FED. COMPUTER WK., Mar. 17, 2003 (describing the unrelenting efforts of technology managers to develop new technologies), available at <http://www.fcw.com/fcw/articles/2003/0317/tec-spam-03-17-03.asp>.

120. See *id.* (discussing advantages that advanced development of technology brings and resources that could be freed if the spam war was ended).

121. See Sorkin, *supra* note 13, at 334-35 (discussing the cost-shifting nature of sending spam and the consequence-free ability of spammers to send their messages).

Illinois businesses.

IV. PROPOSAL: MORE TECHNOLOGY, LESS FUTILE REGULATION

The efforts of the Illinois government to protect its corporate citizens to date has not been effective.¹²² This section first proposes a two-pronged solution that protects Illinois businesses and avoids pre-emption, while not trampling on protected commercial speech. The benefits to both the corporation and to the state are then discussed. Finally, advantages to this proposal over other alternatives are reviewed.

In the past, the now pre-empted Illinois statutes imposed affirmative regulations on spam that risked being overturned due to possible conflicts between the states.¹²³ Enacting further alternative statutes directly addressing spam is futile, as they would contravene CAN-SPAM.¹²⁴ However, Illinois must not remain content with the federal regulations and must therefore seek to supplement CAN-SPAM with local incentive programs.

Illinois should implement a two-pronged strategy to battle spam, with the primary focus of its efforts on its corporate citizens. Initially, Illinois must encourage business investment in technological measures to overcome spam via tax incentives. Second, Illinois must create a right within its fraud statutes that allows private citizens to bring action *on behalf of* the state government against abusive spammers. This proposal allows the state to approach spam through two separate fronts: encouragement of technological innovation and deterrence of spammers.

The first step of this proposal implements a tax incentive

122. See *supra* notes 101-05 and accompanying text (discussing the previous Illinois statutes and their shortcomings).

123. See Armond, *supra* note 40, at 399-400 (summarizing possible constitutional challenges, outside of pre-emption, to state statutes regulating spam). An example of an affirmative regulation on spam would be requiring the sender to label the message as spam or requiring placement of certain messages in the body of the e-mail, such as contact information. *Id.* at 399. The state imposition of an affirmative regulation on an e-mail sender could result in conflicting regulations nationwide, which could ultimately subject the regulation to unconstitutionality. *Id.* at 400.

124. Two of the choices available in terms of statutory regulation are placing affirmative regulations on the sender (regulations that Illinois currently employs), or conducting a complete ban on spam. Neither of these choices will likely stand up to constitutional analysis. See *id.* at 399-400 (lending merit to the idea that affirmative regulations will be subject to being overturned on constitutional grounds). See also Joshua A. Marcus, *Commercial Speech on the Internet: Spam and the First Amendment*, 16 CARDOZO ARTS & ENT. L.J. 245, 284-88 (1998) (analyzing Supreme Court holdings regarding commercial speech and their applicability to the Internet). See *supra* note 10, ¶¶ 9-13 (discussing the high unlikelihood that a complete ban on unsolicited commercial e-mail will survive even an intermediate standard of review).

program designed to encourage business and reward development.¹²⁵ Illinois businesses are currently battling spam on their own initiative,¹²⁶ and this drains the corporate checkbook.¹²⁷ The technological battles that corporations currently wage remain a step behind the technology employed by spammers.¹²⁸ Limited by their own budgets and continually playing “catch up,” the odds of success for businesses are slim.¹²⁹ With the Illinois tax incentive program, the drains on the corporate checkbook would be reduced and Illinois businesses would be able to leap-frog ahead of the spammers.

Specifically, the proposed Illinois program provides incentives in the form of tax reimbursements for corporate expenditures incurred in battling spam. Expenditures such as software development or dedicated human resources cost Illinois businesses millions of dollars each year and are not recoverable under the current tax laws. Providing corporations with an opportunity to recover a portion of these lost dollars will relieve the pressure that spam places on business resources.

