

12-16-2005

The Fight to Save America's Inbox: State Legislation and Litigation in the Wake of CAN-SPAM

Emma Scanlan

Follow this and additional works at: <https://digitalcommons.law.uw.edu/wjlta>



Part of the [Internet Law Commons](#)

Recommended Citation

Emma Scanlan, *The Fight to Save America's Inbox: State Legislation and Litigation in the Wake of CAN-SPAM*, 2 SHIDLER J. L. COM. & TECH. 12 (2005).

Available at: <https://digitalcommons.law.uw.edu/wjlta/vol2/iss3/3>

This Article is brought to you for free and open access by the Law Reviews and Journals at UW Law Digital Commons. It has been accepted for inclusion in Washington Journal of Law, Technology & Arts by an authorized editor of UW Law Digital Commons. For more information, please contact lawref@uw.edu.

THE FIGHT TO SAVE AMERICA'S INBOX: STATE LEGISLATION AND LITIGATION IN THE WAKE OF CAN-SPAM

by Emma Scanlan¹

© 2005 Emma Scanlan

Abstract

The fight to curb the ever-increasing amount of unsolicited commercial email or "spam" showing up in the inboxes of American businesses has generated both state and federal legislation. The CAN-SPAM Act of 2003 was enacted to create a bright-line between spam and legal commercial email. The Act preempted many state spam laws but also left significant enforcement abilities to the individual states. States that elect to create large civil damages for spam without criminalizing the transmission of unsolicited commercial email run the risk of winning cases where the damage awards are largely unenforceable and not effective deterrents to big-time spammers.

The pursuit of civil damages in spam litigation, nonetheless, plays an important role in the overall fight against the flood of unsolicited commercial email. The effect of the use of criminal penalties in combination with large damage awards was illustrated in recent cases in Virginia and Florida. Virginia's spam law, which makes certain types of spamming a felony, is a model for the over 20 states currently considering enacting new spam legislation. Legislative approaches which provide civil liability and criminal penalties for spamming may prove most effective in the fight against spam.

Table of Contents

[Introduction](#)

[Has CAN-SPAM solved the spam problem?](#)

[What does CAN-SPAM require?](#)

[Why is CAN-SPAM so ineffective?](#)

[What CAN-SPAM left to the States](#)

[State law after CAN-SPAM: California, Ohio, Maryland, Georgia, Virginia, and Florida](#)

[Virginia: Home to the Toughest Spam Law in the Nation](#)

[CAN-SPAM and State Law Damage Awards](#)

[Spamming in Florida](#)

[Conclusion](#)

INTRODUCTION

<1> Unsolicited commercial email (UCE) (commonly referred to as "spam") continues to have a significant impact on businesses and Internet Service Providers (ISPs) in the United States. According to a recent report by researchers at Stanford University, the average Internet user spends eighty hours per year dealing with spam, or five minutes out of every hour spent on the Internet.² This translates into lost productivity for businesses and ISPs. What does this mean for a business?

<2> Suppose Company X has 300 full-time employees and each employee uses the computer on a daily basis and works 50 weeks per year. Company X's potential productivity loss from time spent dealing with spam is 3,000 eight-hour workdays per year or ten full workdays per year per employee. In addition to the substantial costs incurred by the business community, ISPs have to maintain enough server space to handle the billions of UCE messages sent through their networks and employ increasingly sophisticated spam filters.

<3> UCE is clogging employee inboxes and costing American business millions of dollars each

year in lost productivity.³ This Article surveys recent State efforts to enact new anti-spam legislation. This Article also focuses on Virginia's criminalization of spamming and how it may provide a model for other states to follow, as well as Florida's use of civil penalties as an alternative approach. Specifically, this Article compares the successful prosecution of a big-time spammer in Virginia with a case under Florida's anti-spam law which provides for civil fines or penalties.

HAS CAN-SPAM SOLVED THE SPAM PROBLEM?

<4> In an effort to control the impact of bulk UCE on Internet users, Congress enacted the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM) in January 2004.⁴ Since CAN-SPAM went into effect, researchers estimate that UCE now comprises approximately 80% of all email sent compared to 50-60% before the enactment of CAN-SPAM.⁵ One recent commentator estimates that UCE will make up 93-95% of all email sent in 2005.⁶

<5> There are several reasons for this continuing increase of UCE. First, UCE is technologically easy to send and hard to trace. Second, there is a tremendous monetary incentive to spam, with spammers expected to receive a 25-50% commission on products sold as a result of their efforts. Third, there are a growing number of "bulletproof" web host services that offer access to stable offshore computer servers which they guarantee will not be shutdown due to complaints about UCE. Fourth, CAN-SPAM requires email recipients to "opt-out" rather than "opt-in" to receive spam. Finally, a spammer is not likely to face significant jail time if prosecuted under CAN-SPAM.⁷