The incentives apply to Illinois businesses or businesses doing a substantial portion of their business in Illinois, including ISPs. The program will also include a special incentive for companies that devote a majority of their efforts to providing third-party

125. The goal is to fund technological initiatives useful in the war on spam. Such approaches include the proposal to place a one-cent stamp on each outgoing e-mail. See Saul Hansell, *Speech by Gates Lends Visibility to E-Mail Stamp in War on Spam*, N.Y. TIMES, Feb. 2, 2004, at C1 (proposing tax on e-mail to stem the tide of spam). Though such proposals are not without merit, they are outside the scope of possible state action. See *supra* note 123 (discussing constitutional implications of state action in interstate commerce).

126. See Sorkin, *supra* note 13, at 344-50 (summarizing the various technical tools that corporations may employ to eliminate spam). Some of the common methods include end-user filtering, third-party “proxy filters,” and “database blacklists.” *Id.* End user filtering is the most common tool, which requires the receiver (either the receiving server or the computer user) to review the sender and subject line to decide whether the message should be downloaded. *Id.* at 344-46. Though this sounds simplistic, complex programs and algorithms are being continuously developed to reduce the end-users time devoted to reviewing e-mail. *Id.* Third-party “proxy filters” are similar to end-user filtering, but on a much larger scale, as these are companies and software developments dedicated solely to battling spam for its clients. *Id.* at 346-47. Finally, database blacklists are devices designed to track e-mail patterns that spammers employ, allowing companies to use the database to identify spammers. *Id.* at 347-49.

127. See *id.* at 356 (discussing the drawbacks to spam, which include the enormous drain on monetary resources by IT departments and ISPs).

128. See *supra* note 112 and accompanying text (discussing the back and forth nature of the spam battle which requires each side to repeatedly upgrade technology every time that the opposing side increases technology).

129. See *You've Got Spam*, *supra* note 68 (arguing that the battle against spam is at times futile due to the continually building investments of both finances and human resources).

solutions, such as software developers. The benefit to Illinois will outweigh the costs in terms of drawing business to Illinois, especially technology companies, which Illinois has struggled in the past to recruit. The incentives must be narrowly drawn and limited to specific reportable activities.¹³⁰

Benefits occur at two levels. First, the incentives free up much needed financial as well as human resources. The money spent battling spam could be re-invested into the company, stimulating growth. In turn, this will positively benefit the state with much needed economic stimulus. In effect, this proposal shifts the fiscal responsibility of battling spam to the state and shifts the technological responsibility of battling spam to those experts devoted to development of spam filtering and blocking devices. With these responsibilities shifted, corporations, especially smaller closely held corporations, may return to running their businesses.

The second major benefit of these proposed incentives is centered on winning the battle against spam. Currently, one of the major hurdles to developing more efficient and effective spam filters and blockers is self-imposed corporate limitations on resources.¹³¹ Removal of these barriers to development through greater resource availability will encourage swift development. With more robust development, Illinois businesses will finally have a greater likelihood of coming out ahead.

This incentive program should be primarily self-regulating and should be as simple for the company to implement as possible. The program would be implemented by the state in the form of a new tax rule; therefore, it would not require many new state resources. Creation of additional bureaucracy should be avoided; existing employment levels at the Illinois State Department of Revenue should suffice.¹³² Further, the implementation for the company should be simple. There should be an ability to enter the

130. Activities may include: development of filtering mechanisms; costs to IT departments for developing, installing and monitoring these filtering mechanisms; payments made to third-party developers for such devices; and lost human resource time spent reacting to spam issues. More variable reimbursements such as lost profits, lost business opportunities, and lost good will should be excluded from the statute and deferred to the judiciary on a case-by-case basis.

131. See generally Mayer & Cha, *supra* note 20 (providing an overview of the corporate response to spam and how businesses are struggling to stay ahead of the spammers). In one example, one of the world's largest ISPs installed a highly sophisticated spam filter. *Id.* Though the cost was high, it was designed to last for a number of years. *Id.* Within the span of one year, thirty percent of spam e-mails were getting through the filter and the company could not budget for an enhanced filter for another year. *Id.*

132. See ILL. DEP'T OF REVENUE, *supra* note 117, at 2-7 (listing employment statistics about the agency and increases in efficiency over the last four years, including an increase in on-line capabilities).

reimbursement requests or receipts on an ongoing basis, ideally in an online environment. When the corporation pays its quarterly taxes, the reimbursements should be applied automatically.