<6> In an attempt to counter these incentives to spam, Virginia enacted legislation in 2003 criminalizing the transmission of bulk UCE by big-time spammers. There are at least 24 additional states currently considering spam legislation.⁸ In addition to allowing for individuals to bring suits against spammers, these states should make the sending of bulk UCE that violates CAN-SPAM a misdemeanor and/or a felony as has been done in Virginia, Maryland, Ohio, and Georgia, taking into consideration the risk that large civil damage awards may be unenforceable. The states' recent efforts to control the UCE problem are largely in response to what many consider to be the ineffectiveness of CAN-SPAM.

What does CAN-SPAM require?

<7> CAN-SPAM imposes limitations, and in some cases penalties, on the Internet transmission of unsolicited commercial electronic mail. In order for UCE to comply with the Act it must (1) have accurate routing information, (2) contain a subject line that is not misleading, (3) provide an opt-out method, (4) be identified as an advertisement, and (5) include the sender's valid physical postal address. Additionally, the UCE sender must respond to any opt-out request within 10 business days absent exigent circumstances.⁹

<8> A transactional or relationship message, which is an email that facilitates an agreed-upon transaction or updates a customer in an existing business relationship,¹⁰ may not have false or misleading routing information, but is otherwise exempt from most provisions of CAN-SPAM.¹¹

Why is CAN-SPAM so ineffective?

<9> Many commentators believe that CAN-SPAM has "legalized spamming itself" by requiring email recipients to "opt-out" of receiving additional messages from a particular sender of UCE instead of requiring that recipients "opt-in" and agree ahead of time to receive the messages.¹² Arguably, that is not the greatest loophole in the Act. Although "opt-out" does allow the transmission of large volumes of UCE, it provides a mechanism for email recipients to avoid receiving multiple messages from the same sender. This ability, coupled with the increasing advances in spam filtering technology, will help email users take back control of their inboxes.

<10> CAN-SPAM has greater problems than its "opt-out" requirement. First, CAN-SPAM does not allow for an individual cause of action with the exception of actions brought by ISPs.

Second, when actions under CAN-SPAM have been successfully brought, the judgments are hard to enforce. Third, the penalties for violating CAN-SPAM are small in comparison to the money being made by big-time spammers through the mass transmission of UCE.

What CAN-SPAM left to the States

<11> One of the driving forces behind the passage of CAN-SPAM was Congress' recognition of the difficulty that varying state spam laws imposed on businesses that were trying to comply with the laws regulating the transmission of UCE. Each state had unique requirements for the transmission of UCE that, due to the geographic amorphousness of email addresses, made it hard for law-abiding businesses to know with which of the disparate statutes they were obligated to comply.¹³

<12> On January 1, 2004, CAN-SPAM went into effect and preempted significant portions of more than 30 states' spam laws.¹⁴ However, CAN-SPAM did not entirely supersede state law regulating UCE. The Act specifically does not preempt "any [state] statute, regulation, or rule ... prohibit[ing] falsity or deception in any portion of a commercial electronic mail message or information attached thereto."¹⁵ The Act also does not preempt state law that is not specific to email, such as state contract, trespass or tort law, or other state laws relating to acts of fraud or computer crime.¹⁶ Since the enactment of CAN-SPAM, several states have enacted legislation to supplement the federal law.

STATE LAW AFTER CAN-SPAM: CALIFORNIA, OHIO, MARYLAND, GEORGIA, VIRGINIA, AND FLORIDA

<13> California allows individual recipients of UCE to bring an action to recover \$1,000 per email up to \$1,000,000 per incident or actual damages.¹⁷ This private right of action is unique to California, allowing individuals, businesses, and anti-spam groups to take a role in the fight against UCE that was previously only available to government entities and ISPs.

<14> Ohio, Maryland, Georgia, and Virginia have enacted legislation that contains felony provisions for the transmission of illegal UCE. Ohio's governor signed a bill on February 11, 2005, creating two "spamming" felonies: (1) illegally transmitting UCE and (2) unauthorized access of a computer.¹⁸ As enacted the bill also provides enhanced criminal penalties for extensive spamming or repeat offenders.¹⁹

<15> Maryland makes it a misdemeanor punishable by imprisonment for up to five years for any person to knowingly send bulk transmissions of UCE with falsified router heading and/or send the UCE through email accounts acquired through fraudulent means.²⁰ In addition, the Maryland law makes the sending of bulk UCE with falsified routing information or through email accounts created by fraudulent means in furtherance of a felony or subsequent to a conviction for spamming under Maryland's or any other relevant law, a felony punishable by up to 10 years in jail.²¹ Maryland's criminal spam law also provides for stiff fines for knowingly sending bulk UCE.²² The Circuit Court of Maryland for Montgomery County declared a previous version of the State's anti-spam law unconstitutional as applied to out-of-state residents.²³ However, most commentators believe this case will have limited, if any, precedential impact.²⁴

<16> On April 19, 2005, Georgia, home of Earthlink, enacted the Georgia Slam Spam E-Mail Act, creating the crime of initiation of deceptive commercial email where a person initiates the transmission of false or misleading commercial email that is sent from, passes through, or is received by a protected computer, punishable by a fine of up to \$1,000 and/or a prison term of up to 12 months.²⁵ However the crime is punishable by a fine of up to \$50,000 and/or a prison term of up to five years where: (1) the volume of UCE transmissions exceeds 10,000 messages in 24 hours; or (2) the volume of UCE transmissions exceeds 100,000 messages in a 30-day period; or (3) the volume of UCE transmissions exceeds one million messages in a one-year period; or (4) where the revenue generated by one UCE is greater than \$1,000; or (5) where the revenue generated by the transmission of UCE to one email service provider or its subscribers exceeds \$50,000; and (6) where a minor is used in any part of the transmission of the UCE.²⁶ The Georgia Act is similar to the Virginia law which criminalizes the transmission of bulk spam out of, through, or into Virginia.

<17> Virginia, "the epicenter of Internet traffic," and home of America Online and several other ISPs, passed one of the toughest anti-spam laws in the nation in 2003.²⁷ The Virginia Computer Crimes Act classifies the sending of unsolicited bulk email (UBE) ²⁸ with falsified transmission or routing information as a Class 6 felony if "[t]he volume of UBE transmitted exceeds: 10,000 attempted recipients in any 24-hour period, 100,000 attempted recipients in any 30-day time period, or one million attempted recipients in any one-year time period" and is sent "through or into the computer network of an electronic mail service provider or its subscribers."²⁹ Considering that an estimated 80% of all email traffic is routed through Virginia, the potential impact of the Virginia Computer Crime Act in the fight against spam could be significant. Recent litigation suggests that it will be.³⁰

<18> In November 2004, a jury convicted Jeremy Jaynes, once considered to be the eighth most prolific spammer in the world,³¹ and his sister, Jessica DeGroot, on three felony counts for violation of Virginia's Computer Crimes Act, in what was the nation's first felony spam trial.³² Jaynes, who prosecutors claimed sent more than 7.5 million spam messages on July 16, 2003, alone, was sentenced to nine years in prison. The trial court has delayed the start of Jayne's prison term while the case is on appeal.³³ DeGroot's conviction, with a penalty fine of \$7,500, was overturned by presiding Circuit Court Judge Thomas D. Horne, because "he could not find 'any rational basis' to find DeGroot guilty."³⁴

<19> By making the transmission of spam with forged routing information a felony, Virginia has put a significant damper on the otherwise minimal consequences of sending illegal spam. For a spammer like Jaynes, with an estimated \$24 million in assets gained through illegal spamming operations, the fines likely to be levied under CAN-SPAM alone would be insignificant. If Jaynes had been prosecuted under CAN-SPAM, he would have been subject to a fine of up to \$6 million,³⁵ if the court found aggravating factors, and a jail sentence of up to three years.³⁶ In contrast, under Virginia law, Jaynes may face a much longer sentence if he loses his appeal.

<20> Virginia's recent prosecution of a large bulk spammer is illustrative of the kind of result states may get if they elect to criminalize the transmission of bulk spam. Spammers will likely be deterred from sending UCE with misleading routing information and no method for recipients to opt-out of future messages if they face significant jail sentences. In contrast, the type of enforcement actions pursued in Florida – where large damages awards are sought and not reinforced by criminal provisions – may not serve as an effective deterrent to bulk spammers who may declare bankruptcy, reincorporate under a new name, and start spamming again.

CAN-SPAM AND STATE LAW DAMAGE AWARDS

<21> Enforcement efforts under CAN-SPAM and state ant-spam laws that do not have felony provisions have resulted in successful injunctions and large judgments. These actions have been initiated mainly by ISPs.