The program should be limited in time, as the battle against spam (much like the battle against telemarketers and fax advertisers) will not draw on for decades. Therefore, the program should be limited to a two-year term, renewable for an additional one-year term. After this point, the incentives should automatically cease via a sunset provision in the tax code. A three-year term provides ample time to spur economic development within the state and generate economic and technological advantages, without leaving room for potential abuse.

In an era of fiscal concern for the state, the primary argument against this proposal is that providing tax incentives cuts at the state's revenue.¹³³ Admittedly, such a program could cost the state much needed revenue up front. Focusing on up-front costs, however, is short-sighted. Rather, the program should be viewed as an investment in the state's future. The economic development and technological advancement that the program will create far outweigh the up-front costs.

The second arm of this proposal requires Illinois to broaden the reach of its current Anti-Fraud and Fair Business Practices Acts.¹³⁴ Under CAN-SPAM, the states retain an ability to regulate fraudulent spam practices within the state.¹³⁵ Given restrained budgets and staffing within the Attorney General's office,¹³⁶ the state should implement a "relator" program where citizens act as watchdogs and bring action on behalf of the state.¹³⁷ Citizens as relators would bring the initial action, gather evidence and pursue prosecution of the matter. Similar to the successful Medicaid

133. See, e.g., Greg Hinz, *Let Them Pay Fees*, CRAIN'S CHI. BUS., Nov. 17, 2003, at 13 (explaining the state's revenue and budget crisis and demonstrating the reluctance of the government to provide new incentives during times of fiscal crisis).

134. Computer Crime Act, 720 ILL. COMP. STAT. 5/16D-1, *et. seq.* (2000); Consumer Fraud and Deceptive Business Practices Act, 815 ILL. COMP. STAT. 505/2Z (2000).

135. CAN-SPAM § 8(b)(2). "This Act shall not be construed to preempt the applicability of (A) State laws that are not specific to electronic mail, including State trespass, contract, or tort law; or (B) other State laws to the extent that those laws relate to acts of fraud or computer crime." *Id.*

136. See *supra* note 81 and accompanying text (referencing restraints on staffing within attorney general offices nationwide and the inability to vigorously prosecute spam cases).

137. Such programs are already in use in other areas of fraud abuse, such as Medicaid Fraud and Abuse Prevention. See 31 U.S.C. § 3730(b) (2000) (allowing private parties to prosecute Medicaid fraud on the government's behalf under the False Claims Act).

Anti-Fraud program,¹³⁸ the state may intervene and prosecute the matter itself after reviewing the merits of the claim. If the state chooses not to prosecute the matter, the citizen still retains the right to prosecute on behalf of the state, without the aid of the state.¹³⁹ If the state proceeds with the action, it can then build upon the evidence that the relator has gathered. The relator at this point becomes key to the prosecution. For his efforts, the relator will be awarded up to one-third of the settlement or damage award.

Revenue generated from successful prosecution is then used in two primary fashions: (a) to replenish the short-term tax loss from the incentive program; and (b) to assist further technological development. The plan spares the state from pursuing spurious claims by only prosecuting once a meritorious claim is established. Furthermore, the plan will have a deterrent effect on spammers. Similar to the incentive program, the relator program must be limited in both time and scope; it should not extend beyond three years from enactment, and should only apply to claims addressing unfair spam practices within the state of Illinois.

V. CONCLUSION

The advent of e-mail systems provided a technological leap for corporate communications. Regrettably, this technological leap is hindered by the battle with spam. Illinois corporations collectively spend millions of dollars and thousands of man-hours annually attempting to hold their ground in this battle. Only through the swift and effective action of the Illinois government can the burden be shifted to provide a much needed opportunity for its hometown businesses to come out ahead of the spammers. Development and enactment of specific technological tax incentives, coupled with an incentive program to reward private citizens for reporting and assisting in the prosecution of spam abusers will create an opportunity to shift the burden to the spammers, while also promoting growth of the Illinois economy and spurring technological advancements within the state.

138. *Id.*

139. Though more than likely the success rate will be lower.