Spamming in Florida

<22> Florida is often referred to as the "spam capital of the world."³⁷ Many spammers run their operations out of Florida because of its personal bankruptcy laws that allow debtors to keep large estates out of the hands of judicial lien creditors.³⁸ Spammers who are prosecuted in Florida and have enormous fines levied against them can potentially declare bankruptcy and keep their houses and other significant assets. For instance, in *Kramer v. Cash Link Systems*, a district court in Iowa granted a default judgment in favor of a small ISP (CIS Internet Services) in Iowa against Cash Link, a Florida corporation and two other companies for \$1 billion in damages.³⁹ This is the largest judgment ever rendered in a spam case.⁴⁰

<23> Robert Kramer, owner of the victorious ISP, asked the court to declare the judgments against the three defendants nondischargeable in bankruptcy, but the court declined to do so

as there were no bankruptcy proceedings before the court.⁴¹ Anti-spam groups have pointed out that the defendants will probably file for bankruptcy, reincorporate, and go on spamming.⁴² It will be easier for the defendants to do because they are incorporated in Florida.⁴³

<24> The Florida Electronic Mail Communications Act was enacted on July 1, 2004. The Act allows plaintiffs (The State of Florida, ISPs, telephone companies or cable providers) to recover actual damages or liquidated damages of \$500 per UCE message that contains falsified or missing routing information, uses a third party's Internet domain name without permission, or contains false or deceptive information in the body of the message that is designed to cause damage.⁴⁴ The law does not require that a particular amount of UCE, such as 10,000 messages per day, be sent by the spammer in order for the plaintiff to recover damages.

<25> In partnership with Microsoft, the Florida Attorney General's office brought a case against two spammers, Scott Filary and Donald Townsend, alleging numerous violations of the new Florida spam law and other state and federal laws.⁴⁵ Microsoft used its MSN Hotmail "spam-traps" to capture 65,000 UCE messages violating one or more provisions of the Florida spam law allegedly sent by Filary and Townsend.⁴⁶ In April 2005, the Attorney General's Office obtained an injunction against the defendants barring them from sending spam while the case is being tried.⁴⁷ If found guilty of sending the 65,000 UCE messages, the defendants could face a penalty of up to \$24 million.⁴⁸

<26> There are two potential problems with trying to enforce a large damage award, such as the one sought by the Florida Attorney General, against bulk spammers. First, the defendants could declare bankruptcy, and with little or no capital, start spamming again. Second, the defendants, as in the Virginia case discussed above, may have more than \$24 million dollars in assets gained through spamming, in which case they could simply pay the fine and continue spamming. Thus, while large civil penalties may be one useful tool, the criminalization of spam presents prosecutors with a complementary tool to punish larger or repeat spammers.

CONCLUSION

<27> CAN-SPAM and many states' laws provide guidelines for the legal transmission of UCE and statutory damages for violations. These laws may not provide enough of a deterrent to stop big-time spammers from sending UCE using illegal means such as false routing information. In combination with the ever-advancing technology of spam filters, and suits for damages brought under CAN-SPAM, state laws criminalizing spamming will help to slow down the most prolific spammers. The recent felony conviction of spammers in Virginia provides a model for one successful method for tackling the stream of unwanted spam that is costing American businesses millions of dollars each year. The threat of incarceration for five years or longer may thwart many of the large-volume spammers and deter those who have not yet entered the business.

[<< Top](#)

Footnotes

1. Emma Scanlan, University of Washington School of Law Class of 2006. Thank you to Professor Anita Ramasastry for her invaluable guidance and endless patience.
2. Norman H. Nie et. al., Stan. Ctr for the Quantitative Stud. of Soc'y, Ten Years After the Birth of the Internet, How Do Americans Use the Internet in Their Daily Lives? 3 (Dec. 2004), at http://www.stanford.edu/group/siqss/SIQSS_Time_Study_04.pdf.
3. Study Shows Deleting Spam Costs \$22 Billion per Year, Messagingpipeline.com, Feb. 3, 2005, at <http://www.messagingpipeline.com/onetoone/59300766>.
4. CAN-SPAM Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003) (codified at 15 U.S.C. §§ 7701-13, 18 U.S.C. § 1037 (2005)).
5. Tom Zeller, Jr., Law Barring Junk E-Mail Allows a Flood Instead, N.Y. Times, Feb.

- 1, 2005, at A1.
6. Susan Kuchinskis, FTC Closing CAN-SPAM Loopholes, internetnews.com (Jan. 28, 2005), at <http://www.internetnews.com/bus-news/article.php/3465931>.
7. Zeller, supra note 5, at A1.
8. Nat'l Conference of State Legislatures, Unsolicited Commercial E-Mail Advertisements (Anti-Spam Legislation) 2004 Legislative Activity (2005), at <http://www.ncsl.org/programs/lis/legislation/spam04.htm> (Apr. 2, 2005). As of April 2005, California, Florida, Georgia, Hawaii, Illinois, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Mississippi, Nebraska, New Hampshire, New Jersey, New York, Ohio, Oklahoma, Pennsylvania, Tennessee, Utah, Vermont, Washington, and West Virginia considered or passed new spam legislation.
9. 15 U.S.C. § 7704 (2005).
10. 15 U.S.C. § 7702(17)(A) (2005).
11. 15 U.S.C. § 7702(2)(B) (2005).
12. Zeller, supra note 5, at A1.
13. 15 U.S.C. § 7701(a)(11) (2005).
14. Grant Gross, State spam laws and the new CAN-SPAM, InfoWorld.com (Feb. 27, 2005), at http://www.infoworld.com/article/04/02/27/09FEspamstates_1.html.
15. 15 U.S.C. § 7707(b)(1) (2005).
16. 15 U.S.C. § 7707(b)(2) (2005).
17. Cal. Bus. & Prof. Code §17529.5(b)(1)(B) (West 2005).
18. Ohio Rev. Code Ann. § 2913.421 (West 2005).
19. Id.
20. Md. Code Ann., Criminal Law, § 3-805.1(c)(3) (West 2005).
21. Md. Code Ann., Criminal Law, § 3-805.1 (c)(6) (West 2005).
22. See Md. Code Ann., Criminal Law, § 3-805.1 (West 2005).
23. Marycle, LLC v. First Choice Internet, Inc., 2004 WL 2895955 (Md. Cir. Ct.) (unpublished opinion).
24. See e.g., Anita Ramasastry, In Virginia, Ohio, and Maryland, Kingpin Spammers Go to the Slammer: State Laws Rightly Criminalize Fraudulent Bulk Spamming, FindLaw.com (Dec. 15, 2005) at <http://writ.corporate.findlaw.com/ramasastry/20041215.html>.
25. Ga. Code Ann. § 16-9-101 (2005).
26. Ga. Code Ann. § 16-9-102 (2005).
27. Swartz, Jon, First Felony spam trial begins in Virginia, USA Today, Oct. 25, 2004, at http://www.usatoday.com/money/industries/technology/2004-10-25-spam_x.htm, (last modified Oct. 26, 2004).
28. Virginia does not distinguish between commercial and non-commercial unsolicited email.
29. Va. Code Ann. § 18.2-152.3:1 (2004).
30. Swartz, supra note 39.
31. Id.
32. Dan Telvock, Judge Drops Convictions For Spammer's Sister, Leesburg2day.com, Mar. 2, 2005, at <http://www.leesburg2day.com/news/2005Mar/spam.cfm>.
33. Matthew Barakat, Judge Sentences Spammer to Nine Years, ABC News, Apr. 8,

2005, at <http://abcnews.go.com/Technology/wireStory?id=653112>.

34. Karin Brulliard, Woman's Spam Conviction Thrown Out, Washington Post, Mar. 2, 2005, at E.1.
35. 15 U.S.C. § 7706(f)(3)(A)-(C) (2005).
36. 18 U.S.C. § 1037(5)(b)(B)(2) (2005).
37. Mike Hoyem, Florida delivers sunshine and spam, USA Today, July 19, 2004, at http://www.usatoday.com/tech/news/Internetprivacy/2004-07-19-spam-central_x.htm.
38. Id.
39. Kramer v. Cash Link Systems, No. 3-03-CV-80109-CRW-TJ, 2004 WL 2952561 (S.D. Iowa).
40. Grant Gross, Internet Service Provider Awarded \$1 Billion in Damages, PCWorld.com (Dec. 20, 2004), at <http://www.pcworld.com/news/article/0,aid,119011,00.asp>.
41. Kramer, 2004 WL 2952561 at 7.
42. Gross, supra note 30.
43. Id.
44. Fla. Stat. Ann. § 668.603 (West 2005).
45. Charlie Crist, Crist Announces First Case Under Florida Anti-Spam Law, Office of the Attorney Gen. of Fla. Elec. Newsletter (Apr. 4, 2005) at <http://myfloridalegal.com/newsrel.nsf/newsreleases/F978639D46005F6585256FD90050AAC9>.
46. Id.
47. Reuters, Florida Wins Injunction against Spammers, Computerworld.com (Apr. 13, 2005), at <http://www.computerworld.com/governmenttopics/government/legalissues/story/0,10801,101051,00>.
48. Crist, supra note 35.